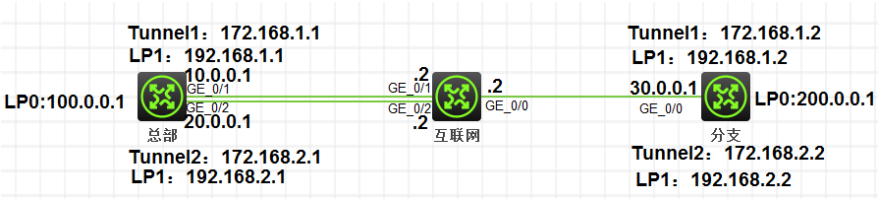
MSR G2 IPSEC双链路备份典型配置案例

孟普 2017-12-21 发表

分支只有一条拨号上网链路，地址不固定，总部有两条公网出口，实现主备。分支访问总部私网的报文需要经过IPSEC隧道保护，为了实现隧道的冗余，客户需要建立两条IPSEC链路实现主备功能。



1、配置思路：

使用GRE OVER IPSEC方式建立主备隧道。首先建立两个GRE隧道连接两边的私网互通，分支去往总部私网的路由指向主备两条GRE隧道，进入隧道后，流量打上GRE隧道的源目的地址后从公网出口出去，公网出口应用IPSEC策略，IPSEC感兴趣流设为GRE隧道的流量，这时就会匹配上IPSEC策略，受IPSEC隧道保护去往总部。因为分支出口公网地址不固定，所有使用野蛮模式，总部使用模板方式建立IPSEC。

2、总部配置

```
#//建立公网路由
ospf 1
 area 0.0.0.0
  network 10.0.0.0 0.0.0.255
  network 20.0.0.0 0.0.0.255
#
//GRE主备隧道的源地址
interface LoopBack1
 ip address 192.168.1.1 255.255.255.255
#
interface LoopBack2
 ip address 192.168.2.1 255.255.255.255
#
//模拟总部私网地址
interface LoopBack100
 ip address 100.0.0.1 255.255.255.255
#
//接口应用IPSEC策略
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 10.0.0.1 255.255.255.0
 ipsec apply policy test
#
//出接口应用IPSEC策略
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
 ip address 20.0.0.1 255.255.255.0
 ipsec apply policy test
#
//建立GRE主隧道
interface Tunnel1 mode gre
 ip address 172.168.1.1 255.255.255.0
 source 192.168.1.1
 destination 192.168.1.2
 keepalive 5 3
#
//建立GRE备隧道
interface Tunnel2 mode gre
```

```
 ip address 172.168.2.1 255.255.255.0
 source 192.168.2.1
 destination 192.168.2.2
 keepalive 5 3
#
//出口默认主备路由和到分支私网的主备路由
 ip route-static 0.0.0.0 0 10.0.0.2
 ip route-static 0.0.0.0 0 20.0.0.2 preference 80
 ip route-static 200.0.0.0 24 Tunnel1 preference 10
 ip route-static 200.0.0.0 24 Tunnel2 preference 20
#
//配置IPSEC安全提议
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//建立IPSEC模板
ipsec policy-template test 1
 transform-set 1
 ike-profile 1
#
ipsec policy-template test2 1
 transform-set 1
 ike-profile 2
#
//建立引用模板的IPSEC策略
ipsec policy test 1 isakmp template test
#
ipsec policy test 2 isakmp template test2
#
//配置ike profile,指定本地和对端地址，引用keychain
ike profile 1
 keychain 1
 exchange-mode aggressive
 match remote identity fqdn fenzhi1
#
ike profile 2
 keychain 2
 exchange-mode aggressive
 match remote identity fqdn fenzhi2
#
//配置ike keychain，设置预共享密钥
ike keychain 1
 pre-shared-key address 30.0.0.1 255.255.255.255 key cipher $c$3$w2z+ALOxUe+ovc+67udpQuMH
0NfDpLSK4w==
#
ike keychain 2
 pre-shared-key address 30.0.0.1 255.255.255.255 key cipher $c$3$qHgE/wIPxHrlgqyFdhPJUv1Ow
N7DO29IJw==
#
```

