用Linux操作系统防火墙防止DOS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_ti2020/144/2021_2022__E7_94_A8Linux_E6_93_c103_144938.htm 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 = 1024net.ipv4.tcp_syncookies = 0net.ipv4.tcp_synack_retries = 5net.ipv4.tcp_syn_retries = 5tcp_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=3sysctl -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。 100Test 下载频道开通，各类考试