用思科路由对DDOS攻击的防御思路 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E7_94_A8_E6_80_9D_E7_A7_91_E8_c101_142591.htm 面对日益复杂的网络环境，各种潜在的安全问题以及不诡的而已攻击，让我们的网络随时处在一个危险之地，在信息时代的今天，保证服务器稳定高效率的运转和防控这些恶意攻击使网管们焦头烂额。特别是DDOS这种简单并且非常迅猛的攻击方式，几乎已经让很多站长、网管焦头烂额了，这里将着重讲述DDOS的防控。 DDOS分布式拒绝服务攻击的简写，是目前网络上最流行、最有效的打垮一个服务器的最有效途径之一。对于他的防控可以说只能被动防控，在挨了打才知道还手，如何才能建立一个预警机制呢？ 先下手为强，建立机制主动防御DDOS Guard和Detector是CISCO公司今年收购的，并将其模块化是最热门模块之一，他们对DDOS的防控可以说是前无来着的产品，效率非常的高。在没有遭到DDOS的时候Guard模块是处于休眠状态，也可以说是离线状态，当Detector收到发往受保护的终端时，通过算法分析和策略匹配，确定受到攻击。此时Detector将以SSH与Guard建立连接，激活Guard对保护终端进行保护。Guard也将进行策略和算法分析，给出适当的处理方案丢弃非法数据包，限制速率等方式，将通过策略和算法分析的数据包发往目的地。整个防御过程就结束了，同时这个模块还有智能学习的功能可以使防御更加精确，这个模块的设置非常的简单，因为可以进行图形化的操作，所以在这里就不再赘述了。 当然要防御DDOS攻击在没有Guard模块的路由器上依然能实现，比如

使用最常用的ip verfy unicast reverse-path接口命令可以将伪装过的数据包抛弃掉，判断的标准最简单的就是有没有反向传输数据包时所需的路由；通过ACL过滤RFC1918中的所有地址，RFC1918就是所有局域网地址的集合如10.*.*.*，192.*.*.*，172.*.*.*这类保留地址。 后来者居上，解除DDOS攻击警报当然，它有疏忽大意而让蟊贼得逞的时候，这个时候网管要做的就是第一时间干掉攻击者，要想干掉攻击者就要做出正确的判断，那些是虚假的IP，那些是真实的，找出真实的IP屏蔽他，这种方式的好处是能立杆见影，立即清除不法分子，但是这个方法的害处是一些无辜的用户也有可能被判定为攻击源。当然你也可以通过对攻击者的路由屏蔽，虽然也能清楚攻击，但是他的误伤概率扩大了，整个通过该路由的访问都将被屏蔽，但是为了更稳定的服务环境也只能这样做了。还有限制ICMP和SYN数据包流量速率的方式都是可以非常有效控制DDOS攻击的。 这里仅仅是提供一个防控的思路，对于使用CISCO路由的用户相信这写操作都是非常简单的，其实在防控DDOS攻击这场战役中受攻击者普遍都只能在降低攻击级别和效果上突破，减轻DDOS攻击的危害程度，它的攻击变化无常，随时都可以更换肉鸡进行攻击，本文中提到CSICO的Guard模块也许是最有效的方式，可以更精确的找到攻击者，在策略的制定上更有研究或许能有更大的突破。