

如何借助路由器来防范网络中的恶意攻击 PDF转换可能丢失
图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/461/2021_2022__E5_A6_82_E4_BD_95_E5_80_9F_E5_c101_461683.htm 除了ADSL拨号上网外，小区宽带上网也是很普遍的上网方式。如果你采用的是小区宽带上网，是否觉得路由器仅仅就是个上网工具呢？其实不然，利用好你的路由器，还能够防范黑客的攻击呢。下面就让我们来实战一番。目的：限制外部电脑连接本小区的192.168.0.1 这台主机的23（telnet）、80（www）、3128等Port. 前提：Router接内部网络的接口是Ethernet0/1，每一个命令之后按Enter执行，以Cisco路由为准。步骤1 在开始菜单中选择运行，在弹出的对话框中输入“cmd”并回车，出现窗口后，在提示符下连接路由器，指令格式为“telnet路由器IP地址”。当屏幕上要求输入telnet password时（多数路由器显示的是“Login”字样），输入密码并确认无误后，再输入指令enable，屏幕上显示要求输入enable password时输入密码。这两个密码一般由路由器生产厂商或者经销商提供，可以打电话查询。步骤2 输入指令 Router# configure terminal 即可进入路由器的配置模式，只有在该模式下才能对路由器进行设置。步骤3 进入配置模式后，输入指令 Router（config）#access-list 101 deny tcp any host 192.168.0.1 eqtelnet 该指令的作用是设定访问列表（access list），该命令表示拒绝连接到IP地址为192.168.0.1的主机的属于端口（Port）23（telnet）的任何请求。步骤4 输入 Router（config）#access-list 101 deny tcp any host 192.168.0.1 eqwww 指令以拒绝来自任何地方对IP地址为192.168.0.1的主机的属于端口80（www）的请求。步骤5

最后需要拒绝的是来自任何地方对IP地址为192.168.0.1 的主机属于端口3128的访问，这需要输入指令 Router (config) #access list 101 deny tcp any host 192.168.0.1 eq3128 来完成。步骤6 到此，已经设置好我们预期的访问列表了。但是，为了让其他的所有IP能够顺利访问，我们还需要输入 Router (config) #access -list 101 permit ip any any 来允许其他访问请求。但是，为了让路由器能够执行我们所做的访问列表，我们还需要把这个列表加入到接口检查程序，具体操作如下。输入指令 Router (config) #interface eO/1 进入接口 (interface) ethernet 0/1 ，然后键入指令 Router (config-if) #ip access-group 101 out 将访问列表实行于此接口上。这样一来，任何要离开接口的TCP 封包，均须经过此访问列表规则的检查，即来自任何地方对IP地址为192.168.0.1 的主机，端口 (port) 属于telnet (23) ， www (80) ， 3128的访问一律拒绝通过。最后，输入指令write 将设定写入启动配置，就大功告成了。这样，你的主机就安全多了。虽然只是禁止了几个常用端口，但是能把不少搞恶作剧的人拒之门外。另外，如果看见有什么端口可能会遭到攻击或者有漏洞了，你也可以通过上面的方法来将漏洞堵住。 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