GREトンネルのキープアライブについて

内容

概要

このドキュメントでは、総称ルーティングカプセル化(GRE)キープアライブとその仕組みについて説明します。

GRE トンネル

GRE トンネルとは、トランスポート プロトコル内で、パッセンジャ パケットをカプセル化する方法を提供する、Cisco ルータ上の論理インターフェイスです。これは、ポイントツーポイント カプセル化スキームを実装するサービスを提供する設計になっているアーキテクチャです。

GRE トンネルは、完全にステートレスになるように設計されています。つまり、各トンネル エンドポイントは、リモート トンネル エンドポイントの状態または可用性に関する情報を保持しないということを意味します。この結果、トンネルのリモート エンドに到達不能な場合、ローカル トンネル エンドポイント ルータは GRE トンネル インターフェイスの回線プロトコルをダウンさせる機能がありません。そのインターフェイスを発信インターフェイスとして使用するルーティング テーブル内のルート（特にスタティック ルート）を削除するために、リンクのリモート エンドが利用できない場合にインターフェイスをダウンとしてマークする機能が使用されます。具体的には、インターフェイスの回線プロトコルがダウンに変更された場合、そのインターフェイスを指すスタティック ルートはルーティング テーブルから削除されます。これにより、代替のネクストホップまたはインターフェイスを選択するために、代替（フローティング）スタティック ルートまたはポリシー ベース ルーティング（PBR）のインストールが可能になります。

通常、GRE トンネルのインターフェイスは、設定されるとすぐにアップし、アップしているインターフェイスまたは有効なトンネル送信元アドレスがある限り、アップした状態を保ちます。トンネルの宛先 IP アドレスもルーティング可能である必要があります。これは、トンネルの反対側が設定されていない場合にも必要です。これは、GRE トンネル インターフェイスを経由するパケットのスタティック ルートまたは PBR フォワーディングは、GRE トンネル パケットがトンネルの他方の終端に到達しない場合でも、依然として有効であることを意味します。

GRE キープアライブが実装される前は、ルータのローカル問題を特定する方法が限られており、仲介ネットワークの問題を特定する方法はありませんでした。たとえば、GRE トンネリングされたパケットが転送に成功しても、トンネルのもう一方の端に達する前に失われるケースです。このようなシナリオでは、PBRを使用する代替ルートまたは別のインターフェイスを経由するフローティングスタティックルートが使用可能であったとしても、GREトンネルを通過するデータパケットは「ブラックホール」になります。GRE トンネルのインターフェイスのキープアライブは、キープアライブが物理インターフェイスで使用されるのと同様にこの問題を解決するために使用されます。

> **注**:GREキープアライブは、どのような状況でもIPSecトンネル保護とともにサポートされません。このドキュメントでは、この問題について説明します。

トンネルのキープアライブの動作方法

GRE トンネル キープアライブ メカニズムは、リモート ルータが GRE キープアライブをサポートしない場合でも一方がリモート ルータとの間でキープアライブ パケットを発信および受信できる点で、PPP キープアライブと似ています。GRE は IP 内で IP をトンネリングするパケット トンネリング メカニズムなので、別の GRE IP トンネル パケットの内部に GRE IP トンネル パケットを構築できます。GRE キープアライブの場合、送信者は元のキープアライブ要求パケット内にキープアライブ応答パケットを事前に構築するため、リモート エンドは外部 GRE IP ヘッダーの標準 GRE カプセル化解除を実行し、内部 IP GRE パケットを送信者に戻すだけで十分です。次のパケットは、IP トンネリングの概念を示しています。この場合、GRE がカプセル化プロトコルで、IP がトランスポート プロトコルです。パッセンジャ プロトコルもまた IP です（Decnet、Internetwork Packet Exchange（IPX）、Appletalk などの別のプロトコルにもできます）。

ノーマル パケット：

IP ヘッダー	TCP ヘッダー	Telnet

トンネリングされたパケット：

GRE IP ヘッダー	GRE	IP ヘッダー	TCP ヘッダー	Telnet

- IP はトランスポート プロトコルです。
- GRE はカプセル化プロトコルです。
- IP はパッセンジャ プロトコルです。

ルータ A から送信され、ルータ B を宛先とするキープアライブ パケットの例を示します。ルータ B がルータ A に戻すキープアライブの応答は内部の IP ヘッダー内にすでにあります。ルータ B は単にキープアライブ パケットをカプセル化解除して、それを物理インターフェイス（S2）に送り返すだけです。その他の GRE IP データ パケットと同様に GRE キープアライブ パケットを処理します。

