Linux操作系统中的防火墙技术及其应用（4） PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/144/2021_2022_Linux_E6_93_8D_E4_BD_c103_144529.htm 四、系统测试 系统配置好以后，可以从内部子网的任意一台主机上“ ping ”一下外部的某个服务器，若能“ ping ”通，则IP伪装配置是正确的。 可能的安全漏洞 对防火墙的不当配置可能造成安全漏洞。如处理TCP分段时，Ipchains需要查看包头中的源端口、目的端口、ICMP代码或“ TCP SYN ”标志等信息，而这些信息只能在TCP分段的第一个IP包中才有。于是从第二个分段开始都不能匹配过滤规则。某些管理者将防火墙配置为仅对第一个分段进行处理。通常，一个TCP连接的第一个TCP分段被防火墙阻挡后，其他的TCP分段被认为不会产生安全性问题，因为在目的主机上由于缺少第一个分段而无法重新组装报文。然而，由于系统缺陷等原因，发送的分段可能使机器瘫痪，甚至人为精心设计的IP包可借此缺陷绕过防火墙。因此配置防火墙需要仔细分析过滤规则如何处理各种类型的分组。对分段的处理最好将系统内核编译为重新组装所有通过的分段，或在应用层另设安全机制。 对基于包过滤防火墙更常见的攻击是利用IP欺骗的方法。IP欺骗是指主机发送自称是另一个主机发送的包。防止IP欺骗的方法是使用源地址确认，它通过配置路由器识别路由代码实现，而不是防火墙。防火墙结合源地址确认能较好地增强系统的安全性。 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