# Entender as diferenças de recuperação SPI de túneis SD-WAN e tradicionais

## Contents



## Introdução

Este documento descreve como recuperar túneis SD-WAN e de terceiros do erro %RECVD_PKT_INV_SPI.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede de longa distância definida pelo software Cisco Catalyst (SD-WAN)
- Segurança de Protocolo Internet (IPSec - Internet Protocol Security).
- Detecção de encaminhamento bidirecional (BFD).

### Componentes Utilizados

As informações neste documento são baseadas em:

- Cisco IOS® XE Catalyst SD-WAN Edges

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Problema

O conceito de uma Associação de Segurança (SA) é fundamental para o IPSec. Um SA é um relacionamento entre dois endpoints que descreve como os endpoints usam serviços de segurança para se comunicar com segurança.

Um Security Parameter Index (SPI) é um número de 32 bits que é escolhido para identificar exclusivamente um SA específico para qualquer dispositivo conectado usando IPSec.

Um dos problemas mais comuns de IPsec é que as SAs podem ficar fora de sincronia devido a um valor de SPI inválido, o que consequentemente causa um status de Túnel IPSEC inativo quando os pacotes são descartados pelo peer e mensagens de syslog são recebidas no Roteador.

Túneis de terceiros:

```
Jan  8 15:00:23.723 EDT: : %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
```

Para túneis SD-WAN:

```
Jan 10 12:18:43.404 EDT: : %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has invalid spi for
```

Esses registros são acompanhados por quedas no Quantum Flow Processor (QFP) que pertence ao Forwarding Processor (FP).

<#root>

```
Router#
show platform hardware qfp active feature ipsec datapath drops

------------------------------------------------------------------------
Drop Type Name                                                  Packets
------------------------------------------------------------------------
1 IN_V4_PKT_HIT_INVALID_SA                                            1
4 IN_US_V4_PKT_SA_NOT_FOUND_SPI 9393888 <-- sub code error

19 IN_OCT_ANTI_REPLAY_FAIL                                          342
```

# Solução

## Recuperação para túneis IPSec tradicionais

Para recuperar os túneis IPSec tradicionais, é necessário forçar manualmente a renegociação da relação dos valores de SAs atuais; isso é feito limpando as SAs IPSec com o comando do modo EXEC:

```
<#root>

Router#

clear crypto sa peer 10.20.20.1
```

## Recuperação para túneis SD-WAN - Cenário 1

O comando EXEC clear crypto sa peer funciona apenas para túneis IPSec tradicionais devido à existência de Internet Key Exchange (IKE), que negocia automaticamente a associação e gera um novo valor SPI. No entanto, não é possível usar esse comando em um túnel SD-WAN. A razão para isso é que em túneis SD-WAN, o IKE não é usado.

Por causa disso, um comando homólogo para túneis SD-WAN é usado:

```
<#root>

Router#

request platform software sdwan security ipsec-rekey
```

O comando request platform software sdwan security ipsec-rekey gera uma nova chave imediatamente e o túnel é ativado. Da maneira oposta, o comando não afeta um túnel IPSec tradicional se ele existir.

---

Observação: o software da plataforma de solicitação sdwan security ipsec-rekey esse comando tem efeito em todos os túneis SD-WAN existentes opostos ao clear crypto sa peer que tem efeito somente no SA especificado.

---

## Recuperação para túneis SD-WAN - Cenário 2

Se, por engano, o comando clear crypto sa peer for usado para excluir um dos SAs de túneis SD-WAN, a exclusão ocorrerá com êxito; no entanto, um novo valor SPI não será gerado novamente, porque em um túnel SD-WAN, o OMP é o que dispara essa ação, não IKE. Uma vez nesse status, mesmo se o comando request platforms software sdwan security ipsec-rekey for emitido após o clear crypto sa peer, o túnel não será ativado. Os encapsulamentos e desencapsulamentos da AS permanecem em zero, consequentemente a sessão BFD permanece em um estado inativo.

```
Router#clear crypto sa peer 10.20.20.1
Router#show crypto ipsec sa peer 10.20.20.1
interface: Tunnel10001
Crypto map tag: Tunnel10001-vesen-head-0, local addr 10.10.10.1

protected vrf: (none)
local ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/12346)
remote ident (addr/mask/prot/port): (10.20.20.1/255.255.255.255/0/12366)
current_peer 10.20.20.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0
```

A única opção de recuperação após a exclusão do SA é com QUALQUER UM DESTES três comandos EXEC:

<#root>

```
Router#
```

**clear sdwan omp all**

O comando clear sdwan omp all sincroniza todas as sessões de BFD presentes no dispositivo.

<#root>

```
Router#
```

**request platforms software sdwan port_hop**

O comando clear sdwan control connections faz com que o TLOC use o próximo número de porta disponível na cor local especificada, o que causa um flap não apenas em todas as sessões BFD dessa cor, mas também nas conexões de controle dessa cor.

<#root>

```
Router#
```

**clear sdwan control connections**

O último comando também auxilia na recuperação, no entanto, o impacto é em todas as conexões de controle e sessões BFD presentes no dispositivo.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.