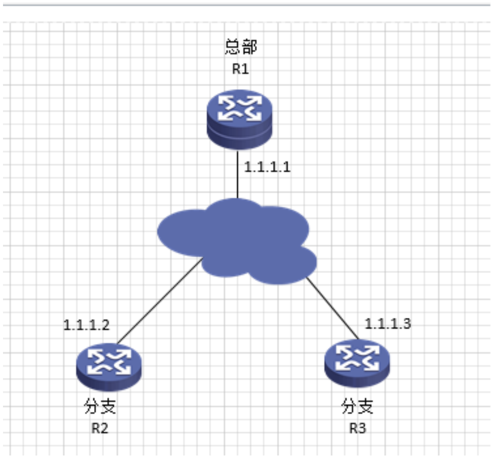
GRE over IPSEC分支地址重叠经验案例

ipoe IPsec 江浩 2016-01-28 发表

R1是总部路由器（V5平台），R2，R3为分支路由器（V7平台）。分支都要能够通过ipsec访问总部，并且需要通过ospf学习到总部路由。分支之间不需要互访。但是两个分支的内网网段地址重叠，都是192.168.1.0网段，会有地址冲突的情况。



IP地址规划如下:

设备	外网口IP	内网口IP	Tunnel口IP
R1	1.1.1.1/24	100.0.0.1	TUN1:12.0.0.1/24 TUN2:13.0.0.1/24
R2	1.1.1.2/24	192.168.1.1/24	12.0.0.2/24
R3	1.1.1.3/24	192.168.1.1/24	13.0.0.3/24

由于客户需要分支通过ospf学习到总部路由，因此可考虑使用gre over ipsec的方案。但是由于分支端ip地址重叠，所以不能直接将分支端的网段通过ospf发给总部。解决的方法就是，在gre tunnel口上做一次nat，将分支的内网ip转换成tunnel口的ip来解决地址重叠的问题。

1. 总部R1配置:

1）配置GRE tunnel，源是本端外网口IP，目的是对端外网口IP

```
#
interface Tunnel1
 ip address 12.0.0.1 255.255.255.0
 source 1.1.1.1
 destination 1.1.1.2
#
interface Tunnel2
 ip address 13.0.0.1 255.255.255.0
 source 1.1.1.1
 destination 1.1.1.3
#
```

2）配置感兴趣流

```
#
acl number 3000
 rule 0 permit ip source 1.1.1.1 0 destination 1.1.1.2 0
acl number 3001
 rule 0 permit ip source 1.1.1.1 0 destination 1.1.1.3 0
#
```

在gre over ipsec的情况下，数据先进行gre封装，再进行ipsec加密。因此ipsec感兴趣流的源和目的IP是经过gre封装后的IP，也就是gre tunnel的 source和destination。

3）配置ike peer

```
#
ike peer r2
 pre-shared-key cipher $c$3$UYUBC/5zGBw77ZgZDLniBXst6B7ejQ==
 remote-address 1.1.1.2
#
ike peer r3
 pre-shared-key cipher $c$3$cUNdODztbuXP26+JFs3boP5G07NwMA==
 remote-address 1.1.1.3
#
```

4）配置ipsec transform-set

```
#
ipsec transform-set 1
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm md5
 esp encryption-algorithm 3des
#
```

5）配置 ipsec policy

```
#
ipsec policy 1 10 isakmp
 security acl 3000
 ike-peer r2
 transform-set 1
#
ipsec policy 1 20 isakmp
 security acl 3001
 ike-peer r3
 transform-set 1
#
```

6）物理接口下调用ipsec policy

```
#
interface Ethernet0/0
 port link-mode route
 ip address 1.1.1.1 255.255.255.0
 ipsec policy 1
#
```

7）配置ospf，把内网口和tunnel口宣告进ospf

```
#
ospf 1
 area 0.0.0.0
  network 100.0.0.1 0.0.0.0
  network 12.0.0.1 0.0.0.0
  network 13.0.0.1 0.0.0.0
#
```

