Falha do mecanismo de criptografia no roteador Cisco ASR 1006 ou ASR 1013 com um único ESP

Contents

Introduction

Este documento descreve como identificar e resolver um problema com operações de IPSec que pode ser observado nas plataformas Cisco Aggregation Services Router (ASR) 1006 ou ASR 1013. Isso pode ocorrer quando há apenas um ESP (Integrated Services Processor, processador de serviços integrados) instalado e ele está encaixado no slot F1.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco 1000 Series ASR 1006 ou no 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.

Informações de Apoio

O portfólio Cisco 1000 Series ASR inclui dois modelos (ASR 1006 e ASR 1013). Cada modelo apresenta processadores de rota redundantes (RP) e ESPs. Em geral, um único ESP é instalado no Cisco ASR 1006 e no Cisco ASR 1013 no slot F0 ou F1, sem restrições. A mesma premissa se aplica aos slots RP.

A numeração de slots é descrita nos guias de instalação do Cisco ASR 1006 e do Cisco ASR 1013.

Problema

O mecanismo de criptografia não é inicializado após um ciclo de energia do dispositivo. Quando o ESP está sentado no slot F1 e não há nenhum ESP em execução no slot F0. O problema ocorre nos seguintes produtos:

Hardware:

- Modelos Cisco ASR 1000 de ESP duplo: ASR1006 ou ASR1013.

Software:

- Para o treinamento do Cisco IOS® XE versão 3.7.xS: Versão 3.7.3S ou anterior; 3.7.4S e posterior não é afetada.
- Para trilhas posteriores do Cisco IOS XE: Versão 3.9.1S ou anterior; 3.9.2S e posterior não é afetada.

Os sintomas do problema incluem:

- Os registros exibem esta mensagem de erro:
  ```
  ISAKMP: Unable to find a crypto engine to allocate IKE SA
  ```
- A saída dos comandos **show crypto eli** e **show crypto ace slot <*number*> status** indica que o mecanismo de criptografia está inativo:
  ```
  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
  ```

Esse problema pode ocorrer nestes cenários:

- Um único ESP é inserido no slot F1 e não há ESP no slot F0. O roteador foi desligado e ligado novamente.
- Há dois ESPs, mas devido a um problema, o ESP em F0 falhou e deixou um único ESP em F1. O roteador foi desligado e ligado novamente.

Insira o comando **show platform** para verificar a disponibilidade do ESP.

Exemplo:

```
    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
```

Solução

O problema é devido à ID de bug da Cisco CSCue45131, "sVTI tunnel I/F does not be up after router reboot" (A I/F do túnel sVTI não aparece após a reinicialização do roteador).
O bug é corrigido nas versões 3.7.4S e 3.9.2S do Cisco IOS XE.

O problema não existe na versão 3.10.0S do Cisco IOS XE.

A melhor solução é certificar-se de que o ESP atualmente em funcionamento esteja instalado no slot F0. Se essa solução não for possível, outras soluções alternativas que podem ser aplicadas remotamente são:

- Recarregue o ESP: **# hw module slot F1 reload**

or

- Recarregue o roteador