

Linux用防火墙伪装抵挡黑客攻击（3）PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/462/2021\\_2022\\_Linux\\_E7\\_94\\_A8\\_E9\\_98\\_c103\\_462216.htm](https://www.100test.com/kao_ti2020/462/2021_2022_Linux_E7_94_A8_E9_98_c103_462216.htm) 当作者在撰写本篇文章时，曾花了点时间测试各种不同的数据卡。Linux支持即插即用装置，所以我买了一块由Amjet生产的无跳脚数据卡，才又发现另一个令人困扰的问题。作者测试用的PC是一部老旧的486，用的是1994年版的AMI BIOS。在插上这块即插即用数据卡后，计算机便无法开机了，画面上出现的是"主硬盘发生故障"（Primary hard disk failure）。经检查，发现即插即用的BIOS居然将原应保留给硬盘控制器的15号中断，配给了数据卡。最后作者放弃了在旧计算机上使用即插即用产品，因为不值得为这些事花时间。所以，请您注意在购买数据卡之前，先看清楚是否有调整COM1到COM4的跳脚。在作者的布告板（<http://trevormarshall.com/BYTE/>）上，看到有几位朋友询问是否可以用多条拨号线来改善Internet的上网速度。这里最好的例子是128K ISDN，它同时运用两条56K通道，以达到128K的速度。当ISP提供这样的服务时，其实会配置两条独立的线路连到同一个IP上。您可以看到，虽然Linux上有EQL这类模块，可让您在计算机上同时使用两块数据卡，但除非ISP对两组拨号连线提供同一个IP，否则这两块数据卡也只是对送出资料有帮助而已。如果您拨接的是一般的ISP PPP线路，那么您会得到一个IP地址，从服务器回传的封包才能在数百万台计算机中找到您；而您每次拨入ISP时，都会得到一个不同的IP地址。你的浏览器所送出的封包中，也包含供服务器资料回传的本地IP地址。EQL可将这些外传的封包，分

散到不同的ISP线路上，但当资料回传时，却只能通过一个IP地址接收，也就是浏览器认为正在使用的那个地址。若是使用ISDN，那么ISP会处理这个问题；一些ISP会为多组线路的拨号接入提供相应的IP地址，但价钱非常昂贵。在追求速度时，请别忽略了Linux防火墙的效率。在作者办公室有六位使用者通过"IP伪装"防火墙，去存取一部56K模拟调制解调器，工作情况十分良好，只有在有人下载大文件时速度才会变慢。在您决定要加装多条ISP拨号线之前，可以先架设一部"IP伪装"服务器试试。Windows处理多重IP的方式并非十分有效率，而将Windows网络与调制解调器隔开，效能的增进将会让您惊讶不已。简而言之，Linux所用的"IP伪装"法，就是把你的IP藏起来，不让网络上的其他人看到。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](http://www.100test.com)