Oracle® Enterprise Session Border Controller

FIPS Compliance Guide
Release E-CZ7.5.0

August 2017

ORACLE

Notices

Contents

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 E-CZ7.5.0. The documentation set for this release is the E-CZ7.5.0 suite.

Documentation Set

The following table describes the documents included in the Oracle Enterprise Session Border Controller E-CZ7.5.0 documentation set.

Document Name	Document Description
ACLI Configuration Guide	Contains conceptual and procedural information for configuring, administering, and troubleshooting the E-SBC.
Administrative Security Guide	Contains conceptual and procedural information for supporting the Admin Security license, the Admin Security ACP license, and JITC on the E-SBC.
Call Traffic Monitoring Guide	Contains conceptual and procedural information for configuration using the tools and protocols required to manage call traffic on the E-SBC.
FIPS Compliance Guide	Contains conceptual and procedural information about FIPS compliance on the E-SBC.
HMR Guide	Contains conceptual and procedural information for header manipulation. Includes rules, use cases, configuration, import, export, and examples.
Installation and Platform Preparation Guide	Contains conceptual and procedural information for system provisioning, software installations, and upgrades.
Release Notes	Contains information about the E-Cz7.5.0 release, including platform support, new features, caveats, known issues, and limitations.
Web GUI User Guide	Contains conceptual and procedural information for using the tools and features of the E-SBC Web GUI.

Revision History

Date	Description
August 2017	• Initial release of ECZ750

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.

The functionality described in this document has been implemented in E-CZ7.5.0 for the Acme Packet 1100 (140-2 level 2), Acme Packet 3900 (140-2 level 2), and VME (140-2 level 1).

License Requirements

FIPS-compliant cryptographic implementation requires the presence of a new FIPS 140-2 license. The license is required for the following FIPS-compliant capabilities:

- power-on self tests
- software integrity test
- conditional tests
- ACLI commands and configuration attributes
  - show security fips
  - signature-algorithm

Platform Support

FIPS-compliant cryptography is available on the following platforms:

- Acme Packet 1100 (140-2 level 2)
- Acme Packet 3900 (140-2 level 2)
- VME (140-2 level 1)

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/nnECZ750b4.bz
Verifying signature of /boot/nnECZ750b4.bz
```

```
Version: Acme Packet ECZ7.5.0 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/nnECZ750b4.bz
Verifying signature of /boot/nnECZ750b4.bz
Version: Acme Packet ECZ7.5.0 Beta 4 (WS Build 48) 201705130547
old boot file /boot/bzImage being replaced with /boot/nnECZ750b4.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 SHA-256 hashing, SHA-256 HMAC, and RNG via the Hash_DRBG method.
- Mocana — This software module provides cryptographic functions to include FIPS 186-4 RSA key generation, signature generation, and signature verification, as well as SHA-2 and SP 800-90A DRBG.

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

Random Number Generator

The Oracle Enterprise Session Border Controller (Acme Packet 1100, Acme Packet 3900, and VME) provides a FIPS-compliant random number generator based upon NIST Special Publication 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), June 2015.

Mocana SSH uses Hash_DRBG which was specified in section 10.1.1 of NIST SP800-90A Revision 1. The rest of DRBG uses CTR_DRBG, specified in section 10.2.1 of the same document.

FIPS States

When you buy a FIPS license with the Oracle Enterprise Session Border Controller, the E-SBC comes equipped with a FIPS 140-2 license, 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
- HMAC-SHA-1 Known Answer Test
- HMAC-SHA-256 Known Answer Test
- RSA Verify Known Answer Test

OpenSSL Self-Tests

- SHA-1 Known Answer Test
- SHA-256 Known Answer Test
- HMAC-SHA-1 Known Answer Test
- HMAC-SHA-256 Known Answer Test
- HMAC-SHA-384 Known Answer Test
- AES (Encrypt/Decrypt) Known Answer Test
- AES GCM (Encrypt/Decrypt) Known Answer Test
- Triple-DES (Encrypt/Decrypt) Known Answer Test
- SP 800-90A DRBG Known Answer Test
- RSA sign/verify Known Answer Test
- ECDSA sign/verify Known Answer Test
- DRBG Known Answer 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 new 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 1100 and Acme Packet 3900 platform output.

```
ACMEPACKET# show security fips

**********************************************************
```

```
*** System is currently operating in FIPS 140-2 compatible mode.
************************************************************
     ACMEPACKET#
```

The following is an example of VME output:

```
sd225v# show security fips

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

If the Oracle Enterprise Session Border Controllertransitions 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*.

