SecPoint使用L2TP拨号接入私网LNS的配置

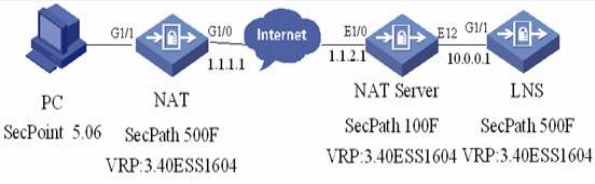
胡俊 2006-11-21 发表

SecPoint使用L2TP拨号接入私网LNS的配置

一、组网需求

L2TP的LAC和LNS端均采用SecPath防火墙设备，PC通过windows自带的拨号软件接入到私网的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，客户端软件是我司SecPoint拨号软件。其中，1.1.0.0/12为公网地址，10.0.0.1/24为私网地址。

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 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
interface GigabitEthernet0/1
interface GigabitEthernet1/0
interface GigabitEthernet1/1
ip address 10.0.0.1 255.255.255.0
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                                    //取消隧道验证
 undo tunnel authentication                     //配置使用名字的方式发起l2
tp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 10.0.0.2 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
```

3.2 NAT Server的配置：

```
[Quidway]dis cu
sysname Quidway
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
interface Aux0
 async mode flow
interface Ethernet0/0
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet1/0
 ip address 1.1.2.1 255.255.255.0
 nat server protocol udp global 1.1.2.1 any inside 10.0.0.1 any    //配
置NAT服务器，指向内网LNS的IP地址
interface Ethernet1/1
interface Ethernet1/2
 ip address 10.0.0.2 255.255.255.0
interface Encrypt2/0
interface NULL0
firewall zone local
 set priority 100
firewall zone trust
 add interface Ethernet1/0
 add interface Ethernet1/2
 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
ip route-static 0.0.0.0 0.0.0.0 1.1.2.2 preference 60
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
 user privilege level 3
return
```

3.3 NAT的配置（略）

3.4 SecPoint的配置

四、配置关键点

请见配置里面的蓝色斜体字和红色标记的位子。