# \*\*医院

# 网络设计方案

# 概述

## 建设背景

随着\*\*医院的业务量增长和业务的高速发展，对IT系统的依赖程度越来越高，医院信息系统面临的网络安全威胁越来越严重。对于二级综合医院，信息系统的业务连续性要求很高：从政策法规层面讲，需要满足《网络安全法》和《等保2.0》 的相关要求。对医院业务本身来说，由于医院业务的特殊性，任何人为或自然因素所导致的应用或系统中断，都会造成医院巨大的经济和名誉损失及严重的法律后果。

\*\*医院信息化建设工作经过多年的发展，信息技术已得到了广泛的应用，主要业务系统如HIS, PACS, LIS, RIS, EMR等都己实现了信息化，一个综合性多功能的医疗信息化服务体系已形成。

随着\*\*医院业务的发展，如何确保医院院区信息系统安全和业务持续运行已成为一项重要而艰巨的任务。网络系统改造是为了适应新形势下“互联网+医疗”的国家战略;同时，也是医院发展互联网医疗的基础，是一项具有战略意义的举措。

为了达到上述目标，\*\*医院对整个医院的硬件支撑平台进行统一梳理和总体信息系统安全方案设计，以保证基础硬件系统的各个组成部分能够高效协同，对业务与应用提供强有力支撑；同时还需要确保总体方案可以落地实施。

## 1.2、**设计依据**

本方案主要依据以下法律、法规进行设计:

