

软盘版Linux防火墙的制作方法介绍 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__E8_BD_AF_E7_9B_98_E7_89_88L_c103_144142.htm 【导读】一般情况下，配置防火墙确实是一件需要很高技术的工作。无论是商业版本的防火墙还是完全免费的防火墙都需要在Linux平台中进行软硬件的配置。Linux下的防火墙(firewall)从诞生到现在，防火墙主要经历了四个发展阶段：第一阶段：基于路由器的防火墙；第二阶段用户化的防火墙工具套；第三阶段：建立在通用操作系统上的防火墙；第四阶段：具有安全操作系统的防火墙。目前世界上大多数防火墙供应商提供的都是具有安全操作系统的软硬件结合的防火墙，象著名的NETEYE、NETSCREEN、TALENTIT等。在Linux操作系统上的防火墙软件也很多，有些是商用版本的防火墙，有的则是完全免费和开源代码的防火墙。大多数Linux教程都提到了如何在Linux平台中使用IPCHAINS来构筑防火墙。设置和管理Linux操作系统中的防火墙是网络系统管理员的重要工作。有没有能随身携带的，使用方便的Linux防火墙呢？答案是有的，现在我就向大家介绍一种能装在普通软盘里面的Linux防火墙。这套名字叫 floppyfw的Linux 防火墙能存放在一张普通的软盘里，并独立的在RAM内存中运行。使用它能启动计算机，利用ipchains过滤掉无用的IP包，还可以使用它来配置IP伪装(IP masquerade),监视端口，通过它可以使主机对其他网络中的计算机进行远程控制。Floppyfw 功能十分强大，但是它运行所需要的硬件环境却非常低，除了需要一张软盘之外，只要8MB的内存就足够了。Floppyfw需要的最的硬件设

备如下：最少8MB内存3.5"软驱显示卡键盘显示器 有的Linux系统中装两块网卡，能使得Floppyfw正常工作，这就需要每一块网卡的IRQ和内存地址都正确无误。在Linux系统中配置双网卡相信很多系统管理员都是轻车熟路的。Floppyfw支持以下的网卡。3Com 3c509 NE2000 compatibles Tulip-based Intel EtherExpress PCI 关于软件：把Floppyfw做成一张可以引导的软磁盘是一件非常简单的事情。不过你要首先到 [//www.zelow.no/floppyfw/download/](http://www.zelow.no/floppyfw/download/) 把Floppyfw下载到计算机的硬盘上。Floppyfw最新的版本应该是 1.0.5或者更高，Floppyfw是一个镜像文件，可以使用 `# dd if=floppyfw-1.0.5.img of=/dev/fd0 bs=72k` 这个命令把镜像文件解压并写到准备好的软盘上。关于设置：需要注意的是，一般的软盘格式化以后都是DOS(FAT)的格式。为了能顺利的启动Linux系统，我们需要在这张软盘上作一些修改。建议使用其他的计算机来修改这张软盘，如果在Linux系统中使用MTOOLS工具修改则更好。使用命令如下：`$ cd /tmp$ mcopy a:config$ vi config$ mcopy config a:` 如果你使用的是其他的操作系统，我想在WINDOWS中可以使用记事本进行修改。在软盘中，我们可以看到floppyfw一共有5个文件：config (主配置文件) firewall.ini (过滤规则) modules.lst (附加的 ip_masq 模块) sysLinux.cfg (内核启动参量) syslog.cfg (syslog 配置, 例如/etc/syslog.conf) 在一般情况下，我们不需要修改sysLinux.cfg 或者modules.lst文件。我们主要的任务就是要修改config这个文件。为了简单明了的说明问题，我在这里不想过多的解释config这个文件里面的具体的配置清单，只是着重说明config文件末尾几个重要的事项。在(/bin/ash) 找

到"OPEN_SHELL controls shell"这行文字，如果您的计算机的内存少于12MB，把 ONLY_8M 设置成"Y"。USE_SYSLOG能测定系统中syslogd是否运行，而 SYSLOG_FLAGS则是判断syslogd启动的标志。用户可以根据自己的实际情况进行修改。附录：配置清单一，这是一个通过测试的标准配置清单。由于这个Linux系统中没有提供DHCP服务，使用的静态的IP，所以仅供有相似服务的用户提供参考。点击这里下载清单一 关于过滤规则：现在，让我们再来看看firewall.ini文件。没有修改之前的floppyfw 的firewall.ini文件默认设置了静态的IP伪装和拒绝一些固定端口的访问。因为我们需要建立自己的防火墙，所以我们需要对 firewall.ini文件进行修改。我们需要全面的设置过滤规则，关闭一些我们认为存在前在危险的端口。在这里因为篇幅的关系我就不再讲解如何设置ipchains。如果您想知道更详细的ipchains的配置方案和具体使用方法，推荐您参考以下的这个国外的Linux防火墙ipchains配置方案。 firewall.ini 的过滤规则的具体设置可以参考配置清单二(ftp://ftp.mfi.com/pub/sysadmin/2001/jan2001.tar.z)，这是一个已经修改好了的配置。如果你对Linux的防火墙不太熟悉，那么可以直接下载这个配置清单来进行参考或者直接使用。清单二可以提供最基本的DNS, SMTP, POP, NNTP, TELNET, SSH, FTP, HTTP, 和 WHOIS服务，一般的客户端计算机都可以通过安全的端口访问网络和使用以上的服务。关于LOG 一般的Linux系统中的LOG文件可不少，主要是记录系统运行中的一些主要参数和记录。上面已经说过了，syslog.cfg就是一个管理和记录 LOG 的文件。Floppyfw能通过这个syslog.cfg文件记录下Linux防火墙系统中的控制记录，

