文章编号:2095-476X(2014)03-0082-05

网络认证客户端通用穿透网关的设计与实现

李健勇, 张静杰, 李建春, 黄道颖

(郑州轻工业学院 计算机与通信工程学院, 河南 郑州 450001)

摘要:网络认证客户端通过监控非绑定Internet接入网卡的活动来实现主机路由限制,从而控制外网向内网的延伸.基于此,利用虚拟机的网络桥接和NAT服务设计了网络认证客户端通用穿透网关方案,实现了网络认证客户端环境下主机外网和内网间的连接.本设计由单网卡或双网卡宿主机配置、微软的3种宿主操作系统和3款不同公司的虚拟机产品互相组合,可形成适应不同应用需求的多种通用穿透网关方案,具有很强的灵活性和实用性.

关键词:网络认证客户端;通用穿透网关;路由;虚拟机

中图分类号:TP393 **文献标志码**:A DOI:10.3969/j.issn.2095-476X.2014.03.019

Design and implementation of generic penetration gateway of network authentication client

LI Jian-yong, ZHANG Jing-jie, LI Jian-chun, HUANG Dao-ying

(*College of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou* 450001, *China*)

Abstract: Network authentication client realizes the restrictions of host routing and the control of extension of Internet and Intranet by monitoring the activities of non-binding Internet access network interface cards. A generic penetration gateway method by utilizing the network bridge and NAT service of virtual machines was proposed. The connection of Internet and Intranet can be realized under the network authentication client environment. Moreover, by composing the host with single or double network cards, three host operating systems of Microsoft and three virtual machine systems designed by different companies, various generic penetration gateway schemes can be generated to meet the needs of different applications. So the proposed method is very flexible and practical.

Key words: network authentication client; generic penetration gateway; routing; virtual machine

0 引言

为了控制网络访问,Internet服务提供商ISP(Internet server provider)采用多种网络接入认证方式.这些认证方式归结起来有以下3种:数字证书[1]、Web网页认证[2]和网络认证客户端[3].前2种方式通过在前端设置NAT路由器进行WAN连接,后端LAN中任意一台主机通过认证后,LAN中的其他主机即可访问Internet[4].这2种方式在服务器端常会设置登录的时限,超过时限后需要重新认证.网络认证客户端是运行在主机上的一个应用程序,根据不同的网络接入媒介及后台运行的认证计

收稿日期:2014-04-27

基金项目:国家自然科学基金项目(60974005);河南省教育厅科学技术研究重点项目(13A520379)

作者简介:李健勇(1969—),男,河南省孟州市人,郑州轻工业学院副教授,硕士,主要研究方向为网络控制、计算机网络.

费系统,不同的 ISP 采用了不同的技术来实现网络认证流程,其共性是这些客户端软件都实时监控主机网卡的状态,定时与位于 ISP 后台的服务器通信,根据 ISP 后台的计费策略和主机当前活动网卡的状态决定主机与网络接连的开关. 直接通过联通、电信等传统 ISP 接入的用户,ISP 多采用 PPPoE 协议认证连接. 而一些大型企业、事业团体类 ISP 则常用锐捷计费系统[3]、Dr. COM 认证计费网关等产品来管理用户的网络接入认证. 由于流量信息具有不确定性,所以网络认证客户端惯常的做法不是限制网络带宽,而是限制主机的连接数. 随着各类网络应用服务的不断丰富,认证客户端的方式极大地限制了终端用户的网络扩展需求,给终端用户带来不便.

针对网络认证客户端路由转发的限制,本文拟利用 Virtual PC 2007, VMware Workstation 10.0.2, VirtualBox 4.3.10 这 3 种虚拟机的网络服务组件中的网络桥接和 NAT 功能,设计一种通用的网络认证客户端的穿透网关方案,并通过虚拟机系统进行测试,以验证该方案的通用性、灵活性和实用性.

1　宿主系统软硬件配置

1.1　宿主操作系统

虚拟机宿主操作系统的选择由用户对用作穿透网关的计算机角色安排和网络认证客户端的运行平台来确定.

