# 了解GRE隧道Keepalive

## 目录


简介

GRE 隧道

隧道 Keepalive 工作原理

GRE隧道Keepalive

GRE 保持连接和单播逆向路径转发

IPsec 和 GRE 保持连接

- 采用 IPsec 的 GRE 隧道
- 将 IPsec 和 GRE 结合使用时保持连接存在的问题
  - 场景 1
  - 场景 2
  - 场景 3
- 解决方法

相关信息


## 简介

本文档介绍通用路由封装(GRE)保持连接及其工作原理。

## GRE 隧道

GRE隧道是路由器上的逻辑接口，它提供了一种将网络协议数据包封装在传输协议内的方法。它是一种通过点对点封装方案为网络流量提供传输的机制。

GRE 隧道设计为完全无状态。这意味着每个隧道终端不会保留有关远程隧道终端的状态或可用性的任何信息。由此产生的后果是，如果无法访问隧道的远程端，本地隧道终端路由器将无法关闭 GRE 隧道接口的线路协议。使用在链路远程端不可用时将接口标记为关闭的功能，是为了删除路由表中使用该接口作为出站接口的所有路由（具体说来是静态路由）。具体而言，如果接口的线路协议更改为关闭，则会从路由表中删除使用该接口的所有静态路由。这样就可以安装备用（浮动）静态路由，或实施基于策略的路由 (PBR)，以便选择备用的下一跳或接口。

通常，GRE隧道接口在配置后会立即启动，只要存在有效的隧道源地址或隧道源接口处于打开状态，该接口就会保持打开状态。隧道目标 IP 地址也必须可路由。即使隧道另一端未进行配置也是如此。这意味着，即使GRE隧道数据包无法到达隧道的另一端，通过GRE隧道接口转发数据包的静态路由或PBR仍然有效。

在实施GRE Keepalive之前，只有一些方法可以因为路由器上的本地问题而不是由于传输网络问题而关闭隧道接口。例如，GRE 隧道数据包转发成功但在到达隧道另一端之前丢失的情况。此类情况将导致通过GRE隧道的数据包被设置为“黑洞”，即使有使用PBR的备用路由或通过其他接口的浮动静态路由可用。GRE 隧道接口上的 Keepalive 可以解决这一问题，方式与 Keepalive 在物理接口上的使用方式相同。

---

注意：在任何情况下均无法同时支持 GRE 保持连接与 IPsec 隧道保护功能。本文档讨论这一问题。

---

# 隧道 Keepalive 工作原理

GRE 隧道保持连接机制与 PPP 保持连接类似，因为即使远程路由器不支持 GRE 保持连接，它也会使一端能够与远程路由器之间进行保持连接数据包收发。GRE 是 IP 内隧道传输 IP 的数据包隧道机制，因此，GRE IP 隧道数据包可以在另一个 GRE IP 隧道数据包里构建。对于 GRE 保持连接，发送方会在原始保持连接请求数据包内预构建保持连接响应数据包，以便远程终端只需对外部 GRE IP 报头执行标准 GRE 解封，然后将内部 IP GRE 数据包回复给发送方即可。这些数据包说明了 IP 隧道的概念，其中 GRE 是封装协议，IP 是传输协议。乘客协议也是IP（尽管也可以是另一个协议，如NHRP）。

正常数据包：

| IP 报头 | TCP 报头 | Telnet |
|---|---|---|

隧道数据包：

| GRE IP 报头 | GRE | IP 报头 | TCP 报头 | Telnet |
|---|---|---|---|---|

- IP 是传输协议。
- GRE 是封装协议。
- IP 是乘客协议。

以下是源自路由器 A 并发往路由器 B 的保持连接数据包的示例。路由器 B 返回给路由器 A 的 Keepalive 响应已在内部 IP 报头中。路由器 B 只是解封 Keepalive 数据包，然后将其发送出物理接口 (S2)。 它处理 GRE Keepalive 数据包的方式与任何其他 GRE IP 数据包一样。

GRE 保持连接：

| GRE IP 报头 | | GRE | IP 报头 | | GRE |
|---|---|---|---|---|---|
| 源 A | 目的 B | PT=IP | 源 B | 目的 A | PT=0 |

