[linux5588](http://forum.ubuntu.com.cn/memberlist.php?mode=viewprofile&u=247966&sid=5da000add2878531971393c135d91057)  
2009-02-15 15:51  
自打2.4版本以后的Linux内核中， 提供了一个非常优秀的防火墙工具。这个工具可以对出入服务的网络数据进行分割、过滤、转发等等细微的控制，进而实现诸如防火墙、NAT等功能。  
一般来说， 我们会使用名气比较的大iptables等程序对这个防火墙的规则进行管理。iptables可以灵活的定义防火墙规则， 功能非常强大。但是由此产生的副作用便是配置过于复杂。一向以简单易用著称Ubuntu在它的发行版中，附带了一个相对iptables简单很多的防火墙配置工具：ufw。  
ufw默认是没有启用的。也就是说， ubuntu中的端口默认都是开放的。使用如下命令启动ufw：  
$sudo ufw default deny  
$sudo ufw enable  
通过第一命令，我们设置默认的规则为allow， 这样除非指明打开的端口， 否则所有端口默认都是关闭的。第二个命令则启动了ufw。如果下次重新启动机器， ufw也会自动启动。  
对于大部分防火墙操作来说， 其实无非就是的打开关闭端口。如果要打开SSH服务器的22端口， 我们可以这样：  
$sudo ufw allow 22  
由于在/etc/services中， 22端口对应的服务名是ssh。所以下面的命令是一样的：  
$sudo ufw allow ssh  
现在可以通过下面命令来查看防火墙的状态了：  
$sudo ufw status  
Firewall loaded  
  
To Action From  
-- ------ ----   
22:tcp ALLOW Anywhere  
22:udp ALLOW Anywhere  
我们可以看到， 22端口的tcp和udp协议都打开了。  
删除已经添加过的规则：  
$sudo ufw delete allow 22  
只打开使用tcp/ip协议的22端口：  
$sudo ufw allow 22/tcp  
打开来自192.168.0.1的tcp请求的80端口：  
$sudo ufw allow proto tcp from 192.168.0.1 to any port 22  
要关系防火墙：  
$sudu ufw disable  
  
  
  
  
ubuntu下的ufw防火墙配置  
2009-06-26 23:47  
UFW防火墙是一个主机端的iptables类防火墙配置工具。这个工具的目的是提供给用户一个可以轻松驾驭的界面，就像包集成和动态检测开放的端口一样。  
在Ubuntu中安装UFW：  
目前这个包存在于Ubuntu 8.04的库中。  
sudo apt-get install ufw  
上面这行命令将把软件安装到您系统中。  
开启/关闭防火墙 (默认设置是’disable’)  
# ufw enable|disable  
转换日志状态  
# ufw logging on|off  
设置默认策略 (比如 “mostly open” vs “mostly closed”)  
# ufw default allow|deny  
许 可或者屏蔽某些入埠的包 (可以在“status” 中查看到服务列表［见后文］)。可以用“协议：端口”的方式指定一个存在于/etc/services中的服务名称，也可以通过包的meta-data。 ‘allow’ 参数将把条目加入 /etc/ufw/maps ，而 ‘deny’ 则相反。基本语法如下：  
# ufw allow|deny [service]  
显示防火墙和端口的侦听状态，参见 /var/lib/ufw/maps。括号中的数字将不会被显示出来。  
# ufw status  
［注意：上文中虽然没有使用 sudo，但是命令提示符号都是“#”。所以……你知道啥意思了哈。原文如此。──译者注］  
UFW 使用范例：  
允许 53 端口  
$ sudo ufw allow 53  
禁用 53 端口  
$ sudo ufw delete allow 53  
允许 80 端口  
$ sudo ufw allow 80/tcp  
禁用 80 端口  
$ sudo ufw delete allow 80/tcp  
允许 smtp 端口  
$ sudo ufw allow smtp  
删除 smtp 端口的许可  
$ sudo ufw delete allow smtp  
允许某特定 IP  
$ sudo ufw allow from 192.168.254.254  
删除上面的规则  
$ sudo ufw delete allow from 192.168.254.254  
------------------------------------------  
我自己还用7.10呢，所以翻译的过程中上面步骤没经过试验。  
Ubuntu的名字都很别嘴，一直记不住：  
\* Ubuntu 6.06 LTS (Dapper Drake)  
\* Ubuntu 6.10 (Edgy Eft)  
\* Ubuntu 7.04 (Feisty Fawn)  
\* Ubuntu 7.10 (Gutsy Gibbon)  
\* Ubuntu 8.04 (Hardy Heron)  
  
