·经验交流·

医院区域医疗接口的网络安全设计与实现

李秋甸，李初民，李　军
（第三军医大学新桥医院信息科，重庆 400037）

摘　要：目的　构筑安全的区域医疗网络接口体系。**方法**　基于网闸的物理隔离技术确保区域医疗网络的高效安全运行。**结果**　多个独立没有任何信息交换的网络，通过隔离网闸互联实现了必要的互联互通，同时也保证了安全系数、避免信息外泄和网络病毒侵扰。**结论**　通过与医院 HIS 系统的整合，区域医疗协同体系已成为现代数字化医院一个重要组成部分。

关键词：用户计算机接口；局部网络；计算机安全；软件设计；网闸
doi：10.3969/j.issn.1671-8348.2011.35.019　　**文献标识码：**B　　**文章编号：**1671-8348(2011)35-3576-02

区域医疗协同系统的建立，与医院信息系统之间必然发生大量的数据交换。出于安全等因素，医院内网的数据库服务器不能直接暴露在因特网上。如何保障医院内网的数据安全，同时又能高效的与外网进行数据交换，基于物理隔离的网闸系统很好的解决了这一问题[1]。

1　区域医疗功能简述

区域医疗又称为区域医疗协同，分为远程会诊、远程预约挂号、远程代理检验、远程查询、远程医疗咨询等，可为百姓就医大大提供方便，从而缓解“看病难”的问题；连同诊疗记录一起网上传递的“上传下送”不仅可以使“医疗资源合理利用”，还能使医疗的连续性得到有效保证，同时又能减少不必要的重复检查检验；将音视频系统与这种医疗协同网络相结合，不仅可以进行远程会诊、远程阅片，还可以进行疑难问题讨论和远程培训，大面积提高基层医师水平，完全可以不做任何额外投资，就能非常经济、方便地解决由于基层医疗水平低而导致大医院拥挤、小医院冷清的矛盾。

2　基于网闸的网络安全设计

传统的互联网安全策略主要有两种，利用网络安全设备构建的安全体系和冷备份定期同步的数据复制模式[2]。采用传统网络安全设备构建理论上能满足单一应用的安全要求，但是在面对多种服务、多种业务提供商的时候，由于业务提供商的安全性并不统一，不能保证每个业务提供商都 100％安全。假设有一个或多个业务提供商被攻破，则整个系统就会处于安全风险之下；采用冷备份定期同步的方式，业务的实时性基本无法保证，只适合做一些信息发布之类的实时性要求不高的业务。

2.1　网闸简介　隔离网闸系统由两套独立工作的计算机系统和一套反射物理隔离（GAP）系统组成，两套计算机系统分别是连接不可信网络的不可信网络端计算机和连接可信网络的可信网络端计算机，两套计算机系统通过反射 GAP 系统相连，处理两个网络交换数据事务。隔离网闸成功地实现了既保证可信网络与不可信网络的物理隔断，又保证两个网络间的数据实时访问，能防止针对网络层和 OS 层的已知的和未知的攻击。为保证可信网络与不可信网络的物理隔断，网闸中包含了精心设计的硬件 ASIC 隔离部件动作系统，使得连接可信网络端和不可信网络端的两组高速 ASIC 隔离部件配合系统数据流分时地“接通”、“断开”。网闸的内部反射 GAP 系统完全基于硬件体系，目的是将不可信网络端计算机存储系统和可信网络端计算机存储系统中的数据进行快速交换。反射 GAP 系统不依赖于任何通信协议和操作系统服务，它具有独立的硬件逻辑电路，通过独立的总线交换数据，实现了网络间数据的高速交换。当网络数据流经网闸时，数据在网闸设备计算机系统上被处理，经过协议终止、协议检查并剥离数据包装，然后剥离出的裸数据被反射 GAP 系统传送到另一方，并重新生成协议后送达目的地。彻底杜绝黑客利用协议对可信网络进行攻击[3]。

2.2　区域医疗系统的网络安全设计　本院选择网闸这种网络安全硬件配合软件系统的中转机制，实现本院区域医疗信息化互联网服务。数据业务逻辑拓扑图，见图 1。

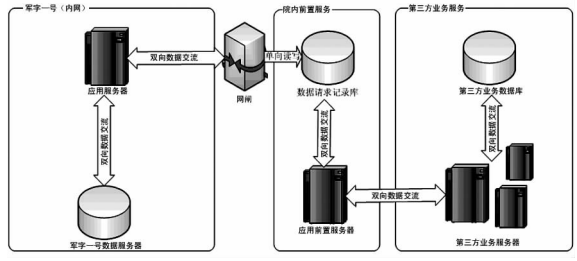

图 1　数据业务流程逻辑拓扑图

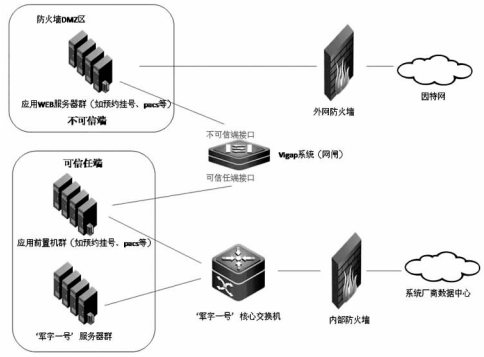

图 2　区域医疗系统接口物理拓扑图

典型应用下，数据请求记录库复制了军字一号数据库的数据结构中与业务相关的表结构，并不复制数据，同时建立一张或者多张业务请求表。当有业务请求发生时，将业务请求写入请求表。军字一号内的应用服务器定时轮询请求表，按照约定的请求格式，将请求的数据结果返回。在约定的格式中限制数据库请求表的范围、字段和数据长度，类似于数据库用户权限管理的功能。网闸限制只能由军字一号应用服务器到数据请

