SD-WANと従来のトンネルの理解SPIのリカバリの相違点

内容

はじめに

このドキュメントでは、%RECVD_PKT_INV_SPIエラーからSD-WANおよびサードパーティのトンネルを回復する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Catalystソフトウェア定義型ワイドエリアネットワーク(SD-WAN)
- インターネットプロトコルセキュリティ(IPSec)。
- 双方向フォワーディング検出(BFD)。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアに基づくものです。

- Cisco IOS® XE Catalyst SD-WANエッジ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

セキュリティアソシエーション(SA)の概念は、IPSecの基盤です。SAは2つのエンドポイント間の関係であり、エンドポイントがセキュリティサービスを使用して安全に通信する方法を示します。

Security Parameter Index（SPI；セキュリティパラメータインデックス）は、IPSecを使用して接続されたデバイスの特定のSAを一意に識別するために選択される32ビットの数値です。

最も一般的なIPSecの問題の1つは、無効なSPI値が原因でSAが同期されなくなることであり、その結果、パケットがピアによって廃棄され、ルータでsyslogメッセージが受信されると、IPSECトンネルダウンステータスが発生します。

サードパーティトンネル：

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

SD-WANトンネルの場合：

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

これらのログには、フォワーディングプロセッサ(FP)に属するQuantum Flow Processor(QFP)でのドロップが伴います。

<#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
```

解決方法

従来のIPSecトンネルのリカバリ

従来のIPSecトンネルを回復するには、現在のSA値関係のネゴシエーションを手動で強制的に行

う必要があります。これを行うには、次のようにEXECモードコマンドでIPSec SAをクリアします。

```
<#root>

Router#

clear crypto sa peer 10.20.20.1
```

SD-WANトンネルの回復 – シナリオ1

clear crypto sa peer EXECコマンドは、Internet Key Exchange（IKE；インターネット鍵交換）が存在するため、従来のIPSecトンネルに対してのみ動作します。これは、 は自動的に関連付けをネゴシエートし、新しいSPI値を生成します。ただし、このコマンドはSD-WANトンネルでは使用できません。これは、SD-WANトンネルではIKEが使用されていないためです。

そのため、SD-WANトンネルに対して同じコマンドが使用されます。

```
<#root>

Router#

request platform software sdwan security ipsec-rekey
```

request platform software sdwan security ipsec-rekeyコマンドを発行すると、新しいキーがすぐに生成され、トンネルが起動します。逆に、このコマンドは従来のIPSecトンネルが存在する場合には、そのトンネルに影響を与えません。

注:request platform software sdwan security ipsec-rekey このコマンドは、指定されたSAでのみ有効になるclear crypto sa peerとは反対の既存のすべてのSD-WANトンネルで有効になります。

SD-WANトンネルの回復 – シナリオ2

誤ってclear crypto sa peerコマンドを使用してSD-WANトンネルSAの1つを削除すると、削除は正常に行われます。ただし、SD-WANトンネルではOMPがIKE以外のアクションをトリガーするものであるため、新しいSPI値は再度生成されません。このステータスになると、コマンド request platforms software sdwan security ipsec-rekeyがclear crypto sa peerの後で発行されたとしても、トンネルは確立されません。SAのカプセル化と力プセル化解除はゼ口のままであるため、BFDセッションはダウン状態のままになります。

```
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
```

SAを削除した後の唯一の回復オプションは、次の3つのEXECコマンドのいずれかを使用することです。

<#root>

Router#

clear sdwan omp all

clear sdwan omp allコマンドは、デバイスに存在するすべてのBFDセッションをフラップします。

<#root>

Router#

request platforms software sdwan port_hop

clear sdwan control connectionsコマンドを使用すると、指定されたローカルカラーで次に使用可能なポート番号がTLOCで使用されます。これにより、そのカラーのすべてのBFDセッションだけでなく、そのカラーのコントロール接続でもフラップが発生します。

<#root>

Router#

clear sdwan control connections

最後のコマンドも回復に役立ちますが、デバイスに存在するすべての制御接続とBFDセッションに影響します。

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。