详细介绍Linux网络部分优化策略方法 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__E8_AF_A6_E7_BB_86_E4_BB_8B_E7_c103_144703.htm 关于 SYN_RECV 的杂七杂八的东西 Posted by kreny at September 8, 2004 10:38 PM | Trackback URL: http://weblog.dalouis.com/cgi-bin/mt-tb.cgi/147 网页在翻页到一个特定的页面的时候，和服务器80端口的连接被中止。 查看了netstat -anlp 发现有类似以下的记录，而IP就是我的。 tcp 0 2560 61.152.251.68:80 60.26.156.241:1523 SYN_RECV - 由于可能是程序的问题，因为仅仅在浏览这张网页的时候会出现这个问题，但是还是在netstat里面偶尔会看到几个 SYN_RECV ,所以就google了一下，在此总结一下。 1. 对于大量的 SYN_RECV 若怀疑是SYN Flood攻击，有以下建议: 这个攻击的解决方法如下： 1，增加未完成连接队列（q0)的最大长度。 echo 1280>./proc/sys/net/ipv4/tcp_max_syn_backlog 2, 启动SYN_cookie。 echo 1>./proc/sys/net/ipv4/tcp_syncookies 这些是被动的方法，治标不治本。而且加大了服务器的负担，但是可以避免被拒绝攻击（只是减缓） 治本的方法是在防火墙上做手脚。但是现在能在一定程度上防住syn flood攻击的防火墙都不便宜。并且把这个命令加入"/etc/rc.d/rc.local"文件中,如果对 /proc/sys/net/ipv4 下的配置文件进行解释，可以参阅LinuxAid技术站的文章。查看本文全文也可以参阅。 关于 syn cookies， 请参阅 . http://cr.yp.to/syncookies.html,也许使用mod_limitipconn.c来限制apache的并发数 也会有一定的帮助。最终，仅仅修改了这个参数，但是也加上了iptables的防火

墙规则，问题解决。 2.什是 TCP SYN Flood 攻 TCP SYN Flood 是一常，而且有效的端(程)拒服(Denial of Service)攻方式，它透一定的操作破TCP三次握手建立正常接，用耗系源，使得提供TCP服的主系法正常工作。 由於TCP SYN Flood是透路底服器Server行攻的，它可以在任意改自己的路IP地址的同，不被路上的其他所，就防路犯罪部追查犯罪源造成很大的困。在外的站中，攻不。在一拍站上，曾有犯罪分子利用手段，在低位阻止其他用商品拍，干拍程的正常作。 系查 一般情下，可以一些步行查，判系是否正在遭受TCP SYN Flood攻。 1、 服端法提供正常的TCP服。接求被拒或超。 2、透 netstat -an 命令查系，有大量的SYN_RECV接。 3. iptables的设置，引用自CU 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 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com