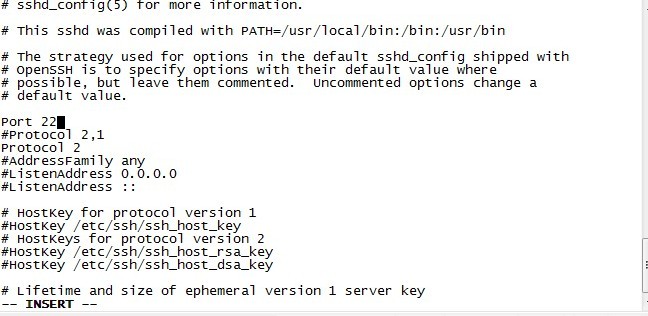
[**linux下SSH攻击解决方法**](http://blog.csdn.net/alone_map/article/details/51850479)

**清明晚上公司网络突然中断，排查了各种可能性（包括环路、arp攻击、DOS、DDOS等）均无果。无奈只好使用专业的流量分析器，发现流量正常，我等一行人直接被拒了...经过仔细观察，发现会话数这里有了问题，SSH会话数量严重超标！随机个跟踪到SSH回话建立于某服务器，将之断网后公司网络恢复正常，至此元凶找到。  
      解决方案：本服务器为linux系统，修改SSH端口，禁止root进行SSH登录，启用Iptables防火墙阻止SSH访问（或开放允许的端口）。  
   
第一步：修改SSH端口**

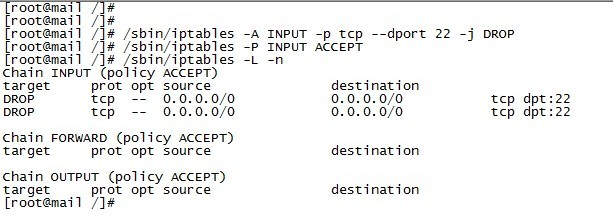
**vi /etc/ssh/sshd\_config**

****

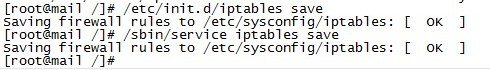
**第二步：修改SSH禁止root登录  
vi /etc/ssh/sshd\_config  
PermitRootLogin no**

****

**第三步：  
iptables做访问控制**

****

**保存防火墙配置**

****

**之前用TCP\_Warppers试过，效果不好。因为TCP\_Warppers是在建立连接后才进行判断的，所以这个方法只维持了半个小时不到网络又阻塞了。**