MSR-G2系列路由器GRE Over IPSec+OSPF穿越NAT多分支互通的配置

高贵贤 2013-07-22 发表

MSR-G2系列路由器
GRE Over IPSec+OSPF穿越NAT多分支互通的配置

一、 组网需求

总部对多个分支提供IPSEC VPN接入，分支出口存在NAT设备，因此总部与分支之间配制成野蛮模式和NAT穿越，总部路由器使用安全模版方式，总部和分支之间通过内网环回口Loopback建立GRE隧道，分支通过配置ACL使分支环回接口和总部环回接口之间的GRE通过IPSEC互通，建立好GRE隧道后，在隧道上运行OSPF，使各内网路由互通，分支之间的流量通过总部转发，需要注意的是环回接口不能通告进OSPF中
设备清单：MSR G2路由器3台

二、 组网图

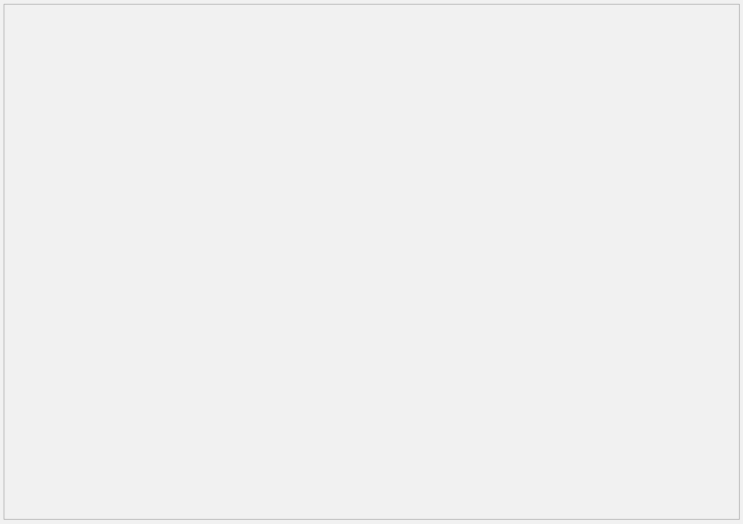

图1 MSR-G2系列路由器GRE over IPsec with OSPF 穿越NAT组网图

三、 配置步骤

使用版本: E0006P05

Router1配置：

```
//配置OSPF，通告总部内网地址，分支机构一的GRE隧道地址和分支结构二的GRE隧道地址
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 11.11.11.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
//配置环回口loopback0，用于建立GRE连接并作为OSPF的Router ID
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
//配置环回口Loopback1，用于模拟内网用户
interface LoopBack1
 ip address 11.11.11.11 255.255.255.255
#
//配置接口GigabitEthernet0/0，并调用IPSEC策略
interface GigabitEthernet0/0
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 ipsec apply policy 123
#
//配置和分支一建立GRE隧道的tunnel0虚拟接口，封装源地址为本端环回“0”口，封装目的地址为R4的环回“0”口
```

```
interface Tunnel0 mode gre
 ip address 192.168.1.1 255.255.255.0
 source LoopBack0
 destination 4.4.4.4
//配置和分支二建立GRE隧道的tunnel0虚拟接口，封装源地址为本端环回“0”口，封装目的地址为R5的环回“0”口
interface Tunnel1 mode gre
 ip address 192.168.2.1 255.255.255.0
 source LoopBack0
 destination 5.5.5.5
#
//配置静态路由，到达R4的静态路由下一跳指向10.1.1.2；到达R5的静态路由下一跳指向10.1.1.3
ip route-static 4.4.4.0 24 10.1.1.2
ip route-static 5.5.5.0 24 10.1.1.3
#
//配置IPSEC提议，使用的加密算法为3des-cbc;使用的认证算法为MD5
ipsec transform-set 123
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC策略模版321，调用IPSEC功能集和ike  profile，并指定本端地址为10.1.1.1，此策略模版用于和R4建立隧道
ipsec policy-template 321 1
 transform-set 123
 local-address 10.1.1.1
 ike-profile 123
#
//配置IPSEC策略模版1234，调用IPSEC功能集和Ike  profile，并指定本端地址为10.1.1.1，此策略模版用于和R5建立隧道
ipsec policy-template 1234 1
 transform-set 123
 local-address 10.1.1.1
 ike-profile 1234
//配置IPSEC策略123，调用两个策略模版
ipsec policy 123 1 isakmp template 321
#
ipsec policy 123 2 isakmp template 1234
#
//配置标识设备的方式为使用User-fqdn
 ike identity user-fqdn
#
//配置ike profile,调用ike钥匙链1，指定使用野蛮模式建立隧道，匹配对端名字为R4，此ike框架用于和R4建立隧道
ike profile 123
 keychain 1
 exchange-mode aggressive
 match remote identity user-fqdn R4
#
//配置ike profile,调用ike钥匙链2，指定使用野蛮模式建立隧道，匹配对端名字为R5，此ike框架用于和R5建立隧道
ike profile 1234
 keychain 2
 exchange-mode aggressive
 match remote identity user-fqdn R5
//配置IKE钥匙链1，PSK后跟对端名称，密钥使用123
ike keychain 1
 pre-shared-key hostname R4 key cipher
$c$3$ofQ1qstshCzEqAVUbnTbJMVdd3JPkw==
#
//配置IKE钥匙链2，PSK后跟端对名称，密钥使用123
ike keychain 2
 pre-shared-key hostname R5 key cipher
$c$3$ofQ1qstshCzEqAVUbnTbJMVdd3JPkw==
```

