IPSec %RECVD_PKT_INV_SPIエラーおよび無効なSPIリカバリ機能情報の確認

内容

はじめに

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）が同期しなくなった場合の 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、暗号化エンドポイントは、ピアが認識していないSAで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=10.10.1.2, prot=50, spi=0xB761863E(3076621886), srcaddr=10.1.1.1
```

注：Cisco IOS® XEルーティングプラットフォーム(Ciscoアグリゲーションサービスルータ(ASR)、Cisco Catalyst 8000シリーズルータなど)では、この特定のドロップは、次の例に示すように、グローバルQuantum Flow Processor(QFP)ドロップカウンタとIPsec機能ドロップカウンタの両方に登録されます。

```
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
```

Cisco IOS®では、明らかなセキュリティ上の理由から、このメッセージが1分ごとにレート制限されることに注意してください。特定のフロー（SRC、DST、またはSPI）に対するこのメッセージがsyslogに1回だけ表示される場合は、IPsecキー再生成と同時に存在する一時的な状態である可能性があります。この場合、ピアデバイスが新しいSAを使用する準備ができていない間に、一方のピアが新しいSAの使用を開始できます。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、同じフローとSPI番号に対して同じメッセージが引き続き表示される場合は、IPSec SAがピア間で同期されていないことを示しています。例：

```
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
```

これは、トラフィックがブラックホール化され、SAが送信側デバイスで期限切れになるか、Dead Peer Detection（DPD；デッドピア検出）がアクティブになるまで回復できないことを示します。

解決方法

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

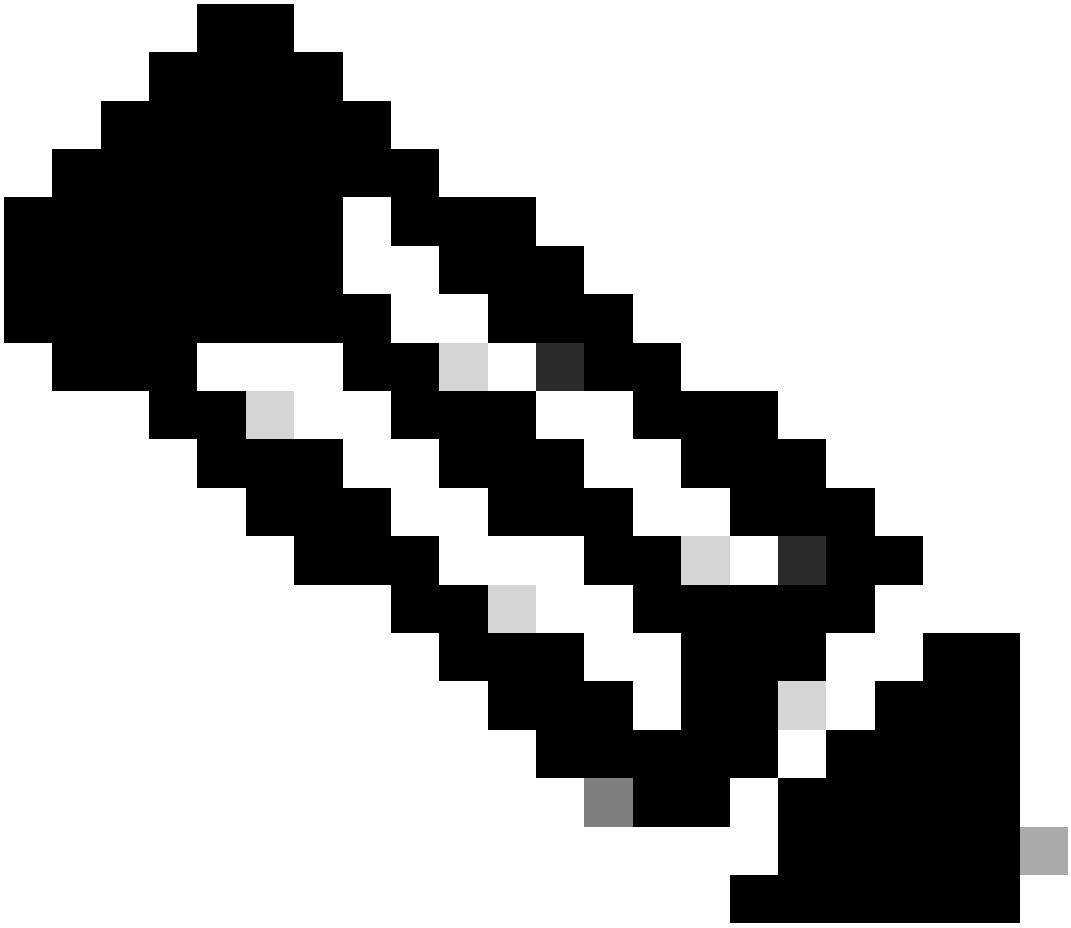
ります。このコマンドを使用しない場合でも、Cisco IOS は SA の送信側ピアに DELETE 通知を送信するときに、無効な SPI のリカバリ機能をすでに実行しています。この通知は、そのピアとの IKE SA がすでに確立されている場合に受信されます。この場合、crypto isakmp invalid-spi-recovery コマンドがアクティブであるかどうかに関係なくこれが発生します。

- 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	Yes
ダイナミック クリプト マップ	いいえ
トンネル保護を使用したP2P GRE	Yes
スタティックNHRPマッピングを使用するmGREトンネル保護	Yes
ダイナミックNHRPマッピングを使用するmGREトンネル保護	いいえ
sVTI	Yes
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用されるEEMスクリプト』を参照してください。

既知のバグ

次のリストは、IPSec SAの同期が外れる原因となるバグ、または無効なSPIの回復に関連するバグを示します。

- Cisco Bug ID CSCvn31824 Cisco IOS XE ISAKMPは、インストール前にrx新しいSPIパケットがあると、新しいSPIを削除します
- Cisco Bug ID CSCvd40554 IKEv2:Cisco IOSがSPIサイズ0のINV_SPI通知を解析できない – INVALID_SYNTAXを送信
- Cisco Bug ID CSCvp16730「0xFFで始まるSPI値の着信ESPパケットが、無効なSPIエラーが原因でドロップされる」

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。