此机制会导致keepalive响应从物理接口而非隧道接口转发出去。这意味着GRE keepalive响应数据包不受隧道接口上的任何输出功能的影响，例如“隧道保护……” QoS、虚拟路由和转发(VRF)等。

注意：如果在 GRE 隧道接口上配置了入站访问控制列表 (ACL)，则必须允许相对设备所发送的 GRE 隧道保持连接数据包。否则，相反的设备GRE隧道会关闭。（ **access-list <编号> permit gre host <隧道源> host <隧道目标>** ）

GRE 隧道保持连接所具有的另一个属性是，两端的保持连接计时器相互独立且不必匹配，类似于 PPP 保持连接。

提示：只在隧道一端配置 Keepalive 的问题在于，如果 Keepalive 计时器过期，只有配置了 Keepalive 的路由器才会将其隧道接口标记为关闭。另一端的 GRE 隧道接口（未配置 Keepalive）保持为打开状态，即使通道另一端关闭也是如此。隧道可能成为从未配置keepalive的一侧定向到隧道的数据包的黑洞。

提示：在大型集中星型GRE隧道网络中，可以只将GRE Keepalive配置在分支端，而不配置在中心端。这是因为辐射点发现中心无法访问，因此切换到备用路径（例如，使用备用蜂窝网接口）通常更为重要。

## GRE隧道Keepalive

使用 Cisco IOS® 软件版本 12.2(8)T，可以在点对点 GRE 隧道接口上配置 Keepalive。通过这一更改，如果 Keepalive 在某一时间段内出现故障，则隧道接口会动态关闭。

有关其他形式保持连接机制的工作方式的详细信息，请参阅 Cisco IOS 上的保持连接机制概述。

注意：仅在点对点 GRE 隧道上支持 GRE 隧道 Keepalive。隧道 Keepalive 可在多点 GRE (mGRE) 隧道上配置，但是没有任何效果。

注意：通常，当在隧道接口上使用VRF且fVRF(tunnel vrf ...)和iVRF(ip vrf forwarding ... on tunnel interface)不匹配时，隧道keepalive无法工作。这对于将keepalive返回请求者的隧道终端至关重要。当收到保持连接请求时，它会在 fVRF 中接收并进行解封。这会显示出预先构建的保持连接应答，随后需将此应答转发回发送方，但此转发是在隧道接口上的 iVRF 上下文中进行的。因此，如果 iVRF 和 fVRF 不匹配，则保持连接应答数据包不会转发回发送方。即使

将iVRF和/或fVRF替换为global，情况也是如此。

此输出显示用于在 GRE 隧道上配置 Keepalive 的命令。

```
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.
```

为了更好地了解隧道保持连接机制的工作方式，请参考以下隧道拓扑和配置示例：




路由器 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
```

路由器 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
```

在此场景中，路由器 A 执行以下步骤：

- 源设置为本地隧道目的地，即 192.168.1.2
- 目标设置为本地隧道源，即192.168.1.1，并且
- 每五秒构建一个内部IP报头，其中添加的GRE报头协议类型(PT)为0。

已由路由器 A 生成但未发送的数据包：

| IP 报头 | | GRE |
|---|---|---|
| 源：192.168.1.2 | 目的地：192.168.1.1 | PT=0 |

将数据包从其隧道接口发送出去，这将导致数据包与外部 IP 报头封装在一起，其中：

- 源设置为本地隧道源，即 192.168.1.1
- 目标设置为本地隧道目标，即192.168.1.2，并且
- GRE报头添加了PT = IP。

从路由器 A 发送到路由器 B 的数据包：

| GRE IP 报头 | | GRE | IP 报头 | | GRE |
|---|---|---|---|---|---|
| 来源：192.168.1.1 | 目的地：192.168.1.2 | PT=IP | 源：192.168.1.2 | 目的地：192.168.1.1 | PT=0 |

- 将隧道保持连接计数器递增 1。
- 假设可以到达远端隧道终点并且隧道线路协议因其他原因未关闭，则数据包会到达路由器 B。然后，它与隧道 0 进行匹配，变为解封状态，并转发到目的地 IP，即路由器 A 上的隧道源 IP 地址。