Router4配置：

```
//配置OSPF，通告GRE隧道接口和内网口地址loopback1
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.0
  network 44.44.44.44 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
//配置环回口Loopback0,用户建立GRE隧道，并作为OSPF进程的RID
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
//配置环回口loopback1,用于模拟内网用户
interface LoopBack1
 ip address 44.44.44.44 255.255.255.255
#
//配置接口GigabitEthernet0/1，调用IPSEC策略
interface GigabitEthernet0/1
 port link-mode route
 ip address 20.1.1.2 255.255.255.0
 ipsec apply policy 123
#
//配置和总部建立GRE隧道使用的tunnel口，封装源地址为Looback0,封装目的地址为总部环回口loopback0
interface Tunnel0 mode gre
 ip address 192.168.1.2 255.255.255.0
 source LoopBack0
 destination 1.1.1.1
#
//配置默认路由，下一跳指向Router2的内联口地址20.1.1.1
 ip route-static 0.0.0.0 0 20.1.1.1
#
//配置安全ACL，匹配本端环回口Loopback0和总部环回口loopback0地址
acl number 3000
 rule 0 permit ip source 4.4.4.4 0 destination 1.1.1.1 0
#
//配置IPSEC提议，使用加密算法为3des-cbc,使用认证算法为MD5
ipsec transform-set 123
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC策略，调用IPSEC提议、安全ACL、Ike框架并指定对端地址为10.1.1.1
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 remote-address 10.1.1.1
 ike-profile 123
#
//配置标识设备的方式为User-fqdn
 ike identity user-fqdn
#
//配置ike profile,调用钥匙链，指定使用野蛮模式，本端user-fqdn为R4
ike profile 123
 keychain 1
 exchange-mode aggressive
 local-identity user-fqdn R4
 match remote identity address 10.1.1.1 255.255.255.255
#
//配置IKE钥匙链，对端地址为10.1.1.1，密钥使用123
ike keychain 1
 pre-shared-key address 10.1.1.1 255.255.255.255 key cipher $c$3$WSf0/ldh1ulP37LdsezZEUbEa6HjeQ==
#
```

