Oracle® Enterprise Session Border Controller

FIPS Compliance Guide

Release S-Cz9.1.0
F51864-01
March 2022

ORACLE

Oracle Enterprise Session Border Controller FIPS Compliance Guide, Release S-Cz9.1.0

F51864-01

Contents

3 Configuring FIPS High Availability

4 Finite State Machine

About this Guide

This guide provides the conceptual and procedural information about the Federal Information Processing Standard (FIPS) functionality in the Oracle® Enterprise Session Border Controller with Release CZ8.4.0. The documentation set for this release is the CZ8.4.0 suite.

This publication is used with Oracle Communications Session Border Controller and Oracle® Enterprise Session Border Controller.

Related Documentation

The following list describes related documentation for the Oracle® Enterprise Session Border Controller. You can find the listed documents on http://docs.oracle.com/en/industries/communications/ in the "Session Border Controller Documentation" and "Acme Packet" sections.

Document Name	Document Description
Acme Packet 3900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3900.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 4900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3950 and Acme Packet 4900.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
Acme Packet 6350 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6350.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
Known Issues & Caveats	Contains known issues and caveats
Configuration Guide	Contains information about the administration and software configuration of the Service Provider Session Border Controller (SBC).
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.

Document Name	Document Description
MIB Guide	Contains information about Management Information Base (MIBs), Oracle Communication's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the SBC's accounting support, including details about RADIUS and Diameter accounting.
HDR Guide	Contains information about the SBC's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Admin Security Guide	Contains information about the SBC's support for its Administrative Security license.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the SBC family of products.
Platform Preparation and Installation Guide	Contains information about upgrading system images and any pre-boot system provisioning.
Call Traffic Monitoring Guide	Contains information about traffic monitoring and packet traces as collected on the system. This guide also includes WebGUI configuration used for the SIP Monitor and Trace application.
HMR Guide	Contains information about configuring and using Header Manipulation Rules to manage service traffic.
REST API	Contains information about the supported REST APIs and how to use the REST API interface.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select `2` for New Service Request.
2. Select `3` for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select `1`.

- For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Revision History

This section provides a revision history for this document.

Date	Description
March 2022	• Initial release

1

FIPS Compliance

The Oracle® Enterprise Session Border Controller provides cryptographic capabilities and algorithms that conform to Federal Information Processing Standards (FIPS). Specific standards implemented include those described in *Security Requirements For Cryptographic Modules* (FIPS PUB 140-2), and others described in NIST Special Publication 800-90A Revision 1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators* (Revised), June 2016.

To validate that your platform/software combination has been certified by NIST, query their Cryptographic Module Validation Program (CMVP) site at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search.

> **Note:**
>
> Not all platforms and all releases are certified.

FIPS Feature Set Requirements

The ESBC supports cryptographic capabilities and algorithms compliant with FIPS 140-2 standards. The FIPS feature set, provisioned via the Data Integrity entitlement, is required for the following FIPS-compliant capabilities:

- power-on self tests
- software integrity test
- conditional tests
- ACLI commands and configuration attributes

Platform Support for Enterprise

FIPS-compliant cryptography is available on the following Enterprise platforms:

- Acme Packet 1100 (140-2 level 1)
- Acme Packet 3900 (140-2 level 1)
- Acme Packet 3950 (140-2 level 1)
- Acme Packet 4900 (140-2 level 1)
- Acme Packet 4600 (140-2 level 1)
- Acme Packet 6300 (140-2 level 1)
- Acme Packet 6350 (140-2 level 1)
- VME (140-2 level 1)

> **Note:**
>
> All FIPS compliant Acme Packet platforms are shipped with the USB interface intentionally covered and inaccessible. This is to prevent users from unintentionally using the USB interface to boot a non-FIPS compliant image and getting locked out of the system.

Verifying and Changing the Bootfile

The **check-boot-file /boot/<filename>** command allows you to verify the image running on the E-SBC.

```
sd225v# check-boot-file /boot/<filename>.bz
Verifying signature of /boot/<filename>.bz
Version: Acme Packet <release#> Beta 4 (WS Build 48) 201705130547
Image integrity verification passed
```

The **set-boot-file /boot/<filename>** command allows you to change the image running on the E-SBC.

```
sd225v# set-boot-file /boot/<filename>.bz
Verifying signature of /boot/<filename>.bz
Version: Acme Packet <release#> Beta 4 (WS Build 48) 201705130547
old boot file /boot/bzImage being replaced with /boot/<filename>.bz
```

Cryptographic Modules

FIPS compliance requires the clear definition of modules that perform cryptographic functions. The following modules are present on the supported Acme Packet platforms.

- OpenSSL — This software module provides cryptographic functions to include the following:
  - AES
  - AES_GCM
  - DRBG800-90A
  - ECDSA2
  - HMAC
  - KDF135
  - RSA2
  - SHA
- OpenSSH — This software module provides cryptographic functions to include the following:
  - AES GCM 128 & 256
  - AES CTR 128 & 192 & 256

  - AES CBC 192 & 256
  - HMAC 20 with SHA-2 32 with SHA-2
- Mocana — This software module provides cryptographic functions to include the following:
  - AES CBC 128, 192 and 256
  - AES-CTR 128 and 256
  - HMAC-SHA-1 and HMAC-SHA-2
  - KDF (IKEv2 and SSH)
  - RSA2 (KeyGen_RandomProbablyPrime3_3 and SigVer15_186-3)
  - SHA (SHA1, SHA2)
- Cavium Nitrox PX1620
  - AES-CBC-KAT
  - AES-CTR-KAT
  - AES-ECB-KAT
  - AES-GCM-KAT
  - AES-CCM-KAT
- Cavium Octeon CN688X and Cavium 78xx 48-Core Octeon III
  - AES-CBC-KAT
  - AES-CTR-KAT
  - AES-ECB-KAT
  - SHA-KAT
  - HMAC-SHA-KAT
  - RSA-SHA1-KAT
  - RSA-SHA2-KAT
  - AES-GCM-KAT
  - AES-CCM-KAT

> **Note:**
>
> Cryptographic modules are described in detail in the relevant *Oracle Security Policy* documents.

Cryptographic Hardware Accleration

Cryptographic hardware acceleration is supported on the Acme Packet 4600 and Acme Packet 6300 platforms for AES, RSA, SHA, and HMAC-SHA.

Cryptographic Algorithm Validation Program Tests

The Cryptographic Algorithm Validation Program (CAVP) Tests apply to the Acme Packet 4600, Acme Packet 6300, and Acme Packet 6350.

