

使用DebianLinux操作系统架设安全网关 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/243/2021_2022__E4_BD_BF_E7_94_A8Debi_c103_243563.htm

1、网关主机设置 服务器上有两块网卡，eth0使用*.*.*.*IP地址连接Internet，eth1连接LAN，则其/etc/network/interfaces的设置如下：

```
auto lo iface lo inet loopback
auto eth0 iface eth0 inet static address *.*.*.* netmask 255.255.255.0 gateway *.*.*.254
auto eth1 iface eth1 inet static address 192.168.0.1 network 192.168.0.0 netmask 255.255.255.0 broadcast 192.168.0.255
```

当然也可以使用ifconfig进行配置：

```
$ ifconfig eth0 *.*.*.* netmask 255.255.255.0
$ route add default gw *.*.*.254
$ ifconfig eth1 192.168.0.1 netmask 255.255.255.0
```

在/etc/resolv.conf中设置，修改或添加nameserver字段：

```
nameserver 202.120.2.101
```

如果ip地址是与mac绑定的，还要修改mac地址：

```
$ ifconfig eth0 down
$ ifconfig eth0 hw ether *:*:*:*:*:*
$ ifconfig eth0 up
```

2、IP伪装（IP-masquerade）这时将lan内主机网关改为192.168.0.1，应该能ping通该网关，但是还是连不上internet。要实现LAN内的机器通过共享一个单独的可访问外网的IP地址来访问Internet资源，还需要在网关上安装ipmasq。

```
$ sudo apt-get install ipmasq
```

会提示进行一些设置，都默认即可。之后lan内主机应该就能连上internet了。

3、端口映射 假设lan内有一ftp192.168.0.2，要从internet上访问该ftp，需要在网关主机上进行一定的端口映射。可使用iptables完成。下面是具体实现的脚本例子：

```
#!/bin/sh
/sbin/modprobe iptable_filter
/sbin/modprobe ip_tables
/sbin/modprobe iptable_nat
/sbin/modprobe ip_nat_ftp
```

```
/sbin/modprobe ip_conntrack /sbin/modprobe ip_conntrack_ftp
iptables -F iptables -P INPUT ACCEPT iptables -P FORWARD
ACCEPT iptables -P OUTPUT ACCEPT iptables -F -t nat iptables
-t nat -A PREROUTING -p tcp -i eth0 -d 202.120.2.101 dport 21 -j
DNAT to 192.168.123.6:21 iptables -t nat -A PREROUTING -p tcp
-i eth0 -d 202.120.2.101 dport 2345 -j DNAT to
192.168.123.116:3389 iptables -t nat -A POSTROUTING -s
192.168.123.0/24 -o eth0 -j SNAT to 202.120.16.34 echo 1 >
/proc/sys/net/ipv4/ip_forward 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
```