从“ 入口 ”把关让路由器更安全 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/466/2021_2022__E4_BB_8E_E2_80_9C_E5_85_A5_E5_c67_466917.htm 随着网络的快速发展，网络接入方式也变得多种多样，无论是ISDN、ADSL还是专线，路由器无疑是近年来企业网络中网络接入的热点设备。而如何保障路由器的安全，对于网络管理员来说也是任重而道远，一旦黑客获得了路由器的控制权，针对路由器发动了攻击，从而浪费路由器的CPU周期，误导信息流量，最终使整个网络陷入瘫痪。而加强路由器的安全配置，也是一项非常大的课题，今天，笔者就谈谈如何从“ 入口 ”把关，从而让我们的路由器尽量减少被黑客攻击的可能。 一、设置配置密码 对于路由器来说，配置方法基本上可以分为三种，控制台、AUX和VTY （Telnet），而VTY和AUX默认情况进行配置访问就需要一个登录密码，如果不设置任何密码，路由器就会拒绝建立会话，并返回一个错误消息，说明错误的原因是“ 密码请求没有设置 ”而导致的。而控制台端口默认情况下是不要求密码，也就是说在没有进行控制台密码设置的情况下，任何人只要有一台笔记本和一根控制线，就可以很容易的进入设备修改备置，因此不仅仅为AUX和VTY设置密码，连控制台端口也要设置登录密码。 我们来分别了解一种三种密码类型的语法： 通过控制台设置密码： Line console 0 Password password Login 通过AUX设置密码： Line aux 0 Password password Login 通过Telnet远程设置密码 Line vty 0 4 Password password Login 有了这个基础后，我们就可以来看看具体的设置过程了（图1）图 1 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