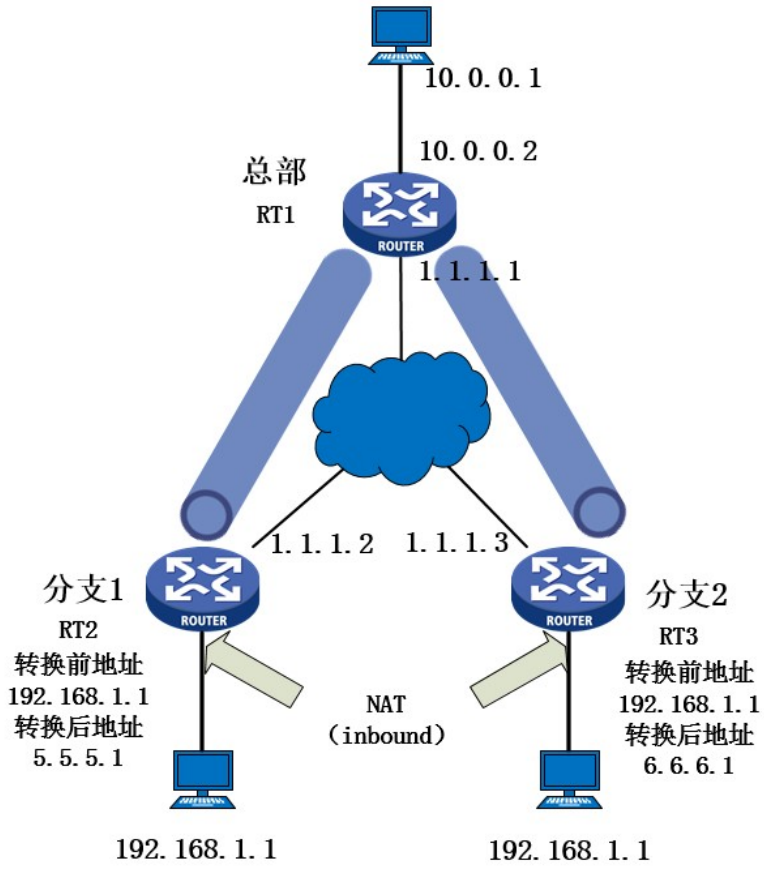
MSR56系列路由器建立IPSec VPN 分支地址重叠经验案例

茆新楼 2017-12-16 发表

RT1为总部路由器，RT2和RT3为分支路由器，两个分支需要通过ipsec vpn与总部内网互访，分支之间无需互访。目前两个分支的内网网段地址出现重叠情况，此时会有地址冲突的问题，从而导致IPSec无法正常通信。



客户现场做ipsec vpn，由于两个分支内网地址冲突，不可以直接将分支内网网段作为源地址去访问总部。此时可以在分支路由器连接PC的接口做nat，方向为inbound，先转换源地址再进行IPSec封装，从而解决地址冲突的问题。

在连接终端的两个分支路由器接口上做nat，方向为inbound，分支访问总部时数据包会先匹配nat，转换报文源地址后再去访问总部内网。配置IPSec的ACL感兴趣流时是转换后的地址。

关键配置如下：

1、 总部RT1配置

1）配置路由（5.5.5.1/6.6.6.1分别是分支1和分支2内网用户转换后的地址）

```
#
 ip route-static 5.5.5.1 32 1.1.1.2
 ip route-static 6.6.6.1 32 1.1.1.3
```

2）配置IPSec感兴趣流

```
#
acl advanced 3000
 rule 0 permit ip source 10.0.0.0 0.0.0.255 destination 5.5.5.1 0
#
acl advanced 3001
 rule 0 permit ip source 10.0.0.0 0.0.0.255 destination 6.6.6.1 0
```

3）配置ipsec transform-set

```
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
```

4）配置ipsec policy

```
#
ipsec policy 1 1 isakmp
```

```
 transform-set 1
 security acl 3000
 local-address 1.1.1.1
 remote-address 1.1.1.2
 ike-profile 1
#
ipsec policy 1 2 isakmp
 transform-set 1
 security acl 3001
 local-address 1.1.1.1
 remote-address 1.1.1.3
 ike-profile 2
#
ike profile 1
 keychain 1
 exchange-mode aggressive
 local-identity address 1.1.1.1
 match remote identity address 1.1.1.2 255.255.255.255
 proposal 1
#
ike profile 2
 keychain 2
 exchange-mode aggressive
 local-identity address 1.1.1.1
 match remote identity address 1.1.1.3 255.255.255.255
 proposal 1
#
ike proposal 1
#
ike keychain 1
 pre-shared-key address 1.1.1.2 255.255.255.0 key cipher
$c$3$sGuOVE3VO5vnH84q/ZJ3jhLw8dOnnA==
#
ike keychain 2
 pre-shared-key address 1.1.1.3 255.255.255.0 key cipher
$c$3$0RAKLYAKVH42xSYqe2J4V/1uOoKrpg==
```

5）接口调用ipsec policy

```
#
interface GigabitEthernet0/0
ip address 1.1.1.1 255.255.255.0
 ipsec apply policy 1
```

