

Oracle® Enterprise Session Border Controller

FIPS Essentials Guide
Release E-CX6.4.1M1

December 2016

Notices

Copyright ©2016 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

About this Guide.....	5
1 FIPS Compliance.....	7
License Requirements.....	7
Platform Support.....	7
Cryptographic Modules.....	7
Random Number Generator.....	8
FIPS States.....	8
Self-Tests.....	8
Power-on Self-Tests.....	8
Conditional Self Tests.....	11
ACLI Commands.....	12
show security fips.....	12
image-integrity-value.....	13
import-image-verification-public-key	13
encrypt-algorithm.....	13
2 Installing a FIPS License and Upgrading a FIPS System.....	15
Installing a FIPS License.....	15
Upgrading the Image on a FIPS enabled System.....	15
.....	15
3 FIPS Security Label and Security Cover Assembly Procedure.....	23
Attaching the Acme Packet 3820/4500 Security Cover.....	23
Applying Security Labels to the Acme Packet 3820/4500.....	24
4 Additional Release Features.....	27
SRTP Re-keying.....	27
SRTP Re-keying Configuration.....	28

About this Guide

This guide provides the information you need to set-up and use the FIPS (Federal Information Processing Standard) functionality in the Oracle Enterprise Session Border Controller with Release E-Cx6.4.1m1. The documentation set for this release is the S-Cx6.4.0 suite. Be sure to reference the Release Notes for E-Cx6.4.0 for additional information.

Related Documentation

Document Name	Document Description
Acme Packet 4500 Hardware Installation and Maintenance Guide	Contains information about the components and installation of the Acme Packet 4500 system.
Acme Packet 3820 Hardware Installation and Maintenance Guide	Contains information about the components and installation of the Acme Packet 3800 system.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the Oracle Communications Session Border Controller.
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 logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet'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 accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about support for the Administrative Security license.

Revision History

Date	Description
February 2015	<ul style="list-style-type: none">Initial release of E-Cx6.4.1

About this Guide

Date	Description
May 2015	<ul style="list-style-type: none">• Added the encrypt-algorithm SNMP configuration parameter to support AES128 encryption in E-Cx6.4.1M1 release.• Added the srtp-rekey-on-reinvite parameter in the chapter on additional release features in E-Cx6.4.1M1.
December 2016	<ul style="list-style-type: none">• Changed supported TLS version to TLSv1 per 5575• Changed Release Date to December 2016.

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 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators* (Revised), March 2007.

The initial functionality described in this document was implemented in S-CX6.3.0 for the Acme Packet 3820/4500. Additional changes have been made for a 2015 certification of this release.

License Requirements

FIPS-compliant cryptographic implementation requires the presence of a new FIPS 140-2 level-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
 - image-integrity-value
 - import-image-verification-public-key
 - signature-algorithm

Platform Support

FIPS-compliant cryptography is available on the following platforms: Acme Packet 3820 and Acme Packet 4500.

Cryptographic Modules

FIPS compliance requires the clear definition of modules that perform cryptographic function. Three such modules are present on the Acme Packet 3820 and Acme Packet 4500 platforms.

1. Broadcom 5862 Security Processor (referred to as the Broadcom processor within this document)— this hardware-accelerated module provides cryptographic functions to include Advanced Encryption Standard (AES)

FIPS Compliance

and Triple Data Encryption Algorithm (3DES) encryption/decryption, SHA-1 hashing, SHA-1 hash-based message authentication codes (HMAC), RSA key generation, and random number generation (RNG).

2. HiFN 8450 Security Processor (referred to as the HiFN processor within this document) — this hardware-accelerated module provides cryptographic functions to include AES and 3DES encryption/decryption, SHA-1 hashing, SHA-1 HMAC.
3. OpenSSL — this software module provides cryptographic functions to include SHA-1 and SHA-256 hashing, SHA-1 and SHA-256 HMAC, and RNG via the Hash_DRBG method.

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

Random Number Generator

The Oracle Enterprise Session Border Controller provides a FIPS-compliant random number generator based upon the Hash_DRBG algorithm specified in Section 10.1.1 of NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007.

The Hash_DRBG requires an input called entropy that is used to introduce randomness into the number generation process. The existing BCM5862 RNG function provides the entropy source. The RNG monitors thermal noise to generate a string of 5120 random bits which is passed to a FIPS certified SHA-256 hashing algorithm. The resulting 256-bit hash output is then input to the Hash_DRBG algorithm.



Note: With Release S-CX6.3.0, and later releases, all RNG operations use the Hash-DRBG algorithm, as described above, without regard to the presence of a FIPS 140-2 level-2 license.

FIPS States

By default, Oracle Enterprise Session Border Controllers equipped with a FIPS 140-2 level-2 license operate in FIPS 140-2 compatible mode, meaning that the Oracle Enterprise Session Border Controller has access to the FIPS capabilities listed in this document. In the event that any of the power-on or conditional tests fail, the Oracle Enterprise Session Border Controller transitions to a non-FIPS 140-2 mode, meaning that it is no longer FIPS-compatible. The Oracle Enterprise Session Border Controller remains in non-FIPS 140-2 mode until a subsequent re-boot with failure-free power-on self tests.

The following restrictions will be on the system in non-FIPS 140-2 mode:

- TLS and SSH connections are not allowed.
- 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

Power-on self-tests are described in the following sections.

AES Known Answer Test

The AES Known Answer Test (KAT) verifies hardware-based AES encryption and decryption. The AES KAT works with known plaintext, known cryptotext, known keys, and known initialization vectors to perform AES encryption and decryption, and verifies that generated and known plaintext and cryptotext are identical. Depending on installed

Network Interface Units (NIU), processor-specific operations verify the integrity of either the HiFN or Broadcom processor. Regardless of processor type, both AES-CBC (Cipher Block Chaining) mode and AES-CTR (Counter) mode are verified. For the HiFN processor, 128 and 256-bit keys are tested for both modes; for the Broadcom processor, 128, 192, and 256-keys are tested for CBC mode, and 128 and 256-bit keys are tested for CTR mode.

