SR6600系列路由器 VPE---GRE接入MPLS VPN的配置方法

MPLS L3VPN ipoe 张盛楠 2011-07-06 发表

一、 组网需求：

用户PC接入到自己的网关（CE）设备，通过网关访问异地的服务器（如图最右方的服务器区），中间通过一段非内部网络（图中用Internet表示）接入到MPLS骨干网络中。由于CE不是通过内部网络或者专线接入到PE上，考虑到网络的安全性，方案采用在CE和PE设备之间启用GRE over IPsec 隧道来确保CE到PE之间的数据安全。

骨干网络中间存在两台PE设备，其中靠近用户侧的PE由于将GRE隧道直接接入到MPLS网络中，因此称其为VPE设备。 VPE和PE设备间不存在P设备，MSR 2.2.2.2 上并没有使能MPLS转发能力，只是进行普通的IP承载，因此VPE和PE之间也需启用GRE隧道，保证MPLS报文的正常转发。

设备清单： VPE、PE:SR6600 路由器 版本 R2507P01

中间设备 MSR

用户CE设备为其它路由器

二、 组网图：

三、 配置步骤：

配置中涉及GRE over IPsec的部分不做过多说明，可以参考GRE over IPsec的配置案例

CE 配置

```
sysname CE
#
 ike local-name CE
#
 domain default enable system
#
 telnet server enable
#
acl number 3000
 rule 0 permit ip source 172.16.1.2 0 destination 172.16.1.1 0
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
ike proposal 1
#
ike peer vpe
 proposal 1
 pre-shared-key simple 12345
 remote-address 172.16.1.1
 local-address 172.16.1.2
#
ipsec proposal 1
#
ipsec policy ce_pe 1 isakmp
 security acl 3000
 ike-peer vpe
 proposal 1
#
user-group system
#
interface NULL0
#
interface LoopBack0                    //用于代替测试PC地址
 ip address 8.8.8.8 255.255.255.255
#
interface GigabitEthernet0/0           //连接VPE的G0/0
 ip address 172.16.1.2 255.255.255.252
 ipsec policy ce_pe
#
interface GigabitEthernet0/1
#
interface GigabitEthernet0/2
#
interface GigabitEthernet0/3
#
interface Tunnel1
 ip address 207.1.1.2 255.255.255.252
 source 172.16.1.2
 destination 172.16.1.1
#
 ip route-static 0.0.0.0 0.0.0.0 Tunnel1
 //配置CE访问服务器的下一跳走Tunnel1
#
```

VPE 配置

```
sysname VPE-SR66
#
 ike local-name vpe
#
 domain default enable system
#
 router id 1.1.1.1
#
 telnet server enable
#
 mpls lsr-id 1.1.1.1
#
ip vpn-instance test              //服务器业务所在的VPN实例
 route-distinguisher 1:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
acl number 3000                   //用于与CE建立IPsec的安全ACL
 rule 0 permit ip source 172.16.1.1 0 destination 172.16.1.2 0
#
mpls
#
mpls ldp
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
```

```
#
ike proposal 1
#
ike peer ce
 proposal 1
 pre-shared-key simple 12345
 remote-address 172.16.1.2
 local-address 172.16.1.1
#
ipsec proposal 1
#
ipsec policy pe_ce 1 isakmp
 security acl 3000
 ike-peer ce
 proposal 1
#
user-group system
#
controller Cpos2/0
#
interface NULL0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet0/0                //连接CE 注意配置IPsec
 ip address 172.16.1.1 255.255.255.252
 ipsec policy pe_ce
#
interface GigabitEthernet0/1                //连接MSR
 ip address 100.1.1.1 255.255.255.252
#
interface GigabitEthernet0/2
#
 interface Tunnel1                          //私网GRE隧道，注意要在
 ip binding vpn-instance test               Tunnel中绑定vpn实例
 ip address 207.1.1.1 255.255.255.252
 source 172.16.1.1
 destination 172.16.1.2

interface GigabitEthernet0/3
#
interface Tunnel0                           //公网GRE隧道注意在隧道上
 ip address 123.1.1.1 255.255.255.252       使能MPLS和LDP能力
 source 100.1.1.1
 destination 200.1.1.1
 mpls
 mpls ldp
#
#
bgp 100
 undo synchronization
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface LoopBack0
 #
 ipv4-family vpn-instance test
  import-route direct
  import-route static     //注意将在VPN中发布的CE网段路由引入BGP
 #
 ipv4-family vpnv4
  peer 3.3.3.3 enable
#
 ip route-static 3.3.3.3 255.255.255.255 Tunnel0
 ip route-static 200.1.1.0 255.255.255.252 100.1.1.2
 ip route-static vpn-instance test 8.8.8.8 255.255.255.255 Tunnel1
   //将CE上的测试网段8.8.8.8 下发到VPN路由表中，注意下一跳要走Tunnel
```

PE设备的配置与VPE是对称的 主要注意在Tunnel上配置使能MPLS和LDP能力

在PE设备上配置loopback接口并绑入VPN test 中 配置地址ip=6.6.6.6 /32测试(代替服务器地址)