  
  
ubuntu 防火墙  
2010-01-14 11:02  
ufw是Ubuntu下的一个简易的防火墙配置工具，底层还是调用iptables来处理的，虽然功能较简单，但对桌面型应用来说比较实用，基本常用功能都有，使用也较为容易。  
==鱼漂(admin.net#163.com)原创，转载请注明==  
==http://www.eit.name==  
  
1.安装  
sudo apt-get install ufw  
  
2.启用  
sudo ufw enable  
sudo ufw default deny  
运行以上两条命令后，开启了防火墙，并在系统启动时自动开启。  
关闭所有外部对本机的访问，但本机访问外部正常。  
  
3.开启/禁用  
sudo ufw allow|deny [service]  
打开或关闭某个端口，例如：  
sudo ufw allow smtp　允许所有的外部IP访问本机的25/tcp (smtp)端口  
sudo ufw allow 22/tcp 允许所有的外部IP访问本机的22/tcp (ssh)端口  
sudo ufw allow 53 允许外部访问53端口(tcp/udp)  
sudo ufw allow from 192.168.1.100 允许此IP访问所有的本机端口  
sudo ufw allow proto udp 192.168.0.1 port 53 to 192.168.0.2 port 53  
sudo ufw deny smtp 禁止外部访问smtp服务  
sudo ufw delete allow smtp 删除上面建立的某条规则  
  
4.查看防火墙状态  
sudo ufw status  
  
一般用户，只需如下设置：  
sudo apt-get install ufw  
sudo ufw enable  
sudo default deny  
以上三条命令已经足够安全了，如果你需要开放某些服务，再使用sudo ufw allow开启。  
  
  
  
  
  
  
  
  
Ubuntu防火墙 UFW 设置简介  
2010-03-03 16:27  
1.安装  
sudo apt-get install ufw  
2.启用  
sudo ufw enable  
sudo ufw default deny  
运行以上两条命令后，开启了防火墙，并在系统启动时自动开启。关闭所有外部对本机的访问，但本机访问外部正常。  
3.开启/禁用  
sudo ufw allow|deny [service]  
打开或关闭某个端口，例如：  
sudo ufw allow smtp　允许所有的外部IP访问本机的25/tcp (smtp)端口  
sudo ufw allow 22/tcp 允许所有的外部IP访问本机的22/tcp (ssh)端口  
sudo ufw allow 53 允许外部访问53端口(tcp/udp)  
sudo ufw allow from 192.168.1.100 允许此IP访问所有的本机端口  
sudo ufw allow proto udp 192.168.0.1 port 53 to 192.168.0.2 port 53  
sudo ufw deny smtp 禁止外部访问smtp服务  
sudo ufw delete allow smtp 删除上面建立的某条规则  
4.查看防火墙状态  
sudo ufw status  
一般用户，只需如下设置：  
sudo apt-get install ufw  
sudo ufw enable  
sudo ufw default deny  
以上三条命令已经足够安全了，如果你需要开放某些服务，再使用sudo ufw allow开启。  
开启/关闭防火墙 (默认设置是’disable’)  
sudo ufw enable|disable  
转换日志状态  
sudo ufw logging on|off  
设置默认策略 (比如 “mostly open” vs “mostly closed”)  
sudo ufw default allow|deny  
许可或者屏蔽端口 (可以在“status” 中查看到服务列表)。可以用“协议：端口”的方式指定一个存在于/etc/services中的服务名称，也可以通过包的meta-data。 ‘allow’ 参数将把条目加入 /etc/ufw/maps ，而 ‘deny’ 则相反。基本语法如下：  
sudo ufw allow|deny [service]  
显示防火墙和端口的侦听状态，参见 /var/lib/ufw/maps。括号中的数字将不会被显示出来。  
sudo ufw status  
UFW 使用范例：  
允许 53 端口  
$ sudo ufw allow 53  
禁用 53 端口  
$ sudo ufw delete allow 53  
允许 80 端口  
$ sudo ufw allow 80/tcp  
禁用 80 端口  
$ sudo ufw delete allow 80/tcp  
允许 smtp 端口  
$ sudo ufw allow smtp  
删除 smtp 端口的许可  
$ sudo ufw delete allow smtp  
允许某特定 IP  
$ sudo ufw allow from 192.168.254.254  
删除上面的规则  
$ sudo ufw delete allow from 192.168.254.254  
  
