远程访问系统在社科院应用模式的研究

范　宇

社科院 计算机网络中心

【摘要】社科院信息化建设已经十年有余，目前自建的数据库 200 多个，外购科研数据资源 100 多个。由于社科院的工作机制，全院近 4,000 员工中绝大部分是科研人员，常年不坐班，迫切需要访问院内自建和外购的数字资源。如今社会上远程访问的案例中解决的主要是报送、报批等「多对单」的应用模式。本文重点研究的是根据我院的特点，搭建适合社科院远程访问应用模式的系统平台，实现安全、高效、「多对多」的访问社科院内网及外购的信息资源，大幅提高现有资源的使用率及我院员工的工作效率。

【关键词】远程访问、SSL VPN

一、背景介绍

我院信息化建设已经走过了十年的历程，十年来我院信息化从无到有、从小到大发展非常迅速，各单位都表现了极大的工作热情，各种应用层出不穷，普遍建立了自己的内外网发布系统，大部分单位建有自己的科研数据库系统。目前我院自建和购买的数据信息资源总量达到了 30 余万亿（TB）字节。这些数据主要存储在院内的服务器中，供我院学者在院内访问和应用。为方便科研人员，近几年我院还从网上购置了 100 多个电子数据库的使用权，提供给研究人员开展学术研究使用，这些资源都放在院外开发商的服务器上，与我院 IP 地址进行绑定，因此这些资源只能在院内访问使用。鉴于我院工作性质，科研人员学术交流多、出差多、出国量大、学者不坐班，这些资源没有发挥出应有的效能，造成了极大

的浪费。

就远程访问技术本身来说，存在多种解决方案，技术上实现起来并不困难，但开放远程访问后所带来的安全和管理问题，如开放后如何保障内网安全、信息安全、数据安全等问题必须引起我们足够的重视。面对全院 51 个信息应用系统，200 余个数据库，近 4,000 人的网络用户，五花八门的系统平台，如何做到科学的、安全的开放远程访问、搭建远程访问系统中应重点注意和保证的问题是什么，本文将在这方面做了一些初步的探讨。

二、我院资源访问现状

目前我院已经实现了内网用户对网络资源的快速访问，同大多数局域网一样，为加强网络安全和信息数据安全，内网资源仅提供给在我院内部用户范围使用，这给许多在社科院外居住和生活的研究人员以及相关人员带来了不便，由于离开了院内部网络范围，以致无法访问到我院内的信息资源，以及我院购置的外网信息资源。现我院的内网信息资源访问状况如图一所示：

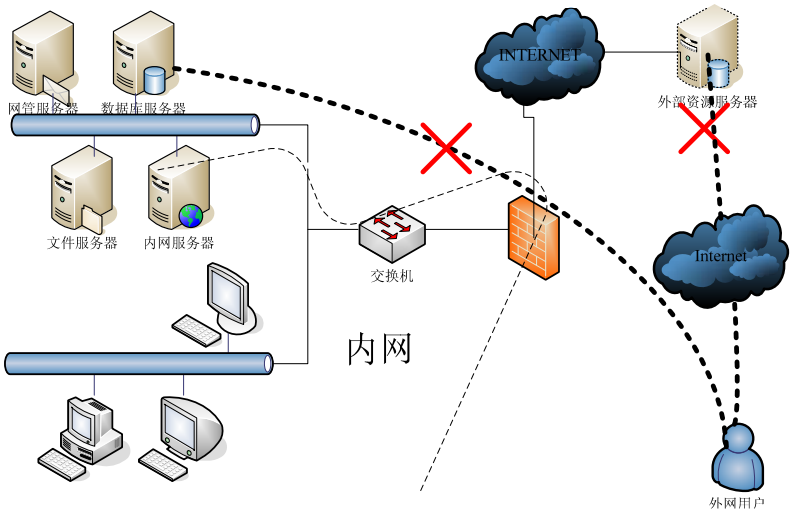

图 1-1 内网信息资源访问现状

1. 院内资源情况

为摸清我院信息系统建设的实际情况，及用户对远程访问的具体需求，有针对性的筛选出一期开放远程访问的信息系统，摸索开发经验，指导进一步的工作，我们设计了一份《统一身份认证及远程访问调查问卷》。通过采取对全院 52 个单位负责信息化建设的领导和管理人员进行面对面的问答，统一填写答卷的方式，比较准确的了解了我院信息化建设和应用的情况。据统计，我院内网上现有 51 个信息应用系统，分布在 41 个所（局）单位，具有初等规模以上的数据库总和已超过 200 个。绝大部分单位都希望能够实现远程访问，并愿意将自己的数据库全院共享。具体情况如下：

