Dos攻击预防

1. 常规Dos攻击预防

1. 每台网络设备或主机都需要随时更新其系统漏洞、关闭不需要的服务、安装必要的防毒和防火墙软件、随时注意系统安全，避免被黑客和自动化的DoS程序植入攻击程序，以免成为黑客攻击的帮凶。

2. 有些DoS会伪装攻击来源，假造封包的来源ip，使人难以追查，这个部份可以透过设定路由器的过滤功能来防止，只要网域内的封包来源是其网域以外的ip，就应该直接丢弃此封包而不应该再送出去；

3. 网域之间保持联络是很重要的，如此才能有效早期预警和防治DoS攻击，有些ISP会在一些网络节点上放置感应器侦测突然的巨大流量，以提早警告和隔绝DoS的受害区域，降低顾客的受害程度。

4．防范dos攻击，还需要对路由器进行相关的安全设置。

5.

1. 低速Dos攻击预防
2. 随机化minRTO方法的优缺点

（1）优点：该方法原理简单，在实际操作中容易实现；

（2）缺点：只是在一定程度上缓解 shrew攻击造成的网络性能低下状况，并没有从根本上消除shrew攻击的影响，可 以说只治了“标”并未“治本”；

将minRTO进行随机化处理需要一定的系 统开销。

路由器辅助检测