  
  
ubuntu iptables设置  
2010年01月30日 星期六 01:59  
使用 ubuntu 已经有两个星期了， 才忽然发现原来一直都没有安装防火墙， 赶紧去找些资料看看， 下面给出我自己的 iptables 设置，供和我一样新来的兄弟们参考，水平有限，多多指教。（对于防火墙的设置，有两种策略：一种是全部通讯口都允许使用，只是阻止一些我们知道的不安全的或者容易被利用的口；另外一种，则是先屏蔽所有的通讯口，而只是允许我们需要使用的通讯端口。这里使用的是第二种原则，如果你需要开启其他端口，请先参考计算机通讯口说明，然后自己添加。）  
代码:  
＃删除原来 iptables 里面已经有的规则  
iptables -F  
iptables -X  
  
＃抛弃所有不符合三种链规则的数据包  
iptables -P INPUT DROP  
iptables -P OUTPUT DROP  
iptables -P FORWARD DROP  
  
＃设置：本地进程 lo 的 INPUT 和 OUTPUT 链接 ； eth1的 INPUT链  
iptables -A INPUT -i lo -j ACCEPT  
iptables -A INPUT -i eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT  
iptables -A INPUT -i eth1 -m state --state NEW,INVALID -j LOG  
iptables -A OUTPUT -o lo -j ACCEPT  
  
＃对其他主要允许的端口的 OUTPUT设置：  
＃ DNS  
iptables -A OUTPUT -o eth1 -p TCP --sport 1024:65535 --dport 53 -j ACCEPT  
iptables -A OUTPUT -o eth1 -p UDP --sport 1024:65535 --dport 53 -j ACCEPT  
  
＃HTTP  
iptables -A OUTPUT -o eth1 -p TCP --sport 1024:65535 --dport 80 -j ACCEPT  
  
#HTTPS  
iptables -A OUTPUT -o eth1 -p TCP --sport 1024:65535 --dport 443 -j ACCEPT  
  
#Email 接受 和发送  
iptables -A OUTPUT -o eth1 -p TCP --sport 1024:65535 --dport 110 -j ACCEPT  
iptables -A OUTPUT -o eth1 -p TCP --sport 1024:65535 --dport 25 -j ACCEPT  
  
＃ FTP 数据和控制  
iptables -A OUTPUT -o eth1 -p TCP --sport 1024:65535 --dport 20 -j ACCEPT  
iptables -A OUTPUT -o eth1 -p TCP --sport 1024:65535 --dport 21 -j ACCEPT  
  
＃DHCP  
iptables -A OUTPUT -o eth1 -p TCP --sport 1024:65535 --dport 68 -j ACCEPT  
iptables -A OUTPUT -o eth1 -p UDP --sport 1024:65535 --dport 68 -j ACCEPT  
  
#POP3S Email安全接收  
iptables -A OUTPUT -o eth1 -p TCP --sport 1024:65535 --dport 995 -j ACCEPT  
  
＃时间同步服务器 NTP  
iptables -A OUTPUT -o eth1 -p TCP --sport 1024:65535 --dport 123 -j ACCEPT  
  
#拒绝 eth1 其他剩下的  
iptables -A OUTPUT -o eth1 --match state --state NEW,INVALID -j LOG  
  
  
最后是有关于iptables存储的命令：  
代码:  
iptables-save > /etc/iptables.up.rule ＃ 存在你想存的地方  
  
代码:  
iptables-restore < /etc/iptables.up.rules ＃调用  
  
  
因为iptables 在每次机器重新启动以后，需要再次输入或者调用，为了方便操作，使用  
代码:  
sudo gedit /etc/network/interfaces  
  
在  
代码:  
auto ath0  
iface ath0 inet dhcp  
后面加上  
代码:  
pre-up iptables-restore < /etc/iptables.up.rules ＃启动自动调用已存储的iptables  
  
代码:  
post-down iptables-save > /etc/iptables.up.rule #关机时，把当前iptables 储存