**TCP Flood攻击**

SYN Flood是当前最流行的DoS（拒绝服务攻击）与DDoS（分布式拒绝服务攻击）的方式之一，这是一种利用TCP协议缺陷，发送大量伪造的TCP连接请求，常用假冒的IP或IP号段发来海量的请求连接的第一个握手包（SYN包），被攻击服务器回应第二个握手包（SYN+ACK包），因为对方是假冒IP，对方永远收不到包且不会回应第三个握手包。导致被攻击服务器保持大量SYN\_RECV状态的“半连接”，并且会重试默认5次回应第二个握手包，塞满TCP等待连接队列，资源耗尽（CPU满负荷或内存不足），让正常的业务请求连接不进来。

**检查方法：**

# netstat -n | awk '/^tcp/ {++S[$NF]} END {for(a in S) print a, S[a]}'

**应急处理方法：**

使用如下方法获取罪证IP：

# netstat -na |grep SYN\_RECV|more

利用iptables临时封掉最大嫌疑攻击的IP或IP号段，例如对方假冒173.\*.\*.\*号段来攻击，短期禁用173.\*.\*.\*这个大号段（要确认小心不要封掉自己的本地IP了！）

# iptables -A INPUT -s  173.0.0.0/8  -p tcp  –dport 80 -j DROP

**常规解决方法：**

采用方式：让客户端先和F5三次握手，连接建立之后F5才转发到后端业务服务器。

**调整系统参数挡攻击**

第一个参数tcp\_synack\_retries = 0是关键，表示回应第二个握手包（SYN+ACK包）给客户端IP后，如果收不到第三次握手包（ACK包）后，不进行重试，加快回收“半连接”，不要耗光资源。（修改这个参数为0的副作用：网络状况很差时，如果对方没收到第二个握手包，可能连接服务器失败，但对于一般网站，用户刷新一次页面即可。这些可以在高峰期或网络状况不好时tcpdump抓包验证下。之所以可以把tcp\_synack\_retries改为0，因为客户端还有tcp\_syn\_retries参数，默认是5，即使服务器端没有重发SYN+ACK包，客户端也会重发SYN握手包。）