基于防火墙策略路由的网络安全应用研究

潘文婵,董艾华,刘尚东
(南京邮电大学 计算机学院,江苏 南京 210023)

摘 要:随着互联网的飞速发展,网络安全逐渐成为一个潜在的巨大问题。防火墙是网络安全的关键技术,策略路由可以使数据包按照用户指定的策略进行转发。针对日益复杂的网络多出口问题,文中介绍了基于源地址的策略路由,提出了一种结合策略路由、网络地址转换等多技术的多出口配置方案,并比较了策略路由和路由策略的区别。基于防火墙设计策略路由,并结合网络地址转换,可以提高网络出口资源利用率,实现网络负载均衡,保护校园网安全。

关键词:策略路由;网络地址转换;防火墙;网络安全
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2013)08-0125-04
doi:10.3969/j.issn.1673-629X.2013.08.032

Research on Application of Network Security Based on Firewall Policy Routing

PAN Wen-chan, DONG Ai-hua, LIU Shang-dong
(School of Comp. Sci. and Tech., Nanjing Univ. of Posts and Telecommunications, Nanjing 210023, China)

Abstract: With the rapid development of Internet, network security has become a potentially huge problem. Firewall is the key technology of network security. Policy-based routing can make the packet forwarding according to the user specified strategy. According to the increasingly complex network of multiple egress problem, introduce the policy-based routing method according to the source address to select routing and compare the difference of policy-based routing and routing strategy. A more suitable configuration for multiple egress network is proposed, based on technologies such as policy-based routing and network address translation. For improving the network resource utilization of the export and protection of the campus network security, it is very important to design policy-based routing in firewall and the network address translation.

Key words: policy-based routing; NAT; firewall; network security

0 引 言

网络安全从本质上讲就是网络上的信息安全,网络系统的软硬件及数据受到保护,避免出现病毒、非法存取、网络资源非法占用等威胁,制止和防御网络黑客的攻击。网络安全来源于安全策略与技术的多样化,随着网络应用于社会各方面,进入网络的方式也越来越多,因此,网络安全技术尤其重要[1]。

防火墙是由软件、硬件设备组成,在内网和外网之间、专用网和公共网之间的界面上建立的保护屏障。防火墙的基本功能是在计算机网络中,控制不同信任程度区域间数据流的传输[2]。比如,只允许符合特定规则的数据包通过,其余的一律禁止通过防火墙。防火墙只允许授权的通信通过,为网络安全起到了保护作用。防火墙是 2 个网络之间的成分集合,具有以下属性:内部网络和外部网络之间的所有网络数据流都必须经过防火墙;只有符合安全策略的数据流才能通过防火墙;防火墙自身具有非常强大的抗攻击免疫力。

防火墙技术中一个重要的研究方向是硬件防火墙,硬件防火墙一般是独立于被保护主机或者网络的一个专用网络设备,处于连接内网与外网的网关处[3]。根据侧重不同,防火墙可分为:包过滤型防火墙、应用层网关型防火墙和服务器型防火墙[4]。

网络通信实验室具有相关配套的软硬件和网络环境,实验室面向学生开放,可以让学生在丰富感性认识的同时消化教材上的理论知识,增强动手实践能力,胜任实际应用。

收稿日期:2012-11-18 **修回日期**:2013-02-26 **网络出版时间**:2013-04-22
基金项目:南京邮电大学教学改革研究项目(JG00412JX57);南京邮电大学实验室建设与设备管理研究课题(2012XSG07)
作者简介:潘文婵(1983-),女,江苏南京人,实验师,硕士,研究方向为网络安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20130422.1721.023.html

