GRE Over IPSec VPN

[GRE Over IPSec VPN](https://ccie43413.blogspot.com/2016/#gre-over-ipsec-vpn)

* [介绍](https://ccie43413.blogspot.com/2016/#%E4%BB%8B%E7%BB%8D)
* [GRE Over IPSec VPN 介绍](https://ccie43413.blogspot.com/2016/#gre-over-ipsec-vpn-%E4%BB%8B%E7%BB%8D)
* [配置GRE Over IPSec VPN](https://ccie43413.blogspot.com/2016/#%E9%85%8D%E7%BD%AEgre-over-ipsec-vpn)
* [传输模式和隧道模式GRE Over IPSec VPN](https://ccie43413.blogspot.com/2016/#%E4%BC%A0%E8%BE%93%E6%A8%A1%E5%BC%8F%E5%92%8C%E9%9A%A7%E9%81%93%E6%A8%A1%E5%BC%8Fgre-over-ipsec-vpn)
* [参考文献](https://ccie43413.blogspot.com/2016/#%E5%8F%82%E8%80%83%E6%96%87%E7%8C%AE)

## **GRE Over IPSec VPN 介绍**

在传统IPSec VPN中需要配置多条access-list来匹配感兴趣的流，从而触发建立IPSec VPN SA，来加密业务流量，这样当流量变得复杂的时候就不利于管理，需要创建很多条access-list配置量大不容易维护。并且没有相应的接口，去维护这些流量，使得不可进行策略管理。  
但是GRE拥有良好的隧道特性，但是不具备加密、可靠性、认证功能。所以，有没有一种可能将IPSes VPN应用在GRE tunnel上呢？一方面提供了接口可以进行策略管理，另外一方面GRE tunnel 可以运行组播，保证了动态路由协议的运行，还提供的逻辑的tunnel接口可以进行策略管理。 这就是将要介绍的GRE Over IPSec VPN。

GRE相比传统IPSes VPN提供了以下特性：  
1. IP组播支持  
2. 提供逻辑接口进行策略控制  
3. 仅需配置一条感兴趣的流用于IPSec VPN建立。

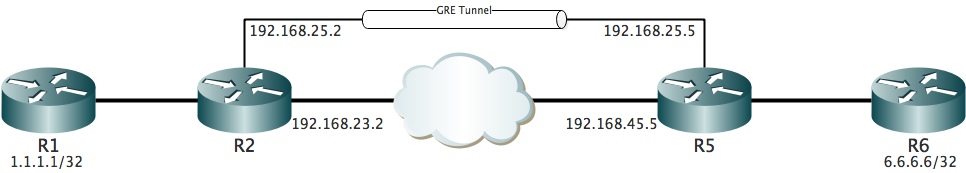
## **配置GRE Over IPSec VPN**

需求：  
1.R2和R5 之间通过GRE Tunnel建立ospf，并且传递彼此1.1.1.1和6.6.6.6的路由  
2.建立ospf更新路由表，在tunnel上的这些路由匹配ipsec vpn，进行加密，无需单独配置感兴趣的流

配置GRE Over IPSec VPN主要分为以下三个步骤：

1. 创建GRE Tunnel
2. 配置基础IPSec 策略包括（isakmp policy、isakmp key、ipsec transform-set、crypto map）
3. 配置感兴趣的流（permit gre），并且在物理接口下应用crypto map

拓扑图如下。



关键配置：

R2：

crypto isakmp policy 10

encr aes

hash md5

authentication pre-share

group 16

crypto isakmp key ccie43413 address 192.168.45.5

!

crypto ipsec transform-set ipsec-police esp-aes esp-sha512-hmac

mode transport

!

crypto map vpn 10 ipsec-isakmp

set peer 192.168.45.5

set transform-set ipsec-police

match address vpn

!

ip access-list extended vpn

permit gre host 192.168.23.2 host 192.168.45.5

!

interface Tunnel1

ip address 192.168.25.2 255.255.255.0

ip ospf 2 area 0

tunnel source 192.168.23.2

tunnel destination 192.168.45.5

!

interface Ethernet0/1

ip address 192.168.23.2 255.255.255.0

ip ospf 1 area 0

crypto map vpn

!

end

R5：

crypto isakmp policy 10

encr aes

hash md5

authentication pre-share

group 16

crypto isakmp key ccie43413 address 192.168.23.2

!

crypto ipsec transform-set ipsec-police esp-aes esp-sha512-hmac

mode transport

!

crypto map vpn 10 ipsec-isakmp

set peer 192.168.23.2

set transform-set ipsec-police

match address vpn

!

interface Tunnel1

ip address 192.168.25.5 255.255.255.0

ip ospf 2 area 0

tunnel source 192.168.45.5

tunnel destination 192.168.23.2

!

interface Ethernet0/3

ip address 192.168.45.5 255.255.255.0

ip ospf 1 area 0

crypto map vpn

!

