使用Linux高效构建无线网关_防火墙（3） PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/143/2021_2022__E4_BD_BF_E7_94_A8Linu_c103_143829.htm 网关/防火墙的安全策略 无线网升级完成后，为了解决网络安全问题，我们进行了一系列的设置。 首先要确保网关本身的安全。我们采取了如下措施。 1．使用TCP Wrapper的访问限制功能，设置仅允许一个指定的IP（由网络管理人员使用）访问，这是通过修改/etc/hosts.allow和/etc/hosts.deny等文件来实现的，具体方法可参见本刊2000年第44期《设置安全的Linux服务器》一文（以下简称《设》文）。 2．在Linux网关上停止一切不必要的服务，包括telnet和ftp，并取而代之以SSH和scp，从而实现网络管理员和网关通讯时仅传输加密数据，并摒弃了口令认证的方式，使用更为先进的密钥交换认证。这是通过修改/etc/inetd.conf文件（可参见《设》文）和安装、配置SSH来实现的。现在SSH已经向SSH2全面转移，可在下载。 3．为了加强网关的开机安全性，我们为BIOS设置口令，并为LILO设置口令，以防止未授权用户使用"Linux single"进入系统单用户模式。 4．在内、外两个边界路由器设置对Linux网关的直接访问限制。具体做法是，在FDDI环的上与Linux网关直接连接的一台900EF上禁止所有指向Linux网关两个IP（分别绑定在有线和无线两块网卡上）的IP包；在内部网的IBM 8274上设置禁止除源地址为网管IP以外的所有指向Linux网关IP的数据包。这里可能有些难以理解，有些人会认为因为这样阻断了Linux网关与外界的连接，使得Linux无法施行路由功能。事实上，所有目的地址不是Linux网关IP的数据包仍然可以通过

网关，被正常路由。在这个方案中，把Linux看作一个可管理的网络设备更恰当。 通过以上的设置，我们几乎可以保证，除了IPChains和路由部分以外，即使Linux有后门，黑客也无法利用之。 然后是通过在Linux网关上设置IP包过滤防火墙来增强内部网的安全性。设置时，我们通过拒绝外来的SYN包来禁止从Internet向内部网发起主动TCP连接。仅允许指向特定IP特定端口（比如E-mail服务器的25端口和Web服务器的80端口）的数据包通过。这样基本上挡住了Internet对内部网络的攻击。这样设置后，内部网络的用户基本上可以透明地访问Internet，对于FTP等少数需要反向连接的应用，在客户端使用被动模式就可以使其恢复正常了。 