基于防火墙的双出口路由策略的设计与实现①

崔 萌 于承斌 (泰山医学院 现代教育技术中心 山东 泰安 271016)

摘 要: 根据校园网双出口的接入实际，设计并实现一种基于防火墙的双出口路由策略。分析原有网络接入现状，指出优化出口路由的必要性，提出了基于防火墙的双出口路由优化策略，利用静态路由与 NAT 技术，均衡双出口流量。最终给出接口与区域、NAT 转换与路由通信以及防火墙日志记录等的配置过程，实现了该优化策略。这种策略可以广泛应用到校园网的双出口路由中，并能实现高速访问、安全稳定的良好效果。

关键词: 路由；防火墙；网络地址转换

Design and Implementation of a Strategy for Double-Export Routing Based on Firewall

CUI Meng, YU Cheng-Bin

(Center of Modern Education Technology, Taishan Medical College, Taian 271016, China)

Abstract: According to the reality of campus network's double-export, this article designs and applies an optimized strategy of double-export routing based on firewall. After analyzing the campus practice and the importance to optimize the double-export routing, a new optimized strategy is designed which can balance the flux between two exports by static routing and NAT technology. An actual configuration and application of interface and area, routing and NAT, the syslog of the firewall are given. So the strategy can be applied in the double-export of campus network to achieve high speed and stability.

Keywords: routing; firewall; NAT

为了提高校园网出口的网络访问速度、减少访问国际流量的费用和提供出口冗余，目前很多高校的校园网都拥有双出口乃至多出口,一般是既有中国教育科研网出口，又有当地运营商的网络出口。出于安全性、负载均衡、实现技术以及访问速度等的需要[1]，充分应用已有网络设备，合理设计与规划路由策略，才能充分利用双出口的带宽，实现链路与设备的冗余备份与网络的高速访问。

1 我校网络接入现状与问题的提出

校园网最早大多采用单一的 CERNET 出口接入。尽管接入 CERNET 的带宽从 2M、34M、100M 提高到了 1G，但访问 CERNET 以外的资源速度仍然很慢，这与 CERNET 与其他 ISP 的连接带宽以及相互之间路由设置的大环境有关，而且通过 CERNET 访问的国际流量费用昂贵，因此大多高校也租用了当地 ISP 网通的链路为第二出口。作为节点，考虑安全问题，而且为另一所高校金融学院的提供到 CERNET 接入，最初我们采用的策略是直接在路由器上做简单的默认路由与静态路由[2]，以使访问公网的流量走 ISP 的链路，访问 CERNET 的流量走 CERNET 出口。具体的网络拓扑如图 1(图示与配置示例中均使用虚地址)。

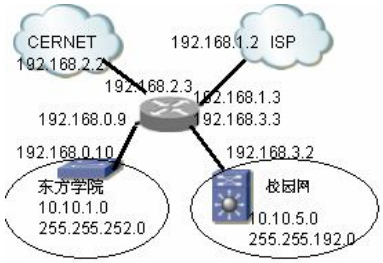

图 1 原出口路由拓扑图

① 收稿时间:2009-09-25;收到修改稿时间:2009-11-14

相关的路由配置如下：

ip route 0.0.0.0 0.0.0.0 192.168.1.2 //默认路由指向 ISP

ip route 203.91.120.0 255.255.248.0 192.168.2.2 //

以下 CERNET 免费访问地址指向 CERNET

ip route 210.25.0.0 255.255.128.0 192.168.2.2

……

如上的路由策略确实启用了两条链路，并且 ISP 线路分担了网络的国际流量，不用按照公安管理部门的要求存留两个月的访问日志，但是此策略并没有提高网络访问的速度。因为 ISP 没有直接回指的路由，故访问后返回的应答内容经 ISP 的层层路由最终被指向 ISP 与 CERNET 对接的路由后，再由 CERNET 的路由线路回指回来，所以访问公网的内容要绕一大圈后再经教育网线路回来，由于路由的增多与 CERNET 带宽的限制，不仅没有加快访问速度，反而使得网速更慢；同时也没有起到两条线路相互备份的作用，事实上，任何一条线路断开，访问都将受到影响，如 CERNET 线路断开，所有网络均不能访问。因此，采取新的优化的出口路由策略势在必行。