分支配置

```
#
//公网路由
ospf 1
 area 0.0.0.0
  network 30.0.0.0 0.0.0.255
#
//GRE主备隧道的源地址
interface LoopBack1
 ip address 192.168.1.2 255.255.255.255
#
```

```
interface LoopBack2
 ip address 192.168.2.2 255.255.255.255
#
//模拟分支私网路由
interface LoopBack100
 ip address 200.0.0.1 255.255.255.255
#
//接口应用IPSEC策略
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 30.0.0.1 255.255.255.0
 ipsec apply policy test
#
//连接两边私网的GRE主隧道
interface Tunnel1 mode gre
 ip address 172.168.1.2 255.255.255.0
 source 192.168.1.2
 destination 192.168.1.1
 keepalive 5 3
#
//连接两边私网的GRE主隧道
interface Tunnel2 mode gre
 ip address 172.168.2.2 255.255.255.0
 source 192.168.2.2
 destination 192.168.2.1
 keepalive 5 3
#
//出口默认路由和到总部私网的主备路由
 ip route-static 0.0.0.0 0 30.0.0.2
 ip route-static 100.0.0.0 24 Tunnel1 preference 10
 ip route-static 100.0.0.0 24 Tunnel2 preference 20
#
//配置IPSEC感兴趣流，匹配GRE隧道的源目的地址
acl advanced 3000
 rule 0 permit ip source 192.168.1.2 0 destination 192.168.1.1 0
#
acl advanced 3001
 rule 0 permit ip source 192.168.2.2 0 destination 192.168.2.1 0
#
//配置IPSEC安全提议
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC策略，指定感兴趣流、IPSEC安全提议、远端地址和IKE协商的profile
ipsec policy test 1 isakmp
 transform-set 1
 security acl 3000
 remote-address 10.0.0.1
 ike-profile center1
#
ipsec policy test 2 isakmp
 transform-set 1
 security acl 3001
 remote-address 20.0.0.1
 ike-profile center2
#
//配置ike profile,指定本地和对端地址，引用keychain
ike profile center1
 keychain 1
 exchange-mode aggressive
 local-identity fqdn fenzhi1
 match remote identity address 10.0.0.1 255.255.255.255
```

```
#
ike profile center2
 keychain 2
 exchange-mode aggressive
 local-identity fqdn fenzhi2
 match remote identity address 20.0.0.1 255.255.255.255
#
//配置ike keychain，设置预共享密钥
ike keychain 1
 pre-shared-key address 10.0.0.1 255.255.255.255 key cipher $c$3$TpzzOZNqMW6WGCqMdkqVXu
KyakVg6SHWHA==
#
ike keychain 2
 pre-shared-key address 20.0.0.1 255.255.255.255 key cipher
$c$3$ziS52yT3pnYnI+ptP3GJiGVQPQ0mo8C2SA==
#
```

3.在总部和分支查看IPSEC隧道建立的情况，可以看到已经建立了两条IPSEC隧道

总部查看隧道建立情况

```
[H3C]dis ike sa
   Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------------
   5               30.0.0.1            RD          IPsec
   6               30.0.0.1            RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY

[H3C]dis ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------
  ----------------------------
  IPsec policy: test
  Sequence number: 1
  Mode: Template
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1444
    Tunnel:
        local  address: 10.0.0.1
        remote address: 30.0.0.1
    Flow:
        sour addr: 192.168.1.1/255.255.255.255  port: 0  protocol: ip
        dest addr: 192.168.1.2/255.255.255.255  port: 0  protocol: ip
    [Inbound ESP SAs]
      SPI: 2978054563 (0xb18181a3)
      Connection ID: 73014444033
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3580
      Max received sequence-number: 8
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active
    [Outbound ESP SAs]
      SPI: 201110815 (0x0bfcb51f)
      Connection ID: 73014444032
```

```
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3580
    Max sent sequence-number: 8
    UDP encapsulation used for NAT traversal: N
    Status: Active
-------------------------------
Interface: GigabitEthernet0/1
-------------------------------
  -----------------------------
  IPsec policy: test
  Sequence number: 2
  Mode: Template
  -----------------------------
    Tunnel id: 1
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1444
    Tunnel:
        local  address: 20.0.0.1
        remote address: 30.0.0.1
    Flow:
        sour addr: 192.168.2.1/255.255.255.255  port: 0  protocol: ip
        dest addr: 192.168.2.2/255.255.255.255  port: 0  protocol: ip
    [Inbound ESP SAs]
      SPI: 1719507709 (0x667d9afd)
      Connection ID: 55834574855
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843192/2947
      Max received sequence-number: 140
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active
    [Outbound ESP SAs]
      SPI: 2983546820 (0xb1d54fc4)
      Connection ID: 47244640261
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843195/2947
      Max sent sequence-number: 135
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

分支查看隧道建立情况