GRE キープアライブ：

GRE IP ヘッダー		GRE	IP ヘッダー		GRE
Source A	Destination B	PT=IP	Source B	Destination A	PT=0

このメカニズムにより、キープアライブの応答はトンネル インターフェイスではなく物理インターフェイスに転送されます。これは、GRE キープアライブ応答パケットが、「tunnel protection ...」、QoS、Virtual Routing and Forwarding（VRF）などのトンネル インターフェイス上のあらゆる出力機能の影響を受けないことを意味します。

> **注**:GREトンネルインターフェイスにインバウンドアクセスコントロールリスト(ACL)が設定されている場合、相手側デバイスが送信するGREトンネルのキープアライブパケットを許可する必要があります。そうでない場合は、反対側のデバイスのGREトンネルがダウンします。(`access-list <number> permit gre host <tunnel-source> host <tunnel-destination>`)

GRE トンネル キープアライブのもう 1 つの特性は、PPP キープアライブと同様に、各側のキープアライブ タイマーが独立しており、一致する必要がないという点です。

> **ヒント**：トンネルの片側だけにキープアライブを設定する場合の問題は、キープアライブタイマーが時間切れになると、キープアライブが設定されているルータだけがトンネルインターフェイスをダウン状態としてマークすることです。キープアライブが設定されていない反対側の GRE トンネルのインターフェイスは、トンネルの相手側がダウンした場合でもアップ状態のままです。キープアライブが設定されていない側からトンネルへ送られたパケットに関して、トンネルがブラックホールになる可能性があります。

> **ヒント**：大規模なハブアンドスポークGREトンネルネットワークでは、GREキープアライブをハブ側ではなくスポーク側でのみ設定するのが適切な場合があります。これは、多くの場合はスポーク側でハブに到達不可能なことを検出して、バックアップ パスに切り替えることの方が重要であるためです（ダイヤル バックアップなど）。

GRE トンネルのキープアライブ

Cisco IOS® ソフトウェア リリース 12.2(8)T では、ポイントツーポイントの GRE トンネル インターフェイスにキープアライブを設定できます。この変更によって、トンネル インターフェイスは、一定期間キープアライブが失敗した場合に、動的にシャットダウンします。

その他の形式のキープアライブの仕組みの詳細は、「Cisco IOS でのキープアライブ メカニズムの概要」を参照してください。

> **注**:GREトンネルのキープアライブは、ポイントツーポイントGREトンネルでのみサポートされます。トンネルのキープアライブは、マルチポイント GRE（mGRE）トンネルでも設定できますが、効果はありません。

> **注**：一般に、VRFがトンネルインターフェイスとfVRF('tunnel vrf ...')およびiVRF ('ip vrf forwarding ...' on tunnel interface)が一致しません。これは、キープアライブを要求者に「反映」させるトンネル エンドポイントでは重要です。キープアライブ要求が受信されるとき、fVRF で受信され、カプセル化解除されます。これにより、送信者に転送する必要がある事前に作成されたキープアライブ応答が表出しますが、その転送はトンネル インターフェイスの iVRF のコンテキストです。したがって、iVRF と fVRF が一致しない場合、キープアライブ応答パケットは送信者に転送されません。このことは、iVRF や fVRF を「global」に置き換えても当てはまります。

この出力は、GRE トンネルにキープアライブを設定するために使用するコマンドを示しています。

```
Router#configure terminal
Router(config)#interface tunnel0
Router(config-if)#keepalive 5 4

!--- The syntax of this command is keepalive [seconds [retries]].



!--- Keepalives are sent every 5 seconds and 4 retries.
!--- Keepalives must be missed before the tunnel is shut down.
!--- The default values are 10 seconds for the interval and 3 retries.
```

トンネル キープアライブ メカニズムの仕組みの理解を深めるため、この例のトンネル トポロジと構成を考えてみましょう。

ルータ A

```
interface loopback 0
ip address 192.168.1.1 255.255.255.255
interface tunnel 0
ip address 10.10.10.1 255.255.255.252
tunnel source loopback0
tunnel destination 192.168.1.2
keepalive 5 4
```

ルータ B

```
interface loopback 0
ip address 192.168.1.2 255.255.255.255
interface tunnel 0
ip address 10.10.10.2 255.255.255.252
tunnel source loopback0
tunnel destination 192.168.1.1
keepalive 5 4
```