2 利用防火墙及其NAT技术优化的双出口路由策略

根据以上实际情况，要充分利用 ISP 出口，使访问公网的请求仍从公网返回，考虑本地 ISP 不会为 CERNET 分配的 IP 地址提供接入路由，故采用 NAT(NetworkAd-dressTranslation 网络地址转换)技术解决此问题则能取得较好的效果。NAT 是一个 IETF 标准，是为了解决 IPv4 网络地址空间不足而产生的一项技术，它允许一个整体机构以一个公用 IP 地址出现在 Internet 上，实质是一种把内部 IP 地址翻译成这个公用 IP 地址的技术[3]。在此方案中，我们选择静态 NAT，将校园网的每个 IP 永久映射为 ISP 提供的合法 IP 地址，并由防火墙具体实现 NAT 转换，形成访问公网的流量 NAT 到 ISP 出口流出，再从该线路返回流入，从而减少层层的路由指向与带宽瓶颈等束缚。而访问 CERNET 的请求数据包则作策略路由，走 CERNET 出口。考虑为另一高校金融学院提供到 CERNET 的网络接入，则把校园网从防火墙出来的链路与金融学院一起通过路由器连接到 CERNET。同时，利用防火墙向校园网方向的 NAT 功能与 VPN 功能，可以从外网建立到校园网的 VPN 隧道[4]，方便网管人员从外网登录到校园网进行网络的管理。具体方案的网络拓扑如图 2。

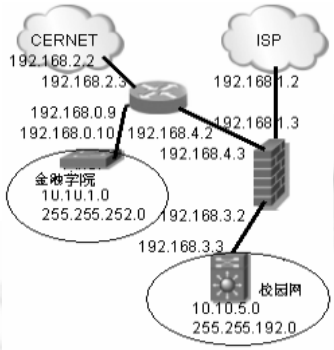

图 2　优化的出口路由拓扑图

3 优化的双出口路由策略的实现

根据上述规划的方案，利用天融信 NGFW-4000 防火墙，较好地实现了方案中提出的双出口路由策略。具体的实现从以下几个方面进行：

3.1 防火墙接口与区域的配置

防火墙接口的配置如图 3 所示，主要是给接口对应的区域命名并配置 IP 地址与设置访问权限以及是否开启日志会话等等，实际配置结合优化方案中的拓扑图给出：

区域名	设备名	IP	访问权限	日志	状态
cnc	eth0	192.168.1.3	允许访问	日志会话	开启
校园网	eth1	192.168.3.2	禁止访问	不做日志	开启
EDU	eth2	192.168.4.3	允许访问	不做日志	开启
global_area	global		允许访问	不做日志	停用

图 3　防火墙接口的配置图

cnc 区域：对应 ISP 网通的入口，接在防火墙的 eth0 接口上，IP 地址为 192.168.1.3，缺省访问权限为允许访问，日志选项为记录日志会话(因为要做 NAT 出去，对外显示的 IP 都是 192.168.1.3，故根据信息安全的需要，设置记录所有外出访问的信息日志)。

校园网区域：对应内网出口，接在防火墙的 eth1 接口上，IP 地址为 192.168.3.2，缺省访问权限为禁止访问(后面将把允许访问的服务器等地址单独加以定义设置)，日志选项为不记录日志会话。

EDU 区域：对应 CERNET 接口，接在防火墙的

eth3 接口上，IP 地址为 192.168.4.3，缺省访问权限为允许访问，日志选项不记录日志会话(因为走 CERNET 的外出信息都是教育网的真实 IP 地址，故不做日至记录)。

其他接口未使用，未配置。

3.2 NAT 功能的实现

在防火墙的访问策略里面增加一条通信策略，源选择内网即校园网，目的选择外网即 cnc，通信方式选择 NAT，指定协议为所有协议，目的端口为所有端口。这样设置即可满足校园网到 cnc 的访问通过 NAT 转换出去，具体配置界面如图 4。

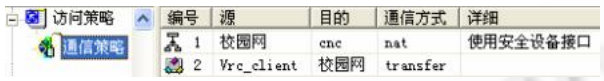

图 4 防火墙的 NAT 设置

3.3 防火墙路由功能的实现

在访问策略里面打开路由表，首先建立默认路由指向，使源地址为所有地址的所有请求都指向 ISP 提供的公网出口 192.168.1.2；其次建立静态路由，使访问教育网的路由设置成源地址为所有地址，目的 IP 地址为教育网提供的免费地址的所有请求都指向与防火墙相连的路由器接口的 IP 地址 192.168.4.2。从而实现访问教育网的资源通过路由器走 CERNET 出口，访问公网的资源则走 ISP 提供的公网出口 192.168.1.2。另外，建立从外网访问校园网的路由，使源地址为所有地址，访问目的地址为校园网地址(IP 地址为 10.10.5.0，掩码是 255.255.192.0)的所有请求都指向校园网的接口 IP 地址 192.168.3.2。