- AES-ECB tests, including GFSbox, KeySbox, Monte Carlo Test (MCT), MMT, VarKey, and VarTxt.
- SHA (SHA-1, SHA-256, SHA-384, SHA-512) tests, including variations such as short message, long message, and Monte Carlo test.
- HMAC-SHA (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512)
- SRTP-KDF
- TLS-KDF
- AES-CBC tests with all the test variations, including GFSbox, KeySbox, Monte Carlo Test (MCT), MMT, VarKey, and VarTxt for 128-bit and 256-bit key sizes.
- AES-GCM encryption and decryption tests with different key sizes such as 128 and 256 including external and internal IV support
- TDES-CBC tests which includes variations such as VarKey, VarTxt, Inverse Permutation (invperm), Permutation Operation (permop), Substitution Table (subtab), Multi-block Message Test (MMT), Monte Carlo Test (MCT).
- RSA tests which include RSA key generation, signature generation, signature verification, and RSADP
- DRBG test
- CRNG test

FIPS States

When you buy a FIPS feature set with the Oracle® Enterprise Session Border Controller, the E-SBC comes equipped with the FIPS 140-2 feature installed, which operates in FIPS 140-2 compatible mode (either level 1 or level 2, depending on platform certification). This means that the E-SBC has access to the FIPS capabilities listed in this document.

> **Note:**
>
> In the event that any of the power-on or conditional tests fail, the E-SBC becomes completely disabled. If this occurs, you must contact your Oracle representative for instructions on how to proceed.

When FIPS is disabled, the following restrictions are placed on the E-SBC:

- Security related ACLI elements are not available.
- Security related ACLI commands are not allowed.

Self-Tests

Section 4.9 of *Security Requirements For Cryptographic Modules* mandates that cryptographic modules perform power-on self-tests and conditional self-tests to ensure that the module is functioning properly. Power-on self-tests are performed when the cryptographic module powers up. Conditional self-tests are performed when an RSA or RNG operation is requested.

Power-on Self-Tests

Acme Packet FIPS-compliant platforms perform the following power-up tests when power is enabled on the module. These self-tests require no input from the user.

Firmware Integrity Test

- RSA 2048 Firmware Integrity Test

Mocana Self-Tests

- AES (Encrypt/Decrypt) Known Answer Test
- Triple-DES (Encrypt/Decrypt) Known Answer Test
- SHA-1 Known Answer Test
- SHA-256 Known Answer Test
- SHA-384 Known Answer Test
- SHA-512 Known Answer Test
- HMAC-SHA-1 Known Answer Test
- HMAC-SHA-256 Known Answer Test
- HMAC-SHA-384 Known Answer Test
- HMAC-SHA-512 Known Answer Test
- RSA Verify Known Answer Test
- IKEv2KDF Known Answer Test

OpenSSL Self-Tests

- SHA-1 Known Answer Test
- SHA-256 Known Answer Test
- SHA-512 Known Answer Test
- HMAC-SHA-1 Known Answer Test
- HMAC-SHA-256 Known Answer Test
- HMAC-SHA-384 Known Answer Test
- HMAC SHA-512 Known Answer Test
- AES (Encrypt/Decrypt) Known Answer Test
- AES CBC Known Answer Test
- AES GCM (Encrypt/Decrypt) Known Answer Test

- AES GCM Known Answer Test
- AES ECB Known Answer Test
- AES CTR Known Answer Test
- Triple-DES (Encrypt/Decrypt) Known Answer Test
- Triple-DES CBC Known Answer Test
- SP 800-90A DRBG Known Answer Test
- RSA sign/verify Known Answer Test
- ECDSA sign/verify Known Answer Test
- DRBG Known Answer Test
- DRBG Health Test

> **Note:**
>
> 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.

Conditional Self-Tests

Conditional self-tests are performed when an RSA or RNG operation is requested.

The following conditional self-tests are supported:

- RSA Consistency Conditional Test
- Continuous Random Number Generation Test

ACLI Commands

These ACLI commands and parameters support FIPS compliancy.

show security fips

The **show security fips** ACLI command displays the FIPS state. The following is an example of Acme Packet platform output.

```
ACMEPACKET# show security fips

************************************************************
***    System is in FIPS 140-2 level-1 compatible mode.   ***
************************************************************
ACMEPACKET##
```

The following is an example of VME output:

```
ACMEPACKET# show security fips

************************************************************
***    System is in FIPS 140-2 level-1 compatible mode.   ***
************************************************************
```

If the Oracle® Enterprise Session Border Controller transitions from FIPS 140-2 to non-FIPS mode due to a self-test fail, the system is no longer accessible and you must use the Oracle Rescue Account and perform a manufacture reset on the module. For more information on performing a manufacture reset, see *Accessing the Oracle Rescue Account*.

```
ORACLE# show security fips

************************************************************
*** System is NOT in FIPS 140-2 level-1 compatible mode.
*** FIPS Error - Software image integrity check failed
************************************************************
ORACLE#
```

The following example displays some of the error messages you may see:

```
AES CBC with 128 bit key test failed.
AES CBC with 192 bit key test failed.
AES CBC with 256 bit key test failed.
AES CTR with 128 bit key test failed.
AES CTR with 192 bit key test failed.
AES CTR with 256 bit key test failed.
3DES CBC test failed.
SHA1 test failed.
SHA256 test failed.
HMAC-SHA1 test failed.
HMAC-SHA256 test failed.
Continuous DRBG failed.
DRBG with known entropy failed.
DRBG instantiate health test failed.
DRBG reseed health test failed.
DRBG generate health test failed.
DRBG conditional test failed.
BCM RNG test failed.
RSA crypto failed.
RSA pairwise consistency test failed.
RSA pairwise consistency Conditional test failed.
Software image integrity check failed.
BCM security processor not present.
HiFN not present on media phy card.
HiFN not present on wancom.
```

show security ssm-accelerator

The **show security ssm-accelerator** command displays the SSM status on the E-SBC, allowing you to verify offloading to Nitrox. The following is an example of Acme Packet platform output:

```
ACMEPACKET# show security ssm-accelerator
SSM (Signaling Security Module) V3 present.

Driver Version: 5.3.1

Driver Compile time defines
---------------------------
MAIN LINE PROTOCOL used : SSL
MICROCODE used : MC2

------------------------------------------------------------------------
-
                             SSL Record Processing
------------------------------------------------------------------------
-
                      Record Encrypt           Record Decrypt
Packet Requests:                 0                        0
Packet Aborts:                   0                        0
Bytes In:                        0                        0
Bytes Out:                       0                        0
------------------------------------------------------------------------
-

                       Crypto Processing
------------------------------------------------------------------------
-
                           Encrypt                  Decrypt
Packet Requests:                 0                        0
Packet Aborts:                   0                        0
Bytes In:                        0                        0
Bytes Out:                       0                        0
------------------------------------------------------------------------
-
                              HMAC
Packet Requests:                 0
Packet Aborts:                   0
Bytes In:                        0
Bytes Out:                       0

ACMEPACKET#
```

Factory Reset for the Oracle® Enterprise Session Border Controller

If you attempt to remove the FIPS feature, some irrevocable changes and information remain on the system. You can return your platforms to their initial factory settings (zeroization) to truly remove all traces of the previous implementation. Depending on if you are performing this on an Acme Packet hardware platform or a Virtual platform, the process is different.

> **Caution:**
>
> Factory reset erases all system data, including licenses and configuration, and reboots the supported Acme Packet platforms using the factory default /boot/*bzImage* file. If the factory image file has been removed, the system will NOT be recoverable without manual intervention, and you may have to return the system to Oracle for factory re-initialization.