```
ACMEPACKET# show security fips

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

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.
```

encrypt-algorithm

The new configuration parameter **encrypt-algorithm** has been added under **SNMP-user-entry** to allow SNMP V3 to use AES128 encryption instead of DES. The **encrypt-algorithm** parameter defaults to DES.

Below is an example of a configured SNMP-user-entry and the corresponding trap-receiver.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# system
ACMEPACKET(system)# SNMP-user-entry
```

```
ACMEPACKET(SNMP-user-entry)#show
snmp-user-entry
        user-name           fips
        auth-password       *****
        priv-password       *****
        encrypt-algorithm   aes128
        last-modified-by    admin@console
        last-modified-date  2015-05-11 14:26:15
```

Subsequently, you must configure **trap-receiver**, where the **user-list** contains the **SNMP-user-entry** just configured.

```
ACMEPACKET(configure)# system
ACMEPACKET(system)# trap-receiver
ACMEPACKET(trap-receiver)# select (select the trap-receiver configured)
trap-receiver
        ip-address              172.30.0.144:161
        filter-level            all
        community-name
        user-list               fips
        last-modified-by        admin@console
        last-modified-date      2015-05-11 16:19:24
```

Note: You must save and activate the configuration after changing the **encrypt-algorithm**.

Accessing the Oracle Rescue Account

As part of Admin Security, JITC, and FIPS compliance, an account called Oracle Rescue Account is supported, using a challenge/response mechanism, to authenticate the user before initiating the privileged operations of factory reset (zeroization) and shell access.

Caution: Factory reset erases all system data, including license keys and configuration, and reboots 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.

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 on 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.

   The Oracle Rescue Account sub-menu currently provides three menu options:

   - **f** - Factory default
   - **!** - start debug shell
   - **x** - exit to main menu

   Note: The above procedure is to be executed by a FIPS Security Officer only.

The following is an example of the console log:

```
Starting acmeboot...
```

```
ACME bootloader Acme Packet ECZ7.5.0 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...
```

2

Installing a FIPS License and Upgrading a FIPS System

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

Installing a FIPS License

Beginning in release ECz7.5.0, FIPS-compliant Acme Packet supported platforms are typically shipped with a FIPS license already installed. However, this procedure describes installing a FIPS license in the event that you need to install one.

The following are required to install the FIPS license:

- Access to the target Acme Packet platform.
- Access to the target Acme Packet platform's management IP address.
- Access to the FIPS software image nnECz750.tar.
- FIPS license hex string from Oracle Support.

  Add the FIPS license key you received from Oracle Support at the superuser prompt. For instructions on adding a license, see "License Key Operations" in the *Oracle Communications Enterprise Session Border Controller ACLI Configuration Guide*.

Upgrading the Image on a FIPS Enabled System

This procedure assumes that a valid FIPS license is already present on the system. If the FIPS license is expired, install a valid FIPS license. For more information on installing a FIPS license, see "Installing a FIPS License".

The following are required to install the FIPS license:

- 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 nnECZ750b4.bz.

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

1. Use SFTP to transfer nnECZ750.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/nnECZ750b4.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/nnECZ750b4.bz
Verifying signature of /boot/nnECZ750b4.bz
Version: Acme Packet ECZ7.5.0 Beta 4 (WS Build 48) 201705130547
old boot file /boot/bzImage being replaced with /boot/nnECZ750b4.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

FIPS Security Label and Security Cover Assembly Procedure

This chapter describes how to replace the FIPS security labels and the security cover on the Acme Packet supported platforms, and assumes the user has a working knowledge of and access to the product.

