**freebsd gateway and ftp**

一、 [网络](http://www.newasp.cn/)环境   
1、主机A：安装freebsd4.7，安装三块网卡fxp0、xl0和xl1。   
fxp0为对外网卡，IP：x.x.x.x ISP为我提供的IP地址   
xl0为对内公共区域网卡，IP：192.168.0.1   
xl1为对内服务提供区域网卡，IP：192.168.80.1   
2、主机B：对外提供www服务主机，ip地址为：192.168.80.80   
3、主机C：对外提供ftp服务主机，ip：192.168.80.3。   
4、其他工作站N台。   
二、编译内核   
  
1、  
  
  
#cd /sys/i386/conf   
#cp GENERIC kernel\_IPF   
  
  
2、编译kernel\_IPF,加入一下选项：   
  
options IPFILTER   
options IPFILTER\_LOG   
options IPFILTER\_DEFAULT\_BLOCK   
  
  
3、   
#/usr/sbin/config kernel\_IPF   
#cd ../../compile/kernel\_IPF   
#make kepend   
#make   
#make install   
  
  
4、编辑/etc/rc.rc.conf,打开以下选项：   
  
defaultrouter="x.x.x.1" x.x.x.1为ISP提供的网关   
gateway\_enable="YES"   
ipfilter\_enable＝"YES"   
ipnat\_enable="YES"   
  
5、重新启动系统：reboot   
三、配置防火墙   
  
1、 设置地址转换ipnat。在/etc下新建文件ipnat.rules,内容为：   
  
map fxp0 192.168.0.0/16 -> 0/32 proxy port ftp ftp/tcp   
map fxp0 192.168.0.0/24 -> 0/32 portmap tcp/udp 10000:30000   
map fxp0 192.168.0.0/24 -> 0/32   
map fxp0 192.168.80.0/24 -> 0/32 portmap tcp/udp 300001:60000   
map fxp0 192.168.80.0/24 -> 0/32 portmap   
rdr fxp0 x.x.x.x/32 port 80 -> 192.168.0.2 port 80   
rdr fxp0 x.x.x.x/32 port ftp -> 192.168.0.3 port ftp   
rdr fxp0 x.x.x.x/32 port 30001-50000 -> 192.168.80.3 port 30001 tcp   
  
  
2、设置包过滤ipfilter。在/etc下新建文件ipf.rules,内容为：   
  
block in log quick all with short   
block in log quick all with ipopts   
block in log quick all with frag   
block in log quick all with opt lsrr   
block in log quick all with opt ssrr   
  
  
以上五句为过滤掉可能会带来安全问题的短数据包或具备路由信息的数据包以及防止非法扫描服务器   
  
  
pass out on xl0 all   
pass in on xlo all   
pass out on xl1 all   
pass in on xl1 all   
pass out quick on lo0 all   
pass in quick on lo0 all   
  
以上为内部[网络](http://www.newasp.cn/)界面和loopback[网络](http://www.newasp.cn/)界面可以自由发送和接受数据包   
  
  
block out on fxp0 all   
  
以上为屏蔽外部[网络](http://www.newasp.cn/)界面向外发送数据包   
  
  
block out log on fxp0 from any to 192.168.0.0/16   
block out log quick on fxp0 from any to 0.0.0.0/8   
block out log quick on fxp0 from any to 169.254.0.0/8   
block out log quick on fxp0 from any to 10.0.0.0/8   
block out log quick on fxp0 from any to 127.16.0.0/12   
block out log quick on fxp0 from any to 127.0.0.0/8   
block out log quick on fxp0 from any to 192.0.2.0/24   
block out log quick on fxp0 from any to 204.152.64.0/23   
block out log quick on fxp0 from any to 224.0.0.0/3   
  
以上为屏蔽不合法地址的输出数据   
  
  
pass out log on fxp0 proto tcp/udp from any to any keep state   
pass out log on fxp0 proto icmp all keep state   
  