Using the Oracle Rescue Account for PNF Zeroization

To enable the Oracle Rescue Account:

1. Connect to the E-SBC's serial console.
2. Reboot the E-SBC and press the spacebar to interrupt the 5 second bootloader countdown.
3. Select **o** to access the Oracle Rescue Account.

   A challenge string displays in the console.
4. Contact Oracle Support and provide the challenge string and the system serial number.

   Oracle Support verifies the challenge string and provides a response string.
5. Enter the response string.

   If it is validated, access is granted to the Oracle Rescue Account and a sub-menu appears providing three menu options:

   - **f**—Factory default
   - **!**—Start debug shell
   - **x**—Exit to main menu

```
Starting acmeboot...

ACME bootloader Acme Packet SCZ<build#> RTM (Build 59) 201706021530

Press the space bar to stop auto-boot...
28
Please contact Oracle Product Support to obtain a Response Key
You will need to provide the following information:
   1. Serial number of the system
   2. This Challenge Key: 069-033-231-180
```

```
Note: Keys are valid for a limited period only, typically 1 day

Enter response key:     006-163-164-054


Oracle Rescue Access Menu

PROCEED WITH CAUTION: You are now in privileged access mode.
Use of these commands is permitted by authorised personnel only.
f                     - factory default
!                     - start debug shell

x                     - exit to main menu


[Oracle Rescue Access]: f

WARNING WARNING WARNING
This command will permanently erase the hard disk, nvram and flash,
returning the system to a factory-default state.

Type: "ERASE_ALL" to confirm factory default, anything else will abort.
[Confirm Factory Default]: ERASE_ALL

Proceeding with factory default. DO NOT INTERRUPT
Removing hard disk user data partitions...
Wiping /code filesystem...
Zeroizing /code filesystem...
Wiping /boot filesystem...
Zeroizing /boot filesystem...
Zeroizing NVRAM...
Checking for NVRAM zeroization...
Setting default boot params...

Completed factory default. Reboot or power off now

Rebooting...
```

Reinstalling the VM for VNF Installation

To perform zeroization on a VM, you must perform a complete image reinstallation.

2

Installing a FIPS Feature Set and Upgrading a FIPS System

This chapter describes the procedure for installing a FIPS feature set (if one is not already present on the system) and upgrading the image on a system that already has FIPS provisioned.

> **Note:**
>
> You enable the FIPS feature set via the Data Integrity entitlement by way of the **setup entitlements** command.
> When enabling the FIPS feature set, the E-SBC warns the user with the following message:
>
> ```
> CAUTION: Enabling this feature activates enhanced FIPS security
> functions. Once saved, factory rest may be required.
> ```

Installing a FIPS Feature Set

For the method in which the FIPS feature is installed, see the *Session Border Controller Release Notes*. For instructions on provisioning the FIPS feature, see the *Session Border Controller ACLI Configuration Guide*.

Upgrading the Image on a FIPS Enabled System

This procedure assumes that the FIPS feature is already installed on the system. If the FIPS feature set on your system expires, you must install a valid FIPS feature. For more information on installing a FIPS feature set, see "Installing a FIPS Feature Set".

The following are required to install the FIPS feature set:

- SSH File Transfer Protocol (SFTP) client with access to the target Acme Packet platform.
- SFTP access to the target Acme Packet platform's management IP address.
- Access to the FIPS software image to which you are upgrading.

> **Note:**
>
> You must follow this procedure on a running device:

1. Use SFTP to transfer <release>.bz into `/boot` on the target Acme Packet platform.
2. Verify the correct image file has been uploaded. The following is an example of how to verify the image:

```
sd225v# check-boot-file /boot/nnECZ750b4.bz
Verifying signature of /boot/<release>.bz
Version: Acme Packet ECZ7.5.0 Beta 4 (WS Build 48) 201705130547
Image integrity verification passed
```

3. Replace the boot file with the newly uploaded image. The following is an example of how to replace the boot file:

```
sd225v# set-boot-file /boot/<release>.bz
Verifying signature of /boot/<release>.bz
Version: Acme Packet <release> Beta 4 (WS Build 48) 201705130547
old boot file /boot/bzImage being replaced with /boot/<release>.bz
```

4. Execute the **reboot force** command to reboot the system.

```
sd225v# reboot force
……
Starting
sysmand...
------------------------------------------------------------

This product contains third-party software provided
under
one or more open source licenses. Type "show about"
after
logging in for full license
details.
------------------------------------------------------------



...


Mocana FIPS Power Up Self Test: Started...
Mocana FIPS Power Up Self Test: Finished

FIPS_RSA_Signature_Verify: PASSED!!!
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tTscfd...
Starting tAppWeb...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Starting snmpd...
Start platform alarm...
```

```
Starting tIFMIBd...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...

************************************************************
*    System is in FIPS 140-2 level-2 compatible mode.      *
*    FIPS: All Power on self test completed successfully.   *
************************************************************
password secure mode is enabled
Admin Security is disabled
Starting SSH...
SSH_Cli_init: allocated memory for 5 connections

************************************************************
***    System is in FIPS 140-2 level-2 compatible mode.   ***
************************************************************
Password:
```

3
Configuring FIPS High Availability

You can configure the supported Acme Packet platforms for High Availability (HA) to conform to the Federal Information Processing Standards (FIPS).

> **Note:**
>
> This chapter highlights the **run setup** command which is not available on all products.

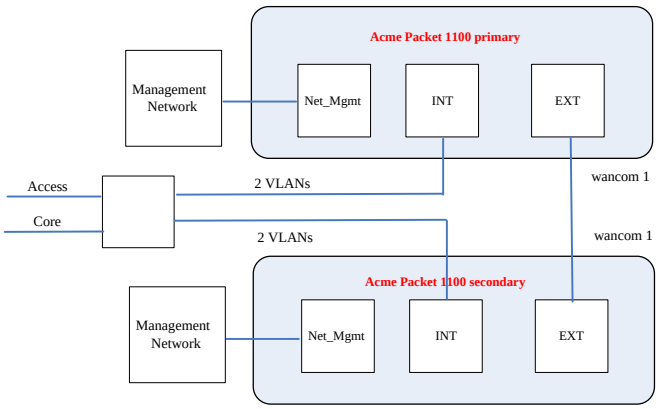
Configuring Acme Packet 1100 FIPS High Availability

FIPS dictates that critical traffic must be encrypted, not currently supported on this platform. The Acme Packet 1100 has only three physical interfaces typically designated as management (SSH, SFTP, etc.), INT, and EXT (both used for media traffic).

In a standard Acme Packet 1100 HA implementation, you configure the "Control" (HA) port to coexist on the management physical port using a different VLAN tag (**sub-port-id**) and addressing scheme. This method, however, does not meet FIPS standards.

