

CCNP实验：GRE隧道流量的IPSEC加密Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/581/2021\\_2022\\_CCNP\\_E5\\_AE\\_9E\\_E9\\_AA\\_8C\\_c101\\_581377.htm](https://www.100test.com/kao_ti2020/581/2021_2022_CCNP_E5_AE_9E_E9_AA_8C_c101_581377.htm) 由于IPSEC只支持对单播流量的加密，所以我们使用GRE隧道可以将广播、组播包封装在一个单播包中，再用IPSEC进行加密。在进行IPSEC配置前

应首先配置好GRE隧道，下面是R1上的GRE隧道配置：R1：

```
interface tunnel0 ip address 192.168.3.1 255.255.255.0 tunnel source s1/1 tunnel destination 192.1.1.20 exit interface s1/1 ip address 192.1.1.40 255.255.255.0 ip access-group perimeter in exit interface lo0 ip address 192.168.1.1 255.255.255.0 exit ip route 0.0.0.0 0.0.0.0 192.1.1.20 !在这里我将总公司内部的骨干网络设为Area0,隧道部分和分公司内部网络设为Area1 router ospf 1 network
```

```
192.168.1.0 0.0.0.255 area 0 network 192.168.3.0 0.0.0.255 area 1 exit ip access-list extended perimeter permit udp host 192.1.1.20 host 192.1.1.40 eq 500 permit esp host 193.1.1.20 host 192.1.1.40 permit gre host 193.1.1.20 host 192.1.1.40 deny ip any any exit R2 :
```

```
interface tunnel0 ip address 192.168.3.2 255.255.255.0 tunnel source s1/0 tunnel destination 192.1.1.40 exit interface s1/0 ip address 192.1.1.20 255.255.255.0 ip access-group perimeter in exit interface lo0 ip address 192.168.2.1 255.255.255.0 exit ip route 0.0.0.0 0.0.0.0 192.1.1.40 router ospf 1 network 192.168.2.0 0.0.0.255 area 1 network 192.168.3.0 0.0.0.255 area 1 exit ip access-list extended perimeter permit udp host 192.1.1.40 host 192.1.1.20 eq 500 permit esp host 192.1.1.40 host 192.1.1.20 permit gre host 192.1.1.40 host 192.1.1.20 deny ip any any exit GRE隧道建立好后，就可以进
```

行IPSEC配置了：R1上的配置：crypto isakmp enable crypto isakmp identity address crypto isakmp policy 10 encryption aes authentication pre-share group 2 hash sha exit crypto isakmp key cisco123 address 192.1.1.20 no-xauth !IPSEC只对进入GRE隧道的流量进行加密 ip access-list extended ToR2 permit gre host 192.1.1.40 host 192.1.1.20 exit !这里的GRE隧道是点对点模式的，所以传输集应使用传输模式 crypto ipsec transform-set trans esp-aes esp-sha-hmac mode transport exit crypto map mymap 10 ipsec-isakmp match address ToR2 set transform-set trans set peer 192.1.1.20 exit interface s1/1 crypto map mymap exit !最后别忘记删除测试隧道时建立的流量：ip access-list extended perimeter no permit gre host 192.1.1.20 host 192.1.1.40 100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)