（1）调查中各单位对远程访问都表示了迫切需求。除涉及敏感信息的系统外，49 个信息应用系统表示愿意并希望实现远程访问，占现有信息应用系统总数的 96.08%。

（2）信息系统在功能方面，表现以专业研究、对外服务和提供基础数据的信息系统为主，分别占 52.94%、49.04%和 45.10%；使用者要求远程访问系统平台可以同时满足远程对各种应用系统的访问。

（3）调查了解到，51 个信息系统中，可以向全院提供服务的系统占调查总数的 70.59%；调查中我们也感觉到，我院各所（局）单位越来越注重信息化发展，愿意将更多的资源数字化，提供给全院科研人员使用。

（4）绝大多数系统都是由数据库支持的动态网页发布，B/S 结构的资源占我院应用系统总数的 80.39%；在技术实现方式上，需要在远程开放该系统应用的同时，还需要对后台数据库开放远程维护，这对我们远程访问系统提出很高的安全性要求。

（5）在对问卷整理和分析时我们发现我院信息系统开发大都是与公司合作完成，开发商涉及到的公司包括天宇、超星、TRS、ECO、SUN、东软、书同文、万方、首创互联等共 30 家公司，使用的开发平台五花八门，还有一些小公司已经很难找到了，这给我们在远程访问的安全控制上带来了很大的困难。

2. 院外购置的资源情况

除我院内部自己建设的信息系统外，我院近几年还从网上购买了大量的电子数据资源供广大研究人员参考、使用，这些资源都放在院外开发商的服务器上。由于是有偿使用，开发商通过对来访地址的限制，只对购买了使用权的单位开放。这部分数据资源对于科学研究工作有很重要的作用，同时也是我院信息化建设的一部分。目前全院共购置了 100 个外部资源数据库，这些数据库均是绑定我院 IP 地址的方式，为我院提供授权访问。目前我院无法为科研人员提供在家或院外办公时访问外购信息资源的途径，使得这部分信息资源得不到充分利用和发挥，这也是科研人员呼声最高、需求最迫切的问题，也是需要尽快实现我院远程访问的主要原因之一。

3. 与其他单位的不同

通过对已使用远程访问的单位的走访让我们认识到我院与其他单位在使用上有着很大的区别，比如中邮公司和泰康人寿保险，两家单位在远程访问的使用上主要用于分支机构或子系统与总部的资料交换，接入的基本为固定的计算机，在管理上非常的方便；新华社、人民网等单位，虽然接入站点远至海外，但一般都通过国际专线传输信息，无论从速度上还是安全上都有较高的保障，而且这两个单位远程访问系统的主要用途还是文字、图片等资源的上传，应用情况较我院简单；在管理机制上，公司和企业单位都是直线式管理，使用的计算机都是统一购置，因此可以很容易的控制计算机上安装软件的种类，这些在我院的体制下是很难做到的。

相比之下，我院的情况就有了很大的不同，

首先，我院目前注册人数已近 4,000 多人，远程访问并发数至少应满足 1,000 人同时在线，加之日常约 2,000 在线人数，开放后网络带宽将受到严重挑战。另外用户的应用多为浏览、检索、上传下载及系统维护，与公司的报表、收发内部邮件等应用方式有很大差异。

其次，我院的信息系统和其他单位有着很大的差异。我院的信息系统主要是发布系统，内容以研究成果为主，由于我院地位特殊，学者的研究成果及发表的论文都有很大的影响力，很容易成为社会关注的焦点。因此，如果开放远程访问，

就需要对服务器本身的安全防范措施提出有很高的要求。

第三，信息系统的开发商涉及 30 多个单位，采用的模式五花八门，标准不统一，需要开放的端口也是多种多样，这对安全策略的统一规划造成很大的不便。

第四，内网服务器分布在全院多个网段，如果每个系统都开通远程访问，基本可以说是将内网全部列入到被访问的范围当中。如果一台服务器被黑，那么全部内网内容就暴露在黑客的眼中。

第五，在管理方式上，由于我院需要开放的资源多为论文、研究成果等，有的科研人员对数据的保护意识不强，会出现将远程访问的账户和密码与院外人员共享，或者用户名密码过于简单，被黑客攻破。这又给如何设置访问人员的权限带来很大的困难。

第六，院外使用远程访问的计算机本身的安全问题。在院内，网络中心部署了统一的病毒库及系统补丁升级服务器，接入院网的计算机可以方便、快速的进行升级。而在院外，个人用机的安全性无法得到保证，我院用户多为文科研究人员，计算机应用水平不高，将带有病毒或木马的机器连入院内网的可能性很高。虽然安装客户端软件可以起到一定的作用，但程序的安装及繁琐的配置务必会加大远程接入用户的负担，影响资源的使用效率，并造成各种各样的问题。而且管理人员的维护量和成本会倍增。

