Linux系统下IPtables防火墙简易设置方法 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/284/2021_2022_Linux_E7_B3_BB_E7_BB_c103_284464.htm iptables.rule为firewall总规则；iptables.allow为充许进入的主机；iptables.deny为不许放的主机；iptables.allow代码如下：＃！/bin/bash # This is an esay firewall. # the inside interface. if you dont have this one # and you must let this be black ex> INIF="" INIF="eth0" INNET="192.168.160.0/20" # 2.0 load the right module PATH=/sbin：/bin：/usr/sbin：/usr/bin export PATH EXTIF INIF INNET modprobe ip_tables > /dev/null 2>amp.1 modprobe ip_nat_ftp > /dev/null 2>amp.1 modprobe ip_conntrack > /dev/null 2>amp.1 modprobe ip_conntrack_irc > /dev/null 2>&amp.1 # 3.0 clear iptables rule /sbin/iptables -F /sbin/iptables -X /sbin/iptables -Z /sbin/iptables -F -t nat /sbin/iptables -X -t nat /sbin/iptables -Z -t nat /sbin/iptables -P INPUT DROP /sbin/iptables -P OUTPUT ACCEPT /sbin/iptables -P FORWARD ACCEPT /sbin/iptables -t nat -P PREROUTING ACCEPT /sbin/iptables -t nat -P POSTROUTING ACCEPT /sbin/iptables -t nat -P OUTPUT ACCEPT # 4.0 start loading trusted and denied file. if [-f /usr/local/virus/iptables/iptables.allow]；then sh /usr/local/virus/iptables/iptables.allow fi if [-f /usr/local/virus/iptables/iptables.deny]；then sh /usr/local/virus/iptables/iptables.deny fi # 5.0 if the following file exist，please executed if [-f /usr/local/virus/httpd-err/iptables.http]；then sh /usr/local/virus/httpd-err/iptables.http fi # 6.0 allow icmp data packet and the establishd data /sbin/iptables -A INPUT -m state

state ESTABLISHED， RELATED -j ACCEPT AICMP="0 3 3/4 4 11 12 14 16 18" for tyicmp in $AICMP do /sbin/iptables -A INPUT -i $EXTIF="eth0" -p icmp icmp-type $tyicmp -j ACCEPT done