从路由器 B 发送到路由器 A 的数据包：

| IP 报头 | | GRE |
|---|---|---|
| 源：192.168.1.2 | 目的地：192.168.1.1 | PT=0 |

- 到达路由器A后，数据包将被解封，对PT的检查结果为0。这表示这是一个保持连接数据包。然后，隧道 Keepalive 计数器重置为 0，丢弃数据包。

如果无法访问路由器 B，路由器 A 会继续构建并发送保持连接数据包以及正常流量。如果保持连接未恢复，只要隧道保持连接计数器小于重试次数（在本例中为 4），隧道线路协议就会保持运行。如果不是这种情况，则当路由器 A 下次尝试将 Keepalive 发送到路由器 B 时，线路协议会关闭。

---

注意：在打开/关闭状态下，隧道不转发或处理任何数据流。不过，它会继续发送 Keepalive 数据包。在收到保持连接响应时，如果此响应暗示隧道终端重新恢复可访问性，则隧道保持连接计数器会重置为 0，并且隧道上的线路协议会运行。

---

要查看保持连接的运行，请启用调试隧道和调试隧道保持连接。

路由器 A 的调试示例：

```
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 保持连接和单播逆向路径转发

单播RPF（单播逆向路径转发）是一项安全功能，它通过根据路由表验证数据包源地址来检测并丢弃伪造IP流量。当单播RPF在严格模式下运行(ip verify unicast source reachable-via rx)时，必须在路由器将用来转发返回数据包的接口上接收数据包。如果在接收GRE Keepalive数据包的路由器的隧道接口上启用了严格模式或松散模式单播RPF，则Keepalive数据包在隧道解封后由RPF丢弃，因为通往数据包源地址（路由器自己的隧道源地址）的路由不是通过隧道接口。可以在 show ip traffic 输出中观察到 RPF 丢包，如下所示：