1)专用穿透网关. 专用穿透网关需要不间断运行,选择 Windows Server 类操作系统比较合适,前提是网络认证客户端有对应的 Windows Server 操作系统的支持版本.

2)兼用穿透网关. 在一些小型网络(如家庭使用环境)中,一般用某一台计算机兼作穿透网关. 这时需根据使用这台计算机的用户之要求来确定宿主操作系统,目前,常用的操作系统为 Windows XP, Windows 7 和 Windows 8.1 等版本. 本文以此为穿透网关的宿主系统来讨论.

1.2　网络接口

考虑到穿透网关要承担局域内网 LAN 和广域外网 WAN 之间所有的通信工作,宿主操作系统网络接口最好选用带宽在 100 M 以上的有线网卡. 根据接口网卡的数量,可分为宿主机单网卡和双网卡 2 种配置方案.

1)在单网卡配置方案中,LAN 和 WAN 共享了网卡的带宽,在轻载的外网访问需求或 WAN 的实际带宽低于网卡带宽一半的情况下,本方案硬件成本低,是最佳选择. 2)在双网卡配置方案中,LAN 和 WAN 的数据传输相互独立,独享各自网卡的带宽. 此方案中 2 个网卡的传输速率要保持一致,单独提高其中一块网卡的传输速率并不能增加内外网之间的带宽. 本方案能满足高速 WAN 的访问需求,可用于高吞吐量的外网访问中.

1.3　虚拟机

1.3.1　软件选型　虚拟机软件种类繁多[6],其中 Virtual PC 2007 适合用在 Windows XP 上,虽然微软不推荐在 Windows 7 上使用,但经过验证,Virtual PC 2007 也可以很好地在 Windows 7 上工作,微软早已不再对 Virtual PC 2007 进行更新,但 Virtual PC 2007 仍能在 Windows 7 之前的操作系统正常工作. 目前,VMware Workstation 的最新版本是 10.0.2,它可以支持 Windows XP, Windows 7 和 Windows 8.1 等操作系统,其功能最强大. VirtualBox 作为 Oracle 公司的开源项目,到 4.3.10 版本已经做到界面友好、功能丰富了. 以上 3 种虚拟机软件中,VMware Workstation 为注册收费软件,其他 2 种虚拟机软件免费. 从长远考虑,VirtualBox 更为经济且有后续支持,是一个不错的选择,但具体选用何型用户还要根据使用偏好来确定.

1.3.2　网络接口设置　以上 3 种虚拟机软件中,对运行穿透网关的虚拟机的网络设置大体相同,都需要在虚拟机中设置 2 块网卡,第 1 块采用 NAT 方式,第 2 块采用桥接方式,直接连接到宿主系统的物理网卡上. 为表述方便,第 1 块 NAT 方式的虚拟网卡命名为“WAN 口”,第 2 块桥接方式的虚拟网卡命名为“LAN 口”. WAN 口的 IP 地址由虚拟机网络组件中的 DHCP 服务提供,Virtual PC 2007 中,这个地址为形如 192.168.XXX.XXX 的 C 类私网地址;VMware Workstation 中相对复杂一些,这个地址由 VMware Workstation 中一个 Virtual Network Editor 来设置,默认的 DHCP 的地址范围也在 192.168.XXX.XXX 范围内,但是可通过这个工具把这个地址范围修改到 A 类私网地址 10.0.0.0 ~ 10.255.255.0 或 B 类私网地址 172.16.0.0 ~ 172.131.255.0 中. 在 VirtualBox 中,网络组件 DHCP 为 NAT 网卡提供 A 类私网地址.

若宿主系统中只有 1 块物理网卡,该网卡在通过网络认证客户端软件认证许可后可连接到 Internet,同时,由虚拟机网络组件将其用 NAT 方式接入

虚拟机中的 WAN 口上. 而虚拟机的 LAN 口也只能桥接到这块物理网卡上,宿主系统对外表现为单一物理网卡上具有 2 个 IP 地址.

