

· 论 著 ·

医院医保网络平台架构探讨与分析

蒋晋鹏, 唐鸿建, 曹美琴, 储颖, 孙启亮, 王祥号

[摘要] 目的 利用医院现有网络设备,在不改变现有网络架构的前提下实现医院同医保中心、省农合数据中心、地方合管办、外省农合数据中心以及合管办相连,来满足更多患者跨市乃至跨省就诊的需求。**方法** 某院采用访问控制列表(access control lists, ACL)和端口映射(network address port translation, NAPT)技术,在防火墙上将医院部分需要访问新农合数据中心、医保中心的设备 IP 地址以及对应的出端口进行映射,转换为可以访问新农合数据中心、医保中心的合法 IP 地址,在网闸(GAP)上采用访问控制与身份认证技术。**结果** 实现医院同新农合数据中心、医保中心相连。**结论** 网络技术与硬件设备相结合,保证网络的畅通,增强医院内部网络数据的安全性,同时还节约了公网 IP 地址。

[关键词] 信息化;访问控制列表;端口映射;网闸

[中图分类号] R197.324 **[文献标志码]** A doi:10.3969/j.issn.1672-271X.2016.01.020

The discussion and analysis on the network platform architecture of the hospital medical insurance

JIANG Jin-peng, TANG Hong-jian, CAO Mei-qin, CHU Ying, SUN Qi-liang, WANG Xiang-hao. IT Department, 81 Hospital of PLA, Nanjing, Jiangsu 210002, China

[Abstract] **Objective** To utilize the network equipment in the hospital without changing existing network architecture. To realize the association between hospital and the medical insurance center, data center of provincial rural cooperation medical care, rural cooperation medical management office, the data center of other provincial rural cooperation medical care, cooperation medical management office, satisfying more patients in new rural cooperative medical care to treatment cross the city even the province. **Methods** Our hospital adopted the ACL(access control lists) and NAPT(network address port translation) technology to translate the IP address of equipment and the corresponding port on the firewall which hospital needs to access the data center of NCMS, and translated to the legal IP address which can access to the data center of NCMS and medical insurance center, employed the control and identity authentication technology on the network gateway (GAP). **Results** The connection with the data center was realized. **Conclusion** Combining the network technology with hardware devices ensures smooth network, enhances the safety of the hospital network data and saves the IP address of public network.

[Key words] informatization; ACL(access control lists); NAPT(network address port translation); GAP

随着当前医疗卫生体制的深化改革,建立健全覆盖城乡居民的基本医疗卫生制度成为医疗体制改革的总体目标。新型农村合作医疗制度(以下简称新农合),已经成为我国基本医疗保障体系的重要组成部分,该制度减轻了农民因患重大疾病而带来的经济负担,减少了农村居民因病致贫和因病返贫现象^[1]。我院是省市医保定点医疗机构,也是江苏省、安徽省新农合即时结算补偿报销定点医院,已与两省多个市、区、县签订了即时结算补偿报销协议以及大病种协议,并在不断总结经验的基础上,逐渐扩展即时结报范围。在运行过程中,如何确保信息安全、网络安全、数据安全,如何稳定可靠

地实现医院 HIS 系统与医保平台的数据交换,是亟待解决的首要问题。经过多年的探索和实践,我院省市医保、新农合工作已逐步完善,安全机制渐行提高,为前来就医的广大患者提供优质的医疗服务和信息安全保障。

1 网络概况

我院目前网络架构主要是由信息终端、接入层、核心层以及数据中心四个主要部分组成。接入层是百兆、千兆自适应交换机,与核心层之间采用的是双上行链路光纤接入,千兆带宽,提高数据传输效率,实现链路冗余与备份。核心层是由两台高端交换机组成,提供应用和服务连续性统一在一起的融合网络环境,减少关键业务数据和服务的中断;集成高性能的网络安全和网络管理,提供接入保护和入侵检测保护;通过万兆光纤连接采用 VSS 架构,实现两台主交换机之间的数据负载均衡,

作者单位: 210002 江苏南京,解放军 81 医院信息科

通讯作者: 唐鸿建, E-mail: njthj_81@sina.com

引用格式: 蒋晋鹏,唐鸿建,曹美琴,等.医院医保网络平台架构探讨与分析[J].东南国防医药,2016,18(1):65-67.

