

保护内网配置路由器防止网络黑客入侵Cisco认证考试 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/557/2021_2022_E4_BF_9D_E6_8A_A4_E5_86_85_E7_c101_557850.htm 正是由于企业网应用的复杂化，使得网络资源变得更加紧张，在这样的环境下，企业网远端管理成为企业网管理员的心病。各大网络设备生产商也在企业网路由器产品上面下了不少功夫，经过长期对企业网网络应用环境的研究分析，开发出一系列针对复杂应用环境下网络应用的优化措施和高级功能。例如：路由器的远程管理，这样可以减轻了管理员的负担，也为企业节约了维护成本。但万事都有两面性，在方便自己的同时，也方便了某些恶意用户。如果设置不当，安全措施不到位，企业路由器极有可能被黑客接管，整个企业的网络就无安全性可言。对于通常的网络来说，路由器将是保护内部网的第一道关口，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。保护路由器口令假设一个分公司在郊区设立了营销网点，营销网点的员工使用宽带路由器共享上网，和公司总部保持联系。如果出现了问题，管理员需要坐两个多小时的车到营销网点对宽带路由器进行维护，非常疲惫。不过，他想到了启用宽带路由器的“远程控制”功能，在总部对路由器进行远程维护。然而，安全问题开始困扰他，在方便自己的同时，这也方便了那些“不怀好意”者，一旦他们得到路由器的管理员账号，就能进行各种破坏活动，后果是不堪设想的。那么，如何才能增强远程控制的安全呢？可见帐户和密码是路由器的第一道安

全防线，要想对宽带路由器进行管理，首先必须拥有路由器的管理员账号。但默认情况下，路由器的初始账号和密码都比较简单，特别是启用了路由器的远程控制功能后，公网中的其他用户就有机会访问到路由器。如果不对路由器的初始账号进行修改，使它变得更为复杂，让不怀好意者难以猜测和破解，那么路由器就可能被他人利用。一旦密码泄漏，网络也就毫无安全可言。

开启路由器防火墙 路由器远程管理的安全性大大增强了，但面对网络中无时无刻都在涌现的病毒和黑客攻击，为了更好地利用路由器内置的“防火墙”为路由器的远程控制安全加上“双保险”。在宽带路由器管理界面中，依次点击“安全设置 防火墙设置”，在右侧的设置框中选中“开启防火墙”选项，点击“保存”按钮后启用路由器的防火墙功能。接着点击“高级安全设置”，进入“高级安全设置”页面。这里提供了一些更具体的安全防御功能，如防御DoS攻击、ICMP-FLOOD攻击过滤和TCP-SYN-FLOOD攻击过滤等。设置隐蔽的端口、特定的IP及关闭 为宽带路由器设置了复杂的访问账号，但这只是为远程安全管理路由器打下了好的基础。然而，很多路由器默认是没有启用“远程控制”功能的，因此还要手工启用，而且在启用过程中还有很多增强安全的技巧和方法。在宽带路由器管理界面中，依次点击“安全设置 远端Web管理”，进入“远端Web管理”设置界面。接下来就可启用远程控制功能。默认情况下，路由器使用“80”端口来提供远程管理功能，但这非常不安全，容易被攻击者猜到。因此，可修改口号，使用一个不常用的端口来提供远程管理功能，在“Web管理端口”栏中修改远程管理使用的端口号（如

“8081”）。现在，攻击者就很难猜到端口号了。接下来，在“远端Web管理IP地址”栏中，输入可对路由器进行远程控制的公网计算机的IP地址。最安全的做法是允许某个使用特定IP地址的机器远程登录路由器，将该参数设置为管理员在总部使用的IP地址（如“10.254.*.*”）。现在只有该IP的主机能在公司总部的机器上远程登录路由器，而其他公网机器则不行。关闭telnet命令登录，在大多数情况下，并不需要来自互联网接口的主动的telnet会话，如果开启了Web登录方式完全可以关闭该登录方式，减少被黑客攻击的可能性。禁用IP定向广播，IP定向广播使得攻击者对路由器实施拒绝服务攻击。因此要禁用，避免当攻击者不能登录路由器而采取DDOS攻击，因为一台路由器的内存和CPU难以承受太多的请求，这种结果会导致缓存溢出，从而路由器沦陷。同样的也要禁用IP路由和IP重新定向，因为重定向允许数据包从一个接口进来然后从另一个接口出去，攻击者可以把精心设计的数据包重新定向到专用的内部网路，危害内部网络的安全。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