Linux防火墙iptables的前身叫ipfirewall（在内核1.x时代）。

防火墙的五个钩子函数（规则链）。

1 PREROUTING（路由前）

2 INPUT(数据包流入口)

3 FORWARD(转发关卡)

4 OUTPUT(数据包出口)

5 POSTROUTING（路由后）

Iptables有三个表filter nat mangle

 iptables -L -n -v 查看具体规则

例如129服务器上的防火墙规则如下

Chain INPUT (policy ACCEPT)

target prot opt source destination

ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED

ACCEPT icmp -- anywhere anywhere

ACCEPT all -- anywhere anywhere

ACCEPT tcp -- anywhere anywhere state NEW tcp dpt:ssh

ACCEPT tcp -- anywhere anywhere state NEW tcp dpts:vnc-server:5908

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

ACCEPT tcp -- anywhere anywhere tcp dpt:ssh

ACCEPT tcp -- anywhere anywhere tcp dpt:3001

Chain FORWARD (policy ACCEPT)

target prot opt source destination

REJECT all -- anywhere anywhere reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

ACCEPT tcp -- anywhere anywhere tcp spt:ssh

ACCEPT tcp -- anywhere anywhere tcp spt:3001

使用-I来代替-A可以将规则加在前面

防火墙需要修改配置文件啊

vi /etc/sysconfig/iptables

iptables -I INPUT -p tcp --dport 3001 -j ACCEPT

iptables -I OUTPUT -p tcp --sport 3001 -j ACCEPT

iptables -I INPUT -p tcp --dport 80 -j ACCEPT

iptables -I OUTPUT -p tcp --sport 80 -j ACCEPT