Verificar Erros %RECVD_PKT_INV_SPI de IPsec e Informações Inválidas do Recurso de Recuperação de SPI

Contents

Introduction

Este documento descreve o problema do IPsec quando as associações de segurança (SAs) ficam fora de sincronia entre os dispositivos pares.

Problema

Um dos problemas mais comuns de IPsec é que as SAs podem ficar fora de sincronia entre os dispositivos pares. Como resultado, um dispositivo criptografado criptografa o tráfego com SAs que seu par não conhece. Esses pacotes são descartados pelo peer 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=10.10.1.2, prot=50, spi=0xB761863E(3076621886),
srcaddr=10.1.1.1
```

> **Note**: Com o NAT-T, as mensagens **RECEVD_PKT_INV_SPI** não foram relatadas corretamente até que a ID de bug da Cisco CSCsq59183 fosse corrigida. (O IPsec não relata **mensagens RECVD_PKT_INV_SPI** com NAT-T.)

> **Note**: Na plataforma Cisco Aggregation Services Routers (ASR), as mensagens **%CRYPTO-4-RECVD_PKT_INV_SPI** não foram implementadas até o Cisco IOS® XE Release 2.3.2 (12.2(33)XNC2). Observe também com a plataforma ASR, que essa queda específica é registrada no contador de queda do QFP (Quantum Flow Processor) global, bem como no contador de queda do recurso IPsec, como mostrado nos próximos exemplos.

```
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 0

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
```

Éimportante observar que essa mensagem específica tem taxa limitada no Cisco IOS a uma taxa de um por minuto por motivos óbvios de segurança. Se essa mensagem para um fluxo específico (SRC, DST ou SPI) aparecer apenas uma vez no log, ela só poderá ser uma condição transitória presente ao mesmo tempo que a rechave IPsec, em que um peer pode começar a usar o novo SA enquanto o dispositivo peer não estiver totalmente pronto para usar o mesmo SA. Normalmente, isso não é um problema, pois é apenas temporário e afetaria apenas alguns pacotes. No entanto, houve bugs em que isso pode ser um problema.

> **Tip**: Para obter exemplos, consulte o bug da Cisco ID CSCsl68327 (Perda de pacotes durante o rechaveamento), bug da Cisco ID CSCtr14840 (ASR: o pacote cai durante a rechaveamento da fase 2 sob certas condições) ou o bug da Cisco ID CSCty3063 (o ASR usa o novo SPI antes que o QM termine).

Como alternativa, há um problema se mais de uma instância da mesma mensagem for observada para relatar o mesmo SPI para o mesmo fluxo, como estas mensagens:

```
Sep  2 13:36:47.287: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
has invalid spi for destaddr=10.10.1.2, prot=50, spi=0x1DB73BBB(498547643),
srcaddr=10.1.1.1 Sep 2 13:37:48.039: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet
has invalid spi for destaddr=10.10.1.2, prot=50, spi=0x1DB73BBB(498547643),
srcaddr=10.1.1.1
```

Essa é uma indicação de que o tráfego está em buraco negro e não pode ser recuperado até que as SAs expirem no dispositivo que envia ou até que a detecção de ponto morto (DPD) seja ativada.

Solução

Esta seção fornece informações que você pode usar para resolver o problema descrito na seção anterior.

Recuperação SPI inválida

Para resolver esse problema, a Cisco recomenda que você habilite o recurso de recuperação SPI inválido. Por exemplo, insira o comando **crypto isakmp invalid-spi-recovery**. Aqui estão algumas notas importantes que descrevem o uso desse comando:

- Primeiro, a recuperação SPI inválida serve apenas como um mecanismo de recuperação quando as SAs estão fora de sincronia. Ele ajuda a recuperar-se dessa condição, mas não aborda o problema raiz que fez com que as SAs ficassem fora de sincronia em primeiro lugar. Para entender melhor a causa raiz, você deve habilitar as depurações ISAKMP e IPsec em ambos os pontos finais do túnel. Se o problema ocorrer com frequência, obtenha as depurações e tente abordar a causa raiz (e não apenas mascarar o problema).

- Há um equívoco comum sobre a finalidade e a funcionalidade do comando **crypto isakmp invalid-spi-recovery**. Mesmo sem esse comando, o Cisco IOS já executa um tipo de funcionalidade de recuperação SPI inválida quando envia uma notificação DELETE ao peer emissor para o SA que é recebido se já tiver um SA IKE com esse peer. Novamente, isso ocorre independentemente do comando **crypto isakmp invalid-spi-recovery** estar ativado.

- O comando **crypto isakmp invalid-spi-recovery** tenta endereçar a condição em que um roteador recebe o tráfego de IPsec com SPI inválido e não tem um SA de IKE com esse peer. Nesse caso, ele tenta estabelecer uma nova sessão IKE com o peer e envia uma notificação DELETE sobre a SA IKE recém-criada. No entanto, esse comando não funciona para todas as configurações de criptografia. As únicas configurações para as quais esse comando funciona são mapas de criptografia estáticos, onde o peer é explicitamente definido e pares estáticos que são derivados de mapas de criptografia instanciados, como VTI. Aqui está um resumo das configurações de criptografia comumente usadas e se a recuperação SPI inválida funciona com essa configuração:

Configuração criptografada	Recuperação SPI inválida?
Mapa de criptografia estático	Yes
Mapa de criptografia dinâmico	No
GRE P2P com proteção de túnel	Yes
Proteção de túnel mGRE que usa c/ mapeamento NHRP estático	Yes
Proteção de túnel mGRE que usa c/ mapeamento NHRP dinâmico	No
sVTI	Yes
cliente EzVPN	N/A

Solucionar problemas de mensagens de erro SPI inválidas intermitentes

Muitas vezes a mensagem de erro SPI inválida ocorre intermitentemente. Isso dificulta a identificação e solução de problemas, pois torna-se muito difícil coletar as depurações relevantes. Os scripts do Embedded Event Manager (EEM) podem ser muito úteis nesse caso.

> **Note**: Para obter mais detalhes, consulte o documento EEM Scripts used to Troubleshoot Tunnel Flaps Caused by Invalid Security Parameter Indexes Cisco.

Erros conhecidos

Esta lista mostra bugs que podem fazer com que as SAs IPsec fiquem fora de sincronia ou relacionados à recuperação de SPI inválido:

- ID de bug Cisco CSCvn31824 O ISAKMP do Cisco IOS-XE exclui o novo SPI se o pacote RX novo SPI for concluído antes da instalação
- ID de bug Cisco CSCvd40554 IKEv2: O Cisco IOS não pode analisar a notificação INV_SPI com tamanho 0 de SPI - envia INVALID_SYNTAX
- O bug da Cisco ID CSCvp16730 Pacotes ESP de entrada com valor SPI iniciado com 0xFF são descartados devido a erro de SPI inválido

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.