1 策略路由与 NAT 技术

1.1 策略路由

策略路由(Policy-Based Routing)是一种灵活的数据包路由转发机制,策略路由是指防火墙可以根据源地址或预定义的服务按指定路由访问不同的目的地。传统路由中,路由器在由路由协议产生的路由表中,根据目的地址转发报文。策略路由比传统路由更加灵活,不仅能够根据数据包的目的地址,而且能够根据协议类型、报文大小、应用、IP 源地址或者其他的策略来进行报文的转发。策略路由可以根据实际应用的需要来控制多个路由器之间的线路负载均衡、单一链路上数据包转发的 QoS 或者满足某种特殊需求[5]。

防火墙的策略路由优先级高于静态路由和缺省路由,低于直连路由。策略路由可以在指定位置上灵活修改,添加和删除。一个接口应用策略路由后,将根据预先设定的策略对该接口接收到的所有数据包进行匹配,如果匹配到一条策略,就按照策略路由进行转发;如果没有匹配到任何策略,就按照路由表中转发路径来进行路由。

策略路由分为三种:源地址路由、目的地址路由和智能均衡的策略方式。源地址路由根据路由源地址来实施策略。目的地址路由根据路由的目的地址来实施策略。智能均衡策略,是策略路由的发展方向。

策略路由可应用于电信、网通的互联互通。我国南电信北网通的问题是众所周知的,电信、网通之间互访的速度较慢,对于数据的传输产生很大的影响[6]。解决方案是接入电信、网通双线路,在路由设备上增加策略路由,使用目的地址路由方法,实现了电信数据走电信、网通数据走网通。路由设备能够自动地识别电信、网通线路并且自动采取相应的策略方式,这就是智能均衡策略,也是策略路由的发展趋势。

1.2 NAT

网络地址转换(NAT,Network Address Translation)是指将私有地址转化为合法注册的 IP 地址,进而与 Internet 上的其他主机进行通信。私有地址的范围包括:10.0.0.0 ~ 10.255.255.255,172.16.0.0 ~ 172.31.255.255,192.168.0.0 ~ 192.168.255.255。而连接到 Internet 的 NAT 路由器的出口接口由网络服务提供商(ISP)分配公有 IP 地址。NAT 的作用就是根据路由内部的地址转换表中的映射关系,将私有地址和公有地址进行转换。NAT 可应用于各种类型的网络中和多种 Internet 接入方式。当多个内部主机共享一个合法的 IP 地址时,NAT 的实现方式为端口多路复用,即端口地址转换,是指改变外出数据包的源端口并进行端口转换,从而最大限度地节约 IP 地址资源[7]。NAT 不仅解决了 IP 地址资源缺乏的问题,而且还能够保护内部网络的计算机,有效地避免外部网络的攻击。

NAT 有三种实现方式:静态转换、动态转换和端口多路复用。静态地址转换为每一个内部地址映射一个唯一的全局地址,内部地址与全局地址是一对一的,一成不变的。动态地址转换是指将内部网络的私有 IP 地址转换为合法 IP 地址时,IP 地址是随机的、不确定的。设置一个 NAT 地址池,全局地址在地址池中列出,当内部用户与外部通信时,从 NAT 地址池中随机选择全局地址进行转换。当 ISP 提供的公有 IP 地址数量比内部网络的计算机数量少时,可以采用动态转换的方式。端口多路复用是指改变连接到外部网络接口的数据包的源端口并进行端口映射。端口地址转换也是一种动态地址转换,但是允许多个内部本地地址共用一个合法 IP 地址。目前网络中应用最多的就是端口多路复用方式。

2 基于源地址的策略路由的实现

下面以《计算机通信与网络实验》课程实验为例,说明实验室开放与实验课堂教学的配合。防火墙默认管理端口 IP 地址:192.168.10.100/24,可将管理主机 IP 配置为 192.168.10.200/24,与防火墙 WAN 接口相连,通过 WEB 方式登录防火墙管理界面。

