关闭vm下linux声音及文本界面分辨率Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/645/2021_2022__E5_85_B3_E9_97_ADvm_E4_B8_c103_645001.htm bell-style的取值范围是:none, visible, audible，想要把报警声去掉应该是将/etc/inputrc中的set bell-style visible前的#去掉，如果没这句话，可以自己添上 VM安装rhel或linux后,声音很响,如何关闭在terminal下去行下面命令 1:rmmod pcspkr 2 :xset b off以上方法,只是在启动系统后运行才升效,重新启动后还午运行上边的命令,还在寻找更好的好方法这样就不是很响了,真的很震耳朵 Linux字符界面下设置分辨率 vi /boot/grub/menu.lst | 640x480 800x600 1024x768 1280x1024 256 | 0x301 0x303 0x305 0x307 32k | 0x310 0x313 0x316 0x319 64k | 0x311 0x314 0x317 0x31A 16M | 0x312 0x315 0x318 0x31B 其实简单的很，就是grub即可，编辑grub.conf 在kernel /boot/vmlinuz-2.6.9-1.667 ro root=LABEL=/ rhgb quiet后面加上分辨率的设置： kernel /boot/vmlinuz-2.6.9-1.667 ro root=LABEL=/ vga=791 rhgb quiet 不同色彩和分辨率所对应的值

depth-----640x480----800x600----1024x768-----1280x1024

8bit---------769--------771--------773----------775

15bit--------784--------787--------790----------793

16bit--------785--------788--------791----------794

24bit--------786--------789--------792----------795 lilo: 好像添加一行vga=0x31?就行了（很久没用lilo了，有点记不起来啦） 其中0x31?是设定具体分辨率值，可参考一下列表，不要乱设 1280x1024是0x31a 1024x768是0x317 800x600是0x314 640x480

是0x311 Chain INPUT (policy ACCEPT) target prot opt source destination Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination 什么规则都没有.(2)清除原有规则.不管你在安装linux时是否启动了防火墙,如果你想配置属于自己的防火墙,那就清除现在filter的所有规则. [root@tp ~]# iptables -F 清除预设表filter中的所有规则链的规则 [root@tp ~]# iptables -X 清除预设表filter中使用者自定链中的规则我们在来看一下[root@tp ~]# iptables -L -n Chain INPUT (policy ACCEPT) target prot opt source destination Chain FORWARD (policy ACCEPT) target prot opt source destination Chain OUTPUT (policy ACCEPT) target prot opt source destination 什么都没有了吧,和我们在安装linux时没有启动防火墙是一样的.(提前说一句,这些配置就像用命令配置IP一样,重起就会失去作用),怎么保存. [root@tp ~]# /etc/rc.d/init.d/iptables save这样就可以写到/etc/sysconfig/iptables文件里了.写入后记得把防火墙重起一下,才能起作用.[root@tp ~]# service iptables restart现在IPTABLES配置表里什么配置都没有了,那我们开始我们的配置吧(3)设定预设规则[root@tp ~]# iptables -p INPUT DROP[root@tp ~]# iptables -p OUTPUT ACCEPT[root@tp ~]# iptables -p FORWARD DROP 上面的意思是,当超出了IPTABLES里filter表里的两个链规则(INPUT,FORWARD)时,不在这两个规则里的数据包怎么处理呢,那就是DROP(放弃).应该说这样配置是很安全的. 我们要控制流入数据包而对于OUTPUT链,也就是流出的包我们不用做太多限制,而是采取ACCEPT,也就是说,不在着个规则里的包怎么办呢,那就是通过.可以看