若宿主系统中有 2 块物理网卡,虚拟机网络组件将自动选择认证客户端软件认证许可网卡并用 NAT 方式接入虚拟机的 WAN 口,而虚拟机的 LAN 口就必须连接到另一块物理网卡上. 这项选择工作在 Virtual PC 和 VirtualBox 中比较直观,但在 VMware Workstation 中需要用 Virtual Network Editor 来设置 VMnet0,以便桥接到另一个物理网卡上.

1.3.3 虚拟机内操作系统 要搭建穿透网关,需要路由软件的支持,这类软件在 Windows,Linux 平台下都有多种选择. 考虑到宿主操作系统选用 Windows 系列,虚拟机内操作系统选自带路由管理功能的 Windows Server 来实现. Windows Server 在计算机开机阶段启动路由服务,开机后无需用户登录系统进行设置,使用方便.

Windows Server 从早期的 2003 已经发展到了今天的 2012 R2. 随着功能的不断增强,系统推荐内存和磁盘空间占用也从 2003 的 128 M[5] 和 1.8 G[6] 到 2012 R2 的 512 M[7] 和 9 G 多. 虚拟机内操作系统的选择要结合宿主系统的硬件水平、专用网关或兼用网关来确定.

2 网络拓扑结构

如 1.2 所述,根据局域内网访问外网的网络负载要求,可以选择宿主机单网卡或双网卡 2 种配置方案. 在双网卡配置方案中,又可分为使用无线路由器方案和使用交换机/集线器方案.

2.1 宿主机单网卡网络拓扑方案

图 1 所示宿主机单网卡网络拓扑图中,需要将无线路由器 WAN 口的 IP 地址和宿主机中虚拟机内 LAN 口的 IP 地址设置在同一网段,该网络号不能与虚拟机中自动由虚拟机网络 NAT 组件中的 DHCP 服务所指定的网络号相同.

无线路由器 LAN 端的内网各网络设备要通过无线路由器内的 NAT 来实现与其 WAN 口的连接.

若宿主系统中有多块物理网卡,也可选用图 1 所示的单网卡网络结构. 但需要注意的是,在 1.3.2 中所述的 LAN 口的物理网卡应该选择认证客户端软件所绑定的 Internet 连接网卡.

2.2 宿主机双网卡网络拓扑方案 1

宿主机双网卡网络拓扑方案 1 如图 2 所示,方

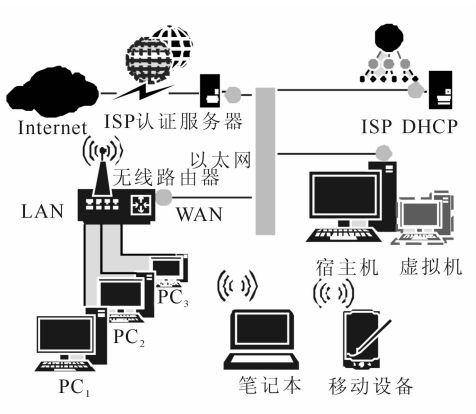

图 1 宿主机单网卡网络拓扑方案

案中无线路由器的 WAN 口要直接与宿主机中虚拟机 LAN 口所对应的物理网卡连接.

在图 1 方案中,并未给出无线路由器的 WAN 口和宿主机物理网卡的以太网连接具体网络设备,原因是有可能在以太网中已经存在多余的交换机或集线器端口,这时直接连接到该端口即可. 如果不存在这个端口,则需要增添 1 个交换机或集线器来实现两者的连接.

在图 2 方案中,无线路由器的 WAN 口和宿主机物理网卡的连接可以采用同样的方法来完成. 更为简便的方法是制作 1 根两端分别按 T568A 和 T568B 标准的交叉网线来连接.

