L2TP OVER IPSEC在私网相同时的典型组网

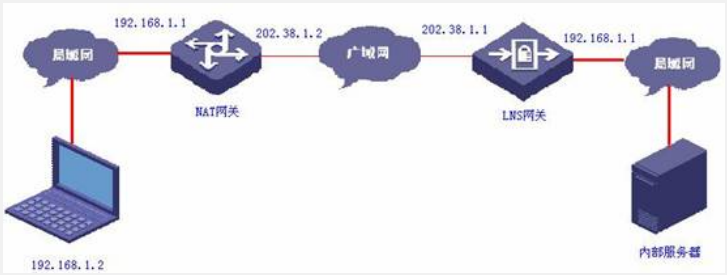
赵彪 2006-09-26 发表

L2TP OVER IPSEC在私网相同时的典型组网

一、 组网需求：

某用户在酒店上网，想通过L2TP OVER IPSEC方式访问公司OA服务器，却拨号不成功，发现酒店的私网地址和公司的私网地址一样，如果只用L2TP方式却可以拨号成功，通过策略路由解决这个问题。

二、 组网图



说明：

1、LNS网关采用SecPath1000F，版本为VRP 3.4-E1604;

2、PC安装了SecPoint，版本为5.06;操作系统为Windows XP。

三、 配置关键点

1. LNS网关的主要配置

使能L2TP

l2tp enable

在本地应用策略路由

ip local policy route-policy test

配置本端IKE名称

ike local-name zhongxin

定义防火墙包过滤规则

firewall packet-filter enable

firewall packet-filter default permit

给用户分配地址池

domain system

 ip pool 1 10.0.0.2 10.0.0.10

配置L2TP帐号

local-user zhaobiao

 password simple 123

 service-type ppp

配置IKE参数

ike peer 1

 exchange-mode aggressive

 pre-shared-key 123456

 id-type name

 remote-name fenzhi

 nat traversal

创建安全提议,采用默认参数

ipsec proposal 1

创建IPSEC模板，并引用IKE和安全提议

ipsec policy-template temp 1

 ike-peer 1

 proposal 1

创建IPSEC策略

ipsec policy pol1 1 isakmp template temp

定义nat转换的ACL

acl number 3000

 rule 0 permit ip source 192.168.1.0 0.0.0.255

 rule 1 deny ip

定义策略路由的ACL

acl number 3001

```
 rule 0 permit udp source-port eq 1701
使能L2TP的虚接口
interface Virtual-Template1
 ppp authentication-mode pap
 ip address 10.0.0.1 255.255.255.0
 remote address pool 1
配置外网口
interface Ethernet0/0
 ip address 202.38.1.1 255.255.255.0
 nat outbound 3000
 ipsec policy pol1
配置内网口
interface Ethernet1/0
 ip address 192.168.1.1 255.255.255.0
将接口加入到区域
firewall zone trust
 add interface Ethernet1/0
 set priority 85
firewall zone untrust
 add interface Ethernet0/0
 add interface Virtual-Template1
 set priority 5
创建L2TP组
l2tp-group 1
 undo tunnel authentication
 allow l2tp virtual-template 1
创建策略路由
route-policy test permit node 10
 if-match acl 3001
 apply output-interface Ethernet0/0
 配置默认路由
 ip route-static 0.0.0.0 0.0.0.0 202.38.1.2
```

2.　　NAT网关的的主要配置

```
定义ACL
acl number 3000
 rule 0 permit ip source 192.168.1.0 0.0.0.255
 rule 1 deny ip
配置外网口
interface Ethernet0/0
 ip address 202.38.1.2 255.255.255.0
 nat outbound 3000
配置内网口
interface Ethernet1/0
 ip address 192.168.1.1 255.255.255.0
配置默认路由
ip route-static 0.0.0.0 0.0.0.0 202.38.1.1
```

四、 配置关键点

见配置步骤说明。