同时还实现了网络中心的设备融灾备份、带宽倍增。核心层与数据中心之间是通过核心交换机连接且也是双上行链路光纤接入,万兆带宽,采用链路聚合技术提高数据传输效率。网关与网闸的接入加强内网的安全接入与认证功能^[2]。我院外来网络接入,如省医保、市医保、江苏农合、安徽农合、银医一卡通等,均是采用专线接入。当对方服务器上程序需要访问我院 HIS 系统或者有外来数据进去我院内网时,需要经过防火墙上访问控制列表(access control lists, ACL)控制列表的筛选、网关与网闸的安全认证,通过才可以访问,否则拒绝。医院内网、因特网之间是完全物理隔离的,提高医院内网数据信息的安全级别。具体网络架构见图 1。

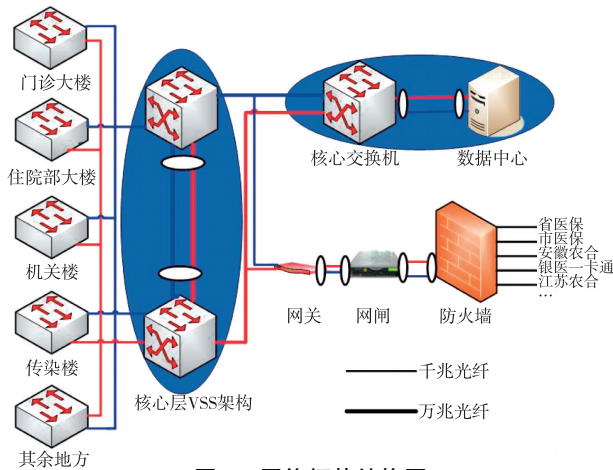


图 1 网络拓扑结构图

2 端口映射

2.1 NAT 地址转换 随着网络技术的发展以及电脑的普及,现有公网的 IP 地址无法满足全球现有用户的使用,为了解决 ipv4 地址短缺的问题,internet 工程工作小组 IETF 提出了网络地址转换(network address translation, NAT)解决方案。IP 地址分为公有地址和私有地址。公有地址统一分配,用于 internet 通讯;私有地址可以自由分配。私有地址包括 A 类:10.0.0.0-10.255.255.255; B 类:172.16.0.0-172.31.255.255; C 类:192.168.0.0-192.168.255.255^[3]。NAT 技术的主要作用是将私有地址转换成公有地址,使私有网络中的主机可以通过共享少量公有 IP 地址访问 internet。

2.2 NAT 转换方式 地址转换目前存在两种方式。第一种是基本 NAT 或者静态 NAT,技术上简单,仅支持地址一对一的转换,不支持端口映射,这就需要对当前应用的每一个私有 IP 地址都对应一个公网 IP 地址。第二种是常用的简记为 NAT 的网络地

址转换,也称 NATP(network address port translation)端口映射^[4],这种方式支持并允许多个私有 IP 地址共享一个公网 IP 地址,把内网中所有可以访问外部网络的私有 IP 地址伪装成一个公网 IP 地址去访问外部网络,且外部无法发现内部私有 IP 地址以及内网架构,在一定程度上提高内网的安全级别。

2.3 NAT 端口映射 NAT 即网络端口与地址同时转换,是常用的一种转换方式,将多个内部地址映射为一个合法公网地址,但以不同的协议端口号与不同的内部地址相对应,也就是内部地址、内部端口同外部地址、外部端口之间的转换。当位于内部网络中的主机通过路由器或者交换机向外部服务器发起会话请求时,路由器或者交换机就会查询 NAT 表,看是否有相关会话记录,如果有相关记录,就会将内部 IP 地址及端口同时进行转换,再转发出去;如果没有相关记录,进行 IP 地址和端口转换的同时,还会在 NAT 表中增加一条该会话的记录。外部主机接收到数据包后,用接受到的合法公网地址及端口作为目的 IP 地址及目的端口来响应, NAT 设备接收到外部回来的数据包,再根据 NAT 表中的记录把目的地址及端口转换成对应的内部 IP 地址及端口,转发给该内部主机^[5]。NAPT 常用于接入设备中,它可以将中小型的网络架构隐藏在一个合法的 IP 地址后面。NAPT 也被称为“多对一”或“多对多”的 NAT,或者叫 PAT(port address translations, 端口地址转换或者端口映射)。

3 网络配置

3.1 内网 IP 划分概况 我院约有 1000 个信息点位,通过 VLAN 划分,分为不同的网段:192.168.100.0-192.168.114.0,彼此之间可以互相访问。假设省医保的服务器地址:20.1.1.2,市医保服务器地址:30.1.1.2,江苏新农合服务器地址:40.1.1.2,安徽农合服务器地址:50.1.1.2,银医一卡通服务器地址:60.1.1.2。当省医保、市医保、安徽农合、江苏农合等多条专线接入时,考虑到医院网络安全问题,我院内部只允许网段为 192.168.100.0 段地址可以访问这些不同专线上的不同网段的服务器且对方不可以访问我院内部服务器。为了解决这个问题,我院防火墙上采用了 ACL 策略与端口映射技术 NAPT。

3.2 配置 ACL 与 NAPT

3.2.1 配置 ACL ACL 是应用在路由器或者交换机接口的指令列表^[6]。这些指令列表用来告诉路由器或者交换机哪些数据包可以收、哪些数据包需要拒绝。至于数据包是被接收还是拒绝,可以由通