To configure FIPS-compliant HA on the Acme Packet 1100, you must configure the EXT physical port (slot 0 port 1) of both SBCs to be used as dedicated HA Control ports in a point-to-point connection with no hubs, switches, or routers between them. When used for HA, this interface is called wancom1. This leaves the second media port, INT, as the only usable media interface, on which you must configure multiple ports (using different VLAN tags) for all

media functionality. See the following diagram:



The following is an example setup console log for a FIPS Acme Packet 1100 primary E-SBC.

```
FIPS_1100_Primary# run setup

------------------------------------------------------------
Thank you for purchasing the Acme Packet SBC. The following
short wizard will guide you through the initial set-up.
A reboot will be required to save changes.
------------------------------------------------------------

'-' = Previous; '?' = Help; '.' = Clear; 'q' = Exit


HIGH AVAILABILITY

This SBC may be a standalone or part of a highly available redundant
pair.
  SBC mode
     1 - standalone
     2 - high availability
    Enter choice [1 - standalone]                        : 2

If this SBC is the primary, enter the configuration.
If it is secondary, you can import settings from the primary
  SBC role
     1 - primary
     2 - secondary
```

```
    Enter choice [1 - primary]                          : 1

Specify the IP address to set on interface connected for redundancy
  Redundancy interface address [169.254.1.1]            :
  Redundancy subnet mask [255.255.255.252]              :

SBC SETTINGS
  Unique target name of this SBC [FIPS_1100_Primary]    :
  IP address on management interface [10.196.145.73]    :
  Subnet mask [255.255.224.0]                           :
  Gateway IP address [10.196.128.1]                     :

PEER CONFIGURATION
  Peer IP address [169.254.1.2]                         :
  Peer target name [sbc02]                              : FIPS_1100_Secondary

OC SDM ACCESS SETTINGS

Configure SBC to allow OC Session Delivery Manager to access it
  OC SDM access (yes/no) [yes]                          : no

-- Summary view
-------------------------------------------------------------------

GUI ACCESS
  1: Enable Web GUI (yes/no)                            : N/A

WEB GUI MODE
 2 : Web GUI Mode                                       : N/A

HIGH AVAILABILITY
 3 : SBC mode                                           : high availability
 4 : SBC role                                           : primary
 5 : Redundancy interface address                       : 169.254.1.1
 6 : Redundancy subnet mask                             : 255.255.255.252
 7 : Redundancy interface VLAN                          : N/A

SBC SETTINGS
 8 : Unique target name of this SBC                     : FIPS_1100_Primary
 9 : IP address on management interface                 : 10.196.145.73
 10: Subnet mask                                        : 255.255.224.0
 11: Management interface VLAN                          : N/A
 12: Gateway IP address                                 : 10.196.128.1

AUTOMATIC CONFIGURATION
 13: Acquire config from the Primary (yes/no)           : N/A

PEER CONFIGURATION
 14: Peer IP address                                    : 169.254.1.2
 15: Peer target name                                   : FIPS_1100_Secondary

OC SDM ACCESS SETTINGS
 16: OC SDM access (yes/no)                             : no
 17: SNMP community string                              : N/A
 18: OC SDM IP address                                  : N/A
```

```
Enter 1 - 18 to modify, 'd' to display summary, 's' to save, 'q' to
exit. [s]:
```

The following is an example setup console log for a FIPS Acme Packet 1100 secondary E-SBC.

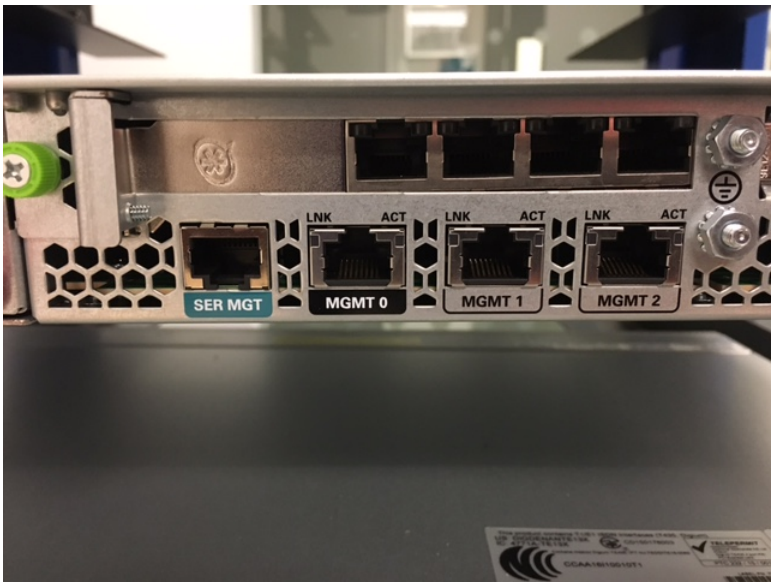
```
FIPS_1100_Secondary# run setup

-----------------------------------------------------------
Thank you for purchasing the Acme Packet SBC. The following
short wizard will guide you through the initial set-up.
A reboot will be required to save changes.
-----------------------------------------------------------

'-' = Previous; '?' = Help; '.' = Clear; 'q' = Exit


HIGH AVAILABILITY

This SBC may be a standalone or part of a highly available redundant
pair.
  SBC mode
     1 - standalone
     2 - high availability
    Enter choice [1 - standalone]                      : 2

If this SBC is the primary, enter the configuration.
If it is secondary, you can import settings from the primary
  SBC role
     1 - primary
     2 - secondary
    Enter choice [1 - primary]                         : 2

Specify the IP address to set on interface connected for redundancy
  Redundancy interface address [169.254.1.2]           :
  Redundancy subnet mask [255.255.255.252]             :

SBC SETTINGS
  Unique target name of this SBC [FIPS_1100_Secondary] :
  IP address on management interface [10.196.145.74]   :
  Subnet mask [255.255.224.0]                          :
  Gateway IP address [10.196.128.1]                    :

PEER CONFIGURATION
  Peer IP address [169.254.1.1]                        :
  Peer target name [sbc01]                             :
FIPS_1100_Primary

OC SDM ACCESS SETTINGS

Configure SBC to allow OC Session Delivery Manager to access it
  OC SDM access (yes/no) [yes]                         : no
```

```
-- Summary view
-----------------------------------------------------------------

GUI ACCESS
  1: Enable Web GUI (yes/no)                          : N/A

WEB GUI MODE
 2 : Web GUI Mode                                     : N/A

HIGH AVAILABILITY
 3 : SBC mode                                         : high availability
 4 : SBC role                                         : secondary
 5 : Redundancy interface address                     : 169.254.1.2
 6 : Redundancy subnet mask                           : 255.255.255.252
 7 : Redundancy interface VLAN                        : N/A

SBC SETTINGS
 8 : Unique target name of this SBC                   : FIPS_1100_Secondary
 9 : IP address on management interface               : 10.196.145.74
 10: Subnet mask                                      : 255.255.224.0
 11: Management interface VLAN                        : N/A
 12: Gateway IP address                               : 10.196.128.1

AUTOMATIC CONFIGURATION
 13: Acquire config from the Primary (yes/no)         : N/A

PEER CONFIGURATION
 14: Peer IP address                                  : 169.254.1.1
 15: Peer target name                                 : FIPS_1100_Primary

OC SDM ACCESS SETTINGS
 16: OC SDM access (yes/no)                           : no
 17: SNMP community string                            : N/A
 18: OC SDM IP address                                : N/A

Enter 1 - 18 to modify, 'd' to display summary, 's' to save, 'q' to exit.
[s]:
```