2. 分支R2配置：

1）配置GRE tunnel

```
#
interface Tunnel0 mode gre
 ip address 12.0.0.2 255.255.255.0
 source 1.1.1.2
 destination 1.1.1.1
 nat outbound
#
```

Tunnel口上配置nat outbound，数据包经过tunnel口时，会先将源地址转换为tunnel口的地址，再进行gre封装。

2）配置感兴趣流

```
#
acl advanced 3000
 rule 0 permit ip source 1.1.1.2 0 destination 1.1.1.1 0
#
```

3）配置ipsec策略

```
#
```

```
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy 1 10 isakmp
 transform-set 1
 security acl 3000
 remote-address 1.1.1.1
 ike-profile 1
#
ike profile 1
 keychain 1
 match remote identity address 1.1.1.1 255.255.255.255
#
ike keychain 1
 pre-shared-key address 1.1.1.1 255.255.255.255 key cipher
$c$3$Zjh8lqvsPg27z8WHRa4jIDOoxCmrjQ==
#
```

4）物理接口下调用ipsec policy

```
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 1.1.1.2 255.255.255.0
 ipsec apply policy 1
#
```

5）配置ospf，把内网口和tunnel口宣告进ospf

```
#
ospf 1
 area 0.0.0.0
  network 12.0.0.2 0.0.0.0
#
```

注意不要把内网口宣告进ospf。

3. 分支R3配置：

1）配置GRE tunnel

```
#
interface Tunnel0 mode gre
 ip address 13.0.0.3 255.255.255.0
 source 1.1.1.3
 destination 1.1.1.1
 nat outbound
#
```

Tunnel口上配置nat outbound，数据包经过tunnel口时，会先将源地址转换为tunnel口的地址，再进行gre封装。

2）配置感兴趣流

```
#
acl advanced 3000
 rule 0 permit ip source 1.1.1.3 0 destination 1.1.1.1 0
#
```

3）配置ipsec策略

```
#
ipsec transform-set 1
 esp encryption-algorithm 3des-cbc
 esp authentication-algorithm md5
#
ipsec policy 1 10 isakmp
 transform-set 1
 security acl 3000
 remote-address 1.1.1.1
 ike-profile 1
#
ike profile 1
 keychain 1
 match remote identity address 1.1.1.1 255.255.255.255
```

```
#
ike keychain 1
 pre-shared-key address 1.1.1.1 255.255.255.255 key cipher
$c$3$Zjh8lqvsPg27z8WHRa4jIDOoxCmrjQ==
#
```

4）物理接口上调用ipsec策略

```
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
 ip address 1.1.1.3 255.255.255.0
 ipsec apply policy 1
#
```

5）配置ospf，把tunnel口宣告进ospf

```
#
ospf 1
 area 0.0.0.0
  network 13.0.0.3 0.0.0.0
#
```

注意不要把内网口宣告进ospf。

4. 在总部端检查配置结果

1）检查ike sa

```
display ike sa
    total phase-1 SAs:  2
    connection-id  peer                    flag        phase   doi
  ----------------------------------------------------------------
      142          1.1.1.3                RD         1       IPSEC
      380          1.1.1.2                RD|ST       1       IPSEC
      358          1.1.1.3                RD         2       IPSEC
      381          1.1.1.2                RD|ST       2       IPSEC

  flag meaning
  RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT RK—REKEY
```

