

## 一、组网需求

PC作为L2TP的LAC端，SecPath防火墙作为LNS端，PC的IP地址为私网地址。希望通过L2TP拨号的方式接入到对端防火墙。

## 二、组网图



如图所示，用户PC作为LAC，使用我司SecPoint作为客户端软件，拨号接入到对端的SecPath防火墙。

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：

```
[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 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
[LNS]dis cu //系统的配置
sysname LNS
l2tp enable //启动L2TP功能
ike local-name test //配置本端ike名称
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 1.0.0.2 1.0.0.10 //配置拨号用户使用的地址池

local-user hujun //配置l2tp拨号的用户和密码

password simple 123
service-type ppp
ike peer 1 //配置ipsec的ike peer
exchange-mode aggressive
id-type name
pre-shared-key 123
remote-name client
```

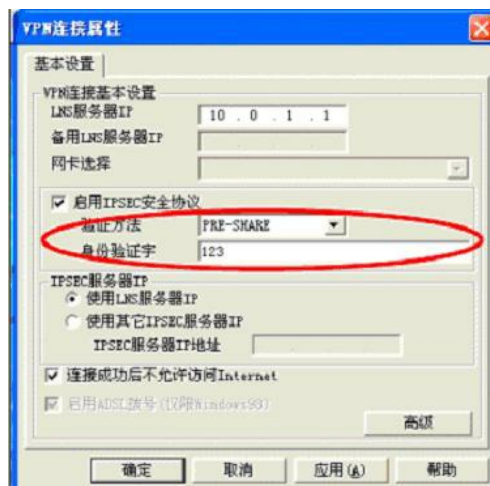
```

nat traversal
ipsec card-proposal 1 //配置ipsec proposal
use encrypt-card 2/0 //使用ipsec加密卡
ipsec policy-template temp 1 //配置ipsec虚模板
ike-peer 1
proposal 1
ipsec policy 1 1 isakmp template temp
interface Virtual-Template1 //配置l2tp虚拟模板
ppp authentication-mode pap //配置认证方式
为pap
ip address 1.0.0.1 255.255.255.0
interface Aux0
async mode flow
interface GigabitEthernet0/0
ip address 10.0.1.1 255.255.255.0
ipsec policy 1 //在接口上面启用ipsec policy
interface GigabitEthernet0/1
interface Encrypt2/0
interface NULL0
firewall zone local
set priority 100
firewall zone trust
add interface GigabitEthernet1/0
add interface GigabitEthernet1/1
add interface Virtual-Template1
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
tunnel password simple 123 //不使用隧道认证
allow l2tp virtual-template 1 //使用虚拟模板1认证
user-interface con 0
user-interface aux 0
user-interface vty 0 4
return

```

### 3.2 SecPoint上的配置:

#### 1) 配置“基本设置”选项



#### 2) 配置“L2TP设置”选项



3) 配置“IPSec设置”选项

4) 配置“IKE设置”选项



3.3 NAT的配置

(略)

#### 四、配置关键点

请见配置里面的蓝色斜体字。