In the event of AES KAT failure, one of the following error messages is displayed:

```
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 Known Answer Test

The 3DES KAT verifies hardware-based DES encryption and decryption. Similar to the AES KAT, this KAT uses known cryptographic resources to perform processor-specific tests that verify the integrity of 3DES encryption/decryption operations on the HiFN processor.

In the event of 3DES KAT failure, the following error message is displayed:

```
3DES CBC test failed.
```

Hashing Known Answer Test

The Hashing KAT takes a known message and the message's known hash value. It applies a FIPS-approved hashing algorithm to the message. The resulting hash is compared to the known hash value. The KAT passes if the hashes are identical; otherwise the KAT fails. Initially, the KAT uses OpenSSL to verify software-based SHA-1 and SHA-256 hashing. It subsequently performs processor-specific operations to verify hardware-based SHA-1 and SHA-256 hashing on the HiFN processor and SHA-1 hashing on the Broadcom processor.

In the event of Hashing KAT failure, one of the following error messages is displayed:

```
SHA1 test failed.  
SHA256 test failed.
```

HMAC Known Answer Test

The HMAC KAT takes a known message, known key, and known HMAC value. It applies a FIPS-approved HMAC algorithm to the message. The resulting HMAC is compared to the known HMAC value. The KAT passes if the values are identical; otherwise the KAT fails. Initially, the KAT uses OpenSSL to verify software-based SHA-1 HMAC and SHA-256 HMAC algorithms. It subsequently performs processor-specific operations to verify hardware-based SHA-1 HMAC computation on the HiFN processor.

In the event of HMAC KAT failure, one of the following error messages is displayed:

```
HMAC-SHA1 test failed.  
HMAC-SHA256 test failed.
```

RSA Pairwise Consistency Test

The RSA Consistency Test verifies hardware-based RSA operations on the Broadcom processor. The test takes a known RSA key pair, known plaintext, and known ciphertext. It first enciphers the plaintext with the RSA public key. The resulting ciphertext is compared to the known ciphertext. The test passes if the ciphertexts are identical; otherwise the test fails. If the ciphertexts match, the test continues by decrypting the ciphertext with the RSA private key. The resulting plaintext is compared to the known plaintext. The test passes if the plaintexts are identical; otherwise the test fails.

In the event of RSA Pairwise Consistency Test failure, the following error message is displayed:

```
RSA pairwise consistency test failed.
```

RSA Signature Verification Test

The RSA Signature Verification Test involves RSA signature generation and verification. The test first computes the hash of a message using SHA1 or SHA2. It encrypts the resulting hash using the RSA private key, then encrypts the result using the RSA public key. After the second encryption, it decrypts the message using the RSA private key and decrypts the resulting hash using the RSA public key. Finally the test computes the hash of the decrypted message, using the same hash algorithm as above, and compares the hash of the original message with the hash of the decrypted message.

The test fails if the comparison fails, otherwise the test passes.

If the RSA Signature Verification Test fails, one of two error messages is displayed:

```
RSA (SHA1) Digital sign-verify test failed.
```

or

```
RSA (SHA256) Digital sign-verify test failed.
```

Software/Firmware Integrity Test

FIPS compliance requires an integrity test to verify the boot image. Verification is based upon a known SHA-256 HMAC value that is computed for the boot image prior to equipment delivery. The image-specific HMAC value is transferred to customer administrators or security officers as part of the delivery process. Later, during Acme Packet SBC configuration, this HMAC value is entered via the ACLI.

A FIPS-compliant device cannot be booted with an externally stored image. To enforce this requirement, the Acme Packet SBC must be booted with a software image file contained in the local `/code/images` directory.

During power-on, the Software/Firmware Integrity Test (S/FIT) initially examines boot parameter values. If the boot file is not in the Acme Packet SBC `/code/images` directory, the test fails.

To verify against a known HMAC-SHA256 value, an HMAC-256 value on the image is pre-computed and the resultant value is stored in the config. Previously, when an image was built, a SHA-256 hash was generated. Currently, for FIPS support, an HMAC-SHA256 value is generated instead.

The key used for the HMAC-256 operation is **acmepacket**. A new configuration parameter has been added under `security-config` with the name `image-integrity-value`. The crypto officer must ensure that an Acme Packet-generated HMAC-SHA256 value is stored under this new field `image-integrity-value`. The system will compute an HMAC-SHA256 value over the entire image and use the key **acmepacket**. The resultant value will be compared with the value stored in `image-integrity-value`. If both values match, the test passes, otherwise the test fails.

Assuming the boot image is properly found in the `/code/images` directory, the S/FIT uses the key `acme packet` to generate a SHA-256 HMAC hash value for the software image file. The resulting hash value is compared against the known HMAC value. If the values match, the S/FIT passes; otherwise, the test fails.

In the event of S/FIT failure, the following error message is displayed:

```
Software image integrity check failed.
```

Hash DRBG Known Answer Test

The Hash DRBG KAT verifies operation of the FIPS-compliant Deterministic Random Bit Generator (DRBG) algorithm, used to generate random number for cryptographic operations. During the test, a known entropy value is used to seed 10 random number generations. The resulting 10 random numbers output by the Hash_DRBG algorithm are compared with a list of known random numbers. If the numbers are identical, the test passes; otherwise, the test fails.

In the event of Hash DRBG KAT failure, the following error message is displayed:

```
Continuous DRBG failed.
```

Hash DRBG Health Test

The Hash DRBG Health Test also verifies the FIPS-compliant Hash_DRBG algorithm. Specifically, this test verifies the instantiation, re-seed, and number generation functions provided by the algorithm. During the instantiation phase, the health test uses a known entropy value to instantiate a new Hash_DRBG instance and compares the returned values (V, the seed, and C, a hash of the seed) with known values. If the values match, the test passes; otherwise, the test fails.

Assuming the instantiation test is successful, the health test next re-seeds the Hash_DRBG instance. As before, the health test compares the returned values (V and C) with known values. If the values match, the test passes; otherwise, the test fails.

Assuming success, the test completes by verifying the number generation function. Again, the health test compares the returned values (V and C, and the returned sequence of random bits) with known values. If the values match, the test passes; otherwise, the test fails.

In the event of Hash DRBG Health Test failure, one of the following error messages is displayed:

```
DRBG with known entropy failed.  
DRBG instantiate health test failed.  
DRBG reseed health test failed.  
DRBG generate health test failed.
```

TLS Key Derivation Function Known Answer Test

The TLS Key Derivation Function Known Answer Test verifies that key derivation functionality is working properly. The (OpenSSL) TLSv1 KDF is tested using a known set of input vectors. The test takes preset values for the following

- Pre-master secret random number
- Server hello random number
- Client hello random number
- Server random number
- Client random number

The above values are used to compute the master secret, which is compared to an expected value. Failing to match the expected value results in a failure of the test.

Conditional Self Tests

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

Conditional self-tests are described in the following sections:

RSA Consistency Conditional Test

The RSA Consistency Conditional Test is run each time an RSA key pair is generated. The test verifies RSA encryption/decryption operations performed by the Broadcom processor.

The test takes a known RSA key pair, known plaintext, and known ciphertext. It first enciphers the plaintext with the RSA public key. The resulting ciphertext is compared to the known ciphertext. The test passes if the ciphertexts are identical; otherwise the test fails. If the ciphertexts match, the test continues by decrypting the ciphertext with the RSA private key. The resulting plaintext is compared to the known plaintext. Identical plaintext strings indicate that the test passes and generation of a new RSA key pair proceeds. The test fails if the plaintexts are not identical, and generation of the RSA key pair is denied.

In the event of RSA Consistency Conditional Test failure, the following error message is displayed:

```
RSA pairwise consistency Conditional test failed.
```

In the event of Hash DRBG KAT failure, the following error message is displayed:

```
Continuous DRBG failed.
```

Continuous Random Number Generation Test

The Continuous Random Number Generation Conditional Test is run each time a new random number is required. The newly generated random number is compared to the previously generated random number, which has been stored for purposes of comparison. If the numbers are identical, the conditional test fails, the number is rejected, and a new random number is generated.

ACLI Commands

These ACLI commands and new parameters support FIPS compliancy.

show security fips

The **show security fips** ACLI command displays the FIPS state.

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

If the Oracle Enterprise Session Border Controller is in non-FIPS 140-2 mode, the **show security fips** command displays the error condition that resulted in the transition to the non-FIPS-compliant state.

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


Other possible error messages are as follows:

```
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.
```

image-integrity-value

The **image-integrity-value** CLI command sets the known SHA-256 HMAC value that is computed for the boot image.

```
ACMEPACKET# configure terminal
ACMEPACKET (configure) # security
ACMEPACKET (security) # security-config
ACMEPACKET (security-config) # image-integrity-value
96691450df2a3dcf26a6071dabf65083e63321200384b5a62cdbfb748443e585
ACMEPACKET (security-config) # show
ocsr-monitoring-traps          enabled
image-integrity-value
96691450df2a3dcf26a6071dabf65083e63321200384b5a62cdbfb748443e585
options
last-modified-by              admin@console
last-modified-date            2010-11-29 16:45:19
ACMEPACKET (security-config) #
```

 **Note:** You must save and activate after changing the **image-integrity-value**.

import-image-verification-public-key

To verify the image, the system must be configured with the appropriate public key. The command **import-image-verification-public-key** has been added for this purpose. The user must run the command without arguments.

```
ACMEPACKET# import-image-verification-public-key
IMPORTANT:
  Please enter the certificate in the PEM format.
  Terminate the certificate with ";" to exit.....

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAWX5u7MLeCb0Dga6JdJjg
BPq4SLmMVkHIOad46IsQLK8fhCz7YYHeTffIloodcKVupL6PdQIU54XBj24mc+b/
x97796f+jCPrOgLknYSUshG1RNbMLjdf1cLJcK4kAJWXBm/GLISJwyHMISXruXCn
oDLdbRMjsuptg4b7ZMVk/Wm0JupcwQHKcwYJ3NCgSUXRuRoTBq7yal72gPQ/SrV9
9dulEmneVxVgsOd+KZUTPQjurfrfTlI/Zvvrik5Ckqv6MW7WBhPivJjUeJ235yTf
D8QX2yZQNM4E8r8g8mAGXe/LelxnGR+bIO95BX+2UZ4dvM1cgQdlvhX09XIw7or5
GQIDAQAB
-----END PUBLIC KEY-----
;ACMEPACKET#
```

If an error occurs during the writing of the key, the following error will be printed:

```
Unable to read the public key!
Public is corrupt or not present
Error: failed to write the cert to disk
```

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**.

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, as well as upgrading the image on a system that already has a valid license.

Installing a FIPS License

This section assumes that a valid FIPS license is not present on the system. The **image-integrity-value** and the public key are not needed for this process. This procedure is also valid if the FIPS license is expired. If you have purchased a FIPS license with a new Acme Packet 3820/4500, the license is already on the system.

The Acme Packet 3820/4500 products manufactured by the contract manufacturer, or products resold by Acme Packet to Acme Packet customers with the FIPS license are subject to the requirements of this procedure.

The following are required to install the FIPS license:

- Telnet access to the target Acme Packet 3820/4500.
- Access to the target Acme Packet 3820/4500 management IP address.
- Access to the FIPS software image nnECX641.tar.
- FIPS license hex string from Oracle Support.

Add the FIPS license you received from Oracle Support at the superuser prompt. The hex value below is an example:

```
ACMEPACKET# add s125o39pvtqhas4v2r2jcl0aen9e01o21b1dmh3
```

Upgrading the Image on a FIPS enabled System


This section assumes that a valid FIPS license is already present on the system. If the FIPS license is not present, the image integrity value and the public key are not needed for this process and those steps can be skipped. If the FIPS license is expired, please install a valid FIPS license (see the previous section FIPS License Installation).

The Acme Packet 3820/4500 products manufactured by the contract manufacturer, or products resold by Acme Packet to Acme Packet customers with the FIPS license are subject to the requirements of this procedure.

The following are required to install the FIPS license:

Installing a FIPS License and Upgrading a FIPS System

- SSH File Transfer Protocol (SFTP) client. access to the target Acme Packet 3820/4500.
- SFTP access to the target Acme Packet 3820/4500 management IP address.
- Access to the FIPS software image nnECX641.tar.
- The image verification public key from Oracle Support.
- The image integrity value from Oracle Support.

 **Note:** Follow this procedure on a running device:

1. Use SSH File Transfer Protocol (SFTP) to transfer nnECX641.tar into /code/images on the target Acme Packet 3820/4500.
2. Import the image verification public key.
You are prompted to enter the public key, including the ----BEGIN PUBLIC KEY ---- and ----END PUBLIC KEY ---- lines. An example is shown below:

```
ACMEPACKET#import-image-verification-public-key
IMPORTANT:
    Please enter the certificate in the PEM format.
    Terminate the certificate with ";" to exit.....

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAWX5u7MLeCb0Dga6JdJjq
BPq4SLmMVkHIOad46IsQLK8fhCz7YYHeTffIloodcKVupL6PdQIU54XBj24mc+b/
x97796f+jCPrOgLknYSUshG1RNbMLjdf1cLJcK4kAJWXBm/GLISJwyHMISXruXCn
oDLdbRMjsuptg4b7ZMVk/Wm0JupcwQHKcwYJ3NCgSUXRuRoTBq7yal72gPQ/SrV9
9du1EmneVxVgsOd+KZUTPQjurfrfT1I/Zvvrik5Ckqv6MW7WBhPivJjUeJ235yTf
D8QX2yZQNM4E8r8g8mAGXe/Le1xnGR+bIO95BX+2UZ4dvM1cgQdlvhX09XIw7or5
QIDAQAB
-----END PUBLIC KEY-----
;ACMEPACKET#
```

If an error occurs during the writing of the key, the following error will be printed:

```
Unable to read the public key!
Public is corrupt or not present
Error: failed to write the cert to disk
```

3. Configure the image integrity value you received from Oracle Support. The hex value below is an example:

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# security-config
ACMEPACKET(security-config)# image-integrity-value
96691450df2a3dcf26a6071dabf65083e63321200384b5a62cdbfb748443e585
```

4. Use the **show** command to ensure that the image integrity value is loaded without error.

```
ACMEPACKET(security-config)# show
security-config
ocsr-monitoring-traps                disabled
image-integrity-value
96691450df2a3dcf26a6071dabf65083e63321200384b5a62cdbfb748443e585
options
last-modified-by                      admin@console
last-modified-date                    2010-11-29 16:45:19
```

5. Exit configuration mode.

```
ACMEPACKET(security-config)#
ACMEPACKET(security-config)# exit
ACMEPACKET(security)# exit
```

6. Configure the boot parameters of the device.

To navigate through the boot parameters, press Enter and the next parameter appears on the following line. You can navigate through the entire list this way. To go back to a previous line, type a hyphen (-) and press Enter. Any value that you enter entirely overwrites the existing value and does not append to it.

You can navigate through the entire list this way. To go back to a previous line, type a hyphen (-) and press Enter. To change a boot parameter, type the new value that you want to use next to the old value. For example, if you want to change the image you are using, type the new filename next to the old one. You can clear the contents of a parameter by typing a period and then pressing Enter. Any value that you enter entirely overwrites the existing value and does not append to it.

```
ACMEPACKET(configure)# bootparam
'.' = clear field; '-' = go to previous field; q = quit

Boot File           : nnSCX630m4.xz  nnECX641.tar
IP Address          : 172.30.85.12
VLAN                : 0
Netmask             : 255.255.0.0
Gateway             : 172.30.0.1
IPv6 Address        :
IPv6 Gateway        :
Host IP             : 172.30.0.125
FTP username        : vxftp
FTP password        : vxftp
Flags               : 0x00000031
Target Name         : 172.30.85.12
Console Device      : VGA
Console Baudrate    : 115200
Other               :
```

NOTE: These changed parameters will not go into effect until reboot. Also, be aware that some boot parameters may also be changed through PHY and Network Interface Configurations.

7. Save and activate the new configuration.

```
ACMEPACKET# save-config
ACMEPACKET# activate-config
```

8. Force the device to reboot.

```
ACMEPACKET# reboot force

/code synced and unmounted
/boot synced and unmounted

Rebooting...

Acme Packet Net-Net 4500
Processor speed: 2.0 GHz
Stage 1 (built Jun 21 2011 09:01:15)
Stage 2 (built Jun 21 2011 09:01:15)

Press the space bar to stop auto-boot...
 0
auto-booting...

Downloading ipsec firmware on eth2... done Downloading ipsec firmware on
eth0... done

boot device           : eth
unit number          : 0
processor number      : 0
host name             : goose
file name             : /code/images/nnECX641.tar
inet on ethernet (e) : 172.30.18.16:ffff0000
gateway inet (g)     : 172.30.0.1
user (u)              : vxftp
ftp password (pw)    : vxftp
flags (f)             : 0x0
```