实验主要描述基于源地址的策略路由,拓扑结构如图 1 所示。

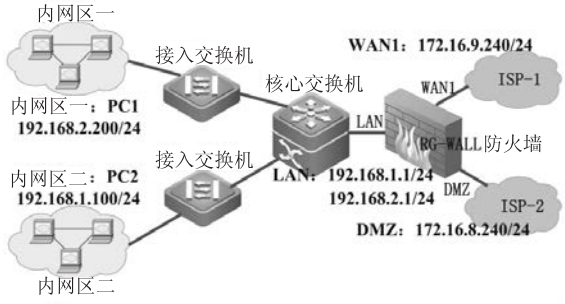

图 1 网络拓扑图

内网用户 PC1 通过锐捷 RG-WALL 防火墙 WAN1 口访问 ISP-1,内网用户 PC2 通过 RG-WALL 防火墙 DMZ 口访问 ISP-2。WAN1 口的 IP 地址:172.16.9.240/24,DMZ 口的 IP 地址:172.16.8.240/24,LAN 口的 IP 地址:192.168.1.1/24、192.168.2.1/24。PC1 的 IP 地址:192.168.2.200/24,PC2 的 IP 地址:192.168.1.100/24。

2.1 配置接入网络的接口 IP 地址

配置 RG-WALL 防火墙 LAN,WAN1,DMZ 三个接口的 IP 地址,如图 2 所示。

2.2 配置针对源地址的策略路由

配置第一条策略路由,源地址为 172.16.8.240,下一跳地址为 172.16.8.1。配置第二条策略路由,源

地址为 172.16.9.240,下一跳地址为 172.16.9.1。配置策略路由时选择 LAN 网口按源 IP 路由进行转发。

网络配置>>接口IP

网络接口	接口IP	掩码
dmz	172.16.8.240	255.255.255.0
lan	192.168.1.1	255.255.255.0
lan	192.168.2.1	255.255.255.0
wan	192.168.10.100	255.255.255.0
wan1	172.16.9.240	255.255.255.0

图 2　接口 IP 地址

配置两条策略路由,如图 3 所示。

网络配置>>策略路由

以下网口是否允许按源IP路由

☐dmz ☑lan ☐wan ☐wan1

确 定

类型	源地址	目的地址	下一跳
源路由	172.16.8.240/255.255.255.255	0.0.0.0/0.0.0.0	172.16.8.1
源路由	172.16.9.240/255.255.255.255	0.0.0.0/0.0.0.0	172.16.9.1

图 3　策略路由

2.3　定义客户端 PC 的 IP 地址对象

定义两个 PC 的 IP 地址对象,PC1(192.168.2.200、255.255.255.255)定义为 NAT-1,PC2(192.168.1.100、255.255.255.255)定义为 NAT-2,配置地址列表。

2.4　配置 NAT 规则

配置 PC2 的 NAT 规则,源地址为 NAT-2,目的地址和服务为 any,源地址转换为 172.16.8.240。同理配置 PC1 的 NAT 规则,源地址转换为 172.16.9.240,如图 4 所示。

安全策略>>安全规则　　相关设置

序号	规则名	源地址	目的地址	服务	类型
☐ 1	p1	NAT-2	any	any	NAT规则
☐ 2	p2	NAT-1	any	any	NAT规则

图 4　NAT 规则

2.5　验证策略路由

客户端 PC1 通过访问 ISP-1,对 ISP-1(172.16.9.1)进行 PING 通测试,结果为可以 PING 通。同理客户端 PC2 也可以 PING 通 ISP-2(172.16.8.1)。因为直连路由的优先级高于策略路由,为了测试策略路由生效,需要 PING 通目的地址为防火墙定义端口网段以外的网络地址。

在防火墙 DMZ 口连接路由器(RG-R 系列或者 RG-RSR 系列路由器),在路由器上设置 IP 地址:与防火墙互联的接口 IP 地址设置为 172.16.8.1,另外设置一个本地环回接口 Loopback,设置 Loopback 接口的 IP 地址为 172.16.6.1。最后在路由器上设置一条缺省路由 ip route 0.0.0.0 0.0.0.0 172.16.8.240。

