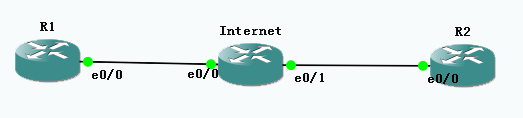
**GRE over IPSec （传统MAP实验）**

****

**R1-Internet：202.100.1.0/24**

**Internet-R2：61.128.1.0/24**

**R1 Config：**

**interface Loopback0**

**ip address 1.1.1.1 255.255.255.0**

**!**

**interface Ethernet0/0**

**ip address 202.100.1.1 255.255.255.0**

**!**

**ip route 0.0.0.0 0.0.0.0 202.100.1.10**

**crypto isakmp policy 100**

**encr 3des**

**authentication pre-share**

**group 2**

**exit**

**crypto isakmp key cisco address 61.128.1.1**

**crypto ipsec transform-set myset esp-3des esp-sha-hmac**

**mode transport**

**crypto map ccie 10 ipsec-isakmp**

**set peer 61.128.1.1**

**set transform-set myset**

**match address vpn**

**！**

**ip access-list extended vpn**

**permit gre host 202.100.1.1 host 61.128.1.1**

**interface Ethernet0/0**

**crypto map ccie**

**！**

**interface Tunnel0**

**ip address 172.16.1.1 255.255.255.0**

**tunnel source Ethernet0/0**

**tunnel destination 61.128.1.1**

**！**

**router ospf 1**

**network 1.1.1.1 0.0.0.0 area 0**

**network 172.16.1.1 0.0.0.0 area 0**

**R2 Config：**

**interface Ethernet0/0**

**ip address 202.100.1.10 255.255.255.0**

**!**

**interface Ethernet0/1**

**ip address 61.128.1.10 255.255.255.0**

**!**

**R3 Config：**

**interface Loopback0**

**ip address 2.2.2.2 255.255.255.0**

**!**

**interface Ethernet0/0**

**ip address 61.128.1.1 255.255.255.0**

**ip route 0.0.0.0 0.0.0.0 61.128.1.10**

**crypto isakmp policy 100**

**encr 3des**

**authentication pre-share**

**group 2**

**crypto isakmp key cisco address 202.100.1.1**

**crypto ipsec transform-set myset esp-3des esp-sha-hmac**

**mode transport**

**crypto map ccie 10 ipsec-isakmp**

**set peer 202.100.1.1**

**set transform-set myset**

**match address vpn**

**！**

**ip access-list extended vpn**

**permit gre host 61.128.1.1 host 202.100.1.1**

**！**

**interface Ethernet0/0**

**crypto map ccie**

**interface Tunnel0**

**ip address 172.16.1.2 255.255.255.0**

**tunnel source Ethernet0/0**

**tunnel destination 202.100.1.1**

**router ospf 1**

**network 2.2.2.2 0.0.0.0 area 0**

**network 172.16.1.2 0.0.0.0 area 0**

**！**

**测试：**

**R2#ping 172.16.1.2**

**Type escape sequence to abort.**

**Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:**

**!!!!!**

**R1#show crypto isakmp sa**

**IPv4 Crypto ISAKMP SA**

**dst src state conn-id status**

**61.128.1.1 202.100.1.1 QM\_IDLE 1001 ACTIVE**

**R1#show ip route（部分路由条目）**

**O 2.2.2.2 [110/1001] via 172.16.1.2, 00:25:57, Tunnel0**

**172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks**

**R1#show crypto engine connections active**

**Crypto Engine Connections**

**ID Type Algorithm Encrypt Decrypt LastSeqN IP-Address**

**1 IPsec 3DES+SHA 0 185 185 202.100.1.1**

**2 IPsec 3DES+SHA 188 0 0 202.100.1.1**

**1001 IKE SHA+3DES 0 0 0 202.100.1.1**