Installing a FIPS License and Upgrading a FIPS System

```
target name (tn)      : estate

Extracting from fd 4
extract acmeOS_x86.xz
extracting file acmeOS_x86.xz, size 16748820 bytes, 32713 blocks
done extracting: acmeOS_x86.xz
1 files read
Decompressing image... 75991293 bytes uncompressed.
93674608
Starting at 0x308000...

Instantiating /ramdrv as rawFs, device = 0x1
CPU frequency is 2.0 GHz
Formatting /ramdrv for DOSFS
Instantiating /ramdrv as rawFs, device = 0x1
Formatting...OK.
Attaching interface lo0... done
Attached IPv4 interface to eth unit 0
Attached IPv6 interface to eth unit 0
LeakSpy initialized

Adding 105565 symbols for standalone.

Starting the application...

boot flags: 0x0
/boot/ - disk check in progress ...

                                                    /boot/ - Volume is
OK
/boot
mounted

/code/ - disk check in
progress ...
/code/ - Volume is
OK
/code
mounted

/ramdrv is default dir
Extracting from /code/images/gguoa.tar to images ...
Extracting from /code/images/gguoa.tar
extract acmeOS_x86.xz
extracting file acmeOS_x86.xz, size 16748820 bytes, 32713 blocks
0x6199b10 (tNetTask): eth0: Link is up (1000Mb/s full duplex)
done extracting: acmeOS_x86.xz
extract pubkey.pem
extracting file pubkey.pem, size 451 bytes, 1 blocks
done extracting: pubkey.pem
extract cert.pem
extracting file cert.pem, size 1168 bytes, 3 blocks
done extracting: cert.pem
end of tape encountered, read until eof...
tarRdBlks: tape block not multiple of 512
done.
Loading BCM5823/BCM5862 driver...
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.
```

```
-----
SSM (Security Service Module) present.
Loading Running Configuration Cache from /code/gzConfig/dataDoc.gz ....
Loading Configuration Cache from /code/gzConfig/dataDoc.gz ....
done
Config data loaded from flash...
Currently licensed features:
    Acme Developer License!,
    32000 sessions,
    SIP,
    MGCP,
    H323,
    IWF,
    QOS,
    ACP,
    Routing,
    Load Balancing,
    Accounting,
    High Availability,
    PAC,
    LI,
    External BW Mgmt,
    TLS,
    Software TLS,
    External CLF Mgmt,
    External Policy Services,
    ENUM,
    H248,
    H248 SCF,
    H248 BGF,
    NSEP RPH,
    LI Debug,
    Session Replication for Recording,
    Transcode Codec AMR,
    Transcode Codec EVRC,
    DoS,
    IKE,
    IPv4-v6 Interworking,
    RTSP,
    IDS,
    Transcode Codec EVRCB,
    FIPS 140-2 level-2*,
    Software PCOM,
    Security Gateway,
    SIP Authorization/Authentication,
    Database Registrar (0 contacts),
    IDS Advanced,
    SLB (20000 endpoints),
    Allow Unsigned SPL files,
    Session Recording,
    Policy Director,
    Transcode Codec AMR-WB,
    CX

Starting task checker...
Starting ACME Net-Net 4500 ECX6.4.1 GA (WS Build 7)
Build Date=03/06/15
Build View=/home/gguo/cc/gguo_BARTFIPS
User=gguo@acme144
Starting tBrokerd...
Starting display manager...
host access bandwidth 10000000 bytes/sec, cpu_max_bw_i 40, cpu_max_bw_f 983
host access max untrusted bandwidth 10000000 bytes/second m 17, e 7
```

Installing a FIPS License and Upgrading a FIPS System

```
host access max untrusted bandwidth ut_pipemticke 9
host access min untrusted bandwidth 3000000 bytes/second, m 17, e 11
APP pipe max/min bandwidth 10000000/10000000 bytes/second
ARP bandwidth is configured for 32000 bytes/second
FRAGMENT bandwidth is configured for 0 bytes/second
IPV6 Support is enabled...
Starting nPsoft...
IDT CAM detected
Phy Card Slot has a QUAD Gigabit Phy Card w/QOS and SECURITY installed
adding ctrl pipe min bandwidth:25000 bytes/sec (max:e=7, m=17; min:e=4,
m=20) adding ARP pipe with bandwidth 32000 bytes/sec (mticke=14,
max:e=4, m=0; min:e=5, m=1)

LOADING IPv6 MICROCODE...
nP3700 Load Boot Response: 0x1234

nP3700 Load Runtime Response: 0xabcd

Setting up ARP table:
-----
Database ID:      3
Num entries:     16384
Srch start addr: 0x0
Data start addr: 0x0
DB_KEY_LENGTH_EPT: 0x4
DB_DATA_LENGTH_EPT: 0x2
Setting up NAT table:
Num entries:     114688
Srch start addr: 0x20000
Data start addr: 0x20000
DB_KEY_LENGTH_NAT: 0x4
DB_DATA_LENGTH_NAT: 0x8
idt_sram_init complete
QoS Doop revision is 0x10103
Adding wancom routes...
Downloading IPSEC firmware for eth0/eth1... done.
Downloading IPSEC firmware for eth2... done.
Starting xntpd...
Starting tBerpd...
berpd: redundancy is disabled
Adding HIP routes...
Set V6 default gateway to
Starting tCliWorker...
Starting tLemd...
Starting tCollect...
Starting tFsWorker...
Starting tAtcpd...
Starting tAsctpd...
Starting tAtcpApp...
Starting tLiTcp...
Starting tMbcd...
Starting tCommMonitord...
Starting tLid...
Starting tAlgd...
Starting tRadd...
Starting tEbmd...
Starting tSipd...
Starting tLrtWorker...
Starting tLrtd...
Starting tH323d...
Starting tH248d...
Starting tBgfd...
Starting tIPTd...
```

```
FIPS_RSA_Signature_Verify: PASSED!!!

master secret result:
2f6962dfbc744c4b2138bb6b3d33054c5ecc14f24851d9896395a44ab3964efc2090c5bf51a0
891209f46c1e1e998f62

key block result:
3088825988e77fce68d19f756e18e43eb7fe672433504feaf99b3c503d9091b164f166db301d
70c9fc0870b4a94563907bee1a61fb786cb717576890bcc51cb9ead97e01d0a2fea99c953377
b195205ff07b369589178796edc963fd80fdbe518a2fc1c35c18ae8d

Starting
tHifnCheck...

Starting
tCertd...

Starting
tSecured...

*****
*   System is in FIPS 140-2 level-2 compatible mode.   *
*   FIPS: All Power on self test completed successfully. *
*****

Password:
```

