MSR-G2系列路由器GRE over ipsec with ospf的典型配置

高贵贤 2013-07-22 发表

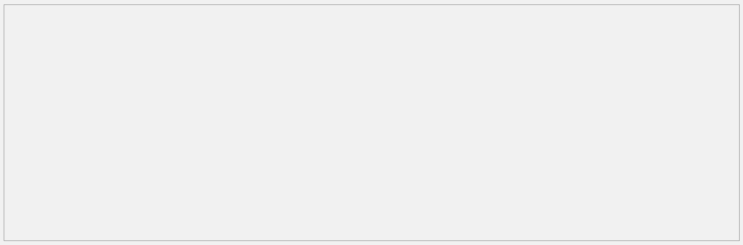
MSR-G2系列路由器
gre over ipsec with ospf的典型配置

一、组网需求

Router1模拟分部出口路由器，Router3模拟总部出口路由器，对分支机构提供GRE OVER IPSEC接入；总部和分支在GRE隧道上启动OSPF路由协议，传送总部和分支的路由信息，该配置实际应用较多，既可以运行OSPF等IGP路由协议，又能对所有总部和分部之间的流量进行加密。

设备清单：MSR G2路由器3台

二、组网图



图一 MSR-G2路由器 GRE over IPSEC with OSPF组网图

三、配置步骤

使用版本：E0006P05

Router1配置：

```
//配置OSPF协议，通告环回口地址和tunnel口地址
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 100.1.1.0 0.0.0.255
#
//配置环回口模拟内网用户
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
//配置接口GigabitEthernet2/0/0，调用IPSEC策略
#
interface GigabitEthernet2/0/0
 port link-mode route
 combo enable copper
ip address 10.1.1.1 255.255.255.0
 ipsec apply policy 123
#
//配置tunnel接口，模式为gre，封装源地址为本端物理口地址，目的地址为Router3的物理口地址
interface Tunnel0 mode gre
 ip address 100.1.1.1 255.255.255.0
 source 10.1.1.1
 destination 20.1.1.2
//配置静态路由，下一跳为10.1.1.2
#
ip route-static 20.1.1.0 24 10.1.1.2
#
//配置安全ACL，保护数据流为tunnel口封装的源、目地址
acl number 3000
 rule 0 permit ip source 10.1.1.1 0 destination 20.1.1.2 0
#
//配置IPSEC提议，加密类型为3des-cbc,认证方式为MD5
ipsec transform-set 123
```

```
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
//配置IPSEC策略，调用安全ACL，IPSEC提议，指定对端地址为Router3物理口地址
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 remote-address 20.1.1.2
#
//配置Ike钥匙链，PSK为123
ike keychain 1
pre-shared-key address 20.1.1.2 255.255.255.255 key cipher
$c$3$ZjXBWzdem34rj6XvnVx7ikq+ARmh+g==
```

Router3配置:

```
//配置OSPF，通过本端环回口和tunnel口地址
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 100.1.1.0 0.0.0.255
#
//配置环回口地址，模拟内网用户
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
//配置接口GigabitEthernet0/1，并调用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tunnel0口，模式为gre，封装源地址为本端物理口地址，目的地址为Router1物
理口地址
interface Tunnel0 mode gre
 ip address 100.1.1.2 255.255.255.0
 source 20.1.1.2
 destination 10.1.1.1
#
//配置静态路由，下一跳指向20.1.1.1
 ip route-static 10.1.1.0 24 20.1.1.1
#
//配置安全ACL,与Router1的安全ACL保护数据互为镜像
acl number 3000
 rule 0 permit ip source 20.1.1.2 0 destination 10.1.1.1 0
#
//配置IPSEC提议，使用加密算法为3des-cbc,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、指定对端地址为Router1的物理口地
址
ipsec policy 123 1 isakmp
 transform-set 123
 security acl 3000
 remote-address 10.1.1.1
#
//配置ike钥匙链，PSK为123
ike keychain 1
 pre-shared-key address 10.1.1.1 255.255.255.255 key cipher $c$3$wJMvMgdr+Mnq
kgnyro+jTFIfJdTQHw==
#
```

