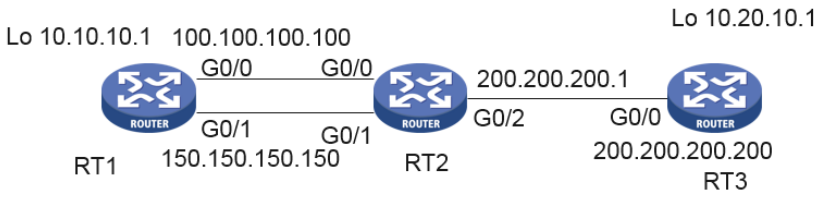
使用公网地址作为GRE隧道地址建立GRE OVER IPSEC 隧道

GRE VPN GRE VPN 杨凌轩 2019-10-18 发表

组网及说明



拓扑如上图所示

配置步骤

RT1

```
#
nqa entry admin 1
 type icmp-echo
  destination ip 192.168.2.2
  frequency 1000
  source ip 192.168.2.1
#
nqa entry admin 2
 type icmp-echo
  destination ip 192.168.2.6
  frequency 1000
  source ip 192.168.2.5
#
 nqa schedule admin 1 start-time now lifetime forever
 nqa schedule admin 2 start-time now lifetime forever
#
interface LoopBack10
 ip address 10.10.10.1 255.255.255.0
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 100.100.100.100 255.255.255.0
 nat outbound 3001
 ipsec apply policy 1
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 150.150.150.150 255.255.255.0
 nat outbound 3001
 ipsec apply policy 2
#
interface Tunnel1 mode gre
 ip address 192.168.2.1 255.255.255.252
 source 100.100.100.100
 destination 200.200.200.200
#
interface Tunnel2 mode gre
 ip address 192.168.2.5 255.255.255.252
 source 150.150.150.150
 destination 200.200.200.200
#
 ip route-static 0.0.0.0 0 100.100.100.1
```

```
 ip route-static 0.0.0.0 0 150.150.150.1 preference 70
 ip route-static 10.20.10.0 24 192.168.2.2
 ip route-static 10.20.10.0 24 192.168.2.6 preference 70
#
acl advanced 3000
 rule 0 permit ip source 100.100.100.100 0 destination 200.200.200.200 0
 rule 5 permit ip source 150.150.150.150 0 destination 200.200.200.200 0
#
acl advanced 3001
 rule 0 deny ip source 100.100.100.100 0 destination 200.200.200.200 0
 rule 5 deny ip source 150.150.150.150 0 destination 200.200.200.200 0
 rule 10 permit ip
#
acl advanced name ipsec
 rule 10 permit ip source 100.100.100.100 0 destination 200.200.200.200 0
 rule 20 permit ip source 150.150.150.150 0 destination 200.200.200.200 0
#
ipsec transform-set 1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec policy 1 10 isakmp
 transform-set 1
 security acl 3000
 remote-address 200.200.200.200
 ike-profile 1
#
ipsec policy 2 10 isakmp
 transform-set 1
 security acl 3000
 remote-address 200.200.200.200
 ike-profile 2
#
ike profile 1
 keychain 1
 match remote identity address 200.200.200.200 255.255.255.255
#
ike profile 2
 keychain 2
 keychain 1
 match remote identity address 200.200.200.200 255.255.255.255
#
ike keychain 1
 pre-shared-key address 200.200.200.200 255.255.255.255 key cipher $c$3$cgW4ni0EpiyuoDT2nn9
nYGKWx6GZlw==

RT2

#
track 1 nqa entry admin test reaction 1
#
nqa entry admin test
 type icmp-echo
  destination ip 100.100.100.100
  frequency 100
  probe count 3
  probe timeout 500
  reaction 1 checked-element probe-fail threshold-type consecutive 1 action-type trigger-only
#
 nqa schedule admin test start-time now lifetime forever
#
interface LoopBack0
 ip address 10.20.10.1 255.255.255.0
#
```

```
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 200.200.200.200 255.255.255.0
 nat outbound 3002
 ipsec apply policy ipsec

#
interface Tunnel1 mode gre
 ip address 192.168.2.2 255.255.255.252
 source 200.200.200.200
 destination 100.100.100.100
#
interface Tunnel2 mode gre
 ip address 192.168.2.6 255.255.255.252
 source 200.200.200.200
 destination 150.150.150.150
#
 ip route-static 0.0.0.0 0 200.200.200.1
 ip route-static 10.10.10.0 24 192.168.2.5 preference 70
 ip route-static 10.10.10.0 24 192.168.2.1 track 1
#
acl advanced 3000
 rule 0 permit ip source 200.200.200.200 0 destination 100.100.100.100 0
#
acl advanced 3001
 rule 0 permit ip source 200.200.200.200 0 destination 150.150.150.150 0
#
acl advanced 3002
 rule 0 deny ip source 200.200.200.200 0 destination 100.100.100.100 0
 rule 5 deny ip source 200.200.200.200 0 destination 150.150.150.150 0
 rule 10 permit ip
#
ipsec transform-set 1
 esp encryption-algorithm aes-cbc-128
 esp authentication-algorithm sha1
#
ipsec policy ipsec 1 isakmp
 transform-set 1
 security acl 3000
 remote-address 100.100.100.100
 ike-profile 1
#
ipsec policy ipsec 2 isakmp
 transform-set 1
 security acl 3001
 remote-address 150.150.150.150
 ike-profile 2
#
ike profile 1
 keychain 1
 match remote identity address 100.100.100.100 255.255.255.255
#
ike profile 2
 keychain 2
 match remote identity address 150.150.150.150 255.255.255.255
#
ike keychain 1
 pre-shared-key address 100.100.100.100 255.255.255.255 key cipher $c$3$kfQeRCcUhHUgMddb3
bZ1lGSsbuQAcw==
#
ike keychain 2
 pre-shared-key address 150.150.150.150 255.255.255.255 key cipher $c$3$YHsqyUmv6TTStZHaS
6a+8x4HnjH6gA==
```

配置关键点

1、两边的GRE地址都是公网地址，需要动态感知接口状态联动tunnel切换

2、为了进行链路探测进行切换，配置了nqa + track + 静态的联动实现gre over ipsec的链路备份