以上为允许TCP 、UDP、ICMP数据包向外发送出去，并且允许回应数据包发送回到内部[网络](http://www.newasp.cn/)   
  
  
block in log on fxp0 from 192.168.0.0/16 to any   
block in log quick on fxp0 from 10.0.0.0/8 to any   
block in log quick on fxp0 from 172.16.0.0/12 to any   
block in log quick on fxp0 from 127.0.0.0/8 to any   
block in log quick on fxp0 from 192.0.2.0/24 to any   
block in log quick on fxp0 from 169.254.0.0/16 to any   
block in log quick on fxp0 from 224.0.0.0/3 to any   
block in log quick on fxp0 from 204.152.64.0/23 to any   
block in log quick on fxp0 from x.x.x.x/32 to any   
block in log quick on fxp0 from any to x.x.x.0/32   
block in log quick on fxp0 from any to x.x.x.255/32   
  
以上为屏蔽具备内部[网络](http://www.newasp.cn/)地址的数据包被转发到外部[网络](http://www.newasp.cn/)   
  
  
pass in quick on fxp0 proto tcp from any to any port = 80 flags S/SA keep state   
pass in quick on fxp0 proto tcp from any to any port = ftp flags S/SA keep state   
pass in quick on fxp0 proto tcp from any to any port = ftp-data flags S/SA keep state   
pass in quick on fxp0 proto tcp from any to any port 30000 >< 50001 flags S/SA keep state   
  
以上为允许www和ftp进入，并且允许对ftp数据端口的数据进行转发   
  
  
block in quick on fxp0 all   
  
禁止其他的连接进入fxp0   
  
  
block in log quick on fxp0 proto icmp from any to any icmp-type redir   
block in log quick on fxp0 proto icmp from any to any   
block in log quick on fxp0 proto icmp from any to any icmp-type echo   
  
以上为禁止别人ping我得[网络](http://www.newasp.cn/)   
  
  
block return-rst in log on fxp0 proto tcp from any to any flags S/SA   
block return-icmp(net-unr) in log on fxp0 proto udp from any to any   
  
以上对其他tcp请求，防火墙回应一个RST数据包关闭连接。对UDP请求，防火墙回应[网络](http://www.newasp.cn/)不可达到的ICMP包。   
或者在/etc/sysctl.conf中加入：   
  
net.inet.tcp.blackhole=2   
net.inet.udp.blackhole=1   
  
能够有效地避免端口扫描   
  
3、然后编辑/etc/rc.conf，加入一下命令，让ipfilter和ipnat在系统启动的时候可以自动加载：   
  
ipfilter\_enables=”YES”   
ipf –C –f /etc/ipf.rules   
ipfilter\_flags=”-E”   
  
ipnat\_enable=”YES”   
ipnat\_program=”/sbin/ipnat –CF -f”   
ipnat\_rules=”/etc/ipnat.rules”   
  
ipmon\_enable=”YES”   
ipmon\_flags=”-D /var/log/ipfilter.log”   
  
4、在/usr/log/建立文件ipfilter.log,并更改其属性为755，这样你的防火墙好志就记录到/var/log/ipfilter.log文件中，可以随时对其进行查看。   
  
四、设置FTP服务器，使其支持被动连接（pasv）   
1．Proftpd：编辑你的proftpd的配置文件proftpd.conf,加入一下内容：   
  
MasqueradeAddress x.x.x.x   
PassivePorts 30001 50000   
  
2．Pure-ftpd:编辑你的FTP配置文件，加入一下内容：   
  
PassivePortRange 30001 50000   
ForcePassiveIP x.x.x.x   
  
3．Serv-U:   
  
a、在serv-U的”本地服务器”―――”设置”―――”高级”―――”PASV端口范围”输入30001 50000   
b、在serv-U的”域”―――”你自己建立的域”―――”设置”―――”高级”选中”允许被动模式传送”，” 使用IP”输入：x.x.x.x