文章编号:1001-5132（2009）02-0212-05

基于复合网关的网络互联策略实现

鞠洪尧

（浙江纺织服装职业技术学院 科研处，浙江 宁波 315211）

摘要：通过对 VPN 和 NAT 技术原理及实用性的研究与分析，在将两者进行有效结合的基础上，提出集 VPN 和 NAT 技术于一体的复合网关网络互联策略，实现了异地局域网可通过 Internet 进行有效互联，解决了远程用户登陆局域网访问内部资源的问题. 测试结果表明：该复合策略具有良好的稳定性和可靠性，且易于实现.

关键词：复合网关；网络互联；VPN；NAT

中图分类号：TP393.03 文献标识码：A

网络互联技术是解决同构或异构网络间顺利实现通信和资源互访的关键技术，随着计算机网络技术的不断进步，网络规模也不断扩大，各种类型的中小型局域网相继涌现，网络中的特色资源建设不断完善，人们生活、工作也已经不再局限于某个固定场所，因此，网络互联互通、资源的便捷访问就变得十分迫切和必要. 而通常情况下的网络互联基本都局限于专线连通，这样的连通方式不但会造成网络中原有的 IP 地址资源在网络连通后发生冲突，而且使网络系统造价及运营成本极其昂贵. 于是，在既不改变原有网络的格局、避免 IP 资源冲突，又能实现异地用户对局域网中的公共和私有资源进行便捷的访问，同时尽量降低网络互联成本的前提下，寻求一种有效、便捷的连接手段和连接方法就变得尤为重要.

通过对虚拟专用网络(VPN)技术[1]和网络地址转换(NAT)技术[2]及其适用性的研究与分析，笔者设计并实现了一种复合网关，该复合网关顺利实现了异地局域网通过 Internet 进行互联、互访公共信息资源，且实现了异地用户对局域网内部私有资源的便捷访问，解决了网络互联及异地办公问题，有效地降低了网络互联成本，提高了异地网络间的通信和资源共享的能力.

1 网络互联系统架构设计

在参与互联的每个局域网与 Internet 连接处设置 1 台服务器作为复合网关，复合网关安装双网卡，一端连接 Internet，另一端连接局域网，并作为局域网的网关，复合网关负责内外网互访公共资源时的 IP 地址转换及授权外网用户访问内网私有资源时的 VPN 接入. 每个局域网配置外部公共应用服务器和内部私有应用服务器各 2 台，分别用负载均衡群集(NLB)技术进行群集[3]，保证应用服务的可靠性和可伸缩性；每个局域网中设置内部 DHCP 服务器及内部 DNS 服务器各 1 台，以完成局域网

收稿日期：2009-01-04. 宁波大学学报（理工版）网址: http://3xb.nbu.edu.cn
基金项目：中国高等教育学会“十一五”教育科学研究规划项目（06AIP0070130）.
作者简介：鞠洪尧（1966－），男，浙江宁波人，副教授，主要研究方向：计算机网络技术. E-mail: juhongyao@163.com

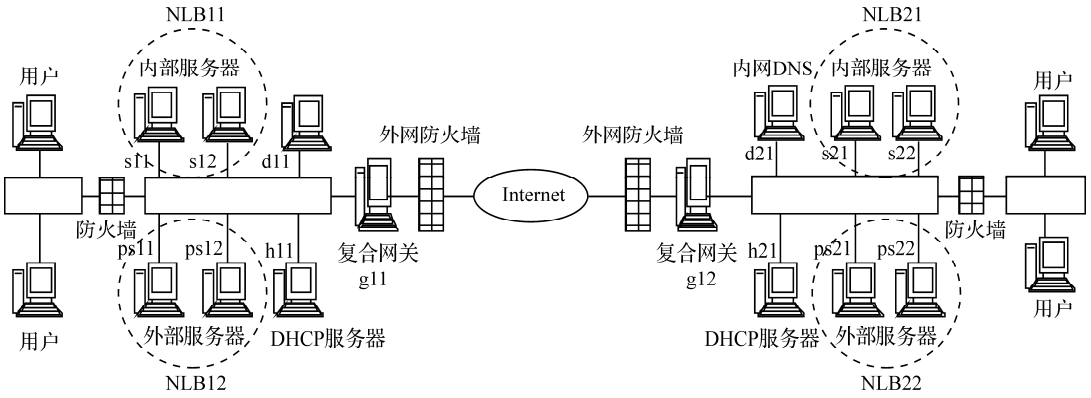

图 1　网络互联系统架构示意图

内部用户 TCP/IP 参数的自动配置和内部域名的解析, 而内部 DNS 服务器通过转置解析功能提供内网用户对外网域名的解析, 文中以 2 个局域网通过 Internet 互联为例, 其系统架构如图 1 所示.

