L2TP接入如何实现多用户分组

齐楠 2006-02-08 发表

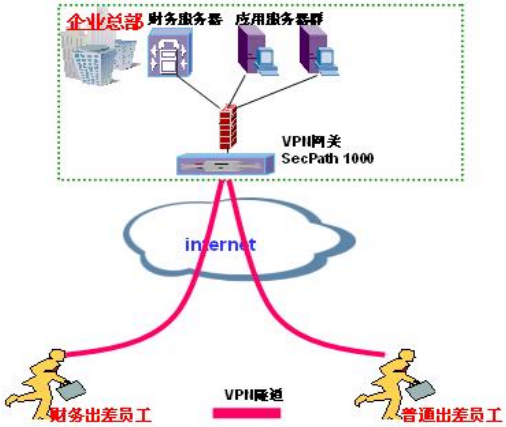
L2TP接入如何实现多用户分组

【客户需求】

企业或机构出差员工利用L2TP隧道技术，通过internet接入到其内部网络，希望对每个员工赋予不同的用户名，同时将用户分组，不同组的用户分配不同的接入地址，从而根据地址在内部网进行相关的权限控制。

【拓扑简介】

下面是一个简单的此类应用拓扑示意。财务部员工在外出差接入用户时允许查看部分财务服务器数据，而普通员工择只可以访问OA等普通服务器。



【实现方式】

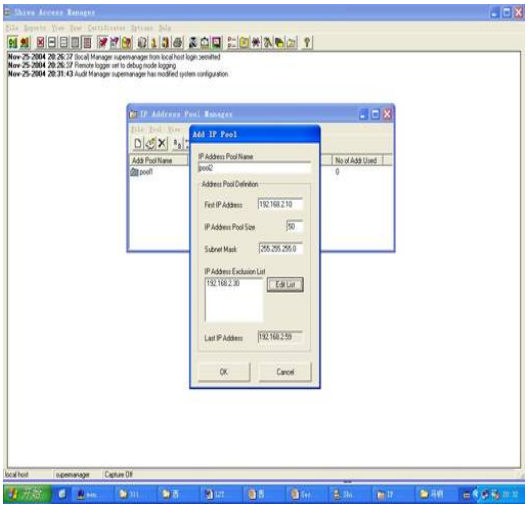
对财务部员工在通过L2TP接入时，分配一个地址池地址如192.168.1.x网段，而对普通员工分配192.168.2.x网段。在内部通过ACL等方式控制不同网段的访问权限。

给员工分配地址时通过Radius服务器实现，shiva5.0等Radius服务器支持此类应用。本配置以shiva5.0做Radius服务器来进行。

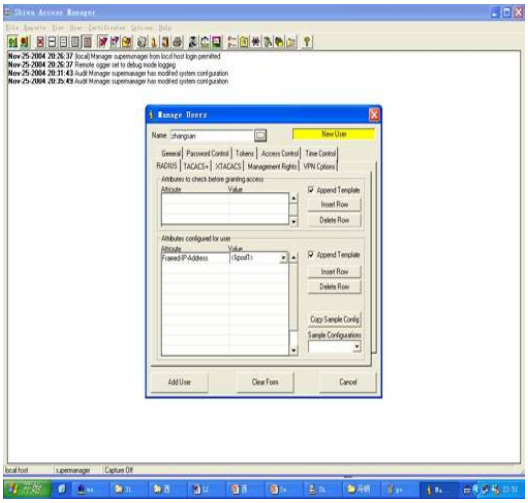
【具体配置步骤】

1．内部安装一台shiva5.0的RADIUS服务器。指定Radius的认证和计费端口号以及认证KEY。

2．在Radius上创建不同的地址池。打开Shiva Access Manager，在options - IP Address Pool Manager上添加两个地址池，如下图：



3．创建各个用户，并为之指定所用地址池。在Users - Manager Users界面下，打开general对话框，输入新的用户名，如zhangsan，指定password，在User Expiration Date选择Dec-31-2029（也可手工输入失效时间）。打开Radius对话框，在Attributed configured for user中点击"insert now"，Attribute选择"Framed-IP-Address"，Value中输入<&*所指定的地址池名*>，如下图。



Radius配置完毕。

4．LNS上的配置与普通L2TP接入配置基本一致，只是要注意Radius的端口号。虚模板的地址注意要涵盖所有用户的网段，如192.168.0.0/16。如果地址分散，如一部分用户为172.16.1.x/24，一部分用户为192.168.1.x/24，则可加两个虚接口，分别定义地址为172.16.1.x/24网段和192.168.1./x网段，这样LNS就知道去往L2TP客户端应该走虚接口。或者只定义一个虚接口，而另一个网段则用手工添加路由的方式指定到该虚接口。

```
#
 aaa enable
 radius server 10.153.98.67 authentication-port 1645 accounting-port 1646
//配置Radius服务器地址和端口号
 radius shared-key 123
#
 aaa authentication-scheme ppp default radius
aaa accounting-scheme ppp default radius
//配置PPP用户采用Radius认证
#
interface Virtual-Template0
 ppp authentication-mode pap
 ip address 192.168.0.1 255.255.0.0
#
l2tp-group 1
 undo tunnel authentication
 allow l2tp virtual-template 0
#
```

5．L2TP客户端按普通的L2TP接入配置，使用时只要输入相应的用户名就可以得到预想的地址了。