nginx+php产生大量TIME_WAIT连接解决办法

问题：当启动nginx和php-fpm时，使用netstat -tunap查看到大量TIME_WAIT连接

由于不知道原因，害怕是受到攻击，马上killall nginx 和php-fpm

会不会是80端口被攻击造成的？尝试修改nginx的80端口为8081，但结果同样是产生大量TIME_WAIT连接

无法知道问题，百度寻找办法

参考链接：http://www.heminjie.com/wordpress/3322.html

还没有解决

到晚上回到家自己重新测试才有所改善，并发现了某些问题

netstat -tunap 与 netstat -tunlp 导致以前没看到这种情况

常见参数

-a (all)显示所有选项，默认不显示LISTEN相关
-t (tcp)仅显示tcp相关选项
-u (udp)仅显示udp相关选项
-n 拒绝显示别名，能显示数字的全部转化成数字。
-l 仅列出有在 Listen (监听) 的服務状态

-p 显示建立相关链接的程序名
-r 显示路由信息，路由表
-e 显示扩展信息，例如uid等
-s 按各个协议进行统计
-c 每隔一个固定时间，执行该netstat命令。

提示：LISTEN和LISTENING的状态只有用-a或者-l才能看到

最后参考各个博客，完成优化

vim /etc/sysctl.conf

在最后增加下列参数：

net.ipv4.tcp_syncookies = 1

net.ipv4.tcp_tw_reuse = 1

net.ipv4.tcp_tw_recycle = 1

net.ipv4.tcp_fin_timeout = 30

net.ipv4.tcp_syn_retries = 5

net.ipv4.tcp_synack_retries = 5

net.ipv4.tcp_keepalive_time = 1200

net.ipv4.ip_local_port_range = 1024 65000

net.ipv4.tcp_max_syn_backlog = 8192

net.ipv4.tcp_max_tw_buckets = 5000

详细参考链接:http://leven.blog.51cto.com/1675811/382097

一 TIME_WAIT产生原因:

1、nginx现有的负载均衡模块实现php fastcgi负载均衡，nginx使用了短连接方式，所以会造成大量处于TIME_WAIT状态的连接。

2、TCP/IP设计者本来是这么设计的

主要有两个原因

⑴ 防止上一次连接中的包，迷路后重新出现，影响新连接

（经过2MSL，上一次连接中所有的重复包都会消失）

⑵ 可靠的关闭TCP连接

在主动关闭方发送的最后一个 ack(fin) ，有可能丢失，这时被动方会重新发 fin, 如果这时主动方处于 CLOSED 状态 ，就会响应 rst 而不是 ack。所以主动方要处于 TIME_WAIT 状态，而不能是 CLOSED 。

二 过多TIME_WAIT危害

TIME_WAIT 并不会占用很大资源的，除非受到攻击。只要把TIME_WAIT所占用内存控制在一定范围。一般默认最大是35600条TIME_WAIT。

三 解决方法

net.ipv4.tcp_syncookies = 1 表示开启SYN Cookies。当出现SYN等待队列溢出时，启用cookies来处理，可防范少量SYN攻击，默认为0，表示关闭；

net.ipv4.tcp_tw_reuse = 1 表示开启重用。允许将TIME-WAIT sockets重新用于

新的TCP连接，默认为0，表示关闭；
net.ipv4.tcp_tw_recycle = 1 表示开启TCP连接中TIME-WAIT sockets的快速回收，默认为0，表示关闭。
net.ipv4.tcp_fin_timeout = 30 表示如果套接字由本端要求关闭，这个参数决定了它保持在FIN-WAIT-2状态的时间。
net.ipv4.tcp_keepalive_time = 1200 表示当keepalive起用的时候，TCP发送keepalive消息的频度。缺省是2小时，改为20分钟。
net.ipv4.ip_local_port_range = 1024 65000 表示用于向外连接的端口范围。缺省情况下很小：32768到61000，改为1024到65000。
net.ipv4.tcp_max_syn_backlog = 8192 表示SYN队列的长度，默认为1024，加大队列长度为8192，可以容纳更多等待连接的网络连接数。
net.ipv4.tcp_max_tw_buckets = 5000 表示系统同时保持TIME_WAIT套接字的最大数量，如果超过这个数字，TIME_WAIT套接字将立刻被清除并打印警告信息。
默 认为180000，改为5000。对于Apache、Nginx等服务器，上几行的参数可以很好地减少TIME_WAIT套接字数量，但是对于Squid，效果却不大。此项参数可以控制TIME_WAIT套接字的最大数量，避免Squid服务器被大量的TIME_WAIT套接字拖死。

注:
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_tw_recycle = 1
设置这两个参数： reuse是表示是否允许重新应用处于TIME-WAIT状态的socket用于新的TCP连接； recyse是加速TIME-WAIT sockets回收