ISA 代理服务器在现代教育网络中的若干主要技术问题

Some Main Technical Problems of ISA Proxy Server on the Modern Education Network

孟万化 傅蓉心（浙江绍兴文理学院实验中心 312000）

摘 要：本文阐述了现代教育网络中代理服务器的选择，介绍了ISA代理服务器的主要性能与优点，并给出了ISA代理服务器在现代教育网络中的若干主要技术问题及解决方法。

关键词：现代教育网络 代理服务器 ISA Internet

随着计算机网络的普及，以计算机为核心的网络教育已成为当前实施素质教育、提高教学质量的一种有效途径。CERNET不断的扩大和发展，用户正在不断地增加，通过Internet技术和计算机多媒体技术进行网络教育将成为网络技术发展研究以及先进教育模式研究的重点。目前，网络教育在我国正以前所未有的态势蓬勃发展，我国高校一般通过学校自己投资建设一个校内Intranet基础设施，再通过DDN或X.25、或租用广电或其他部门提供的光纤带宽、或自己架设光纤通过地区网络中心接入CERNET。

为了方便教学Intranet的管理，满足现代网络教育的需要，使Intranet积极推动教学和科研的发展，不影响学员利用网络的积极性，又能控制学员访问一些不合适的站点或屏蔽某些不良应用程序。同时，更好地分清网络使用中的责、权、利，必须寻求一种既能实现现代网络教育又可控制学员访问范围并且少花钱的解决方法。对于院校内的教学Intranet，使用代理服务器通过校园网接入CERNET，访问Internet，可以较好地满足一系列要求。

1 代理服务器的选择

代理服务器是介于浏览器和外部服务器之间的一台服务器，代理网络用户去取得网络信息，是内部网络和外部网络之间的信息中转站。在现代教育网络中使用代理服务器，具有站点过滤、访问内容控制、安全保护、节省IP地址、提高网络传输速度、节约网络费用与内部费用管理等几方面明显的优势。

目前常用的代理服务器软件很多，有网景公司的Netscape Proxy Server、Qbic公司的Wingate、Sygate公司的Sygate、Ositis公司的WinProxy、北京新世纪遥志软件开发有限公司的CCProxy、微软公司的Microsoft Proxy Server与Microsoft ISA Server等等，这些软件基于不同的应用，在提供的功能和服务上各有侧重。对于主要用于现代教育的内部网，笔者尝试过不少代理服务器，希望找到一个能让学员使用的网络安全、快速、稳定的代理服务器。

应该说，在Windows 2000 Server环境下的现代教育网络，对其IT管理者、网络管理员和信息安全技术人员来说，充分考虑自己网络的安全、性能、管理、运营成本和服务，首选ISA Server——Internet Security and Acceleration（ISA）Server。

2 ISA 代理服务器的主要性能与优点

ISA Server提供了Internet连接方案，它不仅包括特性丰富且功能强大的防火墙，还包括用于加速Internet连接的可伸缩的Web缓存。根据组织网络的设计和需要，ISA Server的防火墙和Web缓存组件可以分开配置，也可以一起安装。利用Windows 2000安全数据库，ISA Server允许根据特定的通信类型，为Windows 2000 Server内定义的用户、计算机和组设置安全规则，具有先进的安全特性。

利用ISA Management控制台，ISA Server使防火墙和缓存管理变得很容易。ISA Management采用MMC，并且广泛使用任务板和向导，大大简化了最常见的管理程序，从而集中统一了服务器的管理，通过使用单一界面进行集中管理，可以得到更高的安全。ISA Server提供强大的基于策略的安全管理。这样，管理员就能将访问和带宽控制应用于所

设置的任何策略单元，如用户、计算机、协议、内容类型、时间表和站点。所有的管理任务可以在一台计算机上执行，而配置却可以用于所有的计算机。ISA Server是一个拥有自己的软件开发工具包和脚本示例的高扩展性平台，利用它管理员可以根据网络业务需要量身定制Internet安全解决方案。

3 ISA代理服务器在现代教育网络中的若干主要技术问题及解决方法

3.1 站点地址列表导入方式设置允许访问站点

第1步：在CERNET站点上下载免费站点地址列表，以文本文件保存在磁盘上（如取名为IP0305.txt）。对这一免费站点地址列表文件按照下载下来的格式进行添加或删除允许访问的站点地址。

第2步：开始→运行→MMC→确定→控制台→打开→C:\Program Files\Microsoft ISA Server\MSISA.msc→打开→控制台→添加与删除管理单元→添加→ActiveX控件→添加→下一步→MSISAcfg.MSISAConfig→下一步→为ActiveX控件选取一个名称（如IPaccess）→完成→关闭→确定。

第3步：在ISA的树窗格中选取“IPaccess”→创建规则集→输入规则集名称（如IP）→确定→确定→选取规则集列表中的“IP”项→导入规则→打开磁盘上保存的允许访问站点地址列表文件（IP0305.txt）。

第4步：在ISA的树格窗中单击本机名称项→Access Policy展开→右击“Site and Content Rules”→新建→Rule…→取名（如WebAccess）→下一步→Allow→Allow access based on destination→下一步→All destinations→下一步→完成。

第5步：在ISA树窗格中单击“Site and Content Rules”→双击右边内容窗格中的“WebAccess”→Destinations→在“This rule applies to”列表框中选择“Selected destination set”，在“Name”列表框中选择“IP”→应用→确定→退出ISA时单击“保存”按钮。