VPE上的路由表项:

```
 dis ip routing-table vpn-instance test
Routing Tables: test
        Destinations : 7        Routes : 7

Destination/Mask    Proto  Pre  Cost        NextHop         Interface

5.5.5.5/32          Direct 0    0           127.0.0.1       InLoop0
6.6.6.6/32          BGP    255  0             3.3.3.3        NULL0
8.8.8.8/32          Static 60   0           207.1.1.1       Tun1
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
207.1.1.0/30        Direct 0    0           207.1.1.1       Tun1
207.1.1.1/32        Direct 0    0           127.0.0.1       InLoop0
```

PE 上的路由表象

```
dis ip routing-table vpn-instance test
Routing Tables: test
        Destinations : 6        Routes : 6

Destination/Mask    Proto  Pre  Cost        NextHop         Interface

5.5.5.5/32          BGP    255  0           1.1.1.1         NULL0
6.6.6.6/32          Direct 0    0           127.0.0.1       InLoop0
8.8.8.8/32          BGP    255  0           1.1.1.1         NULL0
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
207.1.1.0/30        BGP    255  0           1.1.1.1         NULL0
```

在CE上ping 进行测试：

```
 ping 6.6.6.6            // 用207.1.1.2 这个地址作为源地址
  PING 6.6.6.6: 56  data bytes, press CTRL_C to break
    Reply from 6.6.6.6: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 6.6.6.6: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 6.6.6.6: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 6.6.6.6: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 6.6.6.6: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 6.6.6.6 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms

ping -a 8.8.8.8 6.6.6.6   //用8.8.8.8作为源地址，说明CE下PC可以访问服务器
  PING 6.6.6.6: 56  data bytes, press CTRL_C to break
    Reply from 6.6.6.6: bytes=56 Sequence=1 ttl=254 time=1 ms
    Reply from 6.6.6.6: bytes=56 Sequence=2 ttl=254 time=1 ms
    Reply from 6.6.6.6: bytes=56 Sequence=3 ttl=254 time=1 ms
    Reply from 6.6.6.6: bytes=56 Sequence=4 ttl=254 time=1 ms
    Reply from 6.6.6.6: bytes=56 Sequence=5 ttl=254 time=1 ms

  --- 6.6.6.6 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

四、 配置关键点：

配置的关键点在于VPE

1. VPE 上必须与CE间配置GRE+IPsec 隧道将网络加密
2. VPE上需将GRE+IPsec隧道绑入到VPN中，完成GRE隧道到MPLS vpn 隧道的连接
3. 由于MSR上没有配置MPLS能力，因此VPE 和PE之间的GRE隧道上需要配置MPLS和LDP能力
4. VPE上需配置公网路由走GRE Tunnel，而不能走普通IP接口，因为走普通IP 接口会造成LDP 建立异常，最终导致私网路由学习不通。
5. VPE上需将CE下网段的路由发布到VPN，并且import到BGP中发布给对端PE，案例中采用的是静态路由下发，实际中可以采用OSPF 、RIP、 ISIS多实例或者EBGP的方式（方法参照 附录）
6. CE上需要配置到服务器的路由下一跳为VPE

五、附录

1. 采用EBGP的方式将用户私网路由通过GRE隧道引入VPE的配置方法

   此部分只涉及路由引入的配置方法，与原方案相同的配置部分不再赘述

CE 配置

```
#
interface Tunnel1
 ip address 207.1.1.2 255.255.255.252
 source 172.16.1.2
 destination 172.16.1.1
#
bgp 200                          //在CE上配置VPE为EBGP邻居
 import-route direct               //将直连引入
 undo synchronization
 peer 207.1.1.1 as-number 100        //注意采用Tunnel地址作为
peer
```

VPE 配置

```
Bgp 100
 undo synchronization
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface LoopBack0
 #
 ipv4-family vpn-instance test
  peer 207.1.1.2 as-number 200       //注意使用Tunnel地址作为peer
  import-route direct
 #
 ipv4-family vpnv4
  peer 3.3.3.3 enable
```

这里需要注意：在VPE上需要在VPN实例中与CE建立EBGP邻居，因此需要用VPN中与CE的互连地址作为Peer的地址，这样EBGP才能通过IGP找到正确的路由，从而建立对等体关系

2. 采用OSPF 多实例的方法引入用户私网路由

此处仅涉及路由引入的相关配置

CE 配置

```
#
ospf 1
 area 0.0.0.0
  network 207.1.1.0 0.0.0.3
  network 4.4.4.4 0.0.0.0
```

VPE 配置

```
Bgp 100
 undo synchronization
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface LoopBack0
 #
 ipv4-family vpn-instance test
  import-route direct
  import-route ospf 2
 #
 ipv4-family vpnv4
  peer 3.3.3.3 enable
#
ospf 2 router-id 1.1.1.1 vpn-instance test  // OSPF多实例
 area 0.0.0.0
  network 207.1.1.0 0.0.0.3
```

RIP ISIS多实例的配置思路 与OSPF多实例是类似的，均是在VPN实例下与CE建立PEER，然后将路由引入BGP，具体命令请参照手册。