出INPUT,FORWARD两个链采用的是允许什么包通过,而OUTPUT链采用的是不允许什么包通过.这样设置还是挺合理的,当然你也可以三个链都DROP,但这样做我认为是没有必要的,而且要写的规则就会增加.但如果你只想要有限的几个规则是,如只做WEB服务器. 还是推荐三个链都是DROP.注:如果你是远程SSH登陆的话,当你输入第一个命令回车的时候就应该掉了.因为你没有设置任何规则.怎么办,去本机操作呗!(4)添加规则.首先添加INPUT链,INPUT链的默认规则是DROP,所以我们就写需要ACCETP(通过)的链为了能采用远程SSH登陆,我们要开启22端口.[root@tp ~]# iptables -A INPUT -p tcp --dport 22 -j ACCEPT[root@tp ~]# iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT (注:这个规则,如果你把OUTPUT 设置成DROP的就要写上这一部,好多人都是望了写这一部规则导致,始终无法SSH.在远程一下,是不是好了.其他的端口也一样,如果开启了web服务器,OUTPUT 设置成DROP的话,同样也要添加一条链:[root@tp ~]# iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT ,其他同理.)如果做了WEB服务器,开启80端口.[root@tp ~]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT 如果做了邮件服务器,开启25,110端口.[root@tp ~]# iptables -A INPUT -p tcp --dport 110 -j ACCEPT [root@tp ~]# iptables -A INPUT -p tcp --dport 25 -j ACCEPT 如果做了FTP服务器,开启21端口[root@tp ~]# iptables -A INPUT -p tcp --dport 21 -j ACCEPT[root@tp ~]# iptables -A INPUT -p tcp --dport 20 -j ACCEPT如果做了DNS服务器,开启53端口[root@tp ~]# iptables -A INPUT -p tcp --dport 53 -j ACCEPT如果你还做了其他的服务器,需要开启哪个端口,照写就行了.上面主要写的都是INPUT链,凡是不在上面的规则

里的,都DROP允许icmp 包通过,也就是允许ping,[root@tp ~]# iptables -A OUTPUT -p icmp -j ACCEPT (OUTPUT设置成DROP的话)[root@tp ~]# iptables -A INPUT -p icmp -j ACCEPT (INPUT设置成DROP的话)允许loopback!(不然会导致DNS无法正常关闭等问题)IPTABLES -A INPUT -i lo -p all -j ACCEPT (如果是INPUT DROP) IPTABLES -A OUTPUT -o lo -p all -j ACCEPT(如果是OUTPUT DROP) 下面写OUTPUT链,OUTPUT链默认规则是ACCEPT,所以我们就写需要DROP(放弃)的链.减少不安全的端口连接[root@tp ~]# iptables -A OUTPUT -p tcp --sport 31337 -j DROP[root@tp ~]# iptables -A OUTPUT -p tcp --dport 31337 -j DROP有些些特洛伊木马会扫描端口31337到31340(即黑客语言中的 elite 端口)上的服务。既然合法服务都不使用这些非标准端口来通信,阻塞这些端口能够有效地减少你的网络上可能被感染的机器和它们的远程主服务器进行独立通信的机会还有其他端口也一样,像:31335、27444、27665、20034 NetBus、9704、137-139（smb）,2049(NFS)端口也应被禁止,我在这写的也不全,有兴趣的朋友应该去查一下相关资料.当然出入更安全的考虑你也可以包OUTPUT链设置成DROP,那你添加的规则就多一些,就像上边添加允许SSH登陆一样.照着写就行了.下面写一下更加细致的规则,就是限制到某台机器如:我们只允许192.168.0.3的机器进行SSH连接[root@tp ~]# iptables -A INPUT -s 192.168.0.3 -p tcp --dport 22 -j ACCEPT如果要允许,或限制一段IP地址可用 192.168.0.0/24 表示192.168.0.1-255端的所有IP.24表示子网掩码数.但要记得把 /etc/sysconfig/iptables 里的这一行删了.-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT 因为它表示所有地址