3.2 ISA Server下FTP的处理

FTP协议的数据传输有：主动模式和被动模式两种。这两种模式发起连接的方向相反，主动模式是从服务器端向客户发起；被动模式是客户端向服务器端发起连接。笔者在服务器端装有IAS Server与IIS，ISA Server之下FTP的处理步骤如下：

（1）由于IIS和ISA都在同一台计算机上，IIS与ISA都在侦听21号端口，为让IIS只侦听内网地址的PORT 21，在DOS下，输入如下命令：net stop msftpsvc并按回车，进入\Inetpub\adnimscripts目录，输入命令：cscript adsutil.vbs set msftpsvc/disablesocketpooling true回车，再输入命令：net start msftpsvc回车。在IIS控制台面里，Ftp→Property→FTP Site→IP Address改为内网地址。

（2）解决PORT MODE与客户端防火墙的冲突问题。采取修改注册表，打开HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Parameters\，将EnablePortAttack的值由0改为1，然后重新启动FTP服务。

（3）在ISA里，使用Server Publish的方法发布FTP服务，其中：IP address of internal server填写ISA的内部网卡的IP地址，在IP address of external server填写ISA的外部网卡的IP地址，Mapped server protocol选择FTP server。

（4）在IP Packet Filter建立一条新的RULES，Protocol→TCP，Direction→Outbound，Local Port→Dynamic，Remote Port→All。

3.3 入侵检测

ISA Server在默认情况下，包括45个警报，其中39个是启用的，每一项警报都指定1个事件和4个属性，包括警报条件、事件位置、警报阈值、警报操作。这些已经防止一些常见的攻击手段，还可以应用自定义的应用过滤器防止入侵者的攻击。例如，有人扫描10次以上端口就报警。具体操作为：IP Packet Filters→Configure Packet Filtering and Intrusion Detection→Enabled Intrusion Detection→Intrusion Detection→Port Scan→Detect after attacks on well-known ports→确定。

3.4 代理服务器某种代理服务无法使用

首先检查代理服务器是否允许提供这一代理服务，相关设置是否正确，还应检查此代理服务使用的服务端口是否已被其他服务程序使用，两个使用同一端口的服务程序都无法提供服务，应修改其中一个服务的端口号，如把WWW Proxy的服务端口由80改为8080。

3.5 代理服务器后面的用户不能浏览外部Web站点

（1）服务器在安装ISA Server之前先设置好代理服务器的TCP/IP等协议参数，并确保能与上一级服务器（校园网服务器）连通，经上一级服务器绑定，接入CERNET，访问Internet。

（2）检查代理服务器上的ISA Server是否已经运行，如果已经运行，则检查代理服务器、代理服务器之后的计算机是否都安装了TCP/IP等协议，TCP/IP协议的参数是否设置正确。

（3）检查服务器之后的计算机的IP地址是否与服务器的对内IP地址在同一子网中。如果不在同一子网中，服务器之后计算机无法向代理服务器申请Internet服务。

（4）使用Ping命令检测服务器之后的计算机与代理服务器是否连通。如果不通，应检查网线、Hub集线器、网卡及其驱动程序的设置以及IP地址的设置情况。

（5）局域网内计算机的浏览器（如Internet Explorer）的属性设置是否正确，如“连接”卡片中“局域网设置”，应选取

下转第31页 >>

上接第 36 页

“使用代理服务器”，在地址输入栏中输入代理服务器的地址，端口输入栏中输入代理服务器提供WWW Proxy的服务端口（如8080），并选取“对于本地地址不使用代理服务器”。

（6）如果代理服务器之后的计算机连接Internet总是被询问用户名和口令时，首先考虑代理服务器是否指定了用户身份验证，如果指定用户身份验证，用户必须使用正确的用户名和口令来登录，但要指出：对于现代教育网络，用户所用计算机一般是不固定的，二是同一计算机用户多，不采用登录时询问用户名和密码界面。其次，用户端计算机是否安装其他代理软件（如笔者在实验中服务器端系统安装的是Windows NT 4.0，代理服务器采用Microsoft Proxy Server 2.0，用户端计算机安装了Microsoft Proxy client，现把服务器端系统改装为Windows 2000 Server，用户端系统没有改变），如果有其他代理软件，则卸载其他代理软件，重新启动计算机。

（7）用户端计算机浏览网页时显示“The page cannot be displayed”提示信息，说明这一计算机没有访问此网址的权限，或者代理服务器的设置不正确。

Windows 2000 Server下的现代教育网络选择使用ISA 代理服务器，使网络具有高度的安全、优越的性能、方便的管理等功能。如何更有效地发挥ISA Server优势，既能为学员用户提供快速、安全、经济的Internet服务，又能为单位节省资源成本，排除ISA Server中的连接、安全和服务等方面的故障，尽可能满足现代网络教育的需要，值得现代教育网络IT管理者、网络管理员和信息安全技术人员进一步研究。

参考文献

1 郭放，校园网的设计与安全运行[J]，计算机应用研究，2001，(2)。

2 孔雷、赵锦蓉，网络安全与代理技术[J]，计算机工程与应用，2001，(14)。

3 伍卫民、吴和生、蔡圣闻、黄皓、谢立，一种安全高效的透明代理[J]，计算机应用，2002，(10)。

4 何克抗，网络应用技术新发展[J]，电化教育研究，2001，(8)。