ip access-list extended vpn

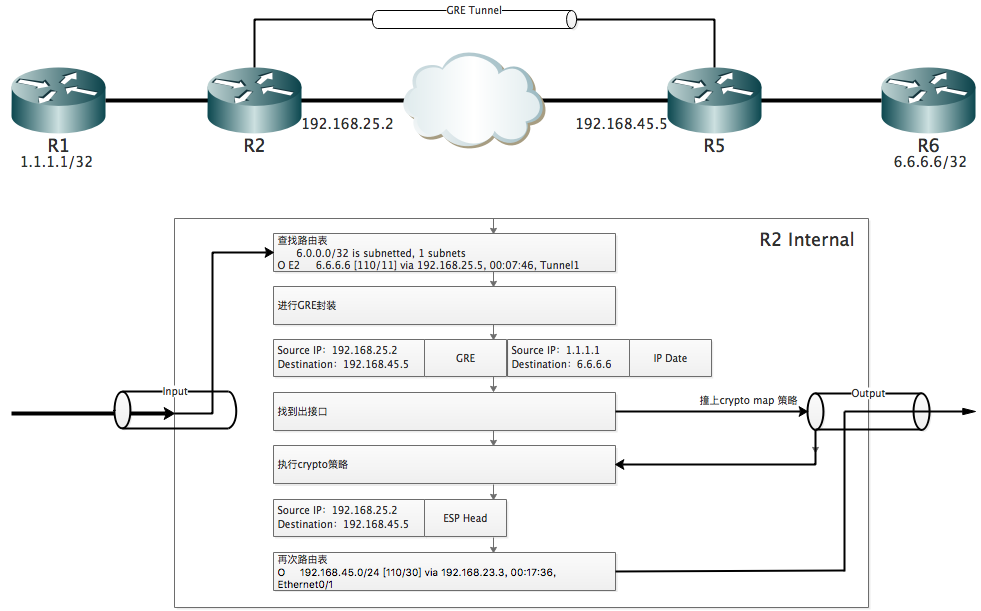
permit gre host 192.168.45.5 host 192.168.23.2

!

end

需要注意：  
1. 在配置感兴趣流的时候使用的是permit gre ，而非permit ip  
2. crypto应用在物理接口上，而非tunnel接口。

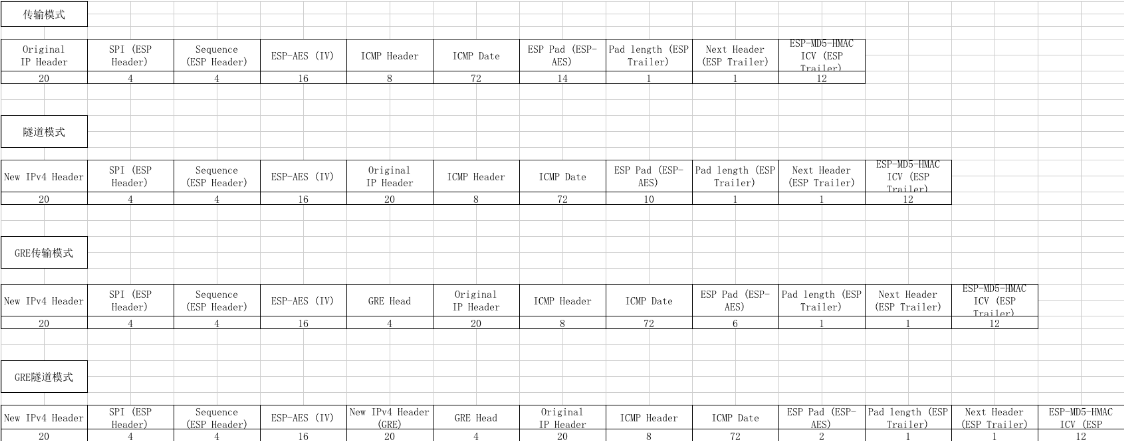
匹配感兴趣的流，需要使用permit gre而非permit ip，这是因为在进行GRE封装之后permit ip匹配的是原始IP，而非new gre ip，所以如果使用permit ip是匹配不到业务流量去触发进行SA建立的。  
第二之所以应用在物理接口上，因为如果应用在tunnel接口上，原始数据会先进行加密，再进行GRE封装，显然这样的流程是不对的。因为先加密必然需要先出去匹配感兴趣的流，这样相当于又走回之前逐条匹配感兴趣流的方式了。所以必须先进行GRE封装得到原始报文，再使用这个原始报文进行加密流程。下图列出了内部的处理流程，参考IPSec VPN实战指南。在原有的基础上加入了一些自己的理解。



可以看到，流量从入接口进入之后先去查找路由表，发现下一跳是tunnel接口，tunnel是GRE，于是先进行GRE封装，打上IP之后准备从出接口发送出去，然后因为出接口有crypto map ，正好match上了GRE的流量，执行crypto流程。完成加密和封装操作之后最后将加密后的报文从出接口发送出去。  
由此可以看到，过去进行match的时候是匹配的内网上的主机到主机。而引入了gre之后，我们只需匹配GRE 头部上的IP地址即可。这样减轻了配置压力。

## **传输模式和隧道模式GRE Over IPSec VPN**

在前面介绍过因为通信点与加密点的不同所以要使用传输模式或隧道模式。然而在GRE Tunnel中引入了新的GRE Head 和GRE IP Head错误的选择可能会造成不必要的开销。如下列出了在GRE Tunnel中传输模式和隧道模式的报文。



这里或许会有疑问，在GRE over ipsec 隧道模式中，会有三个IP头，分别是 ESP封装 NEW-IP-Head ，GRE IP和原始IP Head。那么这三者的ip地址分别是多少呢？  
笔者通过使用ESP-null 的方式获取到了数据得出如下解包。发现GRE IP和原始IP部分是一致的，所以在实际使用中如果不涉及NAT的问题，就可以使用传输模式这样可以节约24个字节的带宽，以免造成不必要的浪费。具体详见如下。

## **参考文献**

1. 《IPSec VPN实战指南》
2. [IPSec Overhead Calculator Tool](https://cway.cisco.com/tools/ipsec-overhead-calc/)