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 3820/4500. This chapter assumes that the operator 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 3820/4500:

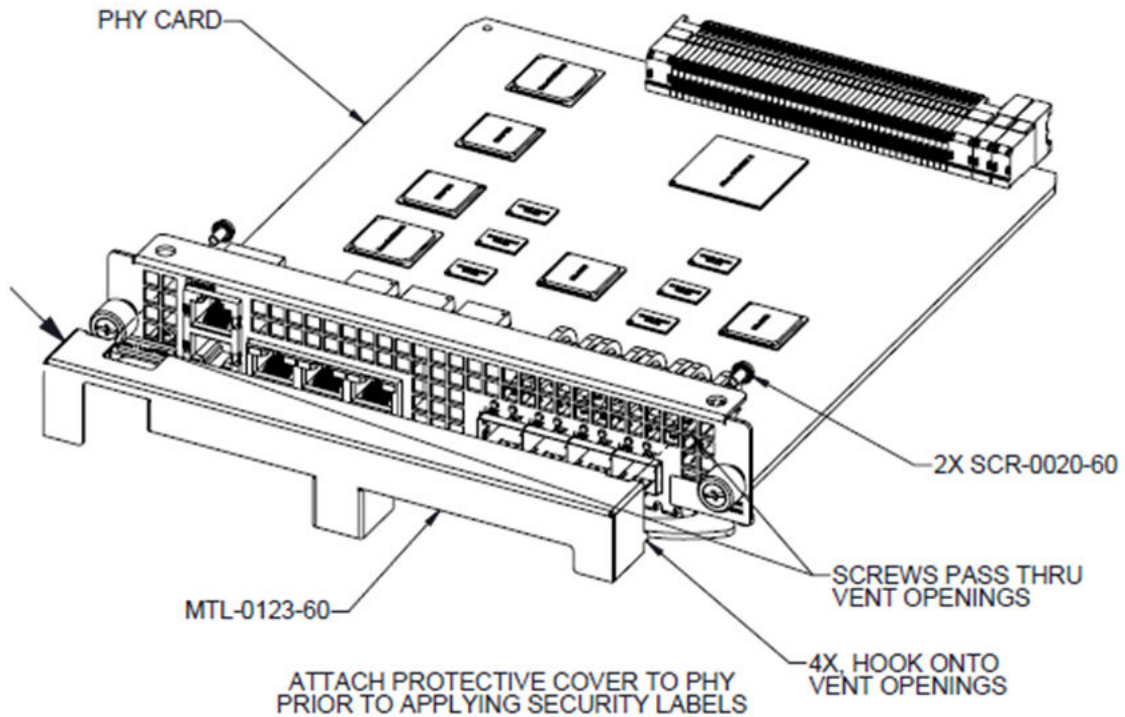
- Physical access to the Acme Packet 3820/4500
- (1x) Security Cover - MTL-0123-60
- (2x) Screw - SCR-0020-60
- (5x) Security Labels- LBL-0140-60
- Supplies to clean adhesive from the bezel after existing label removal

Attaching the Acme Packet 3820/4500 Security Cover

Parts required:

- (1x) Security Cover - MTL-0123-60
 - (2x) Screw - SCR-0020-60
1. Remove top cover.
 2. Attach security cover to PHY card using supplied screws.

FIPS Security Label and Security Cover Assembly Procedure



3. Install the PHY card assembly.

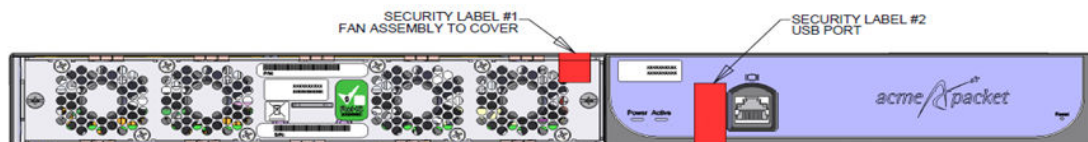


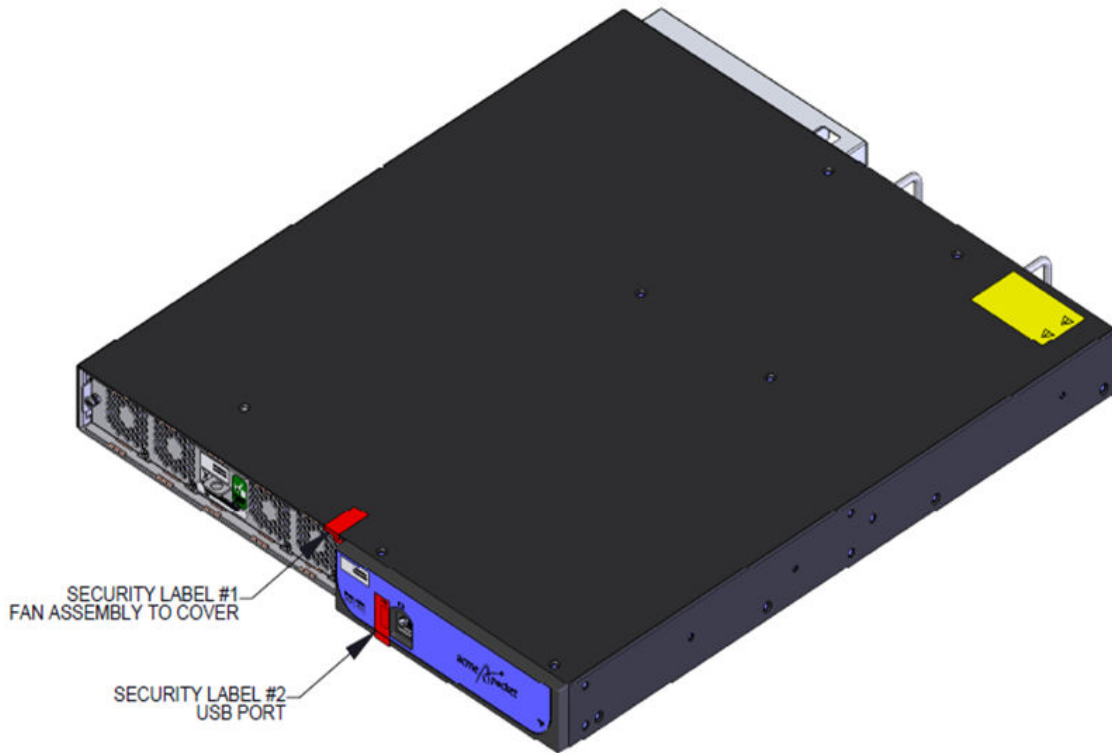
Applying Security Labels to the Acme Packet 3820/4500

