保护路由器安全的十四招必杀技 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__E4_BF_9D_E6_8A_A4_E8_B7_AF_E7_c101_142706.htm 在互联网的世界里，路由器是不可或缺的重要部件，没有它我们将没有办法和五彩斑斓的外部世界建立联系。因此，路由器的管理一直是网络管理员最重要的日常工作之一。 本文作者结合自己的工作实践，总结了14条保护路由器、防止非法入侵的办法，您不妨一试。 路由器是网络系统的主要设备，也是网络安全的前沿关口。如果路由器连自身的安全都没有保障，整个网络也就毫无安全可言。因此在网络安全管理上，必须对路由器进行合理规划、配置，采取必要的安全保护措施，避免因路由器自身的安全问题而给整个网络系统带来漏洞和风险。 下面是一些加强路由器安全的具体措施，用以阻止对路由器本身的攻击，并防范网络信息被窃取。 1. 为路由器间的协议交换增加认证功能，提高网络安全性。 路由器的一个重要功能是路由的管理和维护，目前具有一定规模的网络都采用动态的路由协议,常用的有：RIP、EIGRP、OSPF、IS-IS、BGP等。当一台设置了相同路由协议和相同区域标示符的路由器加入网络后，会学习网络上的路由信息表。但此种方法可能导致网络拓扑信息泄漏，也可能由于向网络发送自己的路由信息表，扰乱网络上正常工作的路由信息表，严重时可以使整个网络瘫痪。这个问题的解决办法是对网络内的路由器之间相互交流的路由信息进行认证。当路由器配置了认证方式，就会鉴别路由信息的收发方。有两种鉴别方式，其中“ 纯文本方式 ”安全性低，建议使用“ MD5方式 ”。 2. 路由器的物理

安全防范。 路由器控制端口是具有特殊权限的端口，如果攻击者物理接触路由器后，断电重启，实施“ 密码修复流程 ”，进而登录路由器，就可以完全控制路由器。 3. 保护路由器口令。 在备份的路由器配置文件中，密码即使是用加密的形式存放，密码明文仍存在被破解的可能。一旦密码泄漏，网络也就毫无安全可言。 4. 阻止察看路由器诊断信息。 关闭命令如下： no service tcp-small-servers no service udp-small-servers 5. 阻止查看到路由器当前的用户列表。 关闭命令为：no service finger。 6. 关闭CDP服务。 在OSI二层协议即链路层的基础上可发现对端路由器的部分配置信息: 设备平台、操作系统版本、端口、IP地址等重要信息。可以用命令: no cdp running或no cdp enable关闭这个服务。 7. 阻止路由器接收带源路由标记的包，将带有源路由选项的数据流丢弃。“ IP source-route ”是一个全局配置命令，允许路由器处理带源路由选项标记的数据流。启用源路由选项后，源路由信息指定的路由使数据流能够越过默认的路由，这种包就可能绕过防火墙。关闭命令如下： no ip source-route。 8. 关闭路由器广播包的转发。 sumrf D.o.S攻击以有广播转发配置的路由器作为反射板，占用网络资源，甚至造成网络的瘫痪。应在每个端口应用“ no ip directed-broadcast ”关闭路由器广播包。