このシナリオでは、ルータ A で次のステップを実行します。

1. 次のようにして、内部 IP ヘッダーを 5 秒ごとに生成します。

送信元はローカルのトンネルの宛先（192.168.1.2）として設定宛先はローカルのトンネルの送信元（192.168.1.1）として設定

また、GRE ヘッダーに 0 のプロトコル タイプ（PT）を追加します

ルータ A によって生成されるが送信されないパケット

2. そのパケットをトンネル インターフェイスから送信し、その結果、次のように外部 IP ヘッダーでパケットがカプセル化されます。

   送信元はローカルのトンネルの送信元（192.168.1.1）として設定宛先はローカルのトンネルの宛先（192.168.1.2）として設定

   また、GRE ヘッダーに PT = IP を追加します。

   ルータ A からルータ B に送信されたパケット：

3. トンネル キープアライブ カウンタを 1 ずつ増加させます。

4. 遠端トンネルのエンドポイントに到達する方法があり、トンネルの回線プロトコルが何らかの理由によりダウンしていない場合には、パケットはルータ B に到達します。トンネル 0 に対して照合され、カプセル化解除されると、ルータ A のトンネル送信元 IP アドレスの宛先 IP に転送されます。

   ルータ B からルータ A へ送信：

5. ルータ A で着信すると、パケットはカプセル化解除され、PT のチェックが 0 になります。このことは、これがキープアライブ パケットであることを示します。その後、トンネルのキープアライブ カウンタは 0 にリセットされ、パケットは廃棄されます。

ルータ B が到達不能な場合、ルータ A は通常のトラフィックとともにキープアライブ パケットの生成と送信を続行します。キープアライブが戻ってこない場合、トンネルの回線プロトコルは、トンネル キープアライブ カウンタが再試行回数（このケースでは 4 回）未満である限り、アップ状態のままになります。この条件が true でない場合、次回ルータ A がルータ B にキープアライブを送信しようとするときに回線プロトコルがダウンします。

注：アップ/ダウン状態では、トンネルはデータトラフィックを転送または処理しません。ただし、キープアライブ パケットを送信し続けます。キープアライブ応答を受信し、トンネル エンドポイントが到達可能であることが再度示唆されると、トンネル キープアライブ カウンタは 0 にリセットされ、トンネルの回線プロトコルはアップ状態になります。

操作でキープアライブを確認するには、**debug tunnel** と **debug tunnel keepalive** を有効にします。

ルータ A からのデバッグの例：

```
debug tunnel keepalive
Tunnel keepalive debugging is on
01:19:16.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=15
01:19:21.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=16
01:19:26.019: Tunnel0: sending keepalive, 192.168.1.1->192.168.1.2
(len=24 ttl=0), counter=17
```

GRE キープアライブと Unicast Reverse Path Forwarding

ユニキャスト RPF (Unicast Reverse Path Forwarding) は、ルーティング テーブルに対してパケット送信元アドレスの検証を行うことでスプーフィングされた IP トラフィックを検出および破棄できるセキュリティ機能です。 ユニキャスト RPF がストリクトモード (**ip verify unicast source reachable-via rx**) で実行されるときは、戻りパケットを転送するためにルータが使用するインターフェイスでパケットを受信する必要があります。GREキープアライブパケットを受信するルータのトンネルインターフェイスでstrictモードまたはlooseモードのユニキャストRPFが有効になっている場合、パケットの送信元アドレス (ルータ自身のトンネル送信元アドレス) へのルートはトンネルインターフェイスを経由しないため、トンネルのカプセル化解除後にRPFによってキープアライブパケットが廃棄されます。RPF パケット ドロップは、次に示す **show ip traffic 出力で確認できます。**

```
Router#show ip traffic | section Drop
Drop: 0 encapsulation failed, 0 unresolved, 0 no adjacency
0 no route, 156 unicast RPF, 0 forced drop
0 options denied
```

その結果、トンネルのキープアライブの発信側は、キープアライブの戻りパケットが失われたためにトンネルをダウンさせます。このため、GRE トンネル キープアライブが機能するためには、ユニキャスト RPF をストリクト モードまたはルーズ モードで設定してはなりません。ユニキャスト RPF の詳細については、「Unicast Reverse Path Forwarding について」を参照してください。

