服务器虚拟化在代理服务器上的应用①

张 建

(无锡汽车工程学校 信息中心，无锡 214000)

摘 要： 服务器虚拟化技术已逐渐成熟，且应用越来越广泛。基于 Linux 操作系统的内核防火墙具有强大的功能。把 netfilter 架构的防火墙和 vmware server 的虚拟化技术集成在一起，既起企业防火墙作用，又建立了多个虚拟服务器，提供各种服务。利用虚拟化技术和免费开源软件，应用于中小型网络，降低成本，便于管理，易于维护。

关键词： vmware server；虚拟机；防火墙；代理服务器；netfilter

Server Virtualization Used on the Proxy Server

ZHANG Jian

(Information Center, Wuxi Automotive Engineering School, Wuxi 214000, China)

Abstract: The technology “server virtualization” has been in gradual mature and been put in wider use. The kernel firewall based on the operating system “linux” is powerful. With the integration of netfilter firewall for linux and server virtualization of vmware server, it can work as the enterprise firewall as well as the server virtualization which provides all kinds of services. The server virtualization, together with free open-source software is applied in small and medium sized network for the benefit of low cost, effective management and direct maintenance.

Key words: vmware server; virtual machine; firewall; proxy server; netfilter

服务器虚拟化是将服务器物理资源抽象成逻辑资源，让一台服务器变成几台甚至上百台相互隔离的虚拟服务器，或者让几台服务器变成一台服务器来用，不再受限于物理上的界限，而是让 CPU、内存、磁盘、I/O 等硬件变成可以动态管理的“资源池”，从而提高资源的利用率，简化系统管理，实现服务器整合，让 IT 对业务的变化更具适应力。VMware Server 是托管虚拟化平台，可像应用程序一样安装在任何现有的服务器硬件上，并且将一个物理服务器分区为多个虚拟机。它的工作原理是：将每个虚拟机与主机及其他虚拟机相隔离，确保在某个虚拟机崩溃时不会影响其他虚拟机。虚拟机之间不会泄露数据，而且应用程序只能通过配置的网络连接进行通信。在物理服务器上安装 linux 操作系统，共享内网连接互联网，并且对外转发各种服务，该服务器就成为代理服务器。在基于 linux 环境下，Netfilter 提供了一个抽象、通用化的框架，该框架定义的一个子功能的实现就是包过滤子系统。Netfilter 比以前任何一版 Linux 内核的防火墙子系统都要完善强大。iptables 是基于 netfilter 框架的工具，但却有更强的可扩展性，把它称为 iptables 防火墙。

虚拟化是当前最受关注的技术之一。经过近几年的市场培育，虚拟化已经在很多企业得到成功应用，其应用范围也从测试平台、边缘业务逐渐渗透到企业关键的核心业务。

如图 1，本文的网络拓扑结构，方形区域为接入外网的一台曙光服务器，不是硬件路由器，安装 centos5.4 版本的 linux 操作系统，具有三块千兆网卡，接口 IFACE:eth0 网卡连接外网 Internet，ip 地址为 61.139.0.4，接口 IFACE:eth1 连接企业内网，左上方椭圆区域是内网用户，网络地址为 192.168.0.0/24，单位用户通过防火墙的代理共享上网。虚线方形区域内，在 centos5.4 下安装 vmware server 2.0 虚拟软件，可以

① 收稿时间:2010-11-17;收到修改稿时间:2010-12-25

建立多个虚拟机，在虚拟机上建立各种服务，图 1 里建立了 web 服务器作例。IFACE:eth2 连接虚线的椭圆，为日后资金宽余作扩展区域，可以建立真正的 dmz 区域。在本模型里，把 dmz 区域放到防火墙里，用虚拟化技术建立虚拟机，完成 dmz 区域的功能。

