SecPath防火墙作为LAC时PC拨号接入LNS的配置
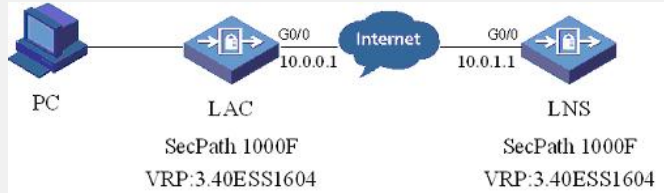
胡俊　2006-09-15 发表

一、组网需求

　　L2TP的LAC和LNS端均采用SecPath防火墙设备，PC通过windows自带的VPN拨号软件接入到LNS后，就可以访问其内网资源了。

二、组网图

　　如图所示，使用SecPath防火墙作为L2TP的LAC和LNS，客户端软件是windows自带的VPN拨号软件。

　　软件版本如下：

　　SecPath1000F：VRP 3.40 ESS 1604;

　　客户端软件：windows XP自带的拨号软件。

三、配置步骤

3.1 LAC端的配置:

[LAC]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 1000F 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

[LAC]dis cu

sysname LAC

l2tp enable　　　　　　　　　　　　　　　//开启l2tp功能

firewall packet-filter enable

 firewall packet-filter default permit

 firewall statistic system enable

radius scheme system

domain system

local-user hujun　　　　　　　　　　　　//配置ppp协商的用户名和密码

 password simple 123

 service-type ppp

interface Virtual-Template1　　　　　　//配置虚拟接口模板及其验证方式

 ppp authentication-mode pap

interface Aux0

 async mode flow

interface GigabitEthernet0/0

 mtu 1400

 tcp mss 1400

 ip address 10.0.0.2 255.255.255.0

interface GigabitEthernet0/1

 pppoe-server bind Virtual-Template 1　　　//在接口上配置pppoe-server，并且绑定到虚拟接口模板1

 interface Encrypt2/0

```
interface NULL0
firewall zone local
 set priority 100
firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet0/1
 add interface Virtual-Template1          //将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
 undo tunnel authentication               //取消隧道验证
 start l2tp ip 10.0.1.2 fullusername hujun    //配置使用名字的方式发起l2tp连接
，
10.0.1.2为LNS的外网接口ip地址
ip route-static 0.0.0.0 0.0.0.0 10.0.0.1 preference 60   //配置一条静态默认路由
user-interface con 0
user-interface aux 0
user-interface vty 0 4
return
3.2 LNS端的配置：
[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 3.0.0.2 3.0.0.10               //配置接入用户使用的地址池
local-user hujun                         //配子用户名和密码

 password simple 123
 service-type ppp
interface Virtual-Template1              //配置虚拟接口模板及其验证方式
 ppp authentication-mode pap
ip address 3.0.0.1 255.255.255.0
interface Aux0
 async mode flow
interface GigabitEthernet0/0
 ip address 10.0.1.2 255.255.255.0
interface GigabitEthernet0/1
interface Encrypt2/0
interface NULL0
interface LoopBack1
 ip address 2.0.0.1 255.255.255.0
firewall zone local
 set priority 100
firewall zone trust
 add interface GigabitEthernet0/0
 add interface GigabitEthernet0/1
 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                              //取消隧道验证
 undo tunnel authentication               //配置使用名字的方式发起l2tp连接,
 allow l2tp virtual-template 1            //使用虚拟接口1来接收隧道连接请求
ip route-static 0.0.0.0 0.0.0.0 10.0.1.2 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
```

四、配置关键点

   请见配置里面的蓝色斜体字。