

路由器上用tcp拦截防止dos攻击 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/250/2021\\_2022\\_\\_E8\\_B7\\_AF\\_E7\\_94\\_B1\\_E5\\_99\\_A8\\_E4\\_c101\\_250990.htm](https://www.100test.com/kao_ti2020/250/2021_2022__E8_B7_AF_E7_94_B1_E5_99_A8_E4_c101_250990.htm)

1) 定义一个acl，目的是要保护的机器：`access-list 101 per tcp any host 202.106.0.20` 由于没必要匹配源地址，一般的dos都伴随着地址欺骗，所以这里的source都是any. 2) 全局下开启tcp intercept. `ip tcp intercept list 101` 3) 设置tcp拦截的模式，tcp拦截有两种模式一种是拦截，一种是监视。拦截模式像是一个找茬的流氓，看谁都不爽，见谁都打。监视模式是一个稍微理性一点的流氓，仅仅当别人在他家门口那片空地赌着不走的时候才大打出手（默认是30秒）。见谁都打，肯定累啊。我们要理性一点。`ip tcp intercept mode watch ip tcp intercept watch-timeout 20` 4) 另外tcp连接你也不能一辈子都让他连着。设置一个tcp超时时间，默认24小时，一般网中特殊服务的需要长连接的应用时候30分钟足啖 `ip tcp intercept connection-timeout 1800` 5) 对于最大半开连接的门限也是可以更改的。默认low 900, high 1100. `ip tcp intercept max-incomplete low 800 ip tcp intercept max-incomplete high 1000` 6) 状态查看 `show tcp intercept connecitons show tcp intercept statistics` 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](http://www.100test.com)