路由器常用ACL和一些简单防护 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/252/2021_2022__E8_B7_AF_E7_94_B1_E5_99_A8_E5_c101_252877.htm 1 IP欺骗简单防护。如过滤非公有地址访问内部网络。过滤自己内部网络地址；回环地址(127.0.0.0/8)；RFC1918私有地址；DHCP自定义地址(169.254.0.0/16)；科学文档作者测试用地址(192.0.2.0/24)；不用的组播地址(224.0.0.0/4)；SUN公司的古老的测试地址(20.20.20.0/24.204.152.64.0/23)；全网络地址(0.0.0.0/8)。 Router(Config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any Router(Config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any Router(Config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any Router(Config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any Router(Config)# access-list 100 deny ip 169.254.0.0 0.0.255.255 any Router(Config)# access-list 100 deny ip 192.0.2.0 0.0.0.255 any Router(Config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any Router(Config)# access-list 100 deny ip 20.20.20.0 0.0.0.255 any Router(Config)# access-list 100 deny ip 204.152.64.0 0.0.2.255 any Router(Config)# access-list 100 deny ip 0.0.0.0 0.255.255.255 any Router(Config)# access-list 100 permit ip any any Router(Config-if)# ip access-group 100 in 2 建议采用访问列表控制流出内部网络的地址必须是属于内部网络的。（可选）如：Router(Config)# no access-list 101 Router(Config)# access-list 101 permit ip 192.168.0.0 0.0.255.255 any Router(Config)# access-list 101 deny ip any any Router(Config)# interface eth 0/1 Router(Config-if)# description “ internet Ethernet ”

Router(Config-if)# ip address 192.168.0.254 255.255.255.0 Router(Config-if)# ip access-group 101 in 其他可选项： 1、 建议启用SSH，废弃掉Telnet。但只有支持并带有IPSec特征集的IOS才支持SSH。并且IOS12.0-IOS12.2仅支持SSH-V1。如下配置SSH服务的例子： Router(Config)# config t Router(Config)# no access-list 22 Router(Config)# access-list 22 permit 192.168.0.22 Router(Config)# access-list deny any Router(Config)# username test privilege 10 **** ! 设置SSH的超时间隔和尝试登录次数 Router(Config)# ip ssh timeout 90 Router(Config)# ip ssh anthentication-retries 2 Router(Config)# line vty 0 4 Router(Config-line)# access-class 22 in Router(Config-line)# transport input ssh Router(Config-line)# login local Router(Config-line)# exit ！启用SSH服务，生成RSA密钥对。 Router(Config)# crypto key generate rsa The name for the keys will be: router.xxx Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys .Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus[512]: 2048 Generating RSA Keys... Router(Config)# 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