Secpath1000F；L2TP VPN

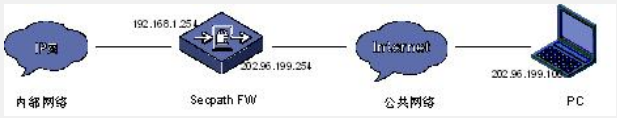
王刚 2006-08-27 发表

Secpath1000F L2TP功能的配置

一、组网需求：

在公网上的移动用户，需要通过VPN的方式连接到公司内部，以便使用内部的网络资源。可以通过L2TP的方式拨入，满足用户需求。

二、组网图



三、防火墙配置方式：

适用防火墙型号： Secpath1000F 及以下所有型号
适用防火墙内核版本： 所有防火墙软内核版本

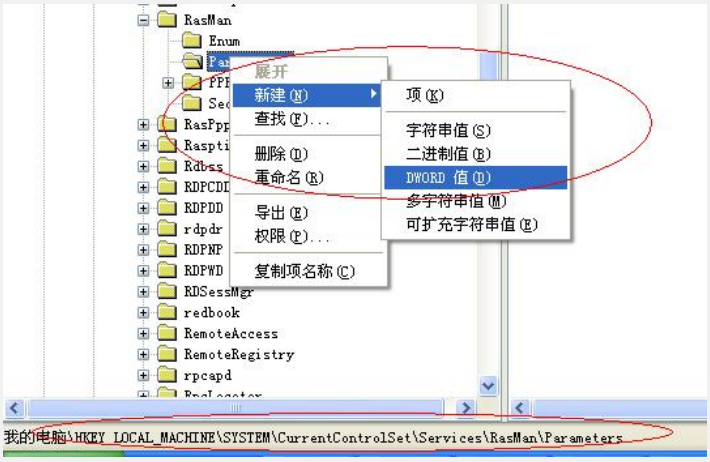
```
#
 sysname Quidway
#
 l2tp enable                                    //启用L2TP
#
 firewall packet-filter enable
 firewall packet-filter default permit
#
 insulate
#
 undo connection-limit enable
 connection-limit default deny
 connection-limit default amount upper-limit 50 lower-limit 20
#
 firewall statistic system enable
#
radius scheme system
#
domain system
domain test.com                                 // 创建一个新的域用来响应拨入
 ip pool 99 172.16.1.1 172.16.1.10              // 创建这个域相应的地址池
#
local-user test                                 // 创建用户用来拨
入
 password simple test
 service-type ppp                               // 注意此处的服务类型为 ppp
#
interface Virtual-Template0                     // 创建虚模板用来响应拨入
 ppp authentication-mode chap                   // 指定验证方式为
chap
 description ## the test.com domain ##          // 注释
 ip address 172.16.1.254 255.255.255.0          // 配置虚拟模板地址
 remote address pool 99                         // 指定远程客户端应获得哪个地址池
```

地址
#
interface Aux0
 async mode flow
#
interface Ethernet0/0
#
interface Ethernet0/1
#
interface Ethernet0/2
#
interface Ethernet0/3
 ip address 192.168.1.254 255.255.255.0
#
interface Ethernet1/0
#
interface Ethernet1/1
#
interface Ethernet1/2
 ip address 202.96.199.254 255.255.255.0
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 add interface Ethernet0/3
 set priority 85
#
firewall zone untrust
 add interface Ethernet1/2
 add interface Virtual-Template0 *// 把虚拟模板加入域*
 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 10
 undo tunnel authentication *// 不使用隧道验证*
 allow l2tp virtual-template 0 remote h3csec-test domain test.com
 // 指定相应的模板响应接入，其中 **h3csec-test** *为远端 PC 名*
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4

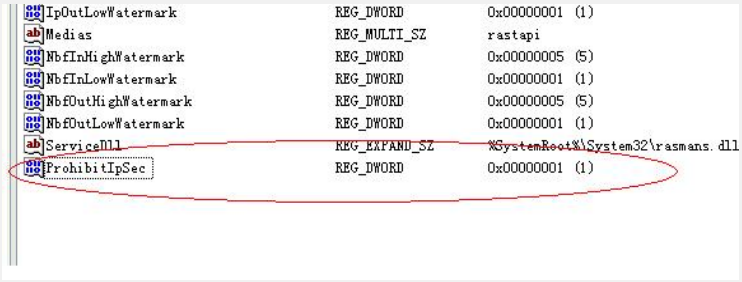
客户端设置：

1． 取消证书认证（通过修改注册表的方式，添加一个ProhibitIpSec为1的键值）

位置如下图所示：



添加的键值如下图所示



2． 建立拨号连接（使用微软的连接建立向导）：

需要注意的选项如下图所示选择 L2TP IPSec VPN；其他选项使用默认值即可

注意用户名和密码与 防火墙 上创建的用户名密码匹配

通过如下方式查看session和tunnel建立情况：

```
<Quidway>dis l2tp session
 Total session = 1
 LocalSID  RemoteSID  LocalTID  IdleTimeLeft
  26744     1          1        NOT SET

<Quidway>dis l2tp tunn
 Total tunnel = 1
 LocalTID RemoteTID RemoteAddress     Port    Sessions RemoteName
KeepStanding
 1        18        202.96.199.100   1701    1        h3csec-test  NO
```

四、 配置关键点：

无