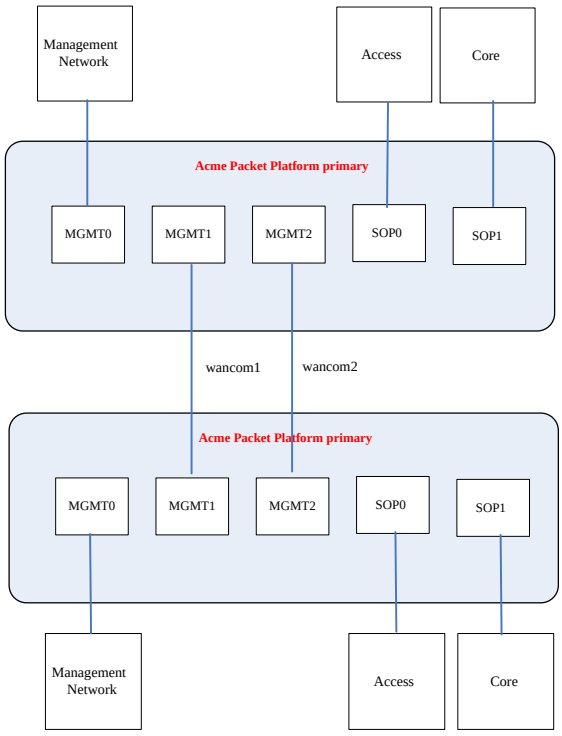
For more information on configuring HA on the Acme Packet 1100, see the *Acme Packet 1100 Hardware Installation and Maintenance Guide* and *Session Border Controller ACLI Configuration Guide*.

Configuring Acme Packet 4600/6300/6350 FIPS HA

FIPS dictates that critical traffic must be encrypted, not currently supported on this platform. Therefore, on each of the Acme Packet supported platforms in the HA pair, there is a dedicated "Control" port used only to send HA sync traffic between the SBCs. This port is labeled "MGMT1".



Plug the "Control" port of one SBC directly into the "Control" port of the second SBC using a single point-to-point cable, with no hubs, switches, or routers between them. See the following diagram:



The following is an example setup console log for a FIPS Acme Packet platform primary E-SBC.

```
FIPS_VM_Primary# run setup

-----------------------------------------------------------
```

```
Thank you for purchasing the Acme Packet SBC. The following
short wizard will guide you through the initial set-up.
A reboot will be required to save changes.
-----------------------------------------------------------

'-' = Previous; '?' = Help; '.' = Clear; 'q' = Exit


GUI ACCESS

If you want to allow GUI to access this SBC, enable this setting
  Enable Web GUI (yes/no) [yes]                          : yes

WEB GUI MODE

Choose which mode to enable for the web GUI
  Web GUI Mode
     1 - basic
     2 - expert
    Enter choice [1 - basic]                             : 2

HIGH AVAILABILITY

This SBC may be a standalone or part of a highly available redundant pair.
  SBC mode
     1 - standalone
     2 - high availability
    Enter choice [1 - standalone]                        : 2

If this SBC is the primary, enter the configuration.
If it is secondary, you can import settings from the primary
  SBC role
     1 - primary
     2 - secondary
    Enter choice [1 - primary]                           : 1

Specify the IP address to set on interface connected for redundancy
  Redundancy interface address [169.254.1.1]             :
  Redundancy subnet mask [255.255.255.252]               :

SBC SETTINGS
  Unique target name of this SBC [FIPS_VM_Primary]       :
  IP address on management interface [10.196.33.48]      :
  Subnet mask [255.255.224.0]                            :
  Management interface VLAN (0 - 4095) [0]               :
  Gateway IP address [10.196.32.1]                       :

PEER CONFIGURATION
  Peer IP address [169.254.1.2]                          :
  Peer target name [sbc02]                               : FIPS_VM_Secondary

OC SDM ACCESS SETTINGS

Configure SBC to allow OC Session Delivery Manager to access it
  OC SDM access (yes/no) [yes]                           : no
```

```
-- Summary view
-------------------------------------------------------------

GUI ACCESS
  1: Enable Web GUI (yes/no)                          : yes

WEB GUI MODE
 2 : Web GUI Mode                                     : expert

HIGH AVAILABILITY
 3 : SBC mode                                         : high
availability
 4 : SBC role                                         : primary
 5 : Redundancy interface address                     : 169.254.1.1
 6 : Redundancy subnet mask                           : 255.255.255.252
 7 : Redundancy interface VLAN                        : N/A

SBC SETTINGS
 8 : Unique target name of this SBC                   : FIPS_VM_Primary
 9 : IP address on management interface               : 10.196.33.48
 10: Subnet mask                                      : 255.255.224.0
 11: Management interface VLAN                        : 0
 12: Gateway IP address                               : 10.196.32.1

AUTOMATIC CONFIGURATION
 13: Acquire config from the Primary (yes/no)         : N/A

PEER CONFIGURATION
 14: Peer IP address                                  : 169.254.1.2
 15: Peer target name                                 :
FIPS_VM_Secondary

OC SDM ACCESS SETTINGS
 16: OC SDM access (yes/no)                           : no
 17: SNMP community string                            : N/A
 18: OC SDM IP address                                : N/A

Enter 1 - 18 to modify, 'd' to display summary, 's' to save, 'q' to
exit. [s]:
```

The following is an example setup console log for a FIPS Acme Packet platform secondary E-SBC.

```
FIPS_VM_Secondary# run setup

------------------------------------------------------------
Thank you for purchasing the Acme Packet SBC. The following
short wizard will guide you through the initial set-up.
A reboot will be required to save changes.
------------------------------------------------------------

'-' = Previous; '?' = Help; '.' = Clear; 'q' = Exit
```

```
GUI ACCESS

If you want to allow GUI to access this SBC, enable this setting
  Enable Web GUI (yes/no) [yes]                          : yes

WEB GUI MODE

Choose which mode to enable for the web GUI
  Web GUI Mode
     1 - basic
     2 - expert
    Enter choice [1 - basic]                             : 2

HIGH AVAILABILITY

This SBC may be a standalone or part of a highly available redundant pair.
  SBC mode
     1 - standalone
     2 - high availability
    Enter choice [1 - standalone]                        : 2

If this SBC is the primary, enter the configuration.
If it is secondary, you can import settings from the primary
  SBC role
     1 - primary
     2 - secondary
    Enter choice [1 - primary]                           : 2

Specify the IP address to set on interface connected for redundancy
  Redundancy interface address [169.254.1.2]             :
  Redundancy subnet mask [255.255.255.252]               :

SBC SETTINGS
  Unique target name of this SBC [FIPS_VM_Secondary]     :
  IP address on management interface [10.196.33.40]      :
  Subnet mask [255.255.224.0]                            :
  Management interface VLAN (0 - 4095) [0]               :
  Gateway IP address [10.196.32.1]                       :

AUTOMATIC CONFIGURATION
  Acquire config from the Primary (yes/no) [yes]         : yes

PEER CONFIGURATION
  Peer IP address [169.254.1.1]                          :

-- Summary view
---------------------------------------------------------------

GUI ACCESS
  1: Enable Web GUI (yes/no)                             : yes

WEB GUI MODE
 2 : Web GUI Mode                                        : expert
```

```
HIGH AVAILABILITY
 3 : SBC mode                                          : high
availability
 4 : SBC role                                          : secondary
 5 : Redundancy interface address                      : 169.254.1.2
 6 : Redundancy subnet mask                            : 255.255.255.252
 7 : Redundancy interface VLAN                         : N/A

SBC SETTINGS
 8 : Unique target name of this SBC                    :
FIPS_VM_Secondary
 9 : IP address on management interface                : 10.196.33.40
 10: Subnet mask                                       : 255.255.224.0
 11: Management interface VLAN                         : 0
 12: Gateway IP address                                : 10.196.32.1

AUTOMATIC CONFIGURATION
 13: Acquire config from the Primary (yes/no)          : yes

PEER CONFIGURATION
 14: Peer IP address                                   : 169.254.1.1
 15: Peer target name                                  : N/A

OC SDM ACCESS SETTINGS
 16: OC SDM access (yes/no)                            : N/A
 17: SNMP community string                             : N/A
 18: OC SDM IP address                                 : N/A

Enter 1 - 18 to modify, 'd' to display summary, 's' to save, 'q' to
exit. [s]:
```

