

教你构建高性能的Linux双效防火墙 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/284/2021\\_2022\\_\\_E6\\_95\\_99\\_E4\\_BD\\_A0\\_E6\\_9E\\_84\\_E5\\_c103\\_284456.htm](https://www.100test.com/kao_ti2020/284/2021_2022__E6_95_99_E4_BD_A0_E6_9E_84_E5_c103_284456.htm)

系统功能说明 包过滤和WEB代理双效合一。由iptables 实现包的过滤，由Linux下大名鼎鼎的squid结合NAT来实现透明WEB代理。SQUID代理的性能本身已经是代理服务器中的佼佼者，本系统将其性能发挥的极至：通过ramdisk技术，让SQUID把网页cache到内存中，这样，你所访问的网页，除了第一次需要到网络上取，以后都将来自内存！下面介绍如何用Redhat来实现的方法和步骤。（1）选择一台比较稳定的计算机，装上两块网卡

，256MB或512MB内存，硬盘10GB（注意：第一块网卡接内网，第二块网卡接外网）。（2）安装RedHat，安装时选择服务器模式，自动分区。（3）大概在10-15分中后系统安装完毕，重启后进入系统，开始配置系统。1、开启包转发 编辑/etc/sysctl.conf，将net.ipv4.ip\_forward=0 该

为net.ipv4.ip\_forward=1，保存修改。其目的是允许Linux内核做IP包的转发：允许IP数据包从一个网络接口穿越到另一个网络接口，只有这样，系统才具有充当包过滤防火墙的条件。

2、激活RamDisk 修改/etc/grub.conf：

```
#boot=/dev/sddefault=0timeout=10splashimage=(hd0,0)/grub/splash.xpm.gztitle RedHat Linux (2.4.7-10) root (hd0,0) kernel /vmlinuz-2.4.7-10 ro root=/dev/sda6 ramdisk=268435 initrd /initrd-2.4.7-10.img
```

其中ramdisk=268435 是我们要添加的内容，目的是告诉系统默认的 ramdisk的大小是268435KB，也就是256MB.注意千万不可以直接写256MB，这样系统是不认识

的，必须要换成KB才行！（摸索了好几个月的心得！），这样设好，重新启动后就系统就回自动生成一个256MB的虚拟盘了。当然，你要根据自己的内存大小来设置这个参数，如果不运行XWINDOWS，设你总内存的一半都没问题，因为Linux系统本身并不需要很多内存的。3、设置squid参数 编辑/etc/squid/squid.conf，在末尾加入以下条目：

```
httpd_accel_host virtualhttpd_accel_port  
80httpd_accel_with_proxy onhttpd_accel_uses_host_header  
onhttp_access allow allcache_dir ufs /squid 256 16 256
```

前面四条参数使squid提供透明代理提供基础。“http\_access allow all”表示允许所有的客户机器都可以访问代理；这里特别强调的是最后一条“cache\_dir ufs /squid 256 16 256”，squid默认的cache\_dir是“/var/spool/squid”，我们因为要让squid将内容cache到内存中，所以这里先改成/squid，接下来要将ramdisk影射到/squid目录中。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)