求记录库的通信可以通过，反向的通信都被阻止。应用前置服务器发起业务后，发起的线程将会一直轮询该条请求的结果或者到超时。除了前置服务器需要与各个系统厂家定制业务逻辑以外，对于第三方业务方来讲，这段过程是不可见的，而所见的业务是透明的。简单来说对于任何业务除了需要稍微等待两个内部的应用服务器各自的处理时间以外，与直接连接军字一号数据库的效果可以说是一样的[4-8]。本院区域医疗系统的物理拓扑图，见图 2。

如远程预约系统，患者利用一卡通号向预约 WEB 服务器发送一个挂号请求，当预约挂号前置机通过网闸的单向摆渡轮询到这个请求后，就将相对应的表发送给军字一号服务器以及一卡通数据中心，最后再通过网闸的 sqlserver 应用通道单向摆渡把数据返还给预约 WEB 服务器。又如远程阅片系统，患者利用一卡通号向 pacsWEB 服务器发送一个阅片和查看阅片报告的请求，当 PACS 应用前置服务器轮询到请求后，就将相对应的阅片报告请求发送给军字一号的 PACS 服务器，最后再把此一卡通号所对应的放射图像和报告通过网闸的 sqlserver 和 http 应用通道返还给 pacsWEB 服务器。其他系统的调用过程都比较类似，就不一一说明了。

从网络安全角度考虑，网闸不可信端的任何服务器、数据库主机被攻破，都不会影响到内网可信任端的任何主机。从网络安全角度可以认为是物理断开了内网和外网的联系[9-10]。各个系统的网闸配置大同小异，需注意的是只能配置一条由内向外的应用通道，工作模式为转发模式。而外网防火墙内安全区的各个应用前置服务器则只需开放所需的业务端口即可。

3 结　语

基于网闸的区域医疗系统，不仅确保了医院内网的信息系统的安全，还能够高效的实现医院内网和因特网间的数据交互，为患者提供了方便。

参考文献：

[1] 王洪强，詹永丰，张蔚，等. 基于网闸实现物理隔离的网上预约挂号系统[J]. 中国数字医学，2010(11)：71-72.

[2] 黄昊，曾凡，王琳华. 开放环境下的医院信息系统安全[J]. 重庆医学，2009，38(11)：12-13.

[3] 王珺，李立新，李福林. 物理隔离和网闸的技术原理浅析[J]. 微计算机信息，2007(24)：53-55.

[4] 何萍，程力立，于广军. 论区域医疗信息化中的网络安全建设[J]. 中国数字医学，2010(1)：65-67.

[5] 丁烽祥，张怡，王勇军. 多网安全隔离交换系统的设计与实现[J]. 厦门大学学报：自然科学版，2007，46(S2)：92-97.

[6] 王相林，江宜为. IDS 与防火墙联动的网络安全模型设计[J]. 科技通报，2011，27(2)：233-237.

[7] 孙松儿. 广域网安全建设的思路和部署[J]. IP 领航，2010(12)：23-28.

[8] 赵季平，郭华源，张震江，等. 区域协同医疗与远程医学助力全民健康[J]. 中国数字医学，2010(11)：58-60.

[9] 张富奎. 互联网与内网接入安全技术研究[J]. 信息网络安全，2011(1)：42-45.

[10] 吴璐，杨健. 基于 Oracle Dataguard 和网闸的内外网数据交换平台[J]. 计算机应用于软件，2010，27(12)：186-187.

（收稿日期：2011-08-09　修回日期：2011-09-20）

·经验交流·

医院会诊管理系统的设计与实现*

黄　荣[1]，李刚荣[1]，周　琳[1]，魏雯雯[1]，李景波[2△]

（重庆第三军医大学西南医院：1. 信息科；2. 医院办公室，重庆 400038）

摘　要：目的　探讨提高会诊质量、会诊效率，优化会诊流程，更好地对院内会诊进行有效的监督。**方法**　利用医院信息系统(HIS)数字化平台以及 PB+ORACLE 数据库进行软件开发，与军字一号完美融合。**结果**　加强了会诊的管理，提高了会诊质量、会诊效率。**结论**　会诊管理系统在医院对会诊的管理、辅助会诊等方面都有重要意义。

关键词：医院信息系统；转诊和会诊；软件设计

doi：10.3969/j.issn.1671-8348.2011.35.020　　**文献标识码：**B　　**文章编号：**1671-8348(2011)35-3577-02

院内会诊是综合性医院在涉及多学科疑难、危重患者诊治过程中采用的常见措施。长期以来，院内会诊工作一直是医疗工作的重要环节，会诊质量的高低是衡量医院医疗质量的重要指标，做好院内会诊工作是保障医疗质量的重要手段，会诊管理一直被作为评价医院管理水平的重要指标[1-2]。为了提高会诊质量、会诊效率，优化会诊流程，更好的对院内会诊进行有效的监督，本院在实际会诊流程的基础上进行优化，自主研发了基于“军字一号”的会诊管理系统。

1 会诊流程存在的问题

以前本院的会诊模式同大多数医院一样采用手工方式完成。申请科室填写会诊申请单，送往应邀科室[3-4]，或者电话通知应邀科室，再手工填写申请单，应邀科室前往会诊，会诊完成后填写会诊记录，这种传统方式存在诸多弊端。

1.1 会诊通知不到位　传统手工传递申请单的方式，都是由申请科室把会诊申请单送往应邀科室护士站，再由护士通知科室住院总或者相应医生会诊，整个过程都没有责任人，这样容

* **基金项目：**广义数字化医院示范工程资助项目(CSTC 2008AA5006)。
△ **通讯作者**，Tel：(023)68754001；E-mail：Lijb003@163.com。