IPSec %RECVD_PKT_INV_SPI エラーと無効な SPI 回復機能に関する情報

目次

概要

このドキュメントでは、ピア デバイス間でセキュリティ アソシエーション（SA）が同期していない状態になる IPSec の問題について説明します。

問題

最も一般的な IPSec の問題の 1 つに、ピア デバイス間で SA が同期していない状態になるというものがあります。 その結果、暗号化デバイスは、ピアが認識しない SA を使用してトラフィックを暗号化します。 ピアはこれらのパケットをドロップし、syslog に次のメッセージが出力されます。

```
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
```

> **注:** NAT-T では、Cisco Bug ID CSCsq59183 が修正されるまでは **RECVD_PKT_INV_SPI** メッセージが正しく報告されません。（IPsec は NAT-T で **RECVD_PKT_INV_SPI** メッセージを報告しません。）

> **注:** シスコ アグリゲーション サービス ルータ（ASR）プラットフォームでは、Cisco IOS® XE リリース 2.3.2 (12.2(33)XNC2) までは **%CRYPTO-4-RECVD_PKT_INV_SPI** メッセージが実装されていませんでした。 また ASR プラットフォームについて、この特定のドロップは、グローバル Quantum Flow Processor（QFP）ドロップ カウンタおよび IPSec 機能ドロップ カウンタの両方に登録されることに注意してください（以降の例を参照）。

```
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
```

明白なセキュリティ上の理由から、Cisco IOS ではこの特定のメッセージの表示が 1 分あたり 1 つに制限されていることにも注意してください。 特定のフロー（SRC、DST、SPI）に関するこのメッセージがログに 1 回だけ出力される場合は、IPSec キー再生成の時点で存在していた一時的な状態（ピア デバイスが新しい SA を使用できる状態ではないときに、ピアがその SA の使用を開始したこと）に過ぎない可能性があります。 これは一時的な状態であり、影響するパケットの数が少ないため、通常は問題ではありません。 ただし、これが問題となる可能性があるバグが存在していました。

> **ヒント**： たとえば、Cisco Bug ID CSCsl68327（キー再生成中のパケット損失）、Cisco Bug ID CSCtr14840（ASR： 特定の状況でフェーズ 2 のキー再生成中にパケットがドロップされる）、または Cisco Bug ID CSCty30063（QM が完了する前に ASR が新しい SPI を使用する）を参照してください。

あるいは、同一メッセージの複数インスタンスから同一フローの同一 SPI が報告されることが見られる場合にも、問題が発生しています。メッセージの例を次に示します。

```
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
```

これは、トラフィックがブラック ホール化し、SA が送信側デバイスで期限切れになったり、デッドピア検出（DPD）がアクティブになったりするまではトラフィックが回復できない可能性があることを示します。

解決策

ここでは、前述のセクションで説明した問題を解決する際に利用できる情報を示します。

無効な SPI のリカバリ

この問題を解決するには、無効な SPI のリカバリ機能をイネーブルにすることが推奨されます。たとえば、**crypto isakmp invalid-spi-recovery** コマンドを入力します。 このコマンドの使用法を説明する重要な注意事項を次に説明します。

- まず、無効な SPI のリカバリは、SA が同期していない場合のリカバリ メカニズムとしてのみ利用できます。 この状態からリカバリする際には役立ちますが、そもそも SA が同期していない状態となった根本的な原因は解決できません。 根本的な原因をより適切に理解するには、トンネルの両端で ISAKMP および IPSec デバッグをイネーブルにする必要があります。問題が頻繁に発生する場合は、デバッグを取得し、（問題を隠すのではなく）根本的な原因を解決してください。

- **crypto isakmp invalid-spi-recovery** コマンドの目的と機能性についてよく誤解される点があります。 このコマンドを使用しない場合でも、Cisco IOS は SA の送信側ピアに DELETE 通知を送信するときに、無効な SPI のリカバリ機能をすでに実行しています。この通知は、そのピアとの IKE SA がすでに確立されている場合に受信されます。 この場合、**crypto isakmp invalid-spi-recovery** コマンドがアクティブであるかどうかに関係なくこれが発生します。

- **crypto isakmp invalid-spi-recovery** コマンドは、ルータが無効な SPI で IPSec トラフィックを受信するが、そのピアとの IKE SA がない状態を解決しようとします。 この場合、ピアとの新しい IKE セッションの確立を試行し、新たに作成された IKE SA を介して DELETE 通知を送信します。 ただし、このコマンドはすべての暗号化設定で機能するわけではありません。 このコマンドが機能する唯一の設定は、ピアが明示的に定義されているスタティック クリプト マップと、VTI などのインスタンス化されたクリプト マップから派生した静的ピアです。 よく使用される暗号化設定と、無効な SPI のリカバリがその設定で機能するかどうかの要約を次に示します。

暗号化設定	**無効な SPI のリカバリ?**
スタティック クリプト マップ	○
ダイナミック クリプト マップ	なし
トンネル 保護の P2P GRE	○
mGRE トンネル 保護静的な NHRPマッピングと使用する	○
mGRE トンネル 保護 ダイナミック NHRPマッピングと使用する	なし
sVTI	○
EzVPN クライアント	N/A

無効な SPI エラー メッセージが断続的に表示される場合のトラブルシューティング

無効な SPI のエラー メッセージが、多数回、断続的に繰り返し表示されます。 そのため、関連するデバッグを収集することが非常に困難であるので、トラブルシューティングが困難になります。 Embedded Event Manager（EEM）スクリプトは、このような場合に非常に役立ちます。

> **注:** 詳細については、シスコのドキュメント『無効なセキュリティ パラメータ インデックスによって発生するトンネル フラップをトラブルシューティングするために使われる EEM スクリプト』を参照してください。