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。

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。

防止同步包洪水（Sync Flood）   
# iptables -A FORWARD -p tcp --syn -m limit --limit 1/s -j ACCEPT   
也有人写作   
#iptables -A INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT   
--limit 1/s 限制syn并发数每秒1次，可以根据自己的需要修改  
防止各种端口扫描   
# iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s -j ACCEPT   
Ping洪水攻击（Ping of Death）   
# iptables -A FORWARD -p icmp --icmp-type echo-request -m limit --limit 1/s -j ACCEPT

|  |  |
| --- | --- |
| 分享至 |  |