Parts required:

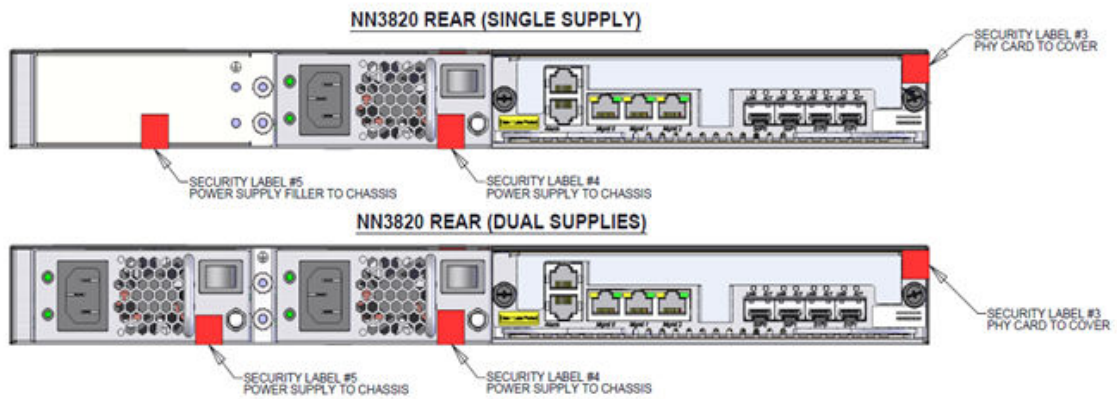
- (5x) Security Label - LBL-0140-60

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

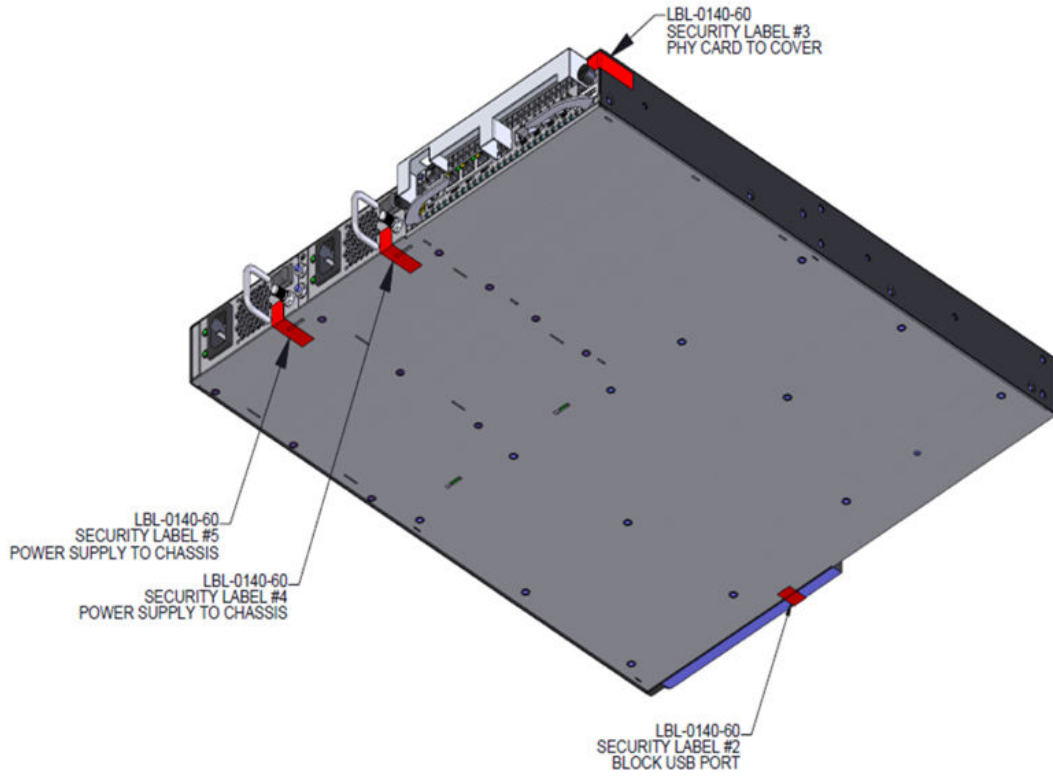




2. Apply label #3, #4, and #5, as shown in diagrams below.



FIPS Security Label and Security Cover Assembly Procedure



Additional Release Features

This chapter presents additions to E-Cx6.4.1M1 which are not part of the Federal Information Processing Standards (FIPS) standards.