四、验证配置

```
<Router1>display ip routing-table
```

```
Destinations : 20       Routes : 20

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
1.1.1.1/32          Direct 0    0           127.0.0.1       InLoop0
2.2.2.2/32          Static 60   0           10.1.1.254      GE2/0/0
3.3.3.3/32          OSPF   10   1562        100.1.1.2       Tun0
//Router1已经学习到了Router3的环回口地址

<Router3>display ip routing-table

Destinations : 19       Routes : 19

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
1.1.1.1/32          OSPF   10   1562        100.1.1.1       Tun0
//Router3学习到了Router1的环回口地址
<Router1>display ike  sa
   Connection-ID   Remote              Flag         DOI
-----------------------------------------------------------------------------
27              20.1.1.2            RD           IPSEC
Flags:
//IKE SA已经存在

IPSEC SA也存在:
<Router1>display ipsec sa
-------------------------------
Interface: GigabitEthernet2/0/0
-------------------------------

 ------------------------------
 IPsec policy: 123
 Sequence number: 1
 Mode: isakmp
 ------------------------------
   Tunnel id: 0
   Encapsulation mode: tunnel
   Perfect forward secrecy:
   Path MTU: 1443
   Tunnel:
       local  address: 10.1.1.1
       remote address: 20.1.1.2
   Flow:
   sour addr: 10.1.1.1/255.255.255.255  port: 0  protocol: ip
   dest addr: 20.1.1.2/255.255.255.255  port: 0  protocol: ip

   [Inbound ESP SAs]
     SPI: 1504282990 (0x59a9896e)
     Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
     SA duration (kilobytes/sec): 1843200/3600
     SA remaining duration (kilobytes/sec): 1843200/3549
     Max received sequence-number: 0
     Anti-replay check enable: Y
     Anti-replay window size: 64
     UDP encapsulation used for nat traversal: N
     Status: active

   [Outbound ESP SAs]
     SPI: 738374673 (0x2c02b411)
     Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
     SA duration (kilobytes/sec): 1843200/3600
     SA remaining duration (kilobytes/sec): 1843199/3549
     Max sent sequence-number: 1
```

```
    UDP encapsulation used for nat traversal: N
    Status: active

------------------------------
IPsec policy: 123
Sequence number: 1
Mode: isakmp
------------------------------
  Tunnel id: 0
  Encapsulation mode: tunnel
  Perfect forward secrecy:
  Path MTU: 1443
  Tunnel:
      local  address: 10.1.1.1
      remote address: 20.1.1.2
  Flow:
  sour addr: 10.1.1.1/255.255.255.255  port: 0  protocol: ip
  dest addr: 20.1.1.2/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 3748049068 (0xdf66b0ac)
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3521
    Max received sequence-number: 2
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for nat traversal: N
    Status: active

  [Outbound ESP SAs]
    SPI: 499347401 (0x1dc36fc9)
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3521
    Max sent sequence-number: 2
    UDP encapsulation used for nat traversal: N
    Status: active

------------------------------
IPsec policy: 123
Sequence number: 1
Mode: isakmp
------------------------------
  Tunnel id: 0
  Encapsulation mode: tunnel
  Perfect forward secrecy:
  Path MTU: 1443
  Tunnel:
      local  address: 10.1.1.1
      remote address: 20.1.1.2
  Flow:
  sour addr: 10.1.1.1/255.255.255.255  port: 0  protocol: ip
  dest addr: 20.1.1.2/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 2748716393 (0xa3d61569)
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843190/3559
    Max received sequence-number: 161
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for nat traversal: N
```

Status: active

[Outbound ESP SAs]
SPI: 1018788745 (0x3cb97b89)
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843191/3559
Max sent sequence-number: 118
UDP encapsulation used for nat traversal: N
Status: active

五、配置关键点

1. 如果存在多分支情况，则总部安全ACL中不能存在deny规则，否则可能造成部分分支不通的情况；
2. 分支ACL和总部ACL互为镜像；
3. IPSEC策略绑定在物理接口，并且此物理接口不能被通告进OSPF进程；
4. 保证总部和分部的外网地址是可以互通的；
5. V7中Tunnel虚接口的配置不同于V5，需要指定模式；
6. V7中需要定义钥匙链，配置预共享密钥；
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。