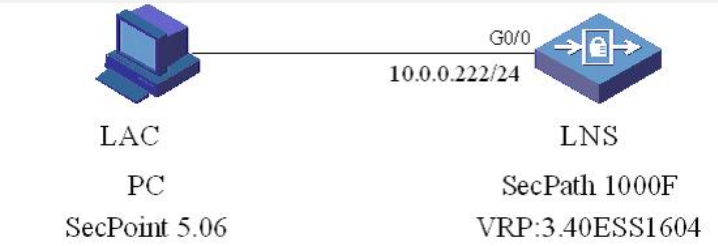
SecPath防火墙采用IPSec加密卡方式接受SecPoint拨号的配置

胡俊 2006-09-08 发表

一、组网需求

PC作为L2TP的LAC端，防火墙作为LNS端。用户希望通过L2TP拨号的方式接入到对端防火墙，其中对端防火墙配置了IPSec，使用IPSec加密卡加密。

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，防火墙上配置了IPSec，使用加密卡进行加密。

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侧配置如下所示：

```
dis cu
sysname secpath
l2tp enable                                  //启动l2tp功能
local-user vpnuser
password simple vpnuser                      //配置l2tp拨号的用户和密码
service-type ppp
domain system
ip pool 1 10.0.1.10 10.0.1.20                //配置拨号用户使用的地址池
ike local-name test                          //配置ipsec参数
ike peer 1                                   //配置ipsec的ike peer
 exchange-mode aggressive
 pre-shared-key 12345
 id-type name
 remote-name client
 nat traversal
ipsec card-proposal p1                       //配置ipsec proposal
 use encrypt-card 2/0                        //使用ipsec加密卡
ipsec policy-template temp1 1
 ike-peer 1
 proposal p1
ipsec policy policy1 1 isakmp template temp1
interface Virtual-Template0                  //配置l2tp虚拟模板
ppp authentication-mode pap                  //配置认证方式为pap
ip address 10.0.1.1 255.255.255.0
interface Encrypt2/0
interface NULL0
interface GigabitEthernet0/0
ip address 10.0.0.222 255.255.255.0
ipsec policy 1                               //在接口上面启用ipsec policy
interface GigabitEthernet0/1
firewall zone local
 set priority 100
firewall zone trust
 add interface GigabitEthernet0/0
 set priority 85
firewall zone untrust
 set priority 5
firewall zone DMZ
```

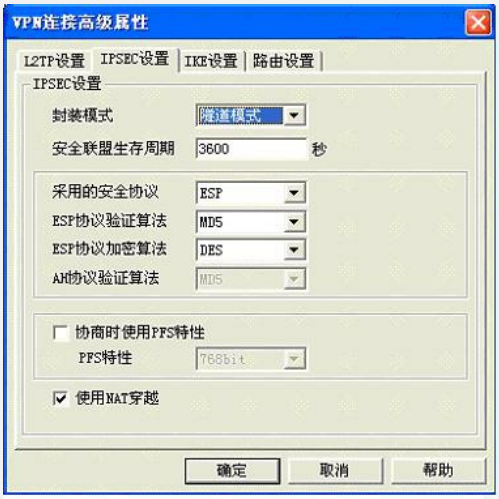
```
 set priority 50
firewall interzone local trust
firewall interzone local untrust
firewall interzone local DMZ
firewall interzone trust untrust
firewall interzone trust DMZ
firewall interzone DMZ untrust
 l2tp-group 1                                  //配置l2tp组
 undo tunnel authentication                    //不使用隧道认证
 allow l2tp virtual-template 0 remote rm   //允许远端隧道名称为rm的用户拨入
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

四、配置关键点

1．配置L2TP拨号用户名和密码的时候，注意要选择服务类型为PPP；

2．拨号用户使用地址池注意要在域下面配置；

3．使用IPSec加密卡时注意加密卡所在的槽位号；

4．配置L2TP虚拟模板时注意配置认证方式；

5．注意在SecPoint上配置使用虚拟模板用户的隧道名称要和在防火墙上配置的名称相同；

6．配置IPSec参数的时候注意和防火墙上面配置的参数一致.