验证策略路由,如图 5 所示,PC2 可以 PING 通 172.16.6.1。如果删除基于源地址的策略路由,配置时不选择 LAN 网口按源 IP 路由进行转发即可,此时 PC2 无法 PING 通 172.16.6.1。

```
Ethernet adapter 本地连接 2:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : D-Link DGE-530T Gi
pter (rev.B)
        Physical Address. . . . . . . . . : 00-26-5A-79-F2-22
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\nanyou>ping 172.16.6.1

Pinging 172.16.6.1 with 32 bytes of data:

Reply from 172.16.6.1: bytes=32 time<1ms TTL=64
Reply from 172.16.6.1: bytes=32 time<1ms TTL=64
Reply from 172.16.6.1: bytes=32 time<1ms TTL=64
Reply from 172.16.6.1: bytes=32 time<1ms TTL=64

Ping statistics for 172.16.6.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 5　测试第一条策略路由

同理,可以在 WAN1 口连接路由器,同样的方法配置路由器:与防火墙的互联接口为 172.16.9.1,Loopback 接口为 172.16.7.1。加策略路由的情况,PC1 可以 PING 通 192.168.7.1,如图 6 所示。删除策略路由,PC1 无法 PING 通 172.16.7.1。

```
Ethernet adapter 本地连接 2:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : D-Link DGE-530T Gi
pter (rev.B)
        Physical Address. . . . . . . . . : 00-26-5A-79-F5-C8
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.2.200
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.2.1

C:\Documents and Settings\nanyou>ping 172.16.7.1

Pinging 172.16.7.1 with 32 bytes of data:

Reply from 172.16.7.1: bytes=32 time<1ms TTL=64
Reply from 172.16.7.1: bytes=32 time<1ms TTL=64
Reply from 172.16.7.1: bytes=32 time<1ms TTL=64
Reply from 172.16.7.1: bytes=32 time<1ms TTL=64

Ping statistics for 172.16.7.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

图 6　测试第二条策略路由

3　策略路由与路由策略

策略路由与路由策略是两个不同的概念,应用领域不同。

策略路由是数据包转发规则,依据用户制定的策略进行路由选择的机制,与单纯依照 IP 报文的目的地址查找路由表进行转发不同,可应用于安全、负载分担等目的[8]。路由器中存在两种类型和层次的表,分别是路由表和转发表。转发表是由路由表映射过来的,策略路由直接作用于转发表,不改变路由表中任何内容。

路由策略是路由发现规则,在正常的路由协议之上,根据某种规则,通过改变某些参数或者设置某种控制方式来改变路由产生、发布、选择的结果,最终改变的是结果(即路由表)。路由策略直接作用于路由表,是在路由发现的时候产生作用。

策略路由的优先级高于路由策略,当路由器进行数据包转发的时候,会优先匹配策略路由的规则,如果匹配一致,则按照策略路由来转发,否则根据路由表中的转发路径来转发[9]。

4 策略路由在多出口校园网中的应用

我国高校信息化建设正在经历巨大变迁,数字校园的建设包括三个层面:基础网络设施;公共服务体系,如邮件服务、安全防护等;业务应用层包括教学应用、科研应用、管理应用等。校园网单一接入教育网的模式已不能满足广大师生的网络需求。许多高校增加了教育网以外的其他 ISP 连接,比如电信、联通等,形成了多出口校园网网络结构。

为了保证网络的可用性,国内许多高校采用同时接入教育网和电信(或联通、移动)等多网接入方案,实现多链路并行[10]。由于教育网和公众网不同网络运营商之间的网络连通性问题,校园网用户访问不同的 ISP 时速度明显变慢。校园网的路由有特殊需求,多出口网络结构使得路由实现及相关问题更加复杂。