例如键盘错误，显示器没有安装等信息也被如是记录下来。这为今后系统管理员分析和解决系统问题提供了有利的依据。syslog.cfg的设置也不难，首先把syslog.cfg设置成某台计算机的主记录文件。例如，在Red Hat系统中，通过编辑/etc/rc.d/init.d/syslog可以达到目的。如果这台计算机的IP是192.168.1.2，那么在syslog.cfg则要配置成一致的IP。具体的配置清单可以参考"清单三"(ftp://ftp.mfi.com/pub/sysadmin/2001/jan2001.tar.z) 一旦你把前面三个主要的文件配置好了以后，那么你就可以通过这张软盘启动Linux系统进行测试了。如果你在配置和测试防火墙中还遇到其他的问题，可以参考以下网址：Floppyfw by Thomas Lundquist: //www.zelow.no/floppyfw/Linux Firewalls by Robert L. Ziegler: Linux-firewall-tools.com/Linux/faq/ 最后，我在这里还要特别介绍一个也是相当不错的Linux防火墙NetMAXFireWall。NetMAX FireWall来自Cybernet Systems公司，该防火墙的主要特点是容易安装，运行稳定，对硬件需求低，安全防范效果非常理想。由于NetMAX防火墙是通过完全的图形用户界面(GUI)来一步步引导用户安装的，那么NetMAX防火墙可以说是非常的适合Linux初学者和对Linux系统了解不多的用户。如果您还记得去年8月的LinuxWorld Conference & Expo盛会的话，那么您可能见过NetMAX防火墙参加过那次Linux博览会的展示。和其他版本的防火墙不同的是NetMAX防火墙具有独特的，安全的Web-based构造来保护Linux系统的安全。配置NetMAX防火墙可以通过网络来进行相应的配置和调试，无疑这为许多用户和系统管理员提供了很大的方便。这也是NetMAX防火墙能吸引人的地方之一。不过，NetMAX

防火墙可不是免费的防火墙版本，如果您需要安装NetMAX防火墙，那么您不得不购买一张NetMAX防火墙的光盘，因为NetMAX防火墙并不支持网络安装模式。使用CD-ROM光盘安装模式安装NetMAX防火墙需要10分钟的时间，这比起使用网络安装模式要快得多了。如果您需要了解更多的NetMAX防火墙信息或者购买NetMAX防火墙光盘，敬请查询以下网址：Cybernet Systems Corporation: www.cybernet.com/好，下面就让我们一起来看一看NetMAX防火墙的简单安装。

测试平台：处理器: Pentium 200 MMX内存: 64 MB RAM 硬盘: 2.1 GB 网络：两块 3Com ISA 3c509B NICs 系统平台：操作系统: Red Hat Linux 6.2 Kernel: 2.2.16 安装之前，需要设置计算机主板上的BIOS，使用CD-ROM驱动器引导计算机。放入NetMAX防火墙光盘。NetMAX防火墙的引导初始化屏幕和RED HAT的安装初始化界面是差不多的，令人惊异的是NetMAX防火墙的版权信息提示看上去就是把RED HAT这几个字换成了NetMA而已。安装过RED HAT的用户就一点也不觉得陌生。NetMAX防火墙的开发公司称NetMAX防火墙就是基于Red Hat Linux发行版本而设计的。所以Red Hat Linux能和NetMAX防火墙相处得很好。初始化界面载入后，NetMAX防火墙和Red Hat Linux相似之处就更加明显了。接着NetMAX防火墙就会尝试着分析和查找计算机上的硬件设备，因为NetMAX防火墙需要安装必要的kernel模块，如果NetMAX防火墙不能正确的识别硬件和载入kernel模块，它会显示错误的提示给用户。NetMAX防火墙是不会一次性安装所有的东西到Linux中取得。它首先会询问用户Linux系统中的网络配置参数让用户确认。然后询问用户是否同意继续进

行console-based 安装。如果选择"NO"，那么NetMAX防火墙就会启动Apache和提供用户一个基于网络的URL参数提供给用户指定和修改。好，如果我们选择"NO"，那么就会出现下面的安装情况，NetMAX防火墙就会在Linux系统中打开了WEB浏览器 (KDE 2s Konqueror)。如果这是我们填入一个URL，那么一个错误的信息就会在屏幕上弹出来。当错误的信息弹出后，NetMAX防火墙就要求用户修正 https URL。至于错误信息弹出的原因，我们尚未清楚，不过，在我们平时安装和配置Apache 的时候也会有类似的情况出现。按照NetMAX防火墙的提示使用https修正初始化安装之后，NetMAX防火墙这是才真正显示出它的授权和放弃信息。这和一般软件在一开始安装就显示版权，授权等信息是不同的。点"Click here to continue" 就可以进一步安装了。需要注意的是，如果您仔细观察，您就会发现NetMAX防火墙的使用手册有228页之多。手册里面有"基本问题解决方法"，如果在安装和使用 NetMAX防火墙遇到问题的时候就可以查看这本手册了。但是不是所有我们在安装的时候遇到的问题都能找到解决的方法。手册上列有的问题解决方法毕竟是有限的。由于NetMAX防火墙采用了图形用户界面的安装模式，所以只要您对Linux系统中的应用软件的安装比较熟悉的话，安装和测试NetMAX防火墙应该是一件非常轻松的事情的。

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