2　网络互联策略设计

2.1　内网用户访问外网资源策略设计

局域网内部用户访问 Internet 网络资源采用复合网关中 NAT 的动态地址转换技术[4], 将复合网关与 Internet 连接的网卡绑定多个合法的 IP 地址. 在局域网用户访问外网时, 将局域网用户使用的私有地址随机地转换为复合网关空闲的合法地址, 以实现将局域网用户的访问转向外网的目的.

在动态地址转换中, 由于绑定在复合网关外联网卡上的合法 IP 地址个数有限, 当局域网用户访问外网的需求增多时, 通过使用同一合法 IP 地址及不同的 TCP/UDP 端口号来标识不同的转换连接, 建立相应的 NAT 转换表项, 以实现多个局域网用户使用私有 IP 地址与同一个合法 IP 地址进行转换, 即端口地址转换方式[5]. 局域网用户访问外网的具体数据传输及地址转换过程见表 1、表 2、表 3 和表 4.

表 1　局域网主机发送访问请求数据包

名称	标识
目标 IP 地址	Internet 资源 IP 地址
源 IP 地址	私有 IP 地址
目标端口	Internet 资源 TCP 或 UDP 端口
源端口	源应用程序 TCP 或 UDP 端口

表 2　NAT 网关发送数据包

名称	标识
目标 IP 地址	Internet 资源 IP 地址
源 IP 地址	ISP 分配的公用地址(可变)
目标端口	Internet 资源 TCP 或 UDP 端口
源端口	重新映射的源应用程序 TCP 或 UDP 端口(可变)

表 3　NAT 网关收到目标主机响应数据包

名称	标识
目标 IP 地址	ISP 分配的公用地址
源 IP 地址	Internet 资源 IP 地址
目标端口	重新映射的源应用程序 TCP 或 UDP 端口
源端口	Internet 资源的 TCP 或者 UDP 端口

表 4　局域网主机收到响应数据包

名称	标识
目标 IP 地址	私有 IP 地址(不可变)
源 IP 地址	Internet 资源 IP 地址
目标端口	源应用程序 TCP 或者 UDP 端口(不可变)
源端口	Internet 资源 TCP 或 UDP 端口

理论上, 1 个合法的 Internet 地址可以支持的全部转换表项为 2^{16} 个, 即 65 536 个. NAT 网关能够同时支持地址转换数量的另一个决定因素是 NAT 网关动态随机存储器(DRAM)的大小, 地址转换表中的每个表项通常约占用 160 Byte, 对于 512 MB 的内存而言, 理论上可约容纳约 335.5 万个地址转换记录. 因此, 可根据实际网络用户的数量扩大 NAT 网关的动态随机存储器容量, 使 NAT 网关能够容

纳更多的表项. 文中使用的 NAT 网关动态随机存储器容量为 2 GB.

2.2 远程用户访问内网公共资源策略设计

内网公共资源如 WEB 和 E-MAIL 服务等应用以同等模式配置在内网的 2 台外部服务器上，并通过负载均衡群集技术在 2 台外部服务器进行群集. 群集通过内部负载均衡机制及服务器的具体状态来确定哪台服务器为用户提供服务，以消除单台外部服务器故障而造成用户无法访问应用的问题.

远程用户访问内网公共资源则采用复合网关中 NAT 的静态 IP 地址映射技术，将复合网关连接 Internet 网卡中绑定的部分合法 IP 地址，静态地映射到局域网中公共应用服务器群集使用的群集 IP 地址上，形成 1:1 的映射关系，使来自 Internet 对合法 IP 地址的访问直接转向局域网内部的私有 IP 地址(VIP). IP 地址静态映射的原理与 IP 地址动态映射原理相同，但映射关系在网关中长久保存，直到人为删除为止.

2.3 授权的远程用户访问内网私有资源策略设计

内网私有资源如 OA 系统、业务管理等的应用以同等模式配置在内网的 2 台内部服务器上，并通过负载均衡群集技术将 2 台内部服务器进行群集，以消除由于单台内部服务器故障造成内部用户及授权的远程用户无法访问内部应用系统的问题.

授权的远程用户访问内网私有资源需通过复合网关中虚拟专用网络(VPN)技术来实现[6]. VPN 网关与 NAT 网关一起被集成在复合网关上，授权的远程用户通过 Internet 与 VPN 网关建立专用隧道连接到局域网上，并获得局域网资源的使用权限，达到使用局域网资源的目的.