For more information on configuring HA on the Acme Packet supported platforms, see the appropriate *Acme packet Hardware Installation and Maintenance Guide* and the *Session Border Controller ACLI Configuration Guide*.

Configuring VM FIPS HA

In a Virtual Machine (VM) HA configuration, connect the network management interface (wancom0) and media interfaces over virtual network switches via the hypervisor. This is no different for a FIPS-compliant HA implementation. Use a RJ45 Ethernet cable to connect wancom1 of the Primary node to wancom1 of the Secondary node.

The following is an example setup console log for a FIPS VME primary E-SBC.

```
FIPS_VM_Primary# run setup

------------------------------------------------------------
Thank you for purchasing the Acme Packet SBC. The following
short wizard will guide you through the initial set-up.
A reboot will be required to save changes.
------------------------------------------------------------
```

```
'-' = Previous; '?' = Help; '.' = Clear; 'q' = Exit


GUI ACCESS

If you want to allow GUI to access this SBC, enable this setting
  Enable Web GUI (yes/no) [yes]                          : yes

WEB GUI MODE

Choose which mode to enable for the web GUI
  Web GUI Mode
     1 - basic
     2 - expert
    Enter choice [1 - basic]                             : 2

HIGH AVAILABILITY

This SBC may be a standalone or part of a highly available redundant pair.
  SBC mode
     1 - standalone
     2 - high availability
    Enter choice [1 - standalone]                        : 2

If this SBC is the primary, enter the configuration.
If it is secondary, you can import settings from the primary
  SBC role
     1 - primary
     2 - secondary
    Enter choice [1 - primary]                           : 1

Specify the IP address to set on interface connected for redundancy
  Redundancy interface address [169.254.1.1]             :
  Redundancy subnet mask [255.255.255.252]               :

SBC SETTINGS
  Unique target name of this SBC [FIPS_VM_Primary]       :
  IP address on management interface [10.196.33.48]      :
  Subnet mask [255.255.224.0]                            :
  Management interface VLAN (0 - 4095) [0]               :
  Gateway IP address [10.196.32.1]                       :

PEER CONFIGURATION
  Peer IP address [169.254.1.2]                          :
  Peer target name [sbc02]                               : FIPS_VM_Secondary

OC SDM ACCESS SETTINGS

Configure SBC to allow OC Session Delivery Manager to access it
  OC SDM access (yes/no) [yes]                           : no

-- Summary view
-------------------------------------------------------------------
```

```
GUI ACCESS
  1: Enable Web GUI (yes/no)                          : yes

WEB GUI MODE
 2 : Web GUI Mode                                     : expert

HIGH AVAILABILITY
 3 : SBC mode                                         : high
availability
 4 : SBC role                                         : primary
 5 : Redundancy interface address                     : 169.254.1.1
 6 : Redundancy subnet mask                           : 255.255.255.252
 7 : Redundancy interface VLAN                        : N/A

SBC SETTINGS
 8 : Unique target name of this SBC                   : FIPS_VM_Primary
 9 : IP address on management interface               : 10.196.33.48
 10: Subnet mask                                      : 255.255.224.0
 11: Management interface VLAN                        : 0
 12: Gateway IP address                               : 10.196.32.1

AUTOMATIC CONFIGURATION
 13: Acquire config from the Primary (yes/no)         : N/A

PEER CONFIGURATION
 14: Peer IP address                                  : 169.254.1.2
 15: Peer target name                                 :
FIPS_VM_Secondary

OC SDM ACCESS SETTINGS
 16: OC SDM access (yes/no)                           : no
 17: SNMP community string                            : N/A
 18: OC SDM IP address                                : N/A

Enter 1 - 18 to modify, 'd' to display summary, 's' to save, 'q' to
exit. [s]:
```

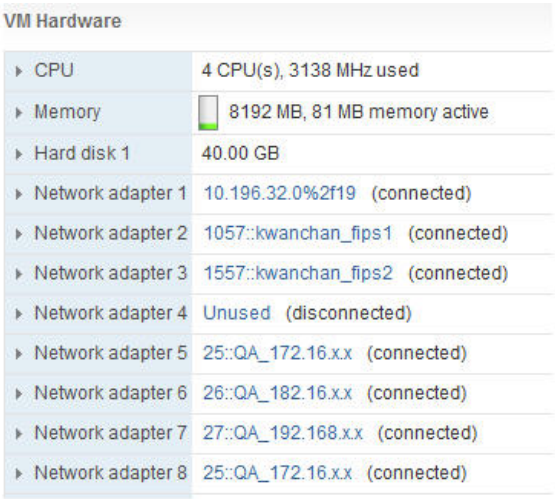
The following is an example setup console log for a FIPS VME secondary E-SBC.