SRTP Re-keying

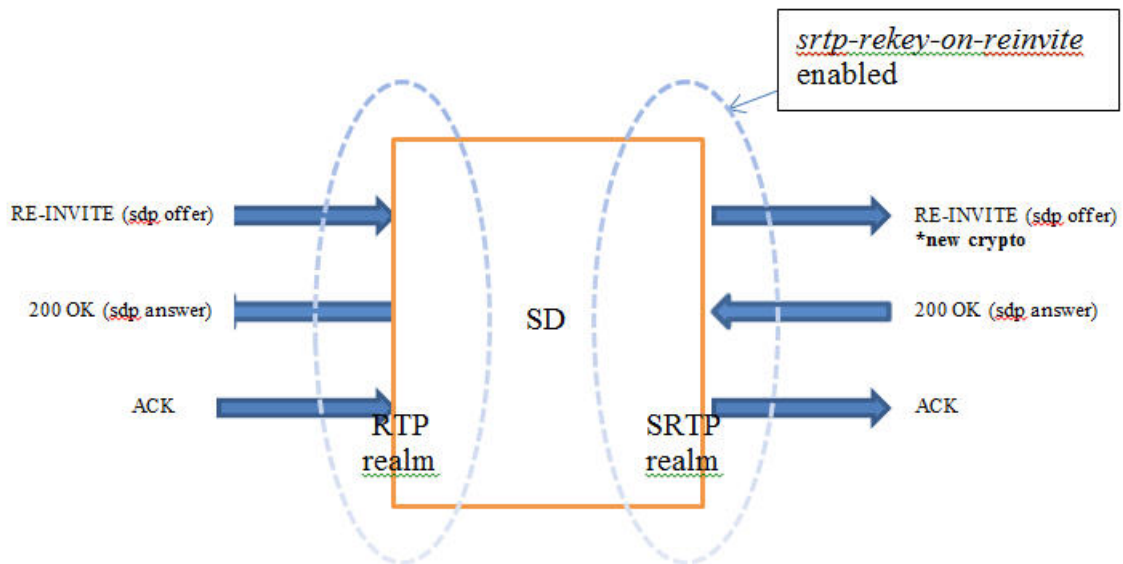
Initialization of SRTP re-keying is supported by the Oracle Enterprise Session Border Controller.

The Oracle Enterprise Session Border Controller can generate a new outbound crypto attribute in the SDP offer in a SIP re-INVITE when the **srtp-rekey-on-reinvite** parameter is set to **enabled**. The system generates the attribute regardless of the state of the flow, active or not.

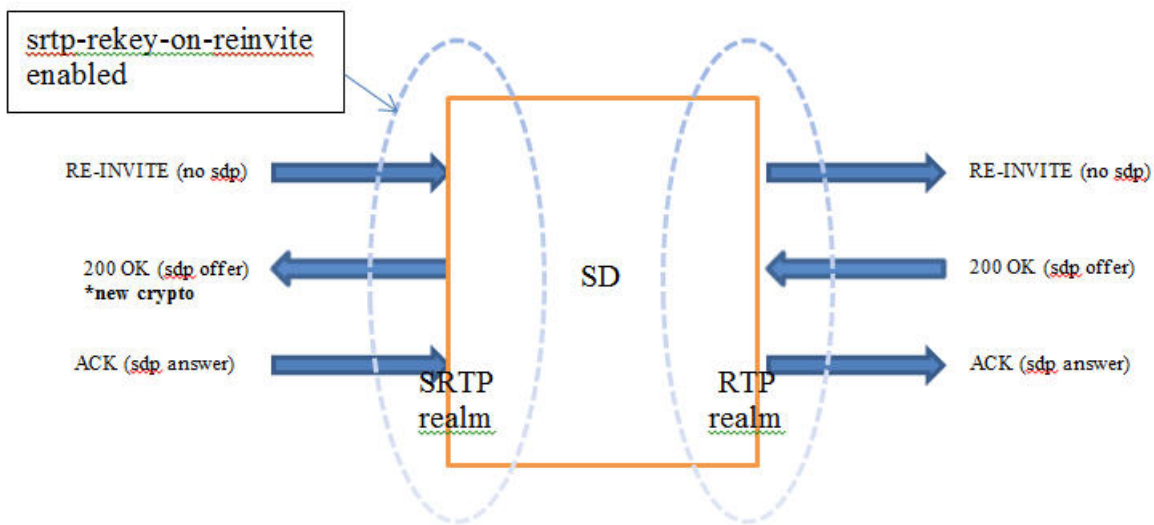
This capability is important for some clients that reside on the SRTP side in a single SRTP termination mode configuration. Any media changes that happen in the RTP side are hidden by the Oracle Enterprise Session Border Controller. This concealment may cause issues in some configurations, where media servers are involved. When the media changes from media server to called phone, the SRTP endpoint is not aware the media source changed because the SDP offer from the Oracle Enterprise Session Border Controller is the same as original invite. The result is that some devices drop packets because of Synchronization Source Identifier (SSRC) values mismatch, unexpected jumps in sequence number, sequence number reversions back to 1 triggering replay attack defense, and so forth. In certain environment it has been found that re-keying on every re-invite eliminates all these issues especially in customer setups that use Microsoft Lync products.

The processing of standard RE-INVITES (those containing an SDP offer) and offerless RE-INVITES is shown below.

With SDP:



No SDP:



If the re-invite message is a refresh and `srtp-rekey-on-reinvite` is enabled, the outbound crypto will change but the SDP version will not be incremented on the outgoing invite. If this scenario causes incompatibility issues with customer equipment then add the `unique-sdp-id` option to `media-manager->option` configuration so the Oracle Enterprise Session Border Controller increments the SDP version in the outgoing invite.

SRTP Re-keying Configuration

Configure `srtp-rekey-on-reinvite` to enable the negotiation and generation of new SRTP keys upon the receipt of a SIP RE-INVITE message that contains SDP.

Confirm that an `sdes-profile` exists.

In the following procedure, change the default state to enabled.

1. Access the `sdes-profile` configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# media-security
ACMEPACKET(media-security)# sdes-profile
ACMEPACKET(sdes-profile)#
```

2. Type **select** to choose and configure an existing object.

```
ACMEPACKET(sdes-profile)# select
<name>:
1:  name=sdesprofile01

selection: 1
ACMEPACKET(sdes-profile)#
```

3. **srtp-rekey-on-reinvite**—Set this parameter to **enabled** for re-keying upon the receipt of a SIP reINVITE that contains SDP.
4. Type **done** to save your configuration.