都可以登陆.或采用命令方式:[root@tp ~]# iptables -D INPUT -p tcp --dport 22 -j ACCEPT然后保存,我再说一边,反是采用命令的方式,只在当时生效,如果想要重起后也起作用,那就要保存.写入到/etc/sysconfig /iptables文件里.[root@tp ~]# /etc/rc.d/init.d/iptables save这样写 !192.168.0.3 表示除了192.168.0.3的ip地址其他的规则连接也一样这么设置.在下面就是FORWARD链,FORWARD链的默认规则是DROP,所以我们就写需要ACCETP(通过)的链,对正在转发链的监控.开启转发功能,(在做NAT时,FORWARD默认规则是DROP时,必须做)[root@tp ~]# iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT[root@tp ~]# iptables -A FORWARD -i eth1 -o eh0 -j ACCEPT丢弃坏的TCP包[root@tp ~]#iptables -A FORWARD -p TCP ! --syn -m state --state NEW -j DROP处理IP碎片数量,防止攻击,允许每秒100个[root@tp ~]#iptables -A FORWARD -f -m limit --limit 100/s --limit-burst 100 -j ACCEPT设置ICMP包过滤,允许每秒1个包,限制触发条件是10个包.[root@tp ~]#iptables -A FORWARD -p icmp -m limit --limit 1/s --limit-burst 10 -j ACCEPT我在前面只所以允许ICMP包通过,就是因为我在这里有限制.二,配置一个NAT表放火墙1,查看本机关于NAT的设置情况[root@tp rc.d]# iptables -t nat -L Chain PREROUTING (policy ACCEPT) target prot opt source destination Chain POSTROUTING (policy ACCEPT) target prot opt source destination SNAT all -- 192.168.0.0/24 anywhere to:211.101.46.235Chain OUTPUT (policy ACCEPT) target prot opt source destination 我的NAT已经配置好了的(只是提供最简单的代理上网功能,还没有添加防火墙规

则).关于怎么配置NAT,参考我的另一篇文章当然你如果还没有配置NAT 的话,你也不用清除规则,因为NAT在默认情况下是什么都没有的如果你想清除,命令是[root@tp ~]# iptables -F -t nat[root@tp ~]# iptables -X -t nat[root@tp ~]# iptables -Z -t nat2,添加规则添加基本的NAT地址转换,(关于如何配置NAT可以看我的另一篇文章),添加规则,我们只添加DROP链.因为默认链全是 ACCEPT.防止外网用内网IP欺骗[root@tp sysconfig]# iptables -t nat -A PREROUTING -i eth0 -s 10.0.0.0/8 -j DROP [root@tp sysconfig]# iptables -t nat -A PREROUTING -i eth0 -s 172.16.0.0/12 -j DROP [root@tp sysconfig]# iptables -t nat -A PREROUTING -i eth0 -s 192.168.0.0/16 -j DROP 如果我们想,比如阻止MSN,QQ,BT等的话,需要找到它们所用的端口或者IP,(个人认为没有太大必要)例：禁止与211.101.46.253的所有连接[root@tp ~]# iptables -t nat -A PREROUTING -d 211.101.46.253 -j DROP禁用FTP(21)端口 [root@tp ~]# iptables -t nat -A PREROUTING -p tcp --dport 21 -j DROP这样写范围太大了,我们可以更精确的定义.[root@tp ~]# iptables -t nat -A PREROUTING -p tcp --dport 21 -d 211.101.46.253 -j DROP 这样只禁用211.101.46.253地址的FTP连接,其他连接还可以.如web(80端口)连接.按照我写的,你只要找到QQ,MSN等其他软件的 IP地址,和端口,以及基于什么协议,只要照着写就行了.最后：0drop非法连接 [root@tp ~]# iptables -A INPUT -m state --state INVALID -j DROP [root@tp ~]# iptables -A OUTPUT -m state --state INVALID -j DROP [root@tp ~]# iptables-A FORWARD -m state --state INVALID -j DROP 允许所有已经建立的和相关的连接 [root@tp ~]# iptables-A INPUT -m state

--state ESTABLISHED,RELATED -j ACCEPT [root@tp ~]# iptables-A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT [root@tp ~]# /etc/rc.d/init.d/iptables save 这样就可以写到/etc/sysconfig/iptables文件里了.写入后记得把防火墙重起一下,才能起作用． [root@tp ~]# service iptables restart