

高手进阶Linux架设最简单的VPN系统 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/237/2021_2022__E9_AB_98_E6_89_8B_E8_BF_9B_E9_c103_237565.htm 公司在北京,但是主要设备都在南京电信的一个主要IDC里,那边有我们的两个PIX525UR(做了故障切换),上面做了严格的访问控制,因此,为了方便公司里的移动,出差及在家的员工办公,才有了做VPN系统的想法.好使具有相应权限的使用者从个人PC通过支持MPPE128的加密隧道连接至公司的VPN Server,再通过VPN Server将数据转发到南京IDC的我公司应用网络,其间的连接也是基于IPSEC的安全VPN隧道.由此可以保证我公司的所有应用需求的安全性和便捷性。

1.硬件资源：服务器一台 PIX 525UR防火墙一台
2.软件资源：Mandrake 9.2 kernelmod pptpd Super-freeswan iptables 公网ip地址
注：我在测试了几种LINUX(包括Redhat,SuSE,Mandrake,Astaro)后,感觉Mandrake是最简单,最稳妥的平台。下面就是安装过程：

1.操作系统安装：安装过程无特殊要求,在选择安装组件的时候除开发工具外其它一概不选,主要是出于安全性考虑。
2.安装kernelmod：
tar zxvf kernelmod-0.7.1.tar.gz cd /kernelmod ./ kernelmod.sh
3.安装pptpd：升级ppp rpm Uvh ppp-2.4.2-0.1b3.i386.rpm 安装pptpd rpm ivh pptpd-1.1.4-1b4.fr.i386.rpm
4.安装Super-freeswan：rpm ivh super-freeswan-1.99.8-8.2.100mdk.i586.rpm
5.升级iptables：rpm Uvh iptables-1.2.8-12.i386.rpm
呵...至此，全部的安装过程就完成了，简单吧，注:以上软件都可以在rpmfind.net找到！

下面是最主要的配置过程：1.操作系统的配置：升级openssh

关闭不需要的服务(sendmail isdn ...) 编辑/etc/sysctl.conf
net.ipv4.ip_forward = 0=>1 net.ipv4.conf.default.rp_filter = 1=>0
2.Pix配置文件(VPN部分) : access-list inside_outbound_nat0_acl
permit ip "南京IP段" 255.255.255.0 "公司VPN用户的IP段"
255.255.255.0 access-list outside_cryptomap_20 permit ip "南京IP
段" 255.255.255.0 "公司VPN用户的IP段" 255.255.255.0 nat
(inside) 0 access-list inside_outbound_nat0_acl sysopt connection
permit-ipsec crypto ipsec transform-set ESP-3DES-MD5 esp-3des
esp-md5-hmac crypto map outside_map 20 ipsec-isakmp crypto
map outside_map 20 match address outside_cryptomap_20 crypto
map outside_map 20 set peer "VPN服务器的IP" crypto map
outside_map 20 set transform-set ESP-3DES-MD5 crypto map
outside_map interface outside isakmp enable outside isakmp key "密
码" address "VPN服务器的IP" netmask 255.255.255.255 no-xauth
no-config-mode isakmp identity address isakmp policy 20
authentication pre-share isakmp policy 20 encryption 3des isakmp
policy 20 hash md5 isakmp policy 20 group 2 isakmp policy 20
lifetime 28800 100Test 下载频道开通，各类考试题目直接下载
。详细请访问 www.100test.com