Erros do IPsec %RECVD_PKT_INV_SPI e informação dos recursos de recuperação do SPI inválido

Índice

[Introdução](#)
[Problema](#)
[Solução](#)
[Recuperação do SPI inválido](#)
[Pesquise defeitos Mensagens de Erro intermitentes do SPI inválido](#)

Introdução

Este documento descreve a edição do IPsec quando as associações de segurança (SA) se tornam fora da sincronização entre os dispositivos de peer.

Problema

Uma da maioria de edições do IPSec comum é que os SA podem se tornar fora da sincronização entre os dispositivos de peer. Em consequência, um dispositivo de criptografia cifra o tráfego com SA que seu par não conhece aproximadamente. Estes pacotes são deixados cair pelo par e esta mensagem aparece no Syslog:

```
Sep  2 13:27:57.707: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
has invalid spi for destaddr=20.1.1.2, prot=50, spi=0xB761863E(3076621886),
srcaddr=10.1.1.1
```

> Nota: Com NAT-T, as mensagens **RECVD_PKT_INV_SPI** não foram relatadas corretamente até que a identificação de bug Cisco CSCsq59183 esteve fixa. (O IPsec não relata mensagens **RECVD_PKT_INV_SPI** com NAT-T.)

> Nota: Na plataforma do Roteadores dos serviços da agregação de Cisco (ASR), as mensagens **%CRYPTO-4-RECVD_PKT_INV_SPI** não foram executadas até a liberação 2.3.2 do ® XE do Cisco IOS (12.2(33)XNC2). Igualmente note com a plataforma ASR, essa esta gota particular é registrado sob ambos o contador de queda global do processador do fluxo do quantum (QFP) assim como no contador de queda da característica do IPsec, segundo as indicações dos exemplos seguintes.

```
Router# show platform hardware qfp active statistics drop | inc Ipsec
IpsecDenyDrop 0 0
IpsecIkeIndicate 0 0
IpsecInput 0 0 <======
IpsecInvalidSa 0 0
IpsecOutput 0 0
IpsecTailDrop 0 0
IpsecTedIndicate 0 0Router# show platform hardware qfp active feature ipsec datapath drops all |
in SPI
```

```
4 IN_US_V4_PKT_SA_NOT_FOUND_SPI 64574 <======
7 IN_TRANS_V4_IPSEC_PKT_NOT_FOUND_SPI 0
12 IN_US_V6_PKT_SA_NOT_FOUND_SPI 0
```

Éimportante notar que este mensagem particular é limite de taxa no Cisco IOS a uma taxa de um pelo minuto para os motivos de segurança óbvios. Se esta mensagem para um fluxo particular (SRC, DST, ou SPI) aparece somente uma vez no log, a seguir pôde somente ser uma condição transitória que estasse presente ao mesmo tempo que o IPsec rekey onde um par pôde começar usar o SA novo quando o dispositivo de peer não for bastante pronto para uso o mesmo SA. Este não é normalmente um problema, porque é somente provisório e afetaria somente alguns pacotes. Contudo, houve os erros onde este pode ser um problema.

> Dica: Para exemplos, veja por favor a identificação de bug Cisco CSCsl68327 (a perda de pacotes durante rekey), a identificação de bug Cisco CSCtr14840 (ASR: as quedas de pacote de informação durante a fase 2 rekey sob certas condições), ou a identificação de bug Cisco CSCty30063 (o ASR use o SPI novo antes que revestimentos QM).

Alternativamente, há um problema se mais de um exemplo da mesma mensagem é observado para relatar o mesmo SPI para o mesmo fluxo, tal como estas mensagens:

```
Router# show platform hardware qfp active feature ipsec datapath drops all | in SPI
4 IN_US_V4_PKT_SA_NOT_FOUND_SPI 64574 <======
7 IN_TRANS_V4_IPSEC_PKT_NOT_FOUND_SPI 0
12 IN_US_V6_PKT_SA_NOT_FOUND_SPI 0
```

Esta é uma indicação que o tráfego preto-está furado e não pôde recuperar até que os SA expirem no dispositivo de envio ou até que o Dead Peer Detection (DPD) esteja ativado.

Solução

Esta seção fornece a informação que você pode usar a fim resolver a edição que é descrita na seção anterior.

Recuperação do SPI inválido

A fim resolver esta edição, Cisco recomenda que você permite os recursos de recuperação do SPI inválido. Por exemplo, incorpore o comando **cripto da inválido-SPI-recuperação do isakmp**. Estão aqui algumas observações importantes que descrevem o uso deste comando:

- Primeiramente, a recuperação do SPI inválido serve somente como um mecanismo de recuperação quando os SA são fora da sincronização. Ajuda a recuperar desta circunstância, mas não endereça a edição da raiz que fez com que os SA se tornassem fora da sincronização no primeiro lugar. A fim compreender melhor a causa de raiz, você deve permitir o ISAKMP e o IPsec debuga em ambos os pontos finais do túnel. Se o problema ocorre frequentemente, a seguir obtenha debuga e tentam endereçar a causa de raiz (e para mascarar não apenas o problema).

- Há uma concepção errada comum sobre a finalidade e a funcionalidade do comando **cripto da inválido-SPI-recuperação do isakmp**. Mesmo sem este comando, o Cisco IOS já executa um tipo de funcionalidade da recuperação do SPI inválido quando envia uma notificação da SUPRESSÃO ao par de emissão para o SA que está recebido se já tem IKE SA com esse par. Além disso, isto ocorre apesar de se o comando **cripto da inválido-SPI-recuperação do**

isakmp está ativado.

- O comando **cripto da inválido-SPI-recuperação do isakmp** tenta endereçar a circunstância onde um roteador recebe o tráfego de IPSec com SPI inválido, e não tem IKE SA com esse par. Neste caso, tenta estabelecer uma sessão de IKE nova com o par e envia uma notificação da SUPRESSÃO sobre IKE recém-criado SA. Contudo, este comando não funciona para todas as configurações de criptografia. As únicas configurações que este comando trabalha para são os mapas estáticos de criptografia onde o par é definido explicitamente e os peer estáticos que são derivados dos mapas cript. instantiated, tais como VTI. Está aqui um sumário das configurações de criptografia de uso geral e se a recuperação do SPI inválido trabalha com essa configuração:

Configuração de criptografia	Recuperação do SPI inválido?
Mapa estático de criptografia	Sim
Mapa cripto dinâmico	Não
P2P GRE com TP	Sim
mGRE TP que se usa com o mapeamento NHRP estático	Sim
mGRE TP que se usa com o mapeamento NHRP dinâmico	Não
sVTI	Sim
Cliente ezvpn	N/A

Pesquise defeitos Mensagens de Erro intermitentes do SPI inválido

Muitas vezes o Mensagem de Erro do SPI inválido ocorre intermitentemente. Isto faz difícil pesquisar defeitos, enquanto se torna muito duro recolher o relevante debuga. Os scripts encaixados do gerente do evento (EEM) podem ser muito úteis neste caso.

> Nota: Para mais detalhes, refira os scripts EEM usados para pesquisar defeitos as aletas do túnel causadas pelo documento Cisco inválido dos deslocamentos predeterminados do parâmetro de segurança.