VPN 是一种仿真的专用网络连接方式，它采用加密和认证技术，在物理网络连接的基础上建立安全可靠的专用隧道来实现网络连接，这种连接是一种专用的逻辑连接，并且依靠对数据通信进行加密来实现.

VPN 在工作过程中需对传输的数据进行封装，然后再加上 1 个 VPN 包头，并且在包头中提供路由信息，以便被封装的数据包能通过公用网络到达目标地址. 为保证数据包在公用网络上传输时的安全性，还必须对封装的数据进行加密，使得数据包具有可靠的保密性、真实性和完整性. VPN 的接收方在收到封装的数据包后，先将 VPN 包头进行解封，再对数据进行解密，并验证数据的真实性和完整性. 于是，在建立连接的不同网络系统之间形成了逻辑上的安全隧道，即 VPN 隧道，而所有的通信过程都在隧道上进行.

以 PPTP VPN 为例. VPN 通信首先建立 PPP 连接, PPP 客户机通过 PPP 连接到 Internet 上，在建立 PPP 连接的过程中进行用户身份验证，然后再对数据进行加密建立 PPTP 控制. 并在 PPP 连接的基础上，PPTP 创建客户机到目标主机的连接控制来管理通信使用的隧道. 最后建立 PPTP 隧道, PPTP 生成加密 PPP 帧的 IP 数据包通过 PPTP 隧道与目标主机进行数据传输，而目标主机对接收到的数据包进行拆封和解密.

3 网络互联策略实现

局域网 LAN1 和 LAN2 中各设备具体参数见表 5、表 6、表 7 及表 8.

(1) 打开 LAN1 中的复合网关服务器，点击“开始”|“管理工具”|“路由和远程访问”选项，在服务器名称上点击鼠标右键，选择“配置并启用路由和远程访问”选项，打开路由和远程访问服务器安装向导，点击“下一步”按钮. 在配置窗口中选择“虚拟专用网络(VPN)访问和 NAT(V)”选项，点击“下一步”按钮.

(2) 在“VPN 连接”窗口中选择连接到外网的网卡，然后选中“通过设置基本防火墙来对选择的接口进行保护”选项，然后点击“下一步”按钮.

(3) 在“IP 地址指定”窗口中选择“自动”按钮，点击“下一步”按钮.

表 5　局域网服务器 IP 配置

设备名称	IP 地址
外部服务器 ps11 及 ps21	192.168.0.1
外部服务器 ps12 及 ps22	192.168.0.2
内部服务器 s11 及 s21	192.168.0.3
内部服务器 s12 及 s22	192.168.0.4
群集 NLB11 及 NLB21	192.168.0.5
群集 NLB12 及 NLB22	192.168.0.6
DHCP 服务器 h11 及 h21	192.168.0.7
DNS 服务器 d11 及 d21	192.168.0.8
LAN1 及 LAN2 中用户	DHCP 分配

表 6　复合网关 IP 配置

设备名称	IP 地址
g11 及 g21 内网网卡	192.168.0.254
g11 外联网卡	218.0.3.66
	218.0.3.67
	218.0.3.68
	218.0.3.69
g21 外联网卡	218.0.3.70
	218.0.3.71
	218.0.3.72
	218.0.3.73

表 7　DHCP 服务器 h11 及 h21 作用域

设备名称	配置参数
IP 地址范围	192.168.0.20~192.168.0.253
子网掩码	255.255.255.0
网关	192.168.0.254
DNS	192.168.0.8

表 8　复合网关静态 IP 地址映射关系表

复合网关	IP 地址	
g11 与 NLB12	192.168.0.6	218.0.3.66
g21 与 NLB22	192.168.0.6	218.0.3.70

(4) 在“管理多个远程访问服务器”窗口中选择“否，使用路由和远程访问来对连接请求进行身份验证”选项，点击“下一步”按钮，仔细观察“摘要”窗口内容并记录，点击“完成”按钮结束复合网关的初步配置.

(5) 展开路由和远程访问服务器中的“IP 路由选择”项，选中“NAT/基本防火墙”项，然后在右边的窗口中选择连接外网的网卡，点击右键并选择“属性”选项，打开外网网卡的属性窗口，选择“地址池”选项卡，点击“添加”按钮，将连接外网的网卡绑定的 4 个连续 IP 地址的起始 IP 地址、子网掩码及结束 IP 地址添入其中，具体信息见表 6.