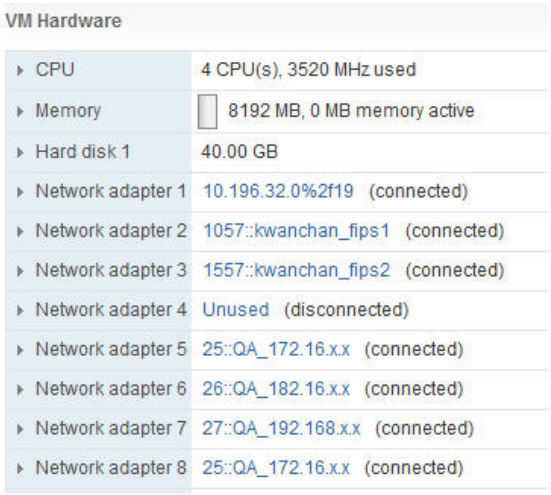
```
FIPS_VM_Secondary# run setup

------------------------------------------------------------
Thank you for purchasing the Acme Packet SBC. The following
short wizard will guide you through the initial set-up.
A reboot will be required to save changes.
------------------------------------------------------------

'-' = Previous; '?' = Help; '.' = Clear; 'q' = Exit


GUI ACCESS

If you want to allow GUI to access this SBC, enable this setting
```

```
  Enable Web GUI (yes/no) [yes]                          : yes

WEB GUI MODE

Choose which mode to enable for the web GUI
  Web GUI Mode
     1 - basic
     2 - expert
    Enter choice [1 - basic]                             : 2

HIGH AVAILABILITY

This SBC may be a standalone or part of a highly available redundant pair.
  SBC mode
     1 - standalone
     2 - high availability
    Enter choice [1 - standalone]                        : 2

If this SBC is the primary, enter the configuration.
If it is secondary, you can import settings from the primary
  SBC role
     1 - primary
     2 - secondary
    Enter choice [1 - primary]                           : 2

Specify the IP address to set on interface connected for redundancy
  Redundancy interface address [169.254.1.2]             :
  Redundancy subnet mask [255.255.255.252]               :

SBC SETTINGS
  Unique target name of this SBC [FIPS_VM_Secondary]     :
  IP address on management interface [10.196.33.40]      :
  Subnet mask [255.255.224.0]                            :
  Management interface VLAN (0 - 4095) [0]               :
  Gateway IP address [10.196.32.1]                       :

AUTOMATIC CONFIGURATION
  Acquire config from the Primary (yes/no) [yes]         : yes

PEER CONFIGURATION
  Peer IP address [169.254.1.1]                          :

-- Summary view
------------------------------------------------------------------

GUI ACCESS
  1: Enable Web GUI (yes/no)                             : yes

WEB GUI MODE
 2 : Web GUI Mode                                        : expert

HIGH AVAILABILITY
 3 : SBC mode                                            : high availability
 4 : SBC role                                            : secondary
 5 : Redundancy interface address                        : 169.254.1.2
```

```
 6 : Redundancy subnet mask                          : 255.255.255.252
 7 : Redundancy interface VLAN                       : N/A

SBC SETTINGS
 8 : Unique target name of this SBC                  :
FIPS_VM_Secondary
 9 : IP address on management interface              : 10.196.33.40
 10: Subnet mask                                     : 255.255.224.0
 11: Management interface VLAN                       : 0
 12: Gateway IP address                              : 10.196.32.1

AUTOMATIC CONFIGURATION
 13: Acquire config from the Primary (yes/no)        : yes

PEER CONFIGURATION
 14: Peer IP address                                 : 169.254.1.1
 15: Peer target name                                : N/A

OC SDM ACCESS SETTINGS
 16: OC SDM access (yes/no)                          : N/A
 17: SNMP community string                           : N/A
 18: OC SDM IP address                               : N/A

Enter 1 - 18 to modify, 'd' to display summary, 's' to save, 'q' to
exit. [s]:
```

The following are examples of FIPS VME primary and secondary deployments where adapter 1 is used for management, adapters 2 and 3 are used as the HA interconnects, 4 is unused, and adapters 5-8 are used as media interfaces.

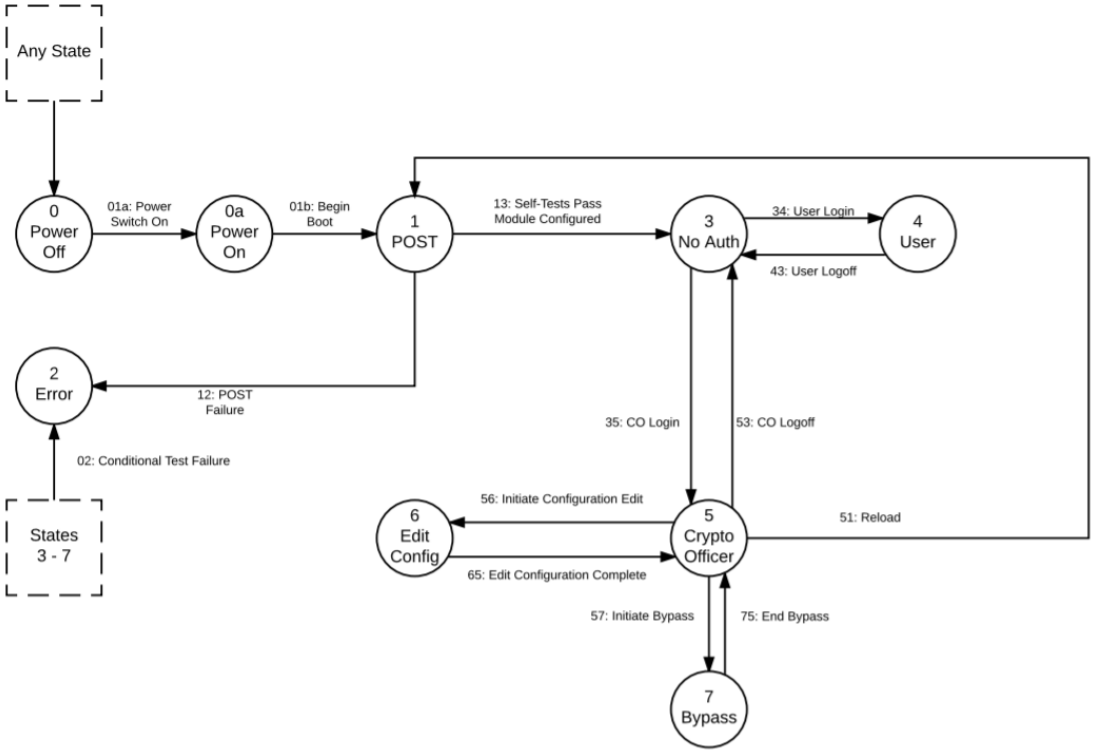



VM Hardware
CPU
4 CPU(s), 3520 MHz used
Memory
8192 MB, 0 MB memory active
Hard disk 1
40.00 GB
Network adapter 1
10.196.32.0%2f19 (connected)
Network adapter 2
1057::kwanchan_fips1 (connected)
Network adapter 3
1557::kwanchan_fips2 (connected)
Network adapter 4
Unused (disconnected)
Network adapter 5
25::QA_172.16.x.x (connected)
Network adapter 6
26::QA_182.16.x.x (connected)
Network adapter 7
27::QA_192.168.x.x (connected)
Network adapter 8
25::QA_172.16.x.x (connected)

4
Finite State Machine

As part of FIPS 140-2 Level 2 compliance, the Acme Packet 1100 and Acme Packet 3900 platforms support a Finite State Machine (FSM).

The following Diagram displays the state model of the FSM in the FIPS 140-approved mode of operation:



State Diagram

The following sections describe all states and transitions that can occur with the Finite State Diagram. The finite state machine never ends in an undefined state. Any combination of data and control inputs always place the FSM in a well-defined state.

> **Note:**
>
> The inputs described in this document for each state are inputs that would result in a successful operation.

State 0 - Power Off

Either the power switch is in the off position, or there is no power connected to the FSM. No services are available in this state. This state is available from every other state, and can be entered using the power switch and cycling power.