**《中华人民共和国网络安全法》**

**《二级综合医院评审标准实施细则》**

**《信息技术网络安全等级保护安全设计技术要求》(简称“等保2.0”)**

# 总体设计

## **2.1、设计**原则**与思路**

**先进性**：世界上计算机技术的发展十分迅速，更新换代周期越来越短。所以，选购设备要充分注意先进性，选择硬件要预测到未来发展方向，选择软件要考虑开放性，工具性和软件集成优势。网络设计要考虑通信发展要求。

**可靠性**：系统能长时间稳定可靠地运行，并保证系统安全，防止非法用户的非法访问。系统不能出现故障，或者说即使有设备出现故障，对网络和网上的数据不构成大的威胁，要有设备对数据作备份。

**实用性**：系统的设计既要在相当长的时间内保证其先进性，还应本着实用的原则，在实用的基础上追求先进性，使系统便于联网，实现信息资源共享。易于维护管理，具有广泛兼容性。

**安全性**：医院网络与外部网络互连互通日益增加，都直接或间接与国际互连网连接。医院的机密文件，病患资料等敏感信息关系到人民的利益。因此，在系统方案设计需考虑到系统的可靠性、信息安全性和保密性的要求。

**可扩充性**：系统规模及档次要易于扩展，可以方便地进行设备扩充和适应工程的变化，以及灵活进行软件版本的更新和升级。为将来系统的升级、扩展打下良好的基础。

## 2.2、设计目标

根据使用人群划分出不同的区域：

运维管理区

医务工作者办公区

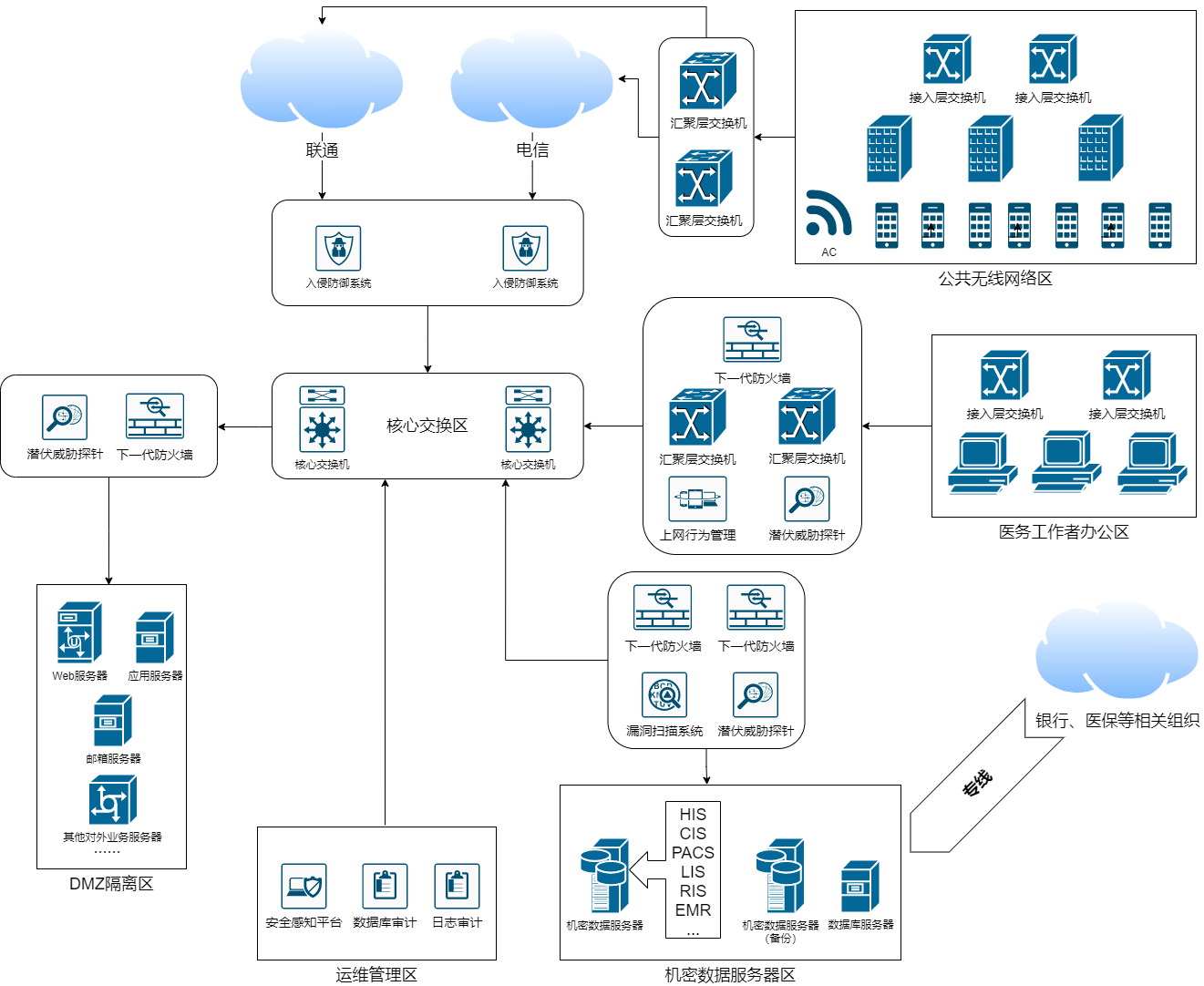
DMZ隔离区

机密数据服务器区

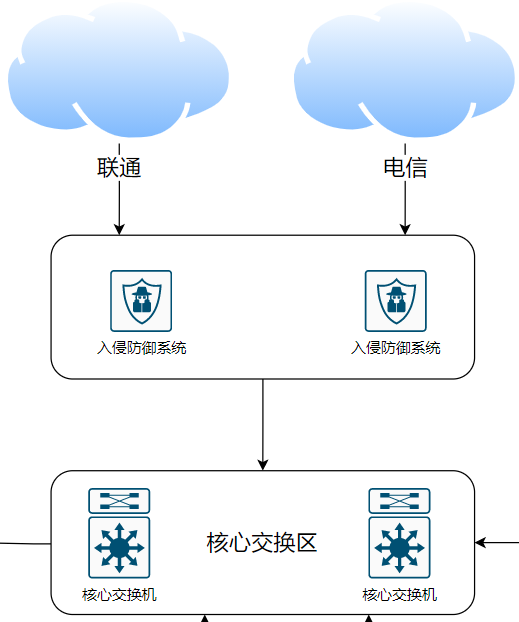
公共无线网络区

并且配置专线与银行、医保等组织进行数据传输

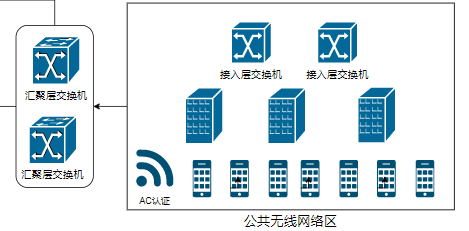
## 2.3、网络拓扑图



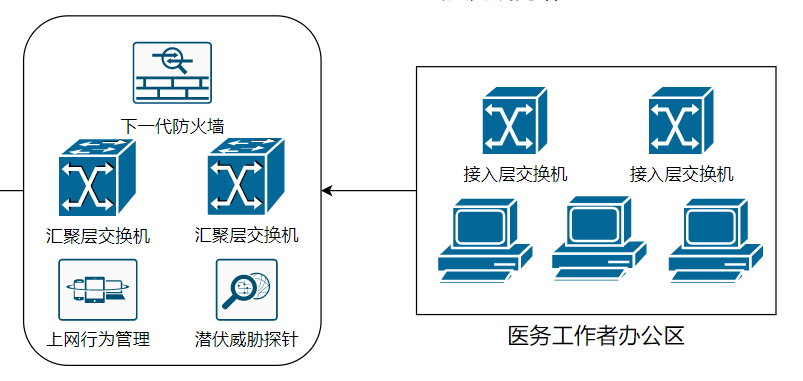
接入外网时，会配置两套入侵防御系统，对接联通跟电信的网络，来防御入侵，建立起第一道防御。



