Linux系统防火墙防止DOS和DDOS攻击 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/290/2021_2022_Linux_E7_B3_BB_E7_BB_c103_290068.htm 用Linux 系统防火墙功能抵御网络攻击 虚拟主机服务商在运营过程中可能会受到黑客攻击，常见的攻击方式有SYN ，DDOS等。通过更换IP，查找被攻击的站点可能避开攻击，但是中断服务的时间比较长。比较彻底的解决方法是添置硬件防火墙。不过，硬件防火墙价格比较昂贵。可以考虑利用Linux 系统本身提供的防火墙功能来防御。? 1. 抵御SYN SYN攻击是利用TCP/IP协议3次握手的原理，发送大量的建立连接的网络包，但不实际建立连接，最终导致被攻击服务器的网络队列被占满，无法被正常用户访问。 Linux内核提供了若干SYN相关的配置，用命令： sysctl -a | grep syn 看到： net.ipv4.tcp_max_syn_backlog = 1024 net.ipv4.tcp_syncookies = 0 net.ipv4.tcp_synack_retries = 5 net.ipv4.tcp_syn_retries = 5 tcp_max_syn_backlog是SYN队列的长度，tcp_syncookies是一个开关，是否打开SYN Cookie功能，该功能可以防止部分SYN攻击。tcp_synack_retries和tcp_syn_retries定义SYN的重试次数。 加大SYN队列长度可以容纳更多等待连接的网络连接数，打开SYN Cookie功能可以阻止部分SYN攻击，降低重试次数也有一定效果。 调整上述设置的方法是： 增加SYN队列长度到2048： sysctl -w net.ipv4.tcp_max_syn_backlog=2048 打开SYN COOKIE功能： sysctl -w net.ipv4.tcp_syncookies=1 降低重试次数： sysctl -w net.ipv4.tcp_synack_retries=3 sysctl -w net.ipv4.tcp_syn_retries=3 为了系统重启动时保持上述配置，可将上述命令加入

到/etc/rc.d/rc.local文件中。 2. 抵御DDOS DDOS，分布式拒绝访问攻击，是指黑客组织来自不同来源的许多主机，向常见的端口，如80，25等发送大量连接，但这些客户端只建立连接，不是正常访问。由于一般Apache配置的接受连接数有限（通常为256），这些“ 假 ”访问会把Apache占满，正常访问无法进行。 Linux提供了叫ipchains的防火墙工具，可以屏蔽来自特定IP或IP地址段的对特定端口的连接。使用ipchains抵御DDOS，就是首先通过netstat命令发现攻击来源地址，然后用ipchains命令阻断攻击。发现一个阻断一个。 *** 打开ipchains功能 首先查看ipchains服务是否设为自动启动： chkconfig --list ipchains 输出一般为： ipchains 0:off 1:off 2:on 3:on 4:on 5:on 6:off 如果345列为on，说明ipchains服务已经设为自动启动 如果没有，可以用命令： chkconfig --add ipchains 将ipchains服务设为自动启动 其次，察看ipchains配置文件/etc/sysconfig/ipchains是否存在。如果这一文件不存在，ipchains 即使设为自动启动，也不会生效。缺省的ipchains配置文件内容如下： # Firewall configuration written by lokkit # Manual customization of this file is not recommended. # Note: ifup-post will punch the current nameservers through the # firewall. such entries will *not* be listed here. :input ACCEPT :forward ACCEPT :output ACCEPT -A input -s 0/0 -d 0/0 -i lo -j ACCEPT # allow http,ftp,smtp,ssh,domain via tcp. domain via udp -A input -p tcp -s 0/0 -d 0/0 pop3 -y -j ACCEPT -A input -p tcp -s 0/0 -d 0/0 http -y -j ACCEPT -A input -p tcp -s 0/0 -d 0/0 https -y -j ACCEPT -A input -p tcp -s 0/0 -d 0/0 ftp -y -j ACCEPT -A input -p tcp -s 0/0 -d 0/0 smtp -y -j ACCEPT -A input -p tcp -s 0/0 -d 0/0 ssh -y -j

ACCEPT -A input -p tcp -s 0/0 -d 0/0 domain -y -j ACCEPT -A input -p udp -s 0/0 -d 0/0 domain -j ACCEPT # deny icmp packet #-A input -p icmp -s 0/0 -d 0/0 -j DENY # default rules -A input -p tcp -s 0/0 -d 0/0 0:1023 -y -j REJECT -A input -p tcp -s 0/0 -d 0/0 2049 -y -j REJECT -A input -p udp -s 0/0 -d 0/0 0:1023 -j REJECT -A input -p udp -s 0/0 -d 0/0 2049 -j REJECT -A input -p tcp -s 0/0 -d 0/0 6000:6009 -y -j REJECT -A input -p tcp -s 0/0 -d 0/0 7100 -y -j REJECT