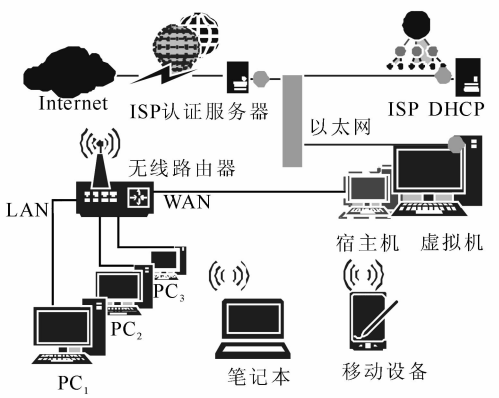

图 2 宿主机双网卡网络拓扑方案 1

2.3 宿主机双网卡网络拓扑方案 2

宿主机双网卡网络拓扑方案 2 如图 3 所示,与前 2 个方案不同,本方案中采用交换机或集线器来连接宿主机中虚拟机的 WAN 口所对应的物理网卡. 这样,虚拟机的 WAN 口可以直接与内网中的各个网络设备通信,无需再经过无线路由器的 NAT 转换.

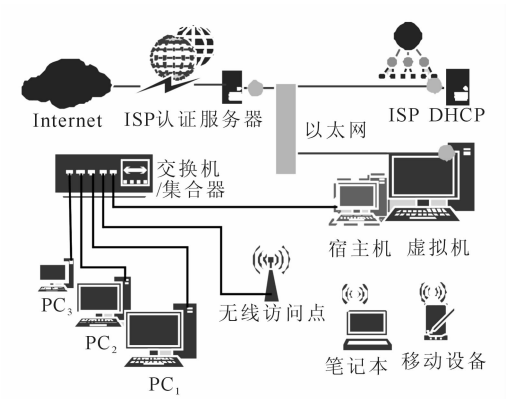

图 3　宿主机双网卡网络拓扑方案 2

3　虚拟机穿透网关设计

3.1　虚拟机的网络服务组件

1) Virtual PC 2007 的网络服务组件为名为 Virtual Machine Network Services 的网络功能服务. 在虚拟机中最多可以设置 4 个网络接口.

2) VMware Workstation 10.0.2 的网络服务组件非常繁杂,通过在宿主系统安装 5 个服务实现网络接口卡的桥接、NAT、仅主机、自定义和 LAN 区段等模式,在网络设置中增加了 VMware Bridge Protocol 网络功能服务. 虚拟机在网络接口数量的配置上不受限制.

3) VirtualBox 4.3.10 在宿主机新增的网络功能服务为 VirtualBox Bridged Networking Driver. 和 Virtual PC 2007 一样,在虚拟中最多可以添加 4 个网络接口.

虚拟机组件的网络传送活动不受认证软件的监控,利用虚拟机的网络组件中的 NAT 服务来实现对网络认证客户端的穿透是本设计实现的核心技术要点.

3.2　路由和远程访问服务安装

在图 1—图 3 所示的 3 种网络拓扑方案中,虚拟机内部的设置完全相同. 在 Windows Server 中,NAT 功能是包含在路由和远程访问服务中的. 因此,需要在相应的 Windows Server 中安装路由和远程访问服务. 在安装 NAT 功能时,需要指定虚拟机的 WAN 口为连接 Internet 的网络接口.

3.3　DHCP 服务和 DNS 服务

在图 1 和图 2 所示方案中,DHCP 服务由无线路由器提供,DNS 服务可以在无线路由器中直接设定为 ISP 所提供的 DNS 服务器地址. 其优点是直接利用了硬件设备的服务,虚拟机中只需实现 NAT 服务即可,方案简单.

在图 3 方案中,DHCP 服务必须由虚拟机提供,需要在 Windows Server 中安装 DHCP 服务. DHCP 服务安装时要注意设置的 DHCP 地址池应该和虚拟机 LAN 口在同一网段. DNS 服务器的地址可在 DHCP 的网络选项中指定,内容由 ISP 提供. 如果有特殊的管理需求,DNS 服务也可以通过在虚拟机中增添 DNS 角色来完成. 这样 DHCP 中的 DNS 网络选项就应该指向虚拟机的 LAN 口的 IP 地址.