对于校园网,需要根据源 IP 地址进行路由选择,强制其通过指定出口进行路由转发,访问教育网资源走教育网出口,访问其他资源走公网出口。这样,一方面提高了出口速度,另一方面也提高校园网出口的冗余,增加校园网的稳定性[11]。在电信、联通出口实现 NAT,禁止校园网用户从教育网出口访问收费站点资源,有效减少教育网的国际流量费用。针对需要访问教育网资源的校园网用户制定源地址路由,这样不仅降低网络运行费用,还能防止校园网一个链路发生故障而断开和 Internet 的连接[12]。文中提出的策略路由和 NAT 相结合的配置方案,能够充分利用现有网络的多出口,尽可能地节约校园网运行成本,为广大师生提供可靠高效的网络访问。

5 结束语

策略路由和 NAT 相结合的方案,可以应用于多出口校园网络环境中,使校园网用户能通过不同的出口访问教育网、电信、联通等不同的网络资源。在出口防火墙应用策略路由,可以合理使用网络有限出口的宽带资源,实现网络负载均衡,提高资源利用率,保障校园网安全。

参考文献:

[1] Cheswick W R, Bellovin S M, Rubin A D. Firewalls and internet security: repelling the wily hacker[M]. Beijing: China Machine Press, 2003.

[2] Al-Tawil K, Al-Kaltham I A. Evaluation and testing of Internet firewalls[J]. International Journal of Network Management, 2002, 9(3): 135-149.

[3] 谈 华. 硬件防火墙在网络安全中的应用[J]. 电脑知识与技术:学术交流, 2007(19): 73-74.

[4] 田 原, 云晓春, 朱晓辉. 防火墙性能基准测试研究[J]. 计算机仿真, 2003, 20(7): 123-125.

[5] 陈志平. 校园网络安全与防火墙技术[J]. 现代计算机, 2007, 25(1): 47-49.

[6] 刘建伟, 张卫东. 网络安全实验教程[M]. 北京: 清华大学出版社, 2007.

[7] 贾学锋, 荆一楠, 王雪平, 等. 基于 TCP 协议的 NAT 穿透技术在 P2P 中的研究与实现[J]. 计算机应用与软件, 2008, 25(6): 186-187.

[8] 张焕杰, 孟庆宇, 杨寿保. 基于 Linux 系统的校园网多出口策略路由实现[J]. 通信学报, 2006(z1): 130-133.

[9] 翟 钰, 武舒凡, 胡建武. 防火墙包过滤技术发展研究[J]. 计算机应用研究, 2004(9): 144-145.

[10] 张红梅. 策略路由在校园网中的应用[J]. 宁波工程学院学报, 2005, 17(4): 28-30.

[11] 姚亚锋, 方贤进, 赛文莉. 新型内容过滤防火墙的研究[J]. 计算机技术与发展, 2010, 20(11): 158-161.

[12] Verma D. Simplifying Network Administration Using Policy Based, Management[J]. IEEE Network, 2002, 16(2): 20-26.

(上接第 124 页)

[9] Rosenberg J, Weinberger J, Huitema C, et al. STUN-Simple Traversal of User Datagram Protocal (UDP) Through Network Address Translators(NATs)[S]. IETF RFC 3489, 2003.

[10] 秦 刘, 智英建, 贺 磊, 等. 802.1X 协议研究及其安全性分析[J]. 计算机工程, 2007, 33(7): 153-154.

[11] 凤 琦, 王震宇, 李向东, 等. 基于 802.1X 的可信网络连接技术[J]. 计算机工程, 2009, 35(5): 165-167.

[12] 刘海韬, 张 浩. 结合 802.1x 技术实现网络安全管理[J]. 计算机技术与发展, 2009, 19(7): 170-172.

基于防火墙策略路由的网络安全应用研究

作者： 潘文婵， 董艾华， 刘尚东， PAN Wen-chan， DONG Ai-hua， LIU Shang-dong
作者单位： 南京邮电大学 计算机学院,江苏 南京,210023

刊名： 计算机技术与发展

ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2013(8)