6）连接pc端口

```
#
interface GigabitEthernet0/2
ip address 10.0.0.2 255.255.255.0
#
Return
```

2、分支RT2配置

1）配置路由去往总部的路由，特别注意的是，在分支路由器上需要配置一条去往转换后地址的路由，下一跳指向PC。

```
#
 ip route-static 5.5.5.1 32 192.168.1.1
 ip route-static 10.0.0.0 24 1.1.1.1
```

2）配置nat数据流

```
#
acl basic 2000
 rule 0 permit source 192.168.1.0 0.0.0.255
```

3）配置nat地址池

```
#
nat address-group 1
 address 5.5.5.1 5.5.5.1
```

4）配置IPSec感兴趣流

```
#
acl advanced 3000
```

```
 rule 0 permit ip source 5.5.5.1 0 destination 10.0.0.0 0.0.0.255
```
5）IPSec 相关配置
```
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3000
 remote-address 1.1.1.1
 ike-profile 1
#
ike profile 1
 keychain 1
 exchange-mode aggressive
 local-identity address 1.1.1.2
 match remote identity address 1.1.1.1 255.255.255.255
 proposal 1
#
ike proposal 1
#
ike keychain 1
 pre-shared-key address 1.1.1.1 255.255.255.0 key cipher $c$3$Zwi7XcMUVOsHP9EfKseIgiHdwGc
mOA==
```
6）物理接口调用ipsec policy
```
#
interface GigabitEthernet0/0
ip address 1.1.1.2 255.255.255.0
 ipsec apply policy 1
```
7）连接PC端口
```
#
interface GigabitEthernet0/1
ip address 192.168.1.2 255.255.255.0
 nat inbound 2000 address-group 1 no-pat
#
Return
```
3、 分支RT3配置

1）配置路由去往总部的路由
```
#
 ip route-static 6.6.6.1 32 192.168.1.1
 ip route-static 10.0.0.0 24 1.1.1.1
```
2）配置nat数据流
```
#
acl basic 2000
 rule 0 permit source 192.168.1.0 0.0.0.255
```
3）配置nat地址池
```
#
nat address-group 1
 address 6.6.6.1 6.6.6.1
```
4）配置IPSec感兴趣流
```
#
acl advanced 3000
 rule 0 permit ip source 6.6.6.1 0 destination 10.0.0.0 0.0.0.255
```
5）IPSec 相关配置
```
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy 1 1 isakmp
 transform-set 1
 security acl 3000
 local-address 1.1.1.3
```

```
 remote-address 1.1.1.1
 ike-profile 1
#
ike profile 1
 keychain 1
 exchange-mode aggressive
 local-identity address 1.1.1.3
 match remote identity address 1.1.1.1 255.255.255.255
#
ike proposal 1
#
ike keychain 1
 pre-shared-key address 1.1.1.1 255.255.255.0 key cipher $c$3$+4wX3GLf/EDkATxVZuay7rzXxWC
+kg==
```

6）物理接口调用ipsec policy

```
#
interface GigabitEthernet0/0
ip address 1.1.1.3 255.255.255.0
 ipsec apply policy 1
```

7）连接PC端口

```
#
interface GigabitEthernet0/1
ip address 192.168.1.2 255.255.255.0
 nat inbound 2000 address-group 1 no-pat
#
Return
```

4、在总部查看IPSec结果

```
<RT1>dis ike sa
   Connection-ID   Remote              Flag        DOI
-------------------------------------------------------------------------
   1               1.1.1.2             RD          IPsec
   2               1.1.1.3             RD          IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
<RT1>dis ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------


  ------------------------------
  IPsec policy: 1
  Sequence number: 1
  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: 1.1.1.1
        remote address: 1.1.1.2
    Flow:
        sour addr: 10.0.0.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 5.5.5.1/255.255.255.255  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 2477823243 (0x93b0950b)
      Connection ID: 4294967296
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3573
```

```
    Max received sequence-number: 4
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 4241327730 (0xfccd8672)
    Connection ID: 4294967297
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3573
    Max sent sequence-number: 4
    UDP encapsulation used for NAT traversal: N
    Status: Active

-----------------------------
IPsec policy: 1
Sequence number: 2
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: 1.1.1.1
      remote address: 1.1.1.3
  Flow:
      sour addr: 10.0.0.0/255.255.255.0  port: 0  protocol: ip
      dest addr: 6.6.6.1/255.255.255.255  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 3732879194 (0xde7f375a)
    Connection ID: 4294967298
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3585
    Max received sequence-number: 4
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 177459744 (0x0a93d220)
    Connection ID: 4294967299
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/3585
    Max sent sequence-number: 4
    UDP encapsulation used for NAT traversal: N
    Status: Active
```

客户现场做IPSec VPN时，当分支内网地址出现冲突时，总部路由无法正常配置。如果在分支上先将私网地址转换掉，然后再去进行IPSec封装，这样就可以解决地址冲突的问题。

需要特别注意的是，在分支上做nat inbound时，需要配置一条指向转换后地址的路由，下一跳指向PC。否则数据包到达分支路由器后无法找到去往5.5.5.1/6.6.6.1的路由，从而导致无法正常通信。