将路由配置为抵御攻击第一道安全屏障 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E5_B0_86_E8_B7_AF_E7_94_B1_E9_c101_461783.htm 在典型的校园网环境中，路由器一般处于防火墙的外部，负责与Internet的连接。这种拓扑结构实际上是将路由器暴露在校园网安全防线之外，如果路由器本身又未采取适当的安全防范策略，就可能成为攻击者发起攻击的一块跳板，对内部网络安全造成威胁。本文将以Cisco2621路由器为例，详细介绍将一台路由器配置为堡垒路由器的实现方法，使之成为校园网抵御外部攻击的第一道安全屏障。 一、基于访问表的安全防范策略 1. 防止外部IP地址欺骗 外部网络的用户可能会使用内部网的合法IP地址或者回环地址作为源地址，从而实现非法访问。针对此类问题可建立如下访问列表：access-list 101 deny ip 10.0.0.0 0.255.255.255 any access-list 101 deny ip 192.168.0.0 0.0.255.255 any access-list 101 deny ip 172.16.0.0 0.0.255.255 any 阻止源地址为私有地址的所有通信流。 access-list 101 deny ip 127.0.0.0 0.255.255.255 any 阻止源地址为回环地址的所有通信流。 access-list 101 deny ip 224.0.0.0 7.255.255.255 any 阻止源地址为多目的地址的所有通信流。 access-list 101 deny ip host 0.0.0.0 any 阻止没有列出源地址的通信流。 注：可以在外部接口的向内方向使用101过滤。 2. 防止外部的非法探测 非法访问者对内部网络发起攻击前，往往会用ping或其他命令探测网络，所以可以通过禁止从外部用ping、traceroute等探测网络来进行防范。可建立如下访问列表： access-list 102 deny icmp any any echo 阻止用ping探测网络。 access-list 102 deny icmp any any

time-exceeded 阻止用traceroute探测网络。 注：可在外部接口的向外方向使用102过滤。在这里主要是阻止答复输出，不阻止探测进入。 3. 保护路由器不受攻击 路由器一般可以通过telnet或SNMP访问，应该确保Internet上没有人能用这些协议攻击路由器。假定路由器外部接口serial0的IP为200.200.200.1，内部接口fastethernet0的IP为200.200.100.1.可以生成阻止telnet、SNMP服务的向内过滤保护路由器。建立如下访问列表：access-list 101 deny tcp any 200.200.200.1 0.0.0.0 eq 23 access-list 101 deny tcp any 200.200.100.1 0.0.0.0 eq 23 access-list 101 deny udp any 200.200.200.1 0.0.0.0 eq 161 access-list 101 deny udp any 200.200.100.1 0.0.0.0 eq 161 注： 在外部接口的向内方向使用101过滤。当然这会对管理员的使用造成一定的不便，这就需要在方便与安全之间做出选择。 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