3.4 对内服务器访问的设置与防火功能的实现

如上在区域与接口配置中把校园网区域设置为禁止访问，从而增加了内网的安全性，但校园网内有一些诸如 www、mail 和 ftp 等服务需要对外放开访问，而利用防火墙的访问控制策略即可把这些少量的服务放开。

首先在网络对象的校园网区域里面，把需要从校园网外部能访问到的校园网内部的服务器定义为一些节点或子网，如图 5，把对外开放的学校主页、邮件、FTP 以及其他一些应用服务器定义成一个子网，名称为服务器，把 DNS 以及图书馆对外的一台服务器分别定义了一个节点。

图 5 访问对象的设置

其次，在访问策略的校园网区域，增加访问这些服务器的策略，具体选择策略源地址为外网地址 cnc 与 EDU，策略目的地址即这些允许外边访问的服务器的地址，策略服务可以根据不同服务器提供的服务类别进一步选择采用允许或禁止访问的策略，而且可以设置允许访问的时间段和是否记录访问日志等等。具体如图 6。

图 6 访问策略的设置

3.5 防火墙日志功能的实现

在区域里把 cnc 对应的接口 IP 地址设为 192.168.1.3，缺省访问权限为允许访问，日志选项为记录日志会话，即可满足其记录日志功能。再从选项设置模块中的安全设备登录控制里面，设置安全登录设备即日志服务器的有关属性，在校园网区域里面选择一台机器作为 syslog 日志服务器，通信端口选择 814，从而把防火墙通过的有关访问日志记录到这台服务器上。在服务器上安装相关日志审计程序，即可实时记录、查看审计、备份防火墙日志。

3.6 CERNET 出口路由的设置实现

在防火墙中，把访问 CERNET 划定的免费访问地址的下一跳都指向了接入 CERNET 的路由器，金融学院也通过该路由器接入 CERNET，为此，在 CISCO 路由器上只需设置如下的静态路由即可：

```
Router# ip route 10.10.5.0 255.255.192.0 192.168.4.3
Router# ip route 10.10.1.0 255.255.252.0 192.168.0.10
Router#ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

3.7 VPN 功能的利用

利用防火墙的 VPN 功能，还能实现从外网到校园

网的 VPN 远程登录，具体实现如下：

首先，根据防火墙配置导入 VRC 客户端证书，并建立用户认证数据库。其次，配置 VPN 的访问策略，主要在特殊对象的用户里面，添加一个 VPN 的用户，其名称为 Vrc_client，并使用 VRC-ser 数据库进行认证。在通信策略里添加一个新的通信方式，源地址为 Vrc_client，目的地址即为所要远程访问的校园网，其通信方式设置为 NAT 方式(如图 4 所示)。最后，在选项设置的防火墙登录控制中添加相应的权限，允许 Vrc_client 登陆。在校园网之外的联网计算机上，启动 VRC 客户端软件并设置登陆防火墙的地址与相应的证书后，便通过 VPN 隧道的形式连接到防火墙，从而方便的对内网中相关网络设备进行管理。

基于以上的配置，我校成功实现了双出口路由策略的优化，效果明显：(1)利用防火墙的 NAT 功能，使访问公网的请求与应答直接经过 ISP 的线路，访问速度明显增加；(2)两条线路真正实现了冗余备份，即使其中一条线路断开，网络访问基本不受影响；(3)与利用路由器做 NAT 比较占用设备的 cpu 与内存资源相比，防火墙实现 NAT 功能基本不占用 CPU 资源，如图 7 所示，CPU 利用仅 0.3%；(4)日志记录功能很好的满足了信息安全的查询需要；(5)区域与节点的访问控制功能，使来自不同路由对服务器访问的权限不同，增强了网络的安全性；(6)通过防火墙的 VPN 功能，无需其它的软硬件工具，即可建立从外网登录到校园网内的 VPN 隧道，方便了网络管理。

图 7　cpu 及内存利用率

参考文献

1 黄敏,张卫东.基于策略路由的网络设计与实践.计算机应用, 2002,22(5):72－73.

2 肖捷.静态路由选择配置方案的设计.计算机工程, 2000,26(8):141－143.

3 禹龙,田生伟.网络地址转换(NAT)技术及其在校园网中的应用.计算机工程, 2004,30(6):192－194.

4 潘建国,陈海强.基于 VPN 技术的网络应用.计算机应用研究, 2001,17(1):87－89.