再谈常见网络攻击工程师教您轻松防制 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/469/2021_2022__E5_86_8D_E8_B0_88_E5_B8_B8_E8_c67_469472.htm Qno侠诺技术服务部最近则发现，很多用户宽带接入持续遭受攻击影响。同时，不仅是以前常受到攻击的网吧，很多企业遭受到攻击影响的案例，也越来越多。Qno侠诺的技术服务部工程师们，根据实战服务经验总结最近攻击案例状况，与读者及用户分享。最近常发生的攻击，可分为四大类别，分别为：ARP攻击、内网IP欺骗、内网攻击、及外网流量攻击四种不同型式。对于不同的攻击的详细介绍，在Qno侠诺官方网站的技术文章中，都有详细介绍及预防措施，对于遭受单一攻击的用户了解细节，有相当的帮助。 以下针对不同攻击现象及解决方式，作简单的说明，让企业与网吧的网管们，能够得到全面性的了解，进提高防范意识，以便能够更好的为单位服务！l ARP攻击 ARP攻击自2006年起，就开始普及。一开始ARP攻击是伪装成网关IP，转发讯息，盗取用户名及密码，不会造成掉线。早期的ARP攻击，只会造成封包的遗失，或是Ping值提高，并不会造成严重的掉线或是大范围掉线。 在这个阶段，防制的措施是以ARP ECHO指令方式，可以解决只是为了盗宝为目的传统ARP攻击。对于整体网络不会有影响。 但是在ARP ECHO的解决方法提出后，ARP攻击出现变本加厉的演变。新的攻击方式，使用更高频率的ARP ECHO，压过用户的ARP ECHO广播。由于发出广播包的次数太多，因此会使整个局域网变慢，或占用网关运算能力，发生内网很慢或上网卡的现象。如果严重时，经常发生瞬断或全网掉线的情

况。 要解决这种较严重的ARP攻击，到现在为止最简单有效的方法仍属于Qno侠诺于2006年10月提出的双向绑定方式，可以有效地缩小影响层面。近来有不同解决方法提出，例如从路由器下载某个imf文件，更改网络堆栈，但效果有限。有些解决方式则在用户与网关间建立PPPoE联机，不但配置功夫大，还耗费运算能力。虽然方法不但，大致都可以防制ARP的攻击。l 内网IP欺骗 内网IP欺骗是在ARP攻击普及后，另一个紧随出现的攻击方式。攻击计算机会伪装成一样的IP，让受攻击的计算机产生IP冲突，无法上网。这种攻击现象，通常影响的计算机有限，不致出现大规模影响。 内网IP欺骗采用双向绑定方式，可以有效解决。先作好绑定配置的计算机，不会受到后来的伪装计算机的影响。因此，等于一次防制ARP及内网IP欺骗解决。若是采用其它的ARP防制方法，则要采用另外的方法来应对。l 内网攻击内 网攻击是从内网计算机发出大量网络包，占用内网带宽。网管会发现内网很慢，Ping路由掉包，不知是那一台影响的。内网攻击通常是用户安装了外挂，变成发出攻击的计算机。有的内网攻击会自行变换IP，让网管更难找出是谁发出的网络包。 Qno侠诺对于内网攻击的解决方案，是从路由器判别，阻断发出网络包计算机的上网能力。因此用户会发现如果用攻击程序测试，立刻就发生掉线的情况，这就是因为被路由器认定为发出攻击计算机，自动被切断所致。正确的测试方法是用两台测试，一台发出攻击包给路由器，另一台看是否能上网。对于内网攻击，另外的防制措施是采用联防的交换机，直接把不正常计算机的实体联机切断，不过具备联防能力交换机的成本较高，甚至比路由器还贵。l 外网流量攻击 外网攻击是从外部

来的攻击，通常发生在使用固定IP的用户。很多网吧因为使用固定IP的光纤，很容易就成为外网攻击的目标。同时又因为外网攻击经常持续变换IP，也不容易加以阻绝或追查。它的现象是看内网流量很正常，但是上网很慢或上不了；观看路由器的广域网流量，则发现下载的流量被占满，造成宽带接入不顺畅。 外网流量攻击，可以用联机数加以辅助判断，但是不容易解决。有些地区可以要求ISP更换IP，但过几天后，就又来攻击了。有些用户搭配多条动态IP拨接的ADSL备援，动态IP就较不易成为攻击的目标。外网流量攻击属于犯法行为，可通知ISP配合执法单位追查，但现在看起来效果并不大。Qno侠诺也曾呼御相关主管单位加以重视，但并没有较好的响应。外网流量攻击成为现在是最难处理的攻击。l 小结以上，Qno侠诺技术服务部整理最近常见的攻击及解决之道，供网吧及企业网管参考。其实只要静下心来，按照以上说明，寻找相关的现象，找出原因，网络攻击并不是不能解决的。Qno侠诺及其它厂商都推出各种解决方案，用户稍用心就可以进行防制措施。 