最大限度减轻DDoS攻击的危害 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/240/2021_2022__E6_9C_80_E5_A4_A7_E9_99_90_E5_c101_240549.htm 大部分网络都很容易受到各种类型的黑客攻击，但是我们可以通过一套安全规范来最大限度的防止黑客攻击的发生。 但是，分布式拒绝服务攻击（DDoS）是一个完全不同的攻击方式，你无法阻止黑客对你的网站发动DDoS攻击，除非你主动断开互联网连接。如果我们无法防止这种攻击，那么怎么做才能最大限度地保护企业网络呢？ 首先你应该清楚的了解DDoS攻击的三个阶段，然后再学习如何将这种攻击的危害降到最低。 理解DDoS攻击 一个DDoS攻击一般分为三个阶段。第一阶段是目标确认：黑客会在互联网上锁定一个企业网络的IP地址。这个被锁定的IP地址可能代表了企业的 Web服务器，DNS服务器，互联网网关等。而选择这些目标进行攻击的目的同样多种多样，比如为了赚钱（有人会付费给黑客攻击某些站点），或者只是以破坏为乐。 第二个阶段是准备阶段：在这个阶段，黑客会入侵互联网上大量的没有良好防护系统的计算机（基本上就是网络上的家庭计算机，DSL宽带或有线电缆上网方式为主）。黑客会在这些计算机中植入日后攻击目标所需的工具。 第三个阶段是实际攻击阶段：黑客会将攻击命令发送到所有被入侵的计算机（也就是僵尸计算机）上，并命令这些计算机利用预先植入的攻击工具不断向攻击目标发送数据包，使得目标无法处理大量的数据或者频宽被占满。聪明的黑客还会让这些僵尸计算机伪造发送攻击数据包的IP地址，并且将攻击目标的IP地址插在数据包的原始地址处，

这就是所谓的反射攻击。服务器或路由器看到这些资料包后会转发（即反射）给原始IP地址一个接收响应，更加重了目标主机所承受的数据流。 因此，我们无法阻止这种DDoS攻击，但是知道了这种攻击的原理，我们就可以尽量减小这种攻击所带来的影响。 减少攻击影响 入侵过滤（Ingress filtering）是一种简单而且所有网络（ISP）都应该实施的安全策略。在你的网络边缘（比如每一个与外网直接相连的路由器），应该建立一个路由声明，将所有数据来来源IP标记为本网地址的数据包丢弃。虽然这种方式并不能防止DDoS攻击，但是却可以预防DDoS反射攻击。 减轻DDoS攻击危害 但是很多大型ISP好像都因为各种原因拒绝实现入侵过滤，因此我们需要其它方式来降低DDoS带来的影响。目前最有效的一个方法就是反追踪（backscatter traceback method）。 要采用这种方式，首先应该确定目前所遭受的是外部DDoS攻击，而不是来自内网或者路由问题。接下来就要尽快在全部边缘路由器的外部接口上进行配置，拒绝所有流向DDoS攻击目标的数据流。另外，还要在这些边缘路由器端口上进行配置，将全部无效或无法定位的数据来源IP的数据包丢弃。比如以下地址：以下是引用片段：10.0.0.0 - 10.255.255.255172.16.0.0 - 172.31.255.255192.168.0.0 - 192.168.255.255 将路由器设置为拒绝这些资料包后，路由器会在每次拒绝数据包时发送一个因特网控制讯息协议（ICMP）包，并将"destination unreachable"信息和被拒绝的数据包打包发送给来源IP地址。 接下来，打开路由器日志，查看那个路由器收到的攻击资料包最多。然后根据所记录的数据包来源IP确定哪个网段的资料量最大。在这个路由器上调整路由器针对这个网段为“ 黑洞 ”状态，并

藉由修改子网掩码的方法将这个网段隔离开。 然后再寻找这个网段的所有者的信息，联系你的ISP以及数据发送网段的ISP，将攻击情况汇报给他们，并请求协助。不论他们是否愿意帮忙，无非是一个电话的问题。 接下来为了让服务和合法流量通过，你可以将其它一些攻击情况较轻的路由器恢复正常，只保留承受攻击最重的那个路由器，并拒绝攻击来源最大的网段。如果你的ISP和对方ISP很负责的协助阻挡攻击数据包，你的网络将很快恢复正常。 结语 DDoS攻击很狡猾，也很难预防，但是你可以借由以上方式及时减轻这种攻击对网络的影响。面对攻击，你只需要快速地响应和正确的方法，就可以及时发现攻击数据流并将其挡掉。 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