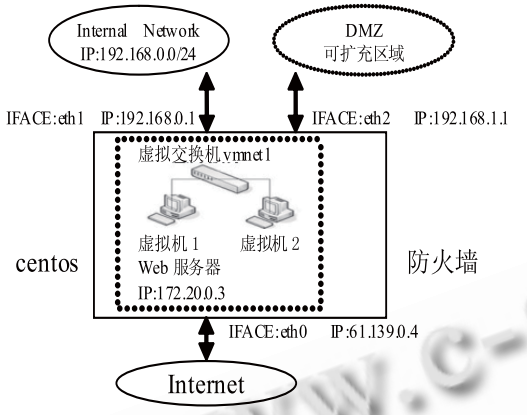

图 1 拓扑结构

1 虚拟化建立

1.1 CentOS 的安装

CentOS 是 linux 的一个发行版本，完全就是对 Red Hat AS 进行改进后发布的，完全免费，在物理服务器上安装 centos5.4 操作系统，对在物理主机上的操作系统成为宿主机，内核升级到 2.6.28。

作为一种网络或系统之间强制实行访问控制的机制，Linux 操作系统上的防火墙软件特点显著,在系统的稳定性、健壮性及价格的低廉性方面都独具优势。更为重要的是，Linux 不但本身的源代码完全开放,Linux 提供的防火墙软件包内置于 Linux 内核中,日后可以通过升级内核提高防火墙的性能，这是硬件防火墙无法比拟的。

宿主机的 CentOS 系统可以根据个人需要，有选择的添加组件。建议最小化安装 CentOS，保留 yum 用于以后宿主机的补丁升级或者安装各种所需要的组件。不推荐在宿主机系统中安装过多的服务，影响宿主机和虚拟服务的性能。

1.2 宿主机的 vmware server 的配置

在宿主机上安装 linux 版本的 vmware server2.0，安装后运行 vmware-congfig.pl 进行对 vmware server 配置，期间注意的是，输入在 vmware 官网申请的序列号，网卡的连接模式选择 hostonly，网络地址输入 172.16.0.0，掩码输入 255.255.255.0，启用 vmnet1，其中 vmnet1 的地址自动为 172.16.0.1。

vmnet1 为防火墙内虚拟交换机，172.16.0.0/16 网段在虚拟交换机上互联，所有的虚拟机系统可以相互通信。虽然宿主机和虚拟机环境隔离开，但网卡的连接模式 host-only 提供了宿主机和虚拟机之间的网络互访， ip 地址 172.16.0.1 是虚拟交换系统的网关，同时也是 centos 系统下的一个虚拟接口，与 IFACE:eth0 和 IFACE:eth1 等同，通过宿主机防火墙的配置，使虚拟系统和宿主机器系统进行相互通信。虚拟机系统的 TCP/IP 配置信息(如 IP 地址、网关地址、DNS 服务器等)，可以是由 vmnet1 虚拟网络的 DHCP 服务器来动态分配的，也可以手动分配。

1.3 安装带有服务器功能的虚拟机

在 vmware server 下安装虚拟机系统，本例中虚拟机 1 服务器，安装 windows 2003，通过 iis 建立 web 服务器，虚拟机的网卡连接方式为 hostonly，ip 地址 172.16.0.3。

至此，在虚拟机系统发布的各种服务，只能在 172.16.0.0/16 这个网段访问，数据包还不能出防火墙，有待下面的防火配置转发，对内网或公网上的客户端提供服务。

1.4 宿主机防火墙优化

在防火墙中，Netfilter 在内核中建立了一个函数指针链表，称为钩子函数链表，加入到链表中的函数指针所指的函数称为钩子函数（Hook Function）。钩子函数的返回值，告诉协议栈如何处理数据包。IPv4 协议栈为实现对 Netfilter 架构的支持，在 ip 包经过 IPv4 协议栈的游历路线中，仔细选择了五个参考点，分别与 Netfilter 架构中的五条链相对应[1]。这五个参考点的位置如图 2 所示。

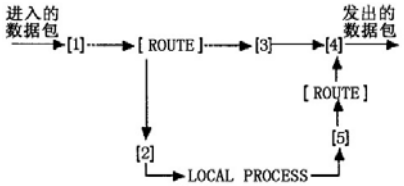

图 2 IP 层中数据包的处理流程及参考点分布

为实现 Netfilter 结构，在这五个参考点对应的函数中各引入了一行对 NF_HOOK()宏函数的一个相应的调用。这个宏检测相应的钩子函数链表是否为空，

如不为空则调用注册的钩子函数，并且根据该函数的处理结果，决定是继续完成 IP 层中的后续处理过程，还是丢弃此数据包，中断数据包的传输；如果不存在注册的钩子函数，则继续完成 IP 层中的后续处理。