Transition Number	Transition	Next State
01a	Module is powered on	0a
Data Input	None	N/A
Data Output	None	N/A
Control Input	Connect Power Supply	N/A
Status Output	LED - power	N/A

State 0a - Power On

The FSM's power switch is turned on. No services are available in this state. The FSM automatically transitions to the Power-On Self-Tests state.

Transition Number	Transition	Next State
01b	Begin boot	1
Data Input	None	N/A
Data Output	None	N/A
Control Input	Power switch on	N/A
Status Output	LED - power	N/A

State 1 - Power-On Self-Tests

The FSM performs a series of self-tests to ensure correct operation; these include a software integrity check, cryptographic known answer tests, and other self-tests described in the Security Policy. If the POSTs are successful, the module continues to boot, and this state automatically transfers to the "No Auth" state. If the POSTs should fail, the module transitions to the "Error" state.

Transition Number	Transition	Next State
13	Self Tests Pass	3
Data Input	None	N/A
Data Output	None	N/A
Control Input	None	N/A
Status Output	Initial login prompt	N/A
12	POST Failure	2
Data Input	None	N/A
Data Output	None	N/A
Control Input	None	N/A
Status Output	Error logged	N/A
20	Power Switch to Off/Reboot	0
Data Input	None	N/A
Data Output	None	N/A

Transition Number	Transition	Next State
Control Input	Disconnect Power Supply	N/A
Status Output	None / Display boot status on startup	N/A

State 2 - Error

This state represents an error, such as a POST failure or Conditional Self-Test Failure. The FSM halts cryptographic operations and the operator must use any of the 3 possible recovery options:

- Reset the FSM
- Reset the FSM and use the bootloader to select the valid image
- Reset the FSM and use the bootloader to zeroize the system to RMA

Transition Number	Transition	Next State
20	Power Switch to Off/Reboot	0
Data Input	None	N/A
Data Output	None	N/A
Control Input	Disconnect Power Supply	N/A
Status Output	None / Display boot status on startup	N/A

State 3 - No Auth

The FSM transitions to this state when startup has completed and the module is fully configured for FIPS mode of operation. In this state no User or Crypto Officer is logged in, and the module is in an idle state. The FSM is operational but is not providing security services or performing cryptographic functions. Cryptographic keys and security parameters are loaded, and the FSM is waiting for data or control inputs. The FSM transitions to the User state when a User is successfully authenticated or it transitions to the Crypto Officer state when a Crypto Officer is successfully authenticated.

Transition Number	Transition	Next State
34	User Login	4
Data Input	User or SSH public key	N/A
Data Output	Acceptance / Denial of Authentication Attempt	N/A
Control Input	Authentication Data	N/A
Status Output	User Authentication Prompt	N/A
35	Crypto Officer Login	5
Data Input	Crypto Officer Authentication Data	N/A
Data Output	Acceptance / Denial of Authentication Attempt	N/A
Control Input	Authentication Data	N/A
Status Output	Crypto Officer Authentication Prompt	N/A

Transition Number	Transition	Next State
30	Power Switch to Off/Reboot	0
Data Input	None	N/A
Data Output	None	N/A
Control Input	Disconnect Power Supply	N/A
Status Output	None / Display boot status on startup	N/A
02	Conditional Test Failure	2
Data Input	None	N/A
Data Output	None	N/A
Control Input	None	N/A
Status Output	Error logged	N/A

State 4 - User

The FSM transitions into this state when a User authenticates to the module or when an encrypted session has been initiated. After successful login, the User has access to the services defined in the Roles, Services, and Authentication section of the Security Policy.

Transition Number	Transition	Next State
43	User Logoff	3
Data Input	None	N/A
Data Output	None	N/A
Control Input	Initiate Log Off	N/A
Status Output	Logoff confirmation	N/A
47	Initial Bypass	7
Data Input	Call from endpoint configured for plaintext received	N/A
Data Output	Plaintext call output	N/A
Control Input	Endpoint Configuration	N/A
Status Output	Call Successful	N/A
30	Power Switch to Off/Reboot	0
Data Input	None	N/A
Data Output	None	N/A
Control Input	Disconnect Power Supply	N/A
Status Output	None / Display boot status on startup	N/A
02	Conditional Test Failure	2
Data Input	None	N/A
Data Output	None	N/A
Control Input	None	N/A
Status Output	Error logged	N/A

State 5 - Crypto Officer

This state is entered when an operator successfully authenticates as a Crypto Officer. A Crypto Officer may configure the FSM as defined in the Secure Operation section of the Security Policy. A Crypto Officer can re-enter the *No Auth* state by logging out. The Crypto Officer may return to *Power On Self Tests* state by rebooting the software. Physically removing power from the module will return it to the Power Off state. The Crypto Officer can transition to the *Edit Configuration* state to edit the running configuration and manipulate keys.

Transition Number	Transition	Next State
56	Initiate Configuration Edit	6
Data Input	Configuration Parameters	N/A
Data Output	None	N/A
Control Input	Configuration Parameters	N/A
Status Output	Configuration Verifications	N/A
53	Crypto Officer Logoff	3
Data Input	None	N/A
Data Output	None	N/A
Control Input	Initiate Log Off	N/A
Status Output	Logoff confirmation	N/A
50	Power Switch to Off/Reboot	0
Data Input	None	N/A
Data Output	None	N/A
Control Input	Disconnect Power Supply	N/A
Status Output	None / Display boot status on startup	N/A
02	Conditional Test Failure	1
Data Input	None	N/A
Data Output	None	N/A
Control Input	None	N/A
Status Output	None	N/A

State 6 - Edit Configuration

This state is entered from the *Crypto Officer* state with various commands to configure the FSM and enter cryptographic keys. Only a Crypto Officer may edit the configuration of the FSM. Once the configuration is complete, the new configurations are effective immediately once the configuration is activated. The FSM returns to the *Crypto Officer* state when the Crypto Officer has completed configuration.

Transition Number	Transition	Next State
65	Edit Configuration Complete	5
Data Input	Configuration Parameters	N/A
Data Output	None	N/A
Control Input	Configuration Parameters	N/A
Status Output	Configuration Verifications	N/A
60	Power Switch to Off/Reboot	0

Transition Number	Transition	Next State
Data Input	None	N/A
Data Output	None	N/A
Control Input	Disconnect Power Supply	N/A
Status Output	None / Display boot status on startup	N/A
02	Conditional Test Failure	2
Data Input	None	N/A
Data Output	None	N/A
Control Input	None	N/A
Status Output	Error logged	N/A

State 7 - Bypass

The FSM is providing services without cryptographic processing (e.g., transferring plaintext calls through the FSM). In this state, the FSM is providing services with non-cryptographic processing (e.g., transferring plaintext through the module). The FSM can transition to a Bypass state when a call is received from an end point configured for non-encrypted calls.

Transition Number	Transition	Next State
74	POST Failure	4
Data Input	None	N/A
Data Output	None	N/A
Control Input	Call is disconnected	N/A
Status Output	Call ends	N/A
70	Power Switch to Off/Reboot	0
Data Input	None	N/A
Data Output	None	N/A
Control Input	Disconnect Power Supply	N/A
Status Output	None / Display boot status on startup	N/A