ubuntu 的防火墙ufw详解

Inux原始的防火墙工具iptables由于过于繁琐，所以ubuntu系统默认提供了一个基于iptable之上的防火墙工具ufw。而UFW支持图形界面操作，只需在命令行运行ufw命令即能看到一系列的操作。

# 安装软件

apt install net-tools

#查看软件使用端口

netstat -anp

a 表示所有

n表示不查询dns

p表示查询占用的程序

:: 1是压缩格式[IPV6](http://en.wikipedia.org/wiki/IPv6)环回地址0：0：0：0：0：0：0：1。它等效于IPV4地址127.0.0.1

1.安装防火墙

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

sudo ls /var/log/ufw\*

#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