Requirements

The following are required to update the security cover and the FIPS security labels on the Acme Packet supported platforms:

- Physical access to the Acme Packet platform
- (1x) Security Cover
- (2x) Screw
- (5x) Security Labels
- Supplies to clean adhesive from the bezel after existing label removal

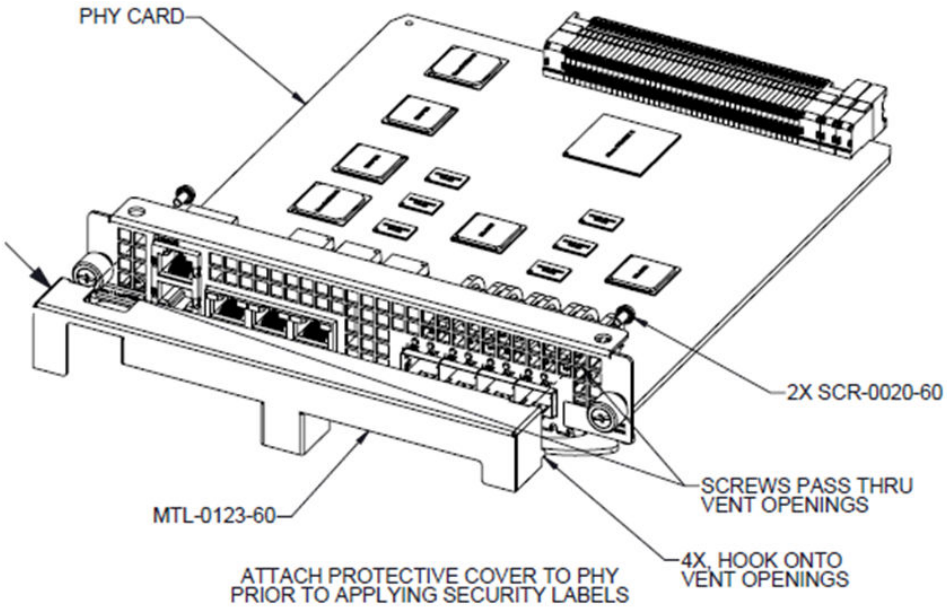
Attaching the Acme Packet Platform Security Cover

Required Parts:

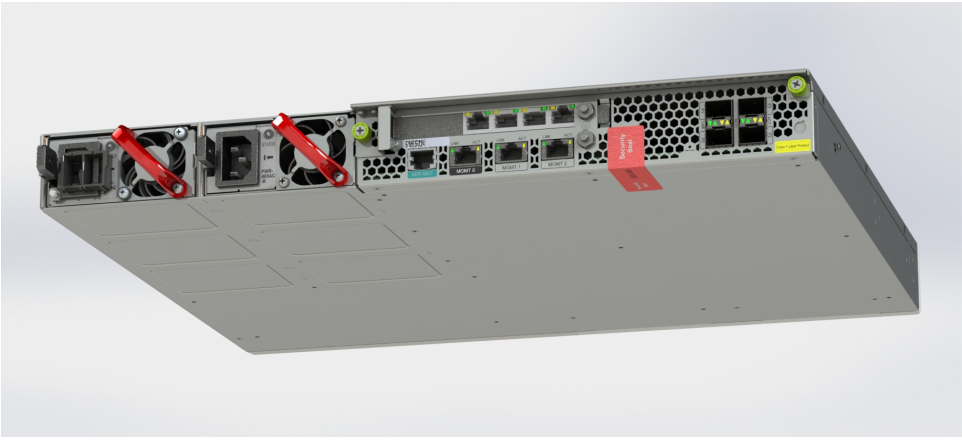
- (1x) Security Cover
- (2x) Screw

1. Remove top cover.

2. Attach security cover to PHY card using supplied screws.



3. Install the PHY card assembly.



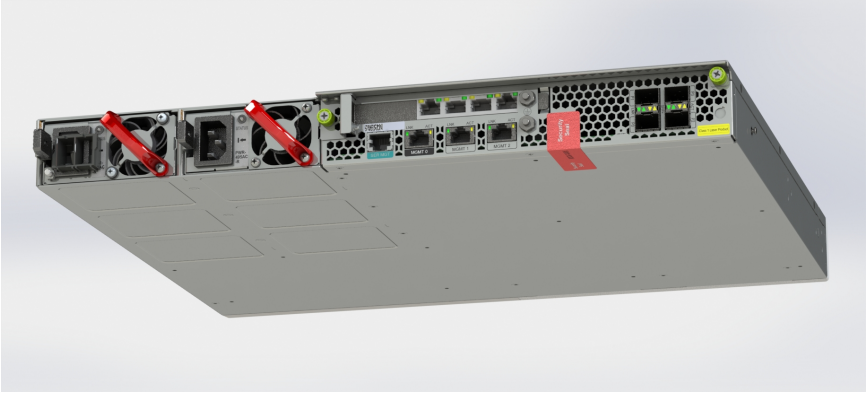
Applying Security Labels to the Acme Packet 1100/3900

Parts required:

- (5x) Security Label

1. Apply label #1 and #2, as shown in diagram below.

2. Apply label #3, #4, and #5, as shown in diagram below.



4

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).