过特定的源地址、目的地址、端口号或者是某一段的源地址、目的地址等特定指示条件来决定,在出端口或入端口引用该策略,当所有数据包到达端口时会与该端口引用的 ACL 策略进行匹配,自动筛选允许通过或者丢弃的数据包。访问控制列表不但可以起到控制网络流量、流向的作用,而且在很大程度上起到保护网络设备、服务器安全的关键作用。

配置如下:

```
F_W (config)# access-list 1 deny 0.0.0.0 255.255.255.255; //建立访问控制列表,拒绝所有外来地址的访问;
```

```
F_W (config)# interface range GigabitEthernet 0/0 - 0/7; //进入防火墙的入端口 0/0 到 0/7;
```

```
F_W (config-if)# ip access-group 1 in; //用于对入防火墙数据包的控制在防火墙的入端口 0/0 到 0/7 激活控制列表。
```

3.2.2 配置市医保 省医保、市医保、江苏农合、安徽农合、银医一卡通,均是专线接入。当我院分别访问这些不同的服务器时,均需要地址转换方可实现。彼此配置方法类似,此处以市医保地址转换为例,配置如下:

```
F_W (config)# interface GigabitEthernet0/1; //进入配置端口
```

```
F_W (config-if)# nameif outside_shiyibao; //端口命名
```

```
F_W (config-if)# ip address 30.1.1.3 255.255.255.128; //配置出口物理端口地址
```

```
F_W (config-if)# object network shiyibao; //进入该端口的端口映射配置模式
```

```
F_W (config-if)# subnet 192.168.100.0 255.255.255.0; //标示内网源地址段地址
```

```
F_W (config-if)# nat (inside,outside_shiyibao) static 30.1.1.2; //映射为出口访问地址
```

```
F_W (config) ip route outside_shiyibao 30.1.1.0 255.255.0.0; //出口访问静态路由,去往市医保的全部经由映射地址出口
```

4 运行状况

配置完成后,试运行效果良好,未出现网络延迟、数据丢失现象。即使当有大量数据需要上传至医保中心、江苏省平台或安徽省平台时也未出现数据丢失现象,未出现外来不明地址访问我院服务器现象。

NAPT 技术的采用,既可以解决 IP 地址不足的问题,又可以优化网络设计隐藏我院内部网络架构,同时又通过 ACL 访问控制列表对一些不明地址

的访问进行控制来进一步提高网络的安全性,使网络的配置既灵活又能节约经济成本;再加上网闸、网关、防火墙的使用,对可以访问我院服务器的对端服务器上的程序以及 IP 地址进一步筛选,阻止非法程序访问。

5 结论

NAPT 使得一系列网络设备可以通过不同的端口号来共享唯一的外部地址,使得所有不同的数据转发过程中源地址为同一个 IP 地址。NAPT 的主要优势在于,能够使用一个有效的 IP 地址获得通用性,而且有效的隐藏了内部网络设备 IP 地址和整个网络的拓扑架构,保证内部网络结构与数据的安全性,节约公网 IP 地址。

6 体会

通过对医院医保网络平台搭建与调试,深刻体会到医院信息化的建设与完善、信息安全等级保护加强是越发的重要。医院信息系统安全直接影响到医院医疗工作的是否能够正常运行,网络瘫痪或者数据丢失,都将会给医院和病人带来巨大的灾难和难以弥补的损失以及名誉上的损失^[7]。我院随着云计算技术、云安全技术以及高端网络设备的引入,显著提高我院医疗机构信息化建设和管理维护水平,为我院医疗工作提供重要保证;此外,在安全方面为我院数据库安全、网络安全、应用安全、防止恶意攻击等提供强有力的保障^[8-9]。

【参考文献】

- [1] 王秋月.新农合即报系统的研制与开发[J].中国数字医学,2014,9(1):109-111.
- [2] 王大勇,李杰.军队网络医疗建设的现状和体会[J].东南国防医药,2012,14(4):385-386.
- [3] 刘立辉,钱海江.医院连接新农合网络专线的配置分析[J].医疗卫生装备,2011,32(11):60-62.
- [4] 唐云,罗俊松.IP地址管理及子网划分[J].制造业自动化,2011,33(2):37-38.
- [5] 孙中廷.NAT技术解决IP地址短缺问题的实现[J].办公自动化杂志,2013(14):42-44.
- [6] 张波,万丽.基于端口映射NAT网络方案分析与实施[J].软件工程师,2015,18(3):12-13.
- [7] 张稳,袁波.加强军队医院信息安全管理实践与体会[J].东南国防医药,2013,15(2):200-201.
- [8] 高芳.医院网络安全与管理[J].信息安全与技术,2012,3(3):29-30.
- [9] 陈伟,王强,袁天祥.医疗云计算技术与信息安全等级保护[J].中国数字医学,2014,9(8):26-28.

(收稿日期:2015-08-21;修回日期:2015-12-15)

(本文编辑:徐燕茹;英文编辑:王建东)