保护路由器安全的14招 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_142766.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。 9. 管理HTTP服务。 HTTP服务提供Web管理接口。“ no ip http server ”可以停止HTTP服务。如果必须使用HTTP，一定要使用访问列表“ ip http access-class ”命令，严格过滤允许的IP地址，同时用“ ip http authentication ”命令设定授权限制。 10. 抵御spoofing(欺骗) 类攻击。 使用访问控制列表，过滤掉所有目标地址为网络广播地址和宣称来自内部网络，实际却来自

外部的包。 在路由器端口配置： ip access-group list in number 访问控制列表如下： access-list number deny icmp any any redirect access-list number deny ip 127.0.0.0 0.255.255.255 any access-list number deny ip 224.0.0.0 31.255.255.255 any access-list number deny ip host 0.0.0.0 any 注: 上述四行命令将过滤BOOTP/DHCP 应用中的部分数据包，在类似环境中使用时要有充分的认识。 11. 防止包嗅探。 黑客经常将嗅探软件安装在已经侵入的网络上的计算机内，监视网络数据流，从而盗窃密码,包括SNMP 通信密码，也包括路由器的登录和特权密码，这样网络管理员难以保证网络的安全性。在不可信任的网络上不要用非加密协议登录路由器。如果路由器支持加密协议，请使用SSH 或 Kerberized Telnet，或使用IPSec加密路由器所有的管理流。 12.校验数据流路径的合法性。 使用RPF (reverse path forwarding)反相路径转发，由于攻击者地址是违法的，所以攻击包被丢弃，从而达到抵御spoofing 攻击的目的。RPF反相路径转发的配置命令为: ip verify unicast rpf。 注意: 首先要支持 CEF(Cisco Express Forwarding) 快速转发。 13. 防止SYN 攻击。 目前，一些路由器的软件平台可以开启TCP 拦截功能，防止SYN 攻击，工作模式分拦截和监视两种，默认情况是拦截模式。（拦截模式: 路由器响应到达的SYN请求，并且代替服务器发送一个SYN-ACK报文，然后等待客户机ACK。如果收到ACK，再将原来的SYN报文发送到服务器. 监视模式：路由器允许SYN请求直接到达服务器，如果这个会话在30秒内没有建立起来，路由器就会发送一个RST,以清除这个连接。） 首先，配置访问列表，以备开启需要保护的IP地址: access list [1-199] [deny|permit] tcp any destination

destination-wildcard 然后，开启TCP拦截： Ip tcp intercept mode intercept Ip tcp intercept list access list-number Ip tcp intercept mode watch 14. 使用安全的SNMP管理方案。 SNMP广泛应用在路由器的监控、配置方面。SNMP Version 1在穿越公网的管理应用方面，安全性低，不适合使用。利用访问列表仅仅允许来自特定工作站的SNMP访问通过这一功能可以来提升SNMP服务的安全性能。配置命令： snmp-server community xxxxx RW xx ；xx是访问控制列表号 SNMP Version 2使用MD5数字身份鉴别方式。不同的路由器设备配置不同的数字签名密码，这是提高整体安全性能的有效手段。 总之，路由器的安全防范是网络安全的一个重要组成部分，还必须配合其他的安全防范措施，这样才能共同构筑起安全防范的整体工程。 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