```
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
```

因此，隧道keepalive的发起方会由于丢失的keepalive返回数据包而关闭隧道。因此，为了使 GRE 隧道保持连接正常工作，单播 RPF 不得配置为严格或宽松模式。有关单播 RPF 的详细信息，请参阅了解单播逆向路径转发。

# IPsec 和 GRE 保持连接

## 采用 IPsec 的 GRE 隧道

GRE 隧道有时与 IPsec 结合使用，因为 IPsec 不支持 IP 组播数据包。因此，动态路由协议无法在 IPsec VPN 网络中成功运行。GRE 隧道支持 IP 组播，因此，动态路由协议可以在 GRE 隧道上运行。所生成的 GRE IP 单播数据包可由 IPsec 加密。

IPsec 可通过以下两种方法加密 GRE 数据包：

- 一种方法是使用加密映射。当使用加密映射时，它会应用到 GRE 隧道数据包的出站物理接口。在这种情况下，执行的一系列步骤如下：

  1. 加密后的数据包到达物理接口。
  2. 数据包被解密并转发到隧道接口。
  3. 数据包被解封，然后以明文形式转发到 IP 目的地。

- 另一种方法是使用隧道保护。如果使用隧道保护，是在 GRE 隧道接口上配置的。Cisco IOS 软件版本 12.2(13)T 提供了隧道保护命令。在这种情况下，执行的一系列步骤如下：

  1. 加密后的数据包到达物理接口。
  2. 数据包转发到隧道接口。
  3. 数据包经过解密和解封，然后以明文形式转发到 IP 目的地。

这两种方法都指定在添加 GRE 封装后执行 IPsec 加密。使用加密映射与使用隧道保护，主要存在以下两个区别：

- IPsec 加密映射被绑定到物理接口，并在从物理接口向外转发数据包时进行检查。GRE 隧道此时已对数据包进行 GRE 封装。
- 隧道保护将加密功能绑定到 GRE 隧道，在对数据包进行 GRE 封装之后，并且在将数据包发送到物理接口之前进行检查。

## 将 IPsec 和 GRE 结合使用时保持连接存在的问题

考虑到两种向 GRE 隧道添加加密的方法，可使用三种不同的方法来设置加密的 GRE 隧道：

1. 在隧道接口上为对等体 A 配置隧道保护，在物理接口上为对等体 B 配置加密映射。
2. 在物理接口上为对等体 A 配置加密映射，在隧道接口上为对等体 B 配置隧道保护。
3. 两个对等体都在隧道接口上配置了隧道保护。

场景 1 和场景 2 中所述的配置通常采用中心辐射型设计。隧道保护在中心路由器上配置以减少配置的大小，而在每个辐射端使用静态加密映射。

请考虑在对等体 B（分支）上启用 GRE 保持连接并且使用隧道模式进行加密的以下每个场景。

场景 1

配置:

- 对等体 A 使用隧道保护。
- 对等体 B 使用加密映射。
- 在对等体 B 上启用保持连接。
- 在隧道模式下执行 IPsec 加密。

在此场景中，由于在对等体 B 上配置了 GRE 保持连接，生成保持连接时发生的一系列事件如下：

1. 对等体 B 生成一个保持连接数据包，该数据包经过 GRE 封装，然后转发到物理接口，在该接口上加密并发送到隧道目的地对等体 A。

   从对等体 B 发送到对等体 A 的数据包：

<table>
<tr><td>IP 报头</td><td>ESP 报头</td><td colspan="2">GRE IP 报头</td><td>GRE 报头</td><td colspan="3"><table><tr><td colspan="2">IP 报头</td><td>GRE</td></tr><tr><td>源A</td><td>目的地 B</td><td>PT=0</td></tr></table></td><td>ESP 报尾</td></tr>
<tr><td>源B</td><td>目的地 A</td><td>源B</td><td>目的地 A</td><td>PT=IP</td><td colspan="3"></td></tr>
</table>

2. 在对等体 A 处，收到已解密的 GRE 保持连接数据包：

<table>
<tr><td colspan="2">GRE IP 报头</td><td>GRE</td><td colspan="3"><table><tr><td colspan="2">IP 报头</td><td>GRE</td></tr><tr><td>源A</td><td>目的地 B</td><td>PT=0</td></tr></table></td></tr>
<tr><td>源B</td><td>目的地 A</td><td>PT=IP</td><td colspan="3"></td></tr>
</table>

解封：

| IP 报头 | | GRE |
|---|---|---|
| 源A | 目的地 B | PT=0 |

然后，内部GRE保持连接响应数据包根据其目的地址（对等体B）进行路由。这意味着在对等A上，数据包会立即从物理接口路由回对等B。由于对等A在隧道接口上使用隧道保护，因此keepalive数据包不会加密。

因此，数据包从对等体 A 发送到对等体 B：

| IP 报头 | | GRE |
|---|---|---|
| 源A | 目的地 B | PT=0 |

注意：保持连接未加密。

3. 对等体 B 现在收到未在其物理接口上加密的 GRE 保持连接响应，但由于在物理接口上配置了加密映射，它预期应收到加密的数据包，因此会丢弃该数据包。

因此，即使对等体A对保持连接作出响应，而路由器对等体B收到响应，它也不会处理这些响应，最终会将隧道接口的线路协议更改为关闭状态。

结果：

在对等体 B 上启用保持连接会导致对等体 B 上的隧道状态更改为“打开/关闭”。

场景 2

配置:

- 对等体 A 使用加密映射。