第七，用户自运营商网络访问其他网络运营商网络内电子资源速度慢的问题。

由于多数远程访问者使用的是当地运营商提供的网络（如电信、网通、铁通等），这些运营商网络之间的访问速度非常慢，导致远程用户通过这些网络访问电子资源的速度很慢，极大的影响了用户使用的满意度。

第八，大量用户访问问题

由于图书馆的资源多数都是购买授权的方式，上游的电子资源服务商对资源的应用是有限制的。除了限制发起的 IP 地址外，还会限制单一 IP 地址所产生的流量。

三、技术实现

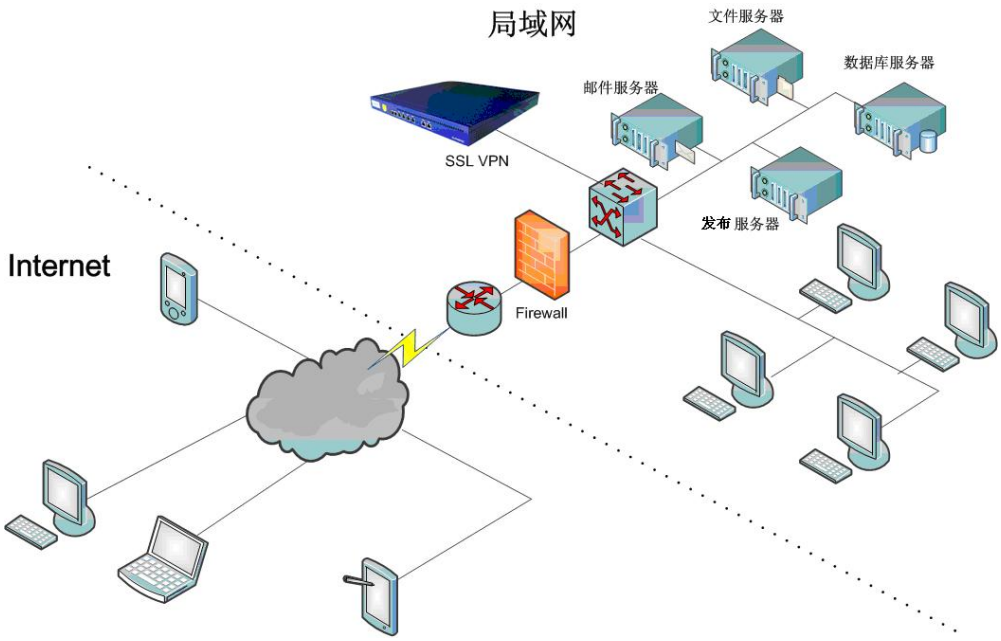

图 3-1 远程访问部署方式

在院网络整体配置上，院 Internet 出口防火墙上需开放至 VPN 网关的 80（可选）、443 端口。远程访问的客户端不需要安装任何程序，只要在浏览器地址栏中输入 SSL VPN 网关对应的公网 IP 地址或域名，通过身份认证即可实现远程访问内网资源或外购资源。远程访问系统将与我院统一身份认证平台相结合，使用一套用户名密码，通过整合个人私密信息，防止用户在主观上泄露登录名及密码；同时配合使用硬件 KEY 的双重方式，进一步提高用户的真实性，从而有效地保护内部信息资源。

针对我院远程访问系统的各项需求，提供一个更为安全、快速、稳定的 VPN 网络，在具体实施搭建该系统的过程中，应考虑以下几个关键点：

1. 无缝部署，良好的网络兼容性

针对目前我院局域网络建设相对完善的这个特点，在搭建远程访问系统的同时，必须要保证现有网络的正常使用。解决方案必须支持支持路由模式，透明模式，单臂模式部署，无缝支持我院现有网络，对现有网络的内部结构，接口类型，服务器，操作系统无任何特殊要求。且用户使用 SSL 协议和标准的浏览器可以

方便的通过任何网络接入 VPN 网络，避免网络兼容性的麻烦。

2. 用户的访问控制

目前我院内网共有 51 个信息系统，其中大多数系统的使用范围已覆盖到全院，例如人事系统、邮件系统、内网网站系统等，开放远程访问后将实现浏览、上传下载或维护等不同权限的操作。鉴于这种情况，我院的远程访问系统应能满足识别同一个用户在不同系统中权限划分的需求，通过 SSL VPN 技术的控制粒度，根据组织的构架，对用户进行多身份管理，并通过 SSL VPN 行为跟踪引擎对每个远程接入用户的所有访问记录都留下了日志记录，为系统审计提供详实的数据来源。