两个分支端的ipsec sa和ike sa都协商起来。

2）检查ipsec sa

```
display ipsec sa
===============================
Interface: Ethernet0/0
    path MTU: 1500
===============================

  -----------------------------
  IPsec policy name: "1"
  sequence number: 10
  acl version: ACL4
  mode: isakmp
  -----------------------------
    PFS: N, DH group: none
    tunnel:
        local  address: 1.1.1.1
        remote address: 1.1.1.2
    flow:
        sour addr: 1.1.1.1/255.255.255.255  port: 0  protocol: IP
        dest addr: 1.1.1.2/255.255.255.255  port: 0  protocol: IP

    [inbound ESP SAs]
      spi: 0x3356AE14(861318676)
      transform: ESP-ENCRYPT-3DES ESP-AUTH-MD5
      in use setting: Tunnel
      connection id: 101
      sa duration (kilobytes/sec): 1843200/3600
      sa remaining duration (kilobytes/sec): 1843180/2950
```

```
   anti-replay detection: Enabled
    anti-replay window size(counter based): 32
   udp encapsulation used for nat traversal: N

  [outbound ESP SAs]
   spi: 0x4054B36C(1079292780)
   transform: ESP-ENCRYPT-3DES ESP-AUTH-MD5
   in use setting: Tunnel
   connection id: 102
   sa duration (kilobytes/sec): 1843200/3600
   sa remaining duration (kilobytes/sec): 1843180/2950
   anti-replay detection: Enabled
    anti-replay window size(counter based): 32
   udp encapsulation used for nat traversal: N
===============================
Interface: Ethernet0/0
  path MTU: 1500
===============================

 -----------------------------
 IPsec policy name: "1"
 sequence number: 20
 acl version: ACL4
 mode: isakmp
 -----------------------------
  PFS: N, DH group: none
  tunnel:
    local  address: 1.1.1.1
    remote address: 1.1.1.3
  flow:
    sour addr: 1.1.1.1/255.255.255.255  port: 0  protocol: IP
    dest addr: 1.1.1.3/255.255.255.255  port: 0  protocol: IP

  [inbound ESP SAs]
   spi: 0x891907CB(2300118987)
   transform: ESP-ENCRYPT-3DES ESP-AUTH-MD5
   in use setting: Tunnel
   connection id: 99
   sa duration (kilobytes/sec): 1843200/3600
   sa remaining duration (kilobytes/sec): 1843158/758
   anti-replay detection: Enabled
    anti-replay window size(counter based): 32
   udp encapsulation used for nat traversal: N

  [outbound ESP SAs]
   spi: 0x8FE5123C(2414154300)
   transform: ESP-ENCRYPT-3DES ESP-AUTH-MD5
   in use setting: Tunnel
   connection id: 100
   sa duration (kilobytes/sec): 1843200/3600
   sa remaining duration (kilobytes/sec): 1843159/758
   anti-replay detection: Enabled
    anti-replay window size(counter based): 32
   udp encapsulation used for nat traversal: N
```

两个sa的保护流，是gre封装后的源和目的ip。

3）检查ospf 邻居

```
display ospf peer

         OSPF Process 1 with Router ID 100.0.0.1
            Neighbor Brief Information

 Area: 0.0.0.0
 Router ID   Address         Pri  Dead-Time  Interface       State
 1.1.1.2      12.0.0.2        1    32         Tun1            Full/ -
 192.168.1.1  13.0.0.3        1    37         Tun2            Full/ -
```

与两个分支tunnel口的邻居都是full状态。邻居地址是tunnel口ip地址。

5. 分支端进行测试，从两个分支，用各自的内网地址telnet总部的内网地址

```
telnet 100.0.0.1 source ip 192.168.1.1
```

```
telnet 100.0.0.1 source 192.168.1.1
```

能同时telnet到总部路由器上

6. 总部端查看telnet用户在线状态

```
display users
The user application information of the user interface(s):
  Idx UI      Delay    Type Userlevel
  82  VTY 0   00:00:46 TEL  3
+ 83  VTY 1   00:00:00 TEL  3
  84  VTY 2   00:00:19 TEL  3

Following are more details.
VTY 0   :
        Location: 12.0.0.2
VTY 1   :
        Location: 1.1.1.4
VTY 2   :
        Location: 13.0.0.3
 +    : Current operation user.
 F    : Current operation user work in async mode.
```

分2个分支端用户可以同时在线，源ip是各分支tunnel口的ip

1、本配置是GRE OVER IPSEC，因此IPSEC感兴趣流acl要匹配GRE封装后的数据包的地址，并且要互为镜像。
2、在GRE OVER IPSEC中，IPSec应用在物理口上。
3、Tunnel口上配置nat outbound，数据包经过tunnel口时，会先将源地址转换为tunnel口的地址，再进行gre封装。