(6) 点击保留公用地址窗口中的“保留”按钮，在打开的窗口中点击“添加”按钮，在添加保留区窗口中按照表 8 中外部 IP 地址与内网应用服务器 IP 地址的映射关系，填入外部IP与内部IP地址218.0.3.66~192.168.0.6，并选中“允许将会话传入到此地址”项，完成复合网关 g11 外联网卡上绑定的合法IP地址与应用服务器群集私有 IP 地址间的静态映射关系的建立，以实现外网用户访问局域网中的公共服务器. g11 网关外联网卡上绑定的其他合法 IP 地址留作LAN1用户动态租用，以实现局域网用户顺利访问外网资源.

(7) 选择服务与端口选项卡，选中允许外网用户访问的内网服务，如 WEB 服务器(HTTP)服务，然后在公用地址栏中选择“在此接口(F)”选项，在专用地址(P)栏后的对话框中输入专用 IP 地址 192.168.0.6，点击“确定”按钮，结束外网用户访问内网公共资源的配置过程.

(8) 选择“DHCP 中继代理程序”并点击右键，选择“新增接口”项，分别添加外网和内网网卡为中继接口. 然后在“DHCP 中继代理程序”上点击右键并选择“属性”项，在打开的窗口的“服务器地址”中添加局域网中 DHCP 服务器的 IP 地址.

(9) 打开复合网关 g11 中的“开始”|“管理工具”|“计算机管理”选项，选择“系统工具”中的“本地用户和组”选项，在“用户”上点击右键，选择“新用户”，输入用户名和密码，创建用于 VPN 连接的用户，如 user1，然后在用户 user1 上点击右键并选择“属性”项，选择“拨入”选项卡，选中“允许拨入”选项，然后，点击“确定”按钮，结束 VPN 用户拨入的权限设置.

(10) LAN2 中复合网关的配置参照上述(1)~(8)步骤即可.

4 测试与分析

在局域网 LAN1 和 LAN2 中，用户均能够访问到彼此内网中公共 WEB 服务器及 Internet 上的服务器. Internet 用户及局域网用户通过 VPN 连接到相应的复合网关后，均能够获得局域网内部 DHCP 服务器分配的私有 IP 地址、子网掩码、网关和 DNS 参数，并能通过内部域名顺利访问局域网的内部 WEB 服务器及授权的应用资源. 测试说明：复合网关顺利实现了局域网通过 Internet 的有效低成本互联，且互联后对原局域网的结构及 IP 地址分配均不产生影响，并实现了远程用户对内部私有资源的便捷访问.

5 结语

基于复合网关的网络互联策略有效的集成了 VPN 与 NAT 技术，实现了局域网通过 Internet 的有效互联，规避了局域网网络互联后 IP 地址的冲突问题，解决了用户通过 Internet 授权访问局域网内部资源的问题以及内部用户通过有限的 IP 地址资源访问 Internet 资源的问题，同时提高了局域网应用服务的安全性，且该网络互联方法实现简便，成本低廉，具有广泛的实用价值.

参考文献:

[1] 鞠洪尧，宋宇新. 实用组网技术[M]. 北京：科学出版社, 2007.
[2] 杜大鹏，岳丽君，杜墨，等. Windows Server 2003 深层解决方案[M]. 北京：中国水利水电出版社, 2005.
[3] 黄道颖，张杰，甘勇，等. 计算机网络[M]. 北京：科学出版社, 2006.
[4] 刘风华，丁贺龙，张永平. 关于 NAT 技术的研究与应用[J]. 计算机工程与设计, 2006, 27(10):1 814-1 817.
[5] 刘雅辉，张全林，祝跃飞. IPSec 穿越 NAT 方案研究与改进[J]. 计算机工程与设计, 2005, 26(7):1 918-1 921.
[6] 林惠君，彭宏，李君. 应用服务器动态负载均衡的设计与实现[J]. 计算机工程与设计, 2007, 28(14):3 388-3 390.

Synthetic Gateway Based Implementation of Network Interconnection Strategy

JU Hong-yao

(Department of Science, Zhejiang Textile & Fashion College, Ningbo 315211, China)

Abstract: A network interconnection strategy based on composite gateway is proposed using the analysis and study on the principle and functionalities of combined technology of both virtual private network and network address translation. The synthetic strategy achieves the interconnection among the local area networks in various areas through Internet, and solves the login problems found with the remote user who attempts to use the local area network to visit private resource. From the perspective of application, the test result demonstrates the stability, reliability and simplicity of the proposed strategy.

Key words: synthetic gateway; network interconnection; virtual private network; network address translation

CLC number: TP393.03 **Document code:** A

（责任编辑 章践立）