- 对等体 B 使用隧道保护。
- 在对等体 B 上启用保持连接。
- 在隧道模式下执行 IPsec 加密。

在此场景中，由于在对等体 B 上配置了 GRE 保持连接，生成保持连接时发生的一系列事件如下：

1. 对等体 B 生成一个保持连接数据包，该数据包经过 GRE 封装，并在隧道接口上由隧道保护功能加密，然后转发到物理接口。

从对等体 B 发送到对等体 A 的数据包：

<table>
<tr><td>IP 报头</td><td>ESP 报头</td><td>GRE IP 报头</td><td>GRE 报头</td><td><table><tr><td>IP 报头</td><td>GRE</td><td></td></tr><tr><td>源A</td><td>目的地 B</td><td>PT=0</td></tr></table></td><td rowspan="2">ESP 报尾</td></tr>
<tr><td>源B</td><td>目的地 A</td><td>源B</td><td>目的地 A</td><td colspan="2">PT=IP</td></tr>
</table>

2. 在对等体 A 处，收到已解密的 GRE 保持连接数据包：

<table>
<tr><td colspan="2">GRE IP 报头</td><td>GRE</td><td><table><tr><td colspan="2">IP 报头</td><td>GRE</td></tr><tr><td>源A</td><td>目的地 B</td><td>PT=0</td></tr></table></td></tr>
<tr><td>源B</td><td>目的地 A</td><td>PT=IP</td></tr>
</table>

解封：

<table>
<tr><td colspan="2">IP 报头</td><td>GRE</td></tr>
<tr><td>源A</td><td>目的地 B</td><td>PT=0</td></tr>
</table>

然后，内部GRE保持连接响应数据包根据其目的地址（对等体B）进行路由。这意味着在对等A上，数据包会立即从物理接口路由回对等B。由于对等A在物理接口上使用加密映射，因此它首先加密此数据包，然后再转发它。

因此，数据包从对等体 A 发送到对等体 B：

<table>
<tr><td colspan="2">IP 报头</td><td rowspan="2">ESP 报头</td><td><table><tr><td colspan="2">IP 报头</td><td>GRE</td></tr><tr><td>源A</td><td>目的地 B</td><td>PT=0</td></tr></table></td><td rowspan="2">ESP 报尾</td></tr>
<tr><td>源B</td><td>目的地 A</td><td></td></tr>
</table>



注意：保持连接响应已加密。

3. 对等B现在收到一个加密的GRE keepalive响应，其目标被转发到隧道接口，然后被解密：

<table>
<tr><td colspan="2">IP 报头</td><td>GRE</td></tr>
<tr><td>源A</td><td>目的地 B</td><td>PT=0</td></tr>
</table>

由于“协议类型”设置为 0，因此对等体 B 知道这是一个保持连接响应，并且会相应地对其进行处理。

结果：

在对等B上启用Keepalive成功根据隧道目标的可用性确定隧道状态。

场景 3

配置:

- 两个对等体都使用隧道保护。
- 在对等体 B 上启用保持连接。
- 在隧道模式下执行 IPsec 加密。

此场景与场景 1 类似，因为当对等体 A 收到加密的保持连接时，会对其进行解密和解封。但是，它不会对转发出去的响应进行加密，因为对等体 A 在隧道接口上使用隧道保护。因此，对等体 B 会丢弃未加密的保持连接响应，并且不对其进行处理。

结果：

在对等体 B 上启用保持连接会导致对等体 B 上的隧道状态更改为“打开/关闭”。

## 解决方法

在必须加密 GRE 数据包的情况下，有三种可能的解决方案：

1. 在对等体 A 上使用加密映射，在对等体 B 上使用隧道保护，并在对等体 B 上启用保持连接。

   由于此类配置主要用在中心辐射型设置中，并且因为在此类设置中，辐射点更需要知道辐射点的可达性，所以解决方案是在辐射点（对等体A）上使用动态加密映射，在辐射点（对等体B）上使用隧道保护，并在辐射点上启用GRE keepalive。这样，尽管中心的 GRE 隧道接口保持打开状态，也会丢失路由邻居以及通过隧道的路由，并且可以建立备用路由。在辐射端，隧道接口关闭可能会触发打开拨号器接口并回拨到中心（或中心的其他路由器），然后建立新连接。

2. 使用除 GRE 保持连接外的方法确定对等体的可访问性。

   如果两台路由器都配置了隧道保护，则无法在任一方向上使用 GRE 隧道保持连接。在这种情况下，唯一的选择是使用路由协议或其他机制（例如服务保证代理）来确定对等体是否可访问。

3. 在对等体 A 和对等体 B 上使用加密映射。

如果两台路由器都配置了加密映射，则隧道保持连接可以在两个方向上完成，而 GRE 隧道接口可以在一个或两个方向上关闭并触发建立备份连接的操作。这是最灵活的方法。

## 相关信息

- RFC 1701，通用路由器封装 (GRE)
- RFC 2890，GRE 密钥和序列号扩展
- 通用路由封装 (GRE) 隧道Keepalive
- IP 分段和 PMTUD
- Cisco IOS 上的保持连接机制的概述
- 技术支持 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。