

Crypto Engine Failure on Cisco ASR 1006 or ASR 1013 Router with a Single ESP

TAC

Document ID: 116878

Contributed by Michal Stanczyk, Cisco TAC Engineer.
Dec 18, 2013

Contents

Introduction

Prerequisites

- Requirements

- Components Used

Background Information

Problem

Solution

Introduction

This document describes how to identify and resolve a problem with IPSec operations that might be observed on the Cisco Aggregation Services Router (ASR) 1006 or ASR 1013 platforms. This can occur when there is only one embedded services processor (ESP) installed and it is seated in slot F1.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco 1000 Series ASR 1006 or the Cisco ASR 1013.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

The Cisco 1000 Series ASR portfolio includes two models (ASR 1006 and ASR 1013). Each model features redundant route processors (RP) and ESPs. In general, a single ESP is installed in the Cisco ASR 1006 and Cisco ASR 1013 in either slot F0 or F1, with no restrictions. The same premise applies to RP slots.

The slot numbering is described in the Cisco ASR 1006 and Cisco ASR 1013 installation guides.

Problem

The crypto engine fails to initialize after a device power-cycle. When ESP is seated in slot F1 and there is no

running ESP in slot F0. The problem is seen on the following products:

Hardware:

- Dual-ESP Cisco ASR 1000 models: ASR1006 or ASR1013.

Software:

- For Cisco IOS® XE Release 3.7.xS train: Version 3.7.3S or earlier; 3.7.4S and later is not affected.
- For later Cisco IOS XE trains: Version 3.9.1S or earlier; 3.9.2S and later is not affected.

Symptoms of the problem include:

- The logs display this error message:

```
ISAKMP: Unable to find a crypto engine to allocate IKE SA
```

- Output from the *show crypto eli* and *show crypto ace slot <number> status* commands indicates that the crypto engine is inactive:

```
ASR1006#show crypto eli
Hardware Encryption: INACTIVE
Number of hardware crypto engines = 1

CryptoEngine IOSXE-ESP(14) details: state = Initializing
Capability      : DES, 3DES, AES, GCM, GMAC, RSA, IPv6, GDOI, FAILCLOSE
IKE-Session    :      0 active, 12287 max, 0 failed
DH              :      0 active, 12287 max, 0 failed
IPSec-Session  :      0 active, 32766 max, 0 failed
```

```
ASR1006#show crypto ace slot 14 stat / inc status
```

```
ACE status: OFFLINE
```

This problem might occur in these scenarios:

- A single ESP is inserted into slot F1 and there is no ESP in slot F0. The router has been power-cycled.
- There are two ESPs, but due to an issue, the ESP in F0 failed and left a single ESP in F1. The router has been power-cycled.

Enter the *show platform* command in order to verify the availability of the ESP.

Example:

```
ASR1006#show platform
Chassis type: ASR1006

Slot  Type                State          Insert time (ago)
0      ASR1000-SIP10           ok             00:32:04
0/0    SPA-8X1GE-V2           ok             00:29:46
1      ASR1000-SIP10           ok             00:32:04
1/0    SPA-8X1GE-V2           ok             00:29:46
R1     ASR1000-RP1             ok, active    00:32:04
F1     ASR1000-ESP10          ok, active    00:32:04
P0     ASR1006-PWR-AC         ok             00:31:12
P1     ASR1006-PWR-AC         ok             00:31:11
```

Solution

The problem is due to Cisco bug ID CSCue45131, "sVTI tunnel I/F does not come up after router reboot."
The bug is fixed in Cisco IOS XE Releases 3.7.4S and 3.9.2S.

The problem does not exist in the Cisco IOS XE Release 3.10.0S train.

The best solution is to make sure that the currently functioning ESP is installed in slot F0. If that solution is not possible, other workarounds that can be applied remotely are:

- Reload the ESP: # *hw module slot F1 reload*

or

- Reload the router

Updated: Dec 18, 2013

Document ID: 116878