Router5配置：

```
//配置OSPF，通告GRE隧道接口和内网口地址loopback1
#
ospf 1 router-id 5.5.5.5
 area 0.0.0.0
  network 55.55.55.55 0.0.0.0
  network 192.168.2.0 0.0.0.255
#
//配置环回口Loopback0,用户建立GRE隧道，并作为OSPF进程的RID
interface LoopBack0
 ip address 5.5.5.5 255.255.255.255
#
//配置环回口loopback1,用于模拟内网用户
interface LoopBack1
 ip address 55.55.55.55 255.255.255.255
#
//配置接口GigabitEthernet0/1，调用IPSEC策略
interface GigabitEthernet0/1
 port link-mode route
 ip address 30.1.1.2 255.255.255.0
 ipsec apply policy 123
#
//配置和总部建立GRE隧道使用的tunnel口，封装源地址为Looback0,封装目的地址为总部环回口loopback0
interface Tunnel0 mode gre
 ip address 192.168.2.2 255.255.255.0
 source LoopBack0
 destination 1.1.1.1
#
//配置默认路由，下一跳指向Router2的内联口地址20.1.1.1
 ip route-static 0.0.0.0 0 30.1.1.1
#
//配置安全ACL，匹配本端环回口Loopback0和总部环回口loopback0地址

acl number 3000
 rule 0 permit ip source 5.5.5.5 0 destination 1.1.1.1 0
#
//配置IPSEC提议，使用加密算法为3des-cbc,使用认证算法为MD5
ipsec transform-set 123
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC策略，调用IPSEC提议、安全ACL、Ike框架并指定对端地址为10.1.1.1
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 remote-address 10.1.1.1
 ike-profile 123
#
//配置标识设备的方式为User-fqdn
 ike identity user-fqdn
#
//配置ike profile,调用钥匙链，指定使用野蛮模式，本端user-fqdn为R5
ike profile 123
 keychain 1
 exchange-mode aggressive
 local-identity user-fqdn R5
 match remote identity address 10.1.1.1 255.255.255.255
#
//配置IKE钥匙链，对端地址为10.1.1.1，密钥使用123
ike keychain 1
 pre-shared-key address 10.1.1.1 255.255.255.255 key cipher $c$3$WSf0/ldh1ulP37LdsezZEUbEa6HjeQ==
#
```

四、 验证过程

```
[Router1]display  ip routing-table
44.44.44.44/32      OSPF   10   1562        192.168.1.2     Tun0
55.55.55.55/32      OSPF   10   1562        192.168.2.2     Tun1

[Router1]display ike  sa
   Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------------------
2              10.1.1.2            RD          IPSEC
2              10.1.1.3            RD          IPSEC

[Router1]display ipsec sa //仅截取Router1和R4之间的IPSEC SA
------------------------------
Interface: GigabitEthernet0/0
------------------------------


 ----------------------------
 IPsec policy: 123
 Sequence number: 1
 Mode: template
 ----------------------------
   Tunnel id: 0
   Encapsulation mode: tunnel
   Perfect forward secrecy:
   Path MTU: 1435
   Tunnel:
       local  address: 10.1.1.1
       remote address: 10.1.1.2
   Flow:
   sour addr: 1.1.1.1/255.255.255.255  port: 0  protocol: ip
   dest addr: 4.4.4.4/255.255.255.255  port: 0  protocol: ip

   [Inbound ESP SAs]
     SPI: 315410071 (0x12ccc697)
     Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
     SA duration (kilobytes/sec): 1843200/3600
     SA remaining duration (kilobytes/sec): 1843187/2265
     Max received sequence-number: 142
     Anti-replay check enable: Y
     Anti-replay window size: 64
     UDP encapsulation used for nat traversal: Y
     Status: active

   [Outbound ESP SAs]
     SPI: 1404173757 (0x53b1fdbd)
     Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
     SA duration (kilobytes/sec): 1843200/3600
     SA remaining duration (kilobytes/sec): 1843194/2265
     Max sent sequence-number: 58
     UDP encapsulation used for nat traversal: Y
     Status: active
```

五、 配置关键点

1. 上述部分配置可以参考IPSec VPN多分支NAT穿越模版方式功能的配置；
2. 分支的ACL可以配置成精确的GRE流量；
3. 建立GRE隧道的地址必须是内网地址；
4. 不能将建立GRE隧道连接的环回接口接入到OSPF中，否则连接会失效；
5. 配置IKE框架（profile），调用keychain、配置野蛮模式等，V5设备在IKE peer中进行配置；
6. V7设备预共享密钥在IKE keychain中配置，V5设备在IKE peer中配置；
7. ipsec安全策略下（ipsec transform-set）默认是没有加密和认证方法的，这点需要注意。