IPsec と GRE キープアライブ

IPsec を使用する GRE トンネル

IPsec は IP マルチキャスト パケットをサポートしないため、GRE トンネルは IPsec と組み合わせることがあります。このため、ダイナミック ルーティング プロトコルは IPsec VPN ネットワークを介して正常に実行できません。GRE トンネルでは IP マルチキャストがサポートされているので、GRE トンネル上ではダイナミック ルーティング プロトコルが動作します。その結果の GRE IP ユニキャスト パケットは、IPsec で暗号化できます。

IPsec が GRE パケットを暗号化できる方法は 2 つあります。

- 1 つは、暗号マップを使用する方法です。暗号マップを使用すると、GRE トンネル パケットのアウトバウンド物理インターフェイスに適用されます。この場合、一連のステップは次のようになります。

  暗号化されたパケットが物理インターフェイスに到達します。パケットは復号され、トンネル インターフェイスに転送されます。パケットはカプセル化解除され、クリア テキストで IP の宛先に転送されます。

- もう 1 つは、トンネル保護を使用する方法です。トンネル保護を使用する場合は、GRE トンネル インターフェイスに設定します。tunnel protection コマンドは、Cisco IOS ソフトウェア リリース 12.2(13)T で導入されました。この場合、一連のステップは次のようになります。

  暗号化されたパケットが物理インターフェイスに到達します。パケットがトンネル インターフェイスに転送されます。パケットは復号されてカプセル化解除され、クリア テキストで IP の宛先に転送されます。

いずれの方法も、IPsec 暗号化が GRE カプセル化の追加後に実行されることを指定します。暗号マップを使用する場合とトンネル保護を使用する場合とには、2 つの主な違いがあります。

- IPsec 暗号マップは物理インターフェイスに関連付けられ、パケットが物理インターフェイスに転送されるときにチェックされます。

  GRE トンネルでは、この時点ですでにパケットを GRE カプセル化しています。
- トンネル保護では暗号化機能が GRE トンネルに結び付けられており、パケットが GRE カプセル化された後、物理インターフェイスに送られる前にチェックされます。

IPsec と GRE を組み合わせる場合のキープアライブの問題

GRE トンネルに暗号化を追加する 2 つの方法を考えると、暗号化された GRE トンネルをセットアップする方法は 3 つあります。

1. ピア A はトンネル インターフェイスでトンネル保護を設定し、ピア B は物理インターフェイスで暗号マップを設定する。
2. ピア A は物理インターフェイスで暗号マップを設定し、ピア B はトンネル インターフェイスでトンネル保護を設定する。
3. 両方のピアがトンネル インターフェイスでトンネル保護を設定する。

シナリオ 1 と 2 で説明する構成は、多くの場合、ハブアンドスポーク設計で行われます。トンネル保護は、設定の規模を小さくするためにハブ ルータで設定し、スタティックな暗号マップは各スポークで使用します。

ピア B (スポーク) で GRE キープアライブを有効にするこれらの各シナリオを検討し、どこで暗号化にトンネル モードを使用するのかを考えてみましょう。

シナリオ 1

設定：

- ピア A はトンネル保護を使用します。
- ピア B は暗号マップを使用します。
- キープアライブはピア B で有効になっています。
- IPsec 暗号化は、トンネル モードで実行されます。

このシナリオでは、GRE キープアライブがピア B で設定されるため、キープアライブが生成されるときの一連のイベントは次のようになります。

1. ピア B はキープアライブ パケットを生成します。これは GRE カプセル化されてから物理インターフェイスに転送され、ここで暗号化されてトンネルの宛先であるピア A に送信されます。

   ピア B からピア A に送信されたパケット：

2. ピア A で、GRE キープアライブは復号化されて受信されます。

   カプセル化解除されます。

   次に、内部 GRE キープアライブ応答パケットが、ピア B となっているその宛先アドレスに基づいてルーティングされます。つまり、ピアAでは、パケットはすぐに物理インターフェイスからピアBにルーティングされて戻されます。ピアAはトンネルインターフェイスでトンネル保護を使用するため、キープアライブパケットは暗号化されません。

   したがって、ピア A からピア B に送信されたパケットは次のとおりです。

   注：キープアライブは暗号化されません。

3. これでピア B は物理インターフェイスで暗号化されていない GRE キープアライブ応答を受信しますが、物理インターフェイスで暗号マップが設定されているため、暗号化されたパケットが要求され、破棄されます。

したがって、ピアAがキープアライブに応答し、ルータPeer Bがその応答を受信しても、ピアBは応答を処理せず、最終的にはトンネルインターフェイスの回線プロトコルをダウン状態に変更します。