对宿主机的 iptables 进行基本的初始化配置，设置防火墙策略的默认配置。首先要开启防火墙的路由功能，从而是数据可以在防火墙的各个接口之间转发，使用以下命令实现[2]：

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

设置默认策略：

```
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT DROP
/sbin/iptables -P FORWARD ACCEPT
```

-P 代表命令的默认模式，即数据包如果找不到处理的钩子函数，就要执行的默认操作，INPUT 匹配的是进入防火墙的数据包，OUTPUT 匹配的是出防火墙的数据包，FORWARD 匹配的是凡是要在防火墙接口之间转发的数据包，DROP 为丢弃操作，ACCEPT 为通过操作。

NAT (Network Address Translation) 意思是网络地址转换，主要的功能就是在提供内部私有网络的频宽分享，同时又是外部网络能访问内部网络。NAT 操作是以 netfilter 节点形式挂接在相应的处理点上，DNAT 挂在 NF_IP_PRE_ROUTING 点上，在 FILTER 表前处理，SNAT 挂接在 NF_IP_POST_ROUTING 点上，在 FILTER 表后处理。

允许内网用户访问外网：

```
iptables -t nat -A POSTROUTING -o eth0 \
－s　192.168.0.0/24 -j SNAT --to 61.139.0.4
```

允许虚拟机系统访问外网：

```
iptables -t nat -A POSTROUTING -o eth0 \
-s　172.16.0.0/24 -j SNAT --to 61.139.0.4
```

以上两个命令在 nat 表的 POSTROUTING 链中添加规则，凡是从 eth0 接口出去的，从内网网段或虚拟机网络进来的数据包，修改数据包的包头，把源 ip 地址改成防火墙的公网 ip 地址，这样使出去的数据包记上回来的地址，同时防火墙建立连接跟踪（conntrack），为每一个经过网络堆栈的数据包，生成一个新的连接记录项，当 Internet 传送回来数据包的时候，NAT 会去查询原本记录的路由资讯，并将目标 IP 由公网 IP 改回原來的内网 ip 地址，这样内网或虚拟机的客户端可以通过代理服务器浏览互联网网络，同时实现数据通信。

利用 iptables 来发布虚拟机中的各种服务，例如 web 服务。

```
iptables －t nat －A PREROUTING -d 61.139.0.4\
－p tcp －dport 80 －j DNAT －-to 172.16.0.3:80
```

以上命令在 nat 表的 PREROUTING 链中添加规则，凡是从 eth0 接口进来的，访问公网 IP 地址的 web 服务，即 80 端口，修改数据包的包头，把目标 ip 地址改成虚拟机的 ip 地址，这样互联网网络的用户通过转发也可以访问虚拟服务。

由于虚拟化的 dmz 区域和防火墙本身集成在一台服务器上，防火墙本身的安全尤为重要，一旦入侵者进入防火墙主机，执行 iptables －F 命令，删除了防火墙规则，那么防火墙命令将全部消失，此外入侵者可能以防火墙为根基，然后对内部网络或虚拟系统进行攻击，因此防火墙脚本设置时，默认策略到防火墙本身的数据包以及从防火墙本身出去的数据包一律都丢弃掉[3]。

2　评测

单位共有 1000 客户端，平均同时在线客户端 300 人，100mpbs 电信接入，代理服务器硬件曙光 a620r-fx，配置为 2 个 amd Opteron 2378 共 8 核，内存 4GB。在宿主机终端运行 top，获取 cpu 和内存的使用率。通过 vi /pro/net/dev 获得两个数据：从本机输出的数据包数，流入本机的数据包数，平均网络负载=(输出的数据包+流入的数据包) / 2，通过在操作系统上添加脚本，计算出网卡的流量。结果如表 1：