```
<H3C>dis ike sa
    Connection-ID   Remote              Flag        DOI
-----------------------------------------------------------------------------
    3               10.0.0.1            RD          IPsec
    4               20.0.0.1            RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
<H3C>dis ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------
  -----------------------------
  IPsec policy: test
  Sequence number: 1
```

```
Mode: ISAKMP
-----------------------------
  Tunnel id: 1
  Encapsulation mode: tunnel
  Perfect Forward Secrecy:
  Inside VPN:
  Extended Sequence Numbers enable: N
  Traffic Flow Confidentiality enable: N
  Path MTU: 1444
  Tunnel:
     local  address: 30.0.0.1
     remote address: 10.0.0.1
  Flow:
     sour addr: 192.168.1.2/255.255.255.255  port: 0  protocol: ip
     dest addr: 192.168.1.1/255.255.255.255  port: 0  protocol: ip
  [Inbound ESP SAs]
    SPI: 201110815 (0x0bfcb51f)
    Connection ID: 2151778615298
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843198/3498
    Max received sequence-number: 40
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active
  [Outbound ESP SAs]
    SPI: 2978054563 (0xb18181a3)
    Connection ID: 47244640262
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843198/3498
    Max sent sequence-number: 40
    UDP encapsulation used for NAT traversal: N
    Status: Active
-----------------------------
IPsec policy: test
Sequence number: 2
Mode: ISAKMP
-----------------------------
  Tunnel id: 0
  Encapsulation mode: tunnel
  Perfect Forward Secrecy:
  Inside VPN:
  Extended Sequence Numbers enable: N
  Traffic Flow Confidentiality enable: N
  Path MTU: 1444
  Tunnel:
     local  address: 30.0.0.1
     remote address: 20.0.0.1
  Flow:
     sour addr: 192.168.2.2/255.255.255.255  port: 0  protocol: ip
     dest addr: 192.168.2.1/255.255.255.255  port: 0  protocol: ip
  [Inbound ESP SAs]
    SPI: 2983546820 (0xb1d54fc4)
    Connection ID: 73014444032
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843195/2832
    Max received sequence-number: 135
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active
```

[Outbound ESP SAs]
SPI: 1719507709 (0x667d9afd)
Connection ID: 1043677052929
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843191/2832
Max sent sequence-number: 156
UDP encapsulation used for NAT traversal: N
Status: Active

4.隧道测试，在分支长ping总部私网，并模拟总部公网主链路不通后的情景，主备切换时会有少量丢包

<H3C>ping -a 200.0.0.1 -c 200 100.0.0.1
Ping 100.0.0.1 (100.0.0.1) from 200.0.0.1: 56 data bytes, press CTRL_C to break
56 bytes from 100.0.0.1: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 100.0.0.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=27 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=30 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=31 ttl=255 time=1.000 ms
Request time out
Request time out
Request time out
Request time out
Request time out
Request time out
Request time out
Request time out
56 bytes from 100.0.0.1: icmp_seq=40 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=41 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=42 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=43 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=44 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=45 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=46 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=47 ttl=255 time=1.000 ms
56 bytes from 100.0.0.1: icmp_seq=48 ttl=255 time=2.000 ms

IPSEC隧道的主备是由GRE隧道的主备决定的，GRE隧道通过Keepalive报文保活，而且IPSEC的建立不需要实际业务流触发，keepalive报文就是IPSEC的感兴趣流，自动触发IPSEC隧道建立并保活。GRE主隧道UP时业务流量从GRE O IPSEC主隧道访问总部，总部主链路物理DOWN后，通过探测报文使主隧道DOWN掉，分支去往总部的路由下一跳就会指向GRE的备隧道TUNNEL2,从而实现主备功能。