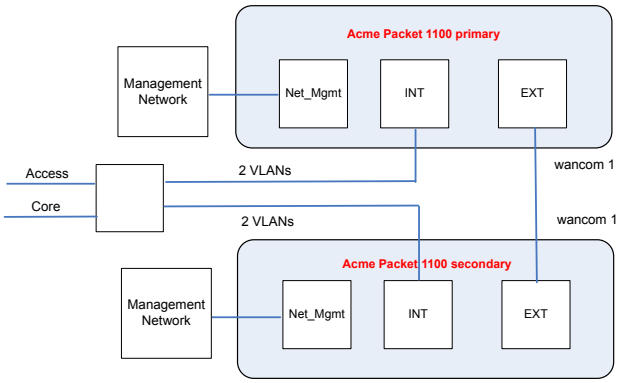
Configuring Acme Packet 1100 FIPS High Availability

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 primary 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
```

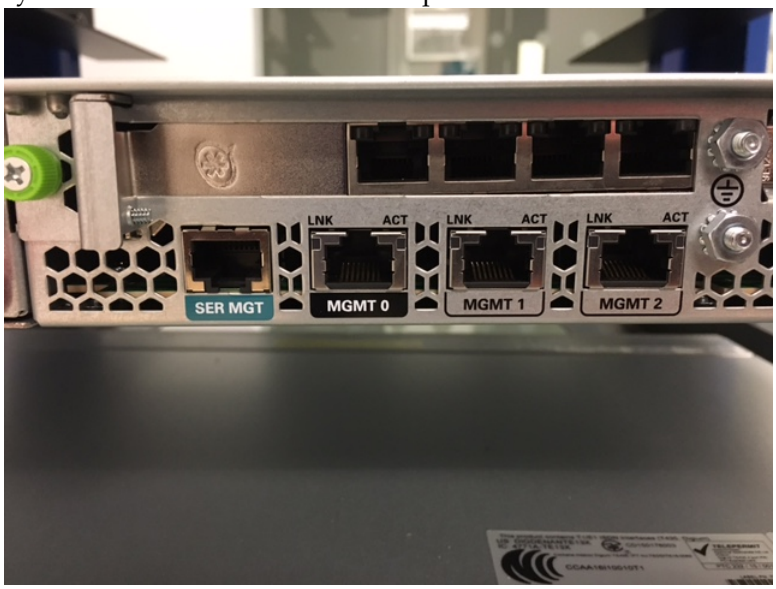
```
 17: SNMP community string                                : N/A
 18: OC SDM IP address                                    : N/A

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

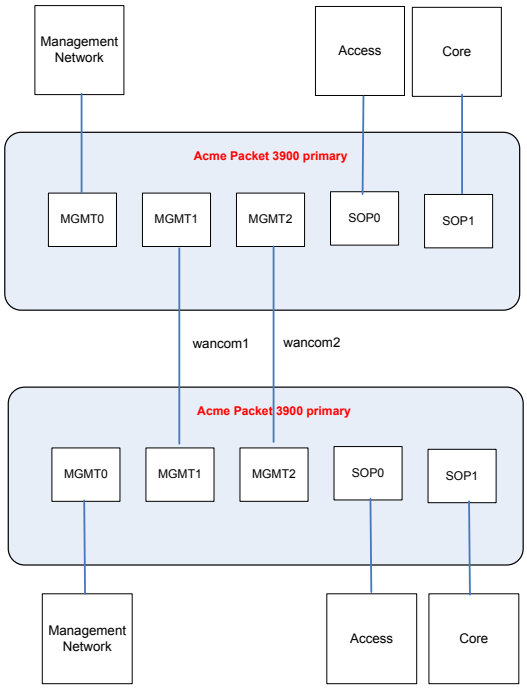
For more information on configuring HA on the Acme Packet 1100, see the *Acme Packet 1100 Hardware Installation and Maintenance Guide* and *Enterprise Session Border Controller ACLI Configuration Guide*.

