通过路由器保护内网安全九大步骤 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__E9_80_9A_E8_BF_87_E8_B7_AF_E7_c101_142429.htm 对于大多数企业局域网来说，路由器已经成为正在使用之中的最重要的安全设备之一。一般来说，大多数网络都有一个主要的接入点。这就是通常与专用防火墙一起使用的“ 边界路由器 ”。 经过恰当的设置，边缘路由器能够把几乎所有的最顽固的坏分子挡在网络之外。如果你愿意的话，这种路由器还能够让好人进入网络。不过，没有恰当设置的路由器只是比根本就没有安全措施稍微好一点。 在下列指南中，我们将研究一下你可以用来保护网络安全的9个方便的步骤。这些步骤能够保证你拥有一道保护你的网络的砖墙，而不是一个敞开的大门。 1.修改默认的口令！ 据国外调查显示，80%的安全突破事件是由薄弱的口令引起的。网络上有大多数路由器的广泛的默认口令列表。你可以肯定在某些地方的某个人会知道你的生日。SecurityStats.com网站维护一个详尽的可用/不可用口令列表，以及一个口令的可靠性测试。 2.关闭IP直接广播（IP Directed Broadcast） 你的服务器是很听话的。让它做什么它就做什么，而且不管是谁发出的指令。Smurf攻击是一种拒绝服务攻击。在这种攻击中，攻击者使用假冒的源地址向你的网络广播地址发送一个“ ICMP echo ”请求。这要求所有的主机对这个广播请求做出回应。这种情况至少会降低你的网络性能。 参考你的路由器信息文件，了解如何关闭IP直接广播。例如，“ Central（config）#no ip source-route ”这个指令将关闭思科路由器的IP直接广播地址。 3.如果可能，关闭路由器

的HTTP设置 正如思科的技术说明中简要说明的那样，HTTP使用的身份识别协议相当于向整个网络发送一个未加密的口令。然而，遗憾的是，HTTP协议中没有一个用于验证口令或者一次性口令的有效规定。 虽然这种未加密的口令对于你从远程位置（例如家里）设置你的路由器也许是非常方便的，但是，你能够做到的事情其他人也照样可以做到。特别是如果你仍在使用默认的口令!如果你必须远程管理路由器，你一定要确保使用SNMPv3以上版本的协议，因为它支持更严格的口令。 4.封锁ICMP ping请求 ping的主要目的是识别目前正在使用的主机。因此，ping通常用于更大规模的协同性攻击之前的侦察活动。通过取消远程用户接收ping请求的应答能力，你就更容易避开那些无人注意的扫描活动或者防御那些寻找容易攻击的目标的“ 脚本小子 ”（script kiddies）。 请注意，这样做实际上并不能保护你的网络不受攻击，但是，这将使你不太可能成为一个攻击目标。 5.关闭IP源路由 IP协议允许一台主机指定数据包通过你的网络的路由，而不是允许网络组件确定最佳的路径。这个功能的合法的应用是用于诊断连接故障。但是，这种用途很少应用。这项功能最常用的用途是为了侦察目的对你的网络进行镜像，或者用于攻击者在你的专用网络中寻找一个后门。除非指定这项功能只能用于诊断故障，否则应该关闭这个功能。 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