Result:

ピア B でキープアライブが有効になっていると、ピア B のトンネルの状態はアップ/ダウンに変更されます。

シナリオ 2

設定：

- ピア A は暗号マップを使用します。
- ピア B はトンネル保護を使用します。
- キープアライブはピア B で有効になっています。
- IPsec 暗号化は、トンネル モードで実行されます。

このシナリオでは、GRE キープアライブがピア B で設定されるため、キープアライブが生成されるときの一連のイベントは次のようになります。

1. ピア B はキープアライブ パケットを生成します。これは GRE カプセル化されてからトンネル インターフェイスでトンネル保護によって暗号化され、物理インターフェイスに転送されます。

   ピア B からピア A に送信されたパケット：

2. ピア A で、GRE キープアライブは復号化されて受信されます。

   カプセル化解除されます。

   次に、内部 GRE キープアライブ応答パケットが、ピア B となっているその宛先アドレスに基づいてルーティングされます。つまり、ピアAでは、パケットはすぐに物理インターフェイスからピアBにルーティングされます。ピアAは物理インターフェイスで暗号マップを使用するため、パケットを転送する前にこのパケットを最初に暗号化します。

   したがって、ピア A からピア B に送信されたパケットは次のとおりです。

   注：キープアライブ応答は暗号化されます。

3. これで、ピア B は、宛先が復号されるトンネル インターフェイスに転送される暗号化された GRE キープアライブ応答を受信します。

   プロトコル タイプが 0 に設定されているため、ピア B はこれがキープアライブ応答であることを認識し、それに応じた処理を行います。

Result:

ピアBでイネーブルにされたキープアライブは、トンネルの宛先のアベイラビリティに基づいて、どのトンネル状態が可能かを正常に判断します。

シナリオ 3

設定：

- 両方のピアでトンネル保護を使用します。
- キープアライブはピア B で有効になっています。
- IPsec 暗号化は、トンネル モードで実行されます。

このシナリオは、ピア A が暗号化されたキープアライブを受信し、復号してカプセル化解除する点でシナリオ 1 と似ています。ただし、応答が転送される場合、ピア A がトンネル インターフェイスでトンネル保護を使用するため、暗号化されません。したがって、ピア B は暗号化されて

いないキープアライブ応答を破棄し、処理しません。

Result:

ピア B でキープアライブが有効になっていると、ピア B のトンネルの状態はアップ/ダウンに変更されます。

回避策

GRE パケットを暗号化する必要があるこのような状況では、利用可能な解決策は 3 つあります。

1. ピア A で暗号マップ、ピア B でトンネル保護を使用し、ピア B でキープアライブを有効にします。

   このタイプの設定は主にハブアンドスポーク設定で使用され、このような設定ではスポークがハブの到達可能性を認識することが重要であるため、解決策はハブ（ピアA）でダイナミック暗号マップを使用し、スポーク（ピアB）でトンネル保護を使用して、スポークでGREキープアライブを有効にすることです。この方法では、ハブの GRE トンネル インターフェイスはアップ状態のままですが、トンネル経由のルーティング ネイバーとルートは失われ、代替ルートを確立できます。スポークでは、トンネル インターフェイスがダウンしたことによって、ダイヤラ インターフェイスの起動とハブ（またはハブで別のルータ）へのコール バックが行われ、新しい接続が確立されます。

2. ピアの到達可能性を判断するために GRE キープアライブ以外の方法を使用します。

   両方のルータでトンネル保護が設定されている場合、GRE トンネル キープアライブはどちらの方向にも使用できません。この場合、ピアが到達可能であるかどうかを検出するための唯一のオプションは、ルーティング プロトコルやサービス保証エージェントなどのその他のメカニズムを使用することです。

3. ピア A とピア B で暗号マップを使用します。

   両方のルータで暗号マップが設定されている場合、トンネル キープアライブは両方向で使用でき、GRE トンネル インターフェイスはいずれかまたは両方向でシャットダウンでき、バックアップ接続の作成をトリガーできます。これは最も柔軟性の高いオプションです。

関連情報

- RFC 1701, Generic Router Encapsulation (GRE)
- RFC 2890, Key and Sequence Number Extensions to GRE
- 総称ルーティング カプセル化（GRE）トンネルのキープアライブ
- IP フラグメンテーションと PMTUD
- Cisco IOS でのキープアライブ メカニズムの概要
- テクニカルサポート - Cisco Systems

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。