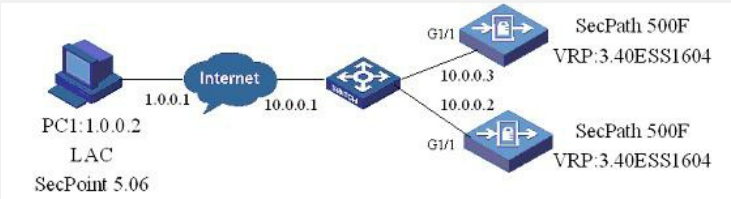
SecPath防火墙作为LNS采用VRRP备份的配置

胡俊 2006-10-09 发表

一、组网需求

L2TP的LNS端采用SecPath防火墙设备建立VRRP组，PC1装载SecPoint客户端软件作为LAC端。PC1通过拨号接入LNS，当其中正在使用LNS发生故障down掉以后，另外一个将代替它的地位，成为新的LNS，PC1仍然可以正常拨号。

二、组网图



如图所示，使用SecPath防火墙作为L2TP的LNS，客户端软件是我司的SecPoint。两台SecPath防火墙通过交换机与Internet相连接。

软件版本如下：

SecPath1000F：VRP 3.40 ESS 1604；

客户端软件：SecPoint 5.06。

三、配置步骤

3.1 LNS端的配置（两个LNS配置相似）：

```
[LNS]dis ver                                        //系统的软件版本
 Copyright Notice:
 All rights reserved (Aug  2 2006).
 Without the owner's prior written consent, no decompiling
 nor reverse-engineering shall be allowed.
 Huawei Versatile Routing Platform Software
 VRP software, Version 3.40, ESS 1604
 Copyright (c) 1998-2006 Huawei Tech. Co., Ltd. All rights reserved.
 Quidway SecPath 500F uptime is 0 week, 0 day, 0 hour, 22 minutes
  CPU type: Mips IDT RC32438 266MHz
  256M bytes DDR SDRAM Memory
  16M bytes Flash Memory
  Pcb Version:3.0
  Logic Version:1.0
  BootROM Version:1.19
  [SLOT 0] 4FE      (Hardware)3.0, (Driver)2.0, (Cpld)1.0
  [SLOT 1] 3FE      (Hardware)3.0, (Driver)2.0, (Cpld)1.0
[LNS]dis cu
sysname LNS
l2tp enable                                         //开启l2tp功能
firewall packet-filter enable
 firewall packet-filter default permit
undo connection-limit enable
 connection-limit default deny
 connection-limit default amount upper-limit 50 lower-limit 20
firewall statistic system enable
radius scheme system
domain system
 ip pool 1 5.0.0.10 5.0.0.20
local-user hujun                                    //配置用户名和密码
 password simple 123
 service-type ppp
interface Virtual-Template1                         //配置虚拟接口模板1及其验证方式

 ppp authentication-mode pap
 ip address 5.0.0.1 255.255.255.0
interface Aux0
 async mode flow
```

```
interface GigabitEthernet0/0
interface GigabitEthernet0/1
interface GigabitEthernet1/0
interface GigabitEthernet1/1
ip address 10.0.0.3 255.255.255.0
vrrp vrid 1 virtual-ip 10.0.0.100                    //配置VRRP备份组和虚拟ip地址
 vrrp vrid 1 priority 120                            //配置VRRP优先级，另一个优先级默认
interface Encrypt2/0
interface NULL0
firewall zone local
 set priority 100
firewall zone trust
add interface GigabitEthernet1/1
 add interface Virtual-Template1                     //把虚拟接口模板添加进入安全域
set priority 85
firewall zone untrust
 set priority 5
firewall zone DMZ
 set priority 50
firewall interzone local trust
firewall interzone local untrust
firewall interzone local DMZ
firewall interzone trust untrust
firewall interzone trust DMZ
firewall interzone DMZ untrust
l2tp-group 1                                         //配置l2tp组1
 undo tunnel authentication                          //取消隧道验证
 allow l2tp virtual-template 1                       //配置使用名字的方式发起l2tp连接
                                                     对端隧道名为lac，域后缀为1

ip route-static 0.0.0.0 0.0.0.0 10.0.0.1 preference 60    //配置静态默认路由
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
return
```

3.2 LAC的配置

1）“基本设置”的配置

2）“L2TP设置”的配置

四、配置关键点

请见配置里面的蓝色斜体字标记。