Configuring Acme Packet 3900 FIPS HA

FIPS dictates that critical traffic must be encrypted, not currently supported on this platform. Therefore, on each of the Acme Packet 3900s 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 3900 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 3900 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 3900, see the *Acme packet 3900 Hardware Installation and Maintenance Guide* and the *Enterprise 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), 3138 MHz used
Memory	8192 MB, 81 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)

VM Hardware

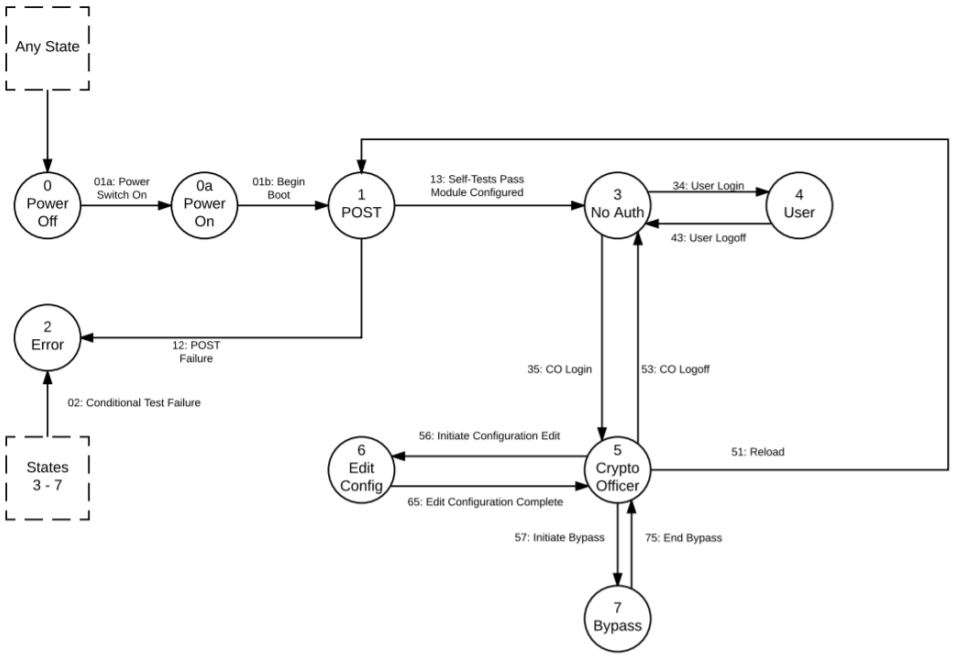
CPU	4 CPU(s), 3520 MHz used
Memory	8192 MB, 0 MB memory active
Hard disk 1	40.00 GB
Network adapter 1	10.196.32.0%2f19 (connected)
Network adapter 2	1057::kwanchan_fips1 (connected)
Network adapter 3	1557::kwanchan_fips2 (connected)
Network adapter 4	Unused (disconnected)
Network adapter 5	25::QA_172.16.x.x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

A

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	1a
Data Input	None	
Data Output	None	
Control Input	Connect Power Supply	
Status Output	LED - power	

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	
Data Output	None	
Control Input	Power switch on	
Status Output	LED - power	

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	
Data Output	None	
Control Input	None	
Status Output	Initial login prompt	
12	POST Failure	2
Data Input	None	
Data Output	None	
Control Input	None	
Status Output	Error logged	
20	Power Switch to Off/Reboot	0

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

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	
Data Output	None	
Control Input	Disconnect Power Supply	
Status Output	None / Display boot status on startup	

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	
Data Output	Acceptance / Denial of Authentication Attempt	
Control Input	Authentication Data	
Status Output	User Authentication Prompt	
35	Crypto Officer Login	5
Data Input	Crypto Officer Authentication Data	
Data Output	Acceptance / Denial of Authentication Attempt	
Control Input	Authentication Data	
Status Output	Crypto Officer Authentication Prompt	
30	Power Switch to Off/Reboot	0
Data Input	None	

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

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

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

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	
Data Output	None	

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

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	
Data Output	None	
Control Input	Call is disconnected	
Status Output	Call ends	
70	Power Switch to Off/Reboot	0
Data Input	None	
Data Output	None	
Control Input	Disconnect Power Supply	
Status Output	None / Display boot status on startup	