表 1　宿主机性能测试结果表

不同时间	Cpu(load average)			内存 (used)	eth0 流量 (mbps)	eth1 流量 (mbps)
	1 分钟	5 分钟	15 分钟			
高峰期	0.27	0.13	0.04	2.6G	80107	77216
低谷期	0.01	0.02	0	2.4G	9811	7308

不同时期，高峰期是指上班下午 2 点左右，低谷期指晚上 10 点，cpu 的 load average 的意思是 cpu 的系统负载，即任务队列的平均长度，三个数值分别为 1 分钟、5 分钟、15 分钟前到现在的平均值[4]。如果数值为 1.00 则该服务器 CPU 得到充分利用，如果数值是 0.50 则是利用到一半的 CPU，2.00 表示 CPU 正忙，

load average:4.00 这时候 CPU 处在高利用的阶段,同时系统性能也会受到影响。从高峰期可以看出，即使要到达接入网速最大使用率了，cpu 负担都不重，而且内存几乎只用了一半，运行流畅。

3 结论与展望

Linux 系统的性能及稳定性比 Windows 要强很多，所以，服务器虚拟化方案建立在 Linux 系统平台下。本问模型具有以下特点：第一：共享多个公网 IP 地址，通过 iptables 的 nat 转发，发布多个虚拟机中的各种服务。第二：宿主机上全部使用免费开源的操作系统及软件，节省软件费用。第三：利用 Linux 下强大的 iptables 来保护服务器，相比 Windows 下的防火墙性能更优秀。第四：可扩展区域通过 eth2 网卡接口外接物理交换机实现，当企业有更多的投入，购买物理服务器，建立 dmz 区域，通过 linux 下防火墙转发，提供各种服务。第五：代理服务器内置虚拟机，管理方便，工作效率提高。

文中涉及到的 iptables 配置，仅仅用于实现对虚拟机中各种服务及端口的发布，未涉及到宿主机及虚拟机中的安全配置。可根据具体的需要，参考其他 iptables 相关的安全文档进行设置。另外，可以将相关的 iptables 命令编写成 shell 脚本，设置开机启动运行。使用 iptables 发布各种服务器，在本文档中只是简单比较典型的实例，可以根据具体的需要参照本文档中的命令，可以实现所有服务及端口的发布。需要注意的是，如果使用的防火墙规则过多，要注意规则的顺序，iptables 对规则的顺序是有要求的。出现设置防火墙策略不生效时，要仔细检查一下顺序是否正常。

最后，服务器硬件的配置，这个可以根据不同的需求配置硬件。增加内存和提高磁盘 IO 是关键。因为运行的虚拟机多了，磁盘 IO 就会成为瓶颈。

虚拟化技术在为用户带来利益的同时，也对用户的数据安全以及基础架构的安全策略提出了新的要求，由于物理世界中的传统的安全策略、经验和做法与在虚拟世界中的可能不一样，更需引起足够重视[5]。本架构由于成本原因，没有考虑冗余，物理服务器一旦崩溃，整个系统就瘫了，这一点就比不上 vmware esx server 虚拟化的多机均衡了。

为节约开支，Vmware server 服务器虚拟化在代理服务器上的应用为企业信息化建设提供了一个很好的方法。虽然此种技术方案规划不多见，但完整的虚拟化布局，需要硬件服务器，外接存储，考究的还要做服务器热备冗余，并且虚拟化 esx 软件是一笔很大的投资。本文这种应用于中小型网络，降低成本，便于管理，易于维护的方法应该是可取的。

参考文献

1 孟晓景,井艳芳,张瑜.Linux 内核 netfilter 防火墙原理与设计.山东科技大学学报(自然科学版),2004,23(2):52−54.
2 张岩,赵霁.基于 Linux 的代理服务器的设计与实现.计算机与数字工程,2005,33(2):87−91.
3 陈勇勋著.更安全的 linux 网络.北京:电子工业出版社,2009.288−291.
4 史军勇,齐艳珂.Linux 操作系统环境下 CPU 平均负载的研究.福建电脑,2009,25(6):119−120.
5 张志国.服务器虚拟化安全风险及其对策研究.晋中学院学报,2010,27(3):83−85.