SR6600系列路由器 VPE--L2tp over IPSec 的配置方法

L2TP 张盛楠 2011-02-16 发表

SR6600系列路由器 L2TP+IPSec VPE的配置方法

一、 组网需求：

1. 用户服务器位于私网中，由于出差频繁，客户需要从PC机通过L2tp拨入MPLS vpn业务访问私网的各种服务。

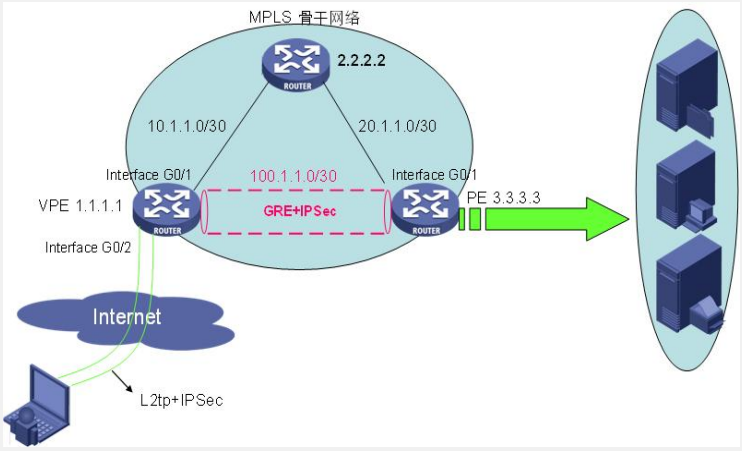
2. MPLS骨干网络中间的P设备不具备MPLS转发能力，只能进行IP转发

需求分析：

PC通过L2tp 拨入MPLS vpn，这就要求客户侧的PE设备可以终结IP vpn （L2tp），即作为VPE出现在网络中

P设备不具备MPLS转发能力，因此我们需要在VPE和PE设备之间建立GRE隧道，将MPLS报文作为GRE的乘客协议 将整个MPLS报文转换为IP报文经过P设备转发后到达PE后再进行MPLS处理

二、 组网图：



组网设备： SR6600 路由器 3台版本R2420P07

PC（预装inode客户端进行 L2tp+IPSec）

三、 配置步骤：

VPE 配置

```
sysname VPE
#
 l2tp enable
#
 ike local-name gateway     //与PC间的IPSec
#
 domain default enable system
#
 router id 1.1.1.1
#
 telnet server enable
#
 mpls lsr-id 1.1.1.1
#
ip vpn-instance test       //私网业务vpn
 route-distinguisher 1:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
acl number 3000           //IPSec 匹配VPE和PE间网段
 rule 0 permit ip source 10.1.1.1 0 destination 20.1.1.2 0
#
mpls
#
mpls ldp
#
domain system
```

```
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 ip pool 0 192.168.1.2 192.168.1.10  //为L2tp用户分配地址
#
ike proposal 1
#
ike peer pc                          //与PC间的IPSec 需用野蛮模式
 exchange-mode aggressive
 proposal 1
 pre-shared-key cipher xxxx
 id-type name
 remote-name pc
#
ike peer pe                          //与PE 间的IPSec
 proposal 1
 pre-shared-key cipher xxxx
 remote-address 20.1.1.2
#
ipsec proposal 1
#
ipsec policy-template pc 1       //与PC间的IPSec需用template
 ike-peer pc
 proposal 1
#
ipsec policy computer 1 isakmp template pc
#
ipsec policy test 1 isakmp
 security acl 3000
 ike-peer pe
 proposal 1
#
user-group system
#
local-user routerman             //配置L2tp用户
 password simple 111
 authorization-attribute level 3
 service-type ppp
#
l2tp-group 1
 allow l2tp virtual-template 1
 tunnel password simple 111111   //可以取消隧道认证
 tunnel name access               //需配置隧道名称
#
interface Virtual-Template1
 ppp authentication-mode pap domain system
 remote address pool
 mtu 1200
 ip binding vpn-instance test    //虚模板绑定vpn实例
 ip address 192.168.1.1 255.255.255.0
#
interface NULL0
#
interface LoopBack0

 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet0/1
 ip address 10.1.1.1 255.255.255.252
 ipsec policy test
interface GigabitEthernet0/2    //与PC直连的接口
 ip address 207.1.1.1 255.255.255.252
 ipsec policy computer
#
interface Tunnel0
 ip address 100.1.1.1 255.255.255.252
 source 10.1.1.1
 destination 20.1.1.2
 mpls                            //使能tunnel的MPLS能力
 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
 #
 ipv4-family vpnv4
  peer 3.3.3.3 enable
#
 ip route-static 3.3.3.3 255.255.255.255 Tunnel0
 //配置到PE 走tunnel 路由
 ip route-static 20.1.1.0 255.255.255.0 10.1.1.2
```

PE 配置

```
#
 sysname PE
#
 domain default enable system
#
 router id 3.3.3.3
#
 telnet server enable
#
 mpls lsr-id 3.3.3.3
#
ip vpn-instance test
 route-distinguisher 1:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
acl number 3000
 rule 0 permit ip source 20.1.1.2 0 destination 10.1.1.1 0
#
mpls
#
mpls ldp
#
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 cipher xxxx
 remote-address 10.1.1.1
#
ipsec proposal 1
#
ipsec policy test 1 isakmp
 security acl 3000
 ike-peer vpe
 proposal 1
#
user-group system
#
l2tp-group 1
 tunnel name test
#
interface NULL0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface LoopBack1                    //测试时替代服务器地址
 ip binding vpn-instance test
 ip address 8.8.8.8 255.255.255.255
#
interface GigabitEthernet0/0
#
interface GigabitEthernet0/1
 ip address 20.1.1.2 255.255.255.252
 ipsec policy test
#
interface Tunnel0
 ip address 100.1.1.2 255.255.255.252
 source 20.1.1.2
 destination 10.1.1.1
 mpls
 mpls ldp
#
bgp 100
 undo synchronization
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack0
 #
 ipv4-family vpn-instance test
  import-route direct
 #
 ipv4-family vpnv4
  peer 1.1.1.1 enable
#
 ip route-static 1.1.1.1 255.255.255.255 Tunnel0
 ip route-static 10.1.1.0 255.255.255.0 20.1.1.1
```

PC 配置方法及效果验证请参照附件

四、 配置关键点：

1. 由于是PC通过L2tp+IPSec 拨入vpn 因此需注意要在virtual-template上绑定vpn实例
2. MPLS+GRE+IPSec 中的IPSec 需要匹配IPSec网关间（VPE与PE）的网段地址
3. GRE tunnel 需要使能MPLS转发能力和LDP能力
4. PC 侧配置L2tp+IPSec参数要与VPE上的一致，具体要根据不同的PC拨号终端决定
是否需要配置L2tp tunnel name 和 tunnel authentication
5. 由于PC的私网地址是VPE分配的，因此IPSec 需要使用野蛮模式和template
6. P设备上仅需要配置正确公网路由即可。
7. 此例中的公网路由由于组网比较简单使用的是静态路由，实际使用可以根据情况选用动态路由。