4　系统测试

4.1　虚拟机安装测试

选择在宿主操作系统为 Microsoft 公司的 Windows XP SP3 32 位,Windows 7 SP1 32 位和 64 位,Windows 8.1 32 位和 64 位上安装 Virtual PC 2007,VMware Workstation 10.0.2 和 VirtualBox 4.3.10 共 3 款虚拟机软件,结果见表 1.

表 1　Windows 平台下虚拟机安装测试结果

Windows 平台	VPC	VMware	VirtualBox
Windows XP SP3 32 位	成功	成功	成功
Windows 7 SP1 32 位	成功	成功	成功
Windows 7 SP1 64 位	成功	成功	成功
Windows 8.1 32 位	失败	成功	成功
Windows 8.1 64 位	失败	成功	成功

4.2　虚拟机内操作系统安装测试

在上述 3 款虚拟机中安装 Windows Server 2003 32 位,Windows Server 2008 32 位和 64 位,Windows Server 2012 R2. 结果见表 2.

Windows Server 2012 R2 为 64 位版本,微软公司不再为 Server 2012 R2 提供 32 位版本.

4.3　内网固定终端和移动终端接入测试

在表 1 和表 2 所示的宿主操作系统中安装 3 种虚拟机,分别在虚拟机中安装 4 种 Windows Server 操作系统,配置 Windows Server 的路由和远程访问服务和 DHCP 服务,宿主机网络认证客户端选用 Dr. COM.

表 2　虚拟机中 Windows Server 安装测试结果

Server 类别	VPC	VMware	VirtualBox
Server 2003 32 位	成功	成功	成功
Server 2008 32 位	成功	成功	成功
Server 2008 64 位	失败	成功	成功
Server2012 R2	失败	成功	成功

测试结果表明,内网有线连接的固定 PC 和无线路由连接的笔记本,以及多种品牌的智能手机均能正常上网.

5 结论

采用本文提出的虚拟机环境下网络认证客户端穿透网关设计方案,在 Windows XP,Windows 7,Windows 8.1 等宿主操作系统运行 Virtual PC 2007,VMware Workstation10.0.2 和 VirtualBox 4.3.10 等虚拟机. 虚拟机中采用 Windows Server 2003,Windows Server 2008 和 Windows Server 2012 R2 等服务器操作系统搭建穿透网关. 测试结果表明: 1)使用单网卡 PC 机,宿主机安装 Windows XP 操作系统,采用 Virtual PC 2007 虚拟机中安装 Windows Server 2003 的方案对系统硬件条件要求最低、安装最简便,但随着 Microsoft 公司对 Windows XP 的支持结束,XP 的安全性前途未知,所以这种方案具有一定的风险; 2)在宿主操作系统为 Windows 8.1 上安装 VMware Workstation 10.0.2 虚拟机且在其中运行 Windows Server 2012 R2 对硬件要求最高、设置最复杂,但使用时界面最友好、管理最方便.

参考文献:

[1] 刘伟,姜童,寇登峰. 一种新型的信息网络安全接入认证模型[J]. 火力与指挥控制,2013,38(6):89.

[2] 袁博,范亮. WLAN 场景的 IPv6 宽带接入认证技术[J]. 邮电设计技术,2013(7):23.

[3] 福建星网锐捷网络有限公司. 产品与解决方案[EB/OL]. (2013 - 05 - 21)[2014 - 03 - 22]. http://www.ruijie.com.cn/.

[4] 丛日权,商宏图,左坚,等. Windows Server 2003 网络架构[M]. 北京:机械工业出版社,2005.

[5] Microsoft Corporation. Determining Hardware Requirements for Windows Server 2003[EB/OL]. (2003 - 03 - 28)[2011 - 04 - 23]. http://technet.microsoft.com/en - us/library/cc782423(WS.10).aspx.

[6] 刘艳红,李健勇,李建春. 基于虚拟机的网络架构课程实验平台的构建[J]. 郑州轻工业学院学报:自然科学版,2011,26(3):63.

[7] Microsoft Corporation. 安装 Windows Server 2012[EB/OL]. (2012 - 02 - 01)[2014 - 04 - 08]. http://technet.microsoft.com/ zh - cn/library/jj134246.aspx.