3. 与第三方兼容的统一认证

SSL VPN 网关必须支持第三方 LDAP/AD、Radius、SecurID、USB KEY、短信密码确认等多种安全认证方式，可以根据相应的安全级别，对客户端组合几种认证方式，最大限度地保证接入用户的合法性。

SSL VPN 网关应能够从微软域服务器或 LDAP 服务器中直接导入用户数据，能和第三方的 LDAP 认证服务器或 RADIUS 认证服务器有效集成。可以和统一身份认证体系相融合，简化部署过程，避免多套认证体系带来更多的维护成本和更多安全风险。

4. 更严格的登录安全

要求在用户通过计算机浏览器打开 SSL 登录界面时，SSL VPN 安全网关通过客户端计算机安全扫描功能，检查计算机系统是否打了补丁、是否安装有相应杀毒程序等，保证 SSL VPN 接入安全，避免客户端计算机的不安全因素通过 SSL VPN 传输到院内部网络，产生安全隐患。

SSL VPN 网关应同时具备防密码暴力猜解功能，这个功能能够防止非法用户采用恶意的手段来进行密码猜测，一旦系统启用防密码暴力功能以后，用户连续输入密码错误次数达到一定的数量以后，系统应将该帐号锁定一段时间，防止密码被暴力猜解。

5. 更严格的注销安全

零痕迹访问功能能够避免安全漏洞，SSL VPN 在用户结束访问退出 SSL VPN 以后，系统平台端应能够自动注销用户及其权限，用户端自动清除 Cookie、临时文件等遗留在客户端计算机上的信息，实现「零痕迹」访问，避免安全隐患。

6. 丰富的日志及统计功能

SSL VPN 网关应能够提供调试、信息、告警、错误四个级别的运行日志，方便的协助管理员进行系统分析，并应能提供用户访问记录、审计和报表，记录、跟踪用户行为。

SSL VPN 系统应能支持第三方日志服务器，对审计日志进行定期导出，在日志系统中可对所有远程用户的登录行为做全面的分析和统计。管理员可按照饼图、柱状图、曲线图等多种显示方式对服务的被访问次数、被拒绝次数，用户的登录次数、告警次数等进行直观显示，并可直接打印和导出。

7. 支持双机热备

SSL VPN 网关应支持双机热备方式进行备份。两台 VPN 网关应能实现实时的信息同步，若主设备配置发生变化（如新增或删除用户等情况反正，）主设备会通知备份设备，备份设备则同步更新相应的配置信息。当主设备发生故障时，备份设备应在短时间内，切换为主设备状态，整个过程自动完成无需人工干预，并及时显示、通知管理人员。

8. 对外购资源的代理访问

除我院内部自己建设的信息系统外，我院现购置了 100 个外部资源数据库，受 IP 地址绑定的限制，只能在院内使用。远程访问系统应能提供对这类资源的高效、安全访问。

9. 多链路优化技术

针对我院学者众多，远程访问用户上网地域随机性很强的问题，SSL VPN 网关需要支持多出口链路速度优化功能。通过建设多链路提供商的出口链路，SSL

VPN 网关可以在用户接入时，通知客户端可选接入链路出口 IP 地址，并通过客户端的 ACTIVE X 控件根据访问速度、延时、和链路负载情况综合判断出最优接入链路，并自动跳转到最优链路上实现具体应用访问。

四、远程访问系统的展望

根据科研和管理人员的使用要求，考虑到我院科研和管理的特点以及信息应用的实际情况，远程访问系统的搭建将为我院科研人员提供了极大的便利，也是实现我院「方便、安全、平稳、快捷」的建网方针不可或缺的工作之一。随着远程访问系统与院内各应用平台的逐步结合，允许访问的范围将逐步扩大，届时，不仅院内外的电子资源得到了充分的利用，更重要的是为科研人员打造方便、快捷的网络环境，使社科院信息化建设迈上新的台阶。但同时必须认真对待随之带来的安全问题。在实现远程访问的同时，必须不断提高使用人员的安全意识；加强安全保证体系的建设；完善安全管理机制、体制；避免信息失控和敏感资源外泄，保证远程访问系统的安全、院内数字资源的安全、科研人员的使用安全。

【作者简介】

范宇　男

职　　称：社科院 计算机网络中心「项目规划与管理处」工程师

研究领域：网络设计与规划

个人简介：2002 年毕业于北京市联合大学应用文理学院，获管理学学士学位，现任社科院计算机网络中心工程师。近年发表的文章为《网络管理—我院信息化重要保证》，近期正在参与《网络配置与管理 1000 问》一书的编撰工作，并具体负责其中 VPN 部分的编写；正在参与的项目—搭建社科院远程访问系统。

联络电话：86-010-85196463

联络邮箱：fanyu@cass.org.cn