**公共无线网络区**是直接接入外网的，会配备汇聚层交换机，同时也会配置链路负载及冗余，来保证网络的可靠性；在用户接入的时候，会提供认证服务（因为与工作无关，所以不考虑安全性，只考虑实用性与可靠性）



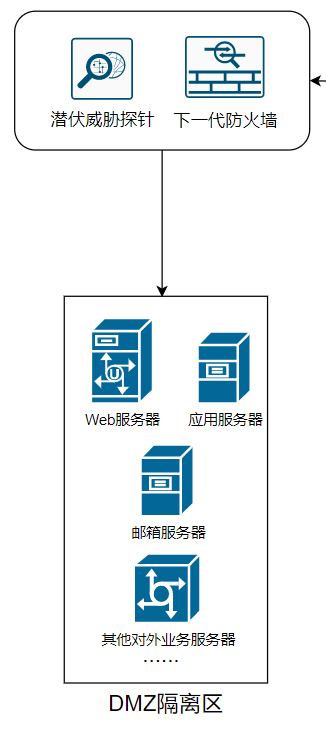
**医务工作者办公区**会配备下一代防火墙，汇聚层交换机，上网行为管理，潜伏威胁探针来保证网络的安全性，同时会配置链路的负载和冗余，保证网络的可靠性。



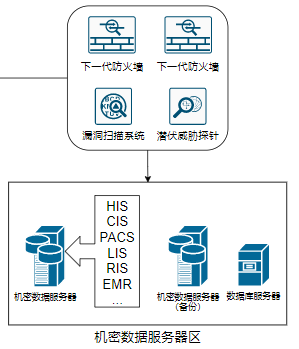
**运维管理区**内部有安全感知平台、数据库审计系统以及日志审计系统。



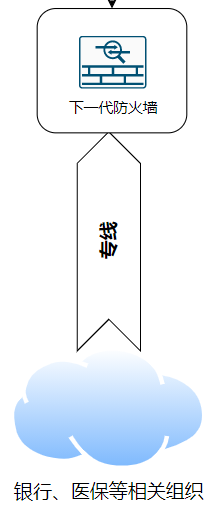
**DMZ隔离区**配备了下一代防火墙和潜伏威胁探针，用来保护服务器的安全。DMZ隔离区内部存放了各种对外服务器，但不包括机密文件服务器。



然后是**机密文件服务器区**，因为医院内部文件的安全系数直接影响到了人民的切身利益，所以这里我们会配备下一代防火墙、潜伏威胁探针、漏洞扫描系统；配置负载和冗余，同时也会对机密文件服务器进行定时备份，最大程度上保证机密信息的安全性。



最后是银行，医保等相关组织，是通过专线来连入内网的，同时也会配备下一代防火墙来保证内网的安全



## 2.4、IP地址的规划

|  |  |
| --- | --- |
| IP段 | 用途 |
| 192. 168. 0.0/24 | 网络设备(交换机、路由器等) |
| 10.0.0.0-------10. 10. 255.255 | 应用服务器 |
| 10. 11. 0.0-------10. 90.255. 255 | 医院本地网络( 按部门分配) |
| 10.91.0.0-------10. 100. 255. 255 | 医院本地AC接入设备 |
| 10. 101.0.0-------10. 150. 255.255 | 医院分院建设（预留）#方便扩充 |

在汇聚层交换机上建立IP池，开启DHCP Server，根据终端所属VLAN，动态分配楼栋各层的设备的IP。对于需要静态IP的设备，由管理员根据IP规划表手动配置。

对于需要被外部访问的服务器，如web服务器、邮件服务器等，需要根据ISP所提供的IP段来进行规划。

## 2.5、Vlan的划分

Vlan的划分是根据不同的部门来进行规划，不同的部门使用不同的Vlan。

# 详细设计及设备选型

## 3.1、核心层

核心层的功能主要是实现骨干网络之间的优化传输，是所有流量的最终承受者和汇聚者，对核心层的设计以及网络设备的要求十分严格，所以我们核心层采用冗余设计，并且选用两台【[华为S6720S-26Q-SI-24S-AC](https://detail.zol.com.cn/switches/index1217944.shtml" \o "华为S6720S-26Q-SI-24S-AC)】设备来进行部署。

## 3.2、汇聚层

汇聚层的功能主要是连接接入层节点和核心层中心。汇聚层设计为连接本地的逻辑中心，需要较高的性能和比较丰富的功能。所以我们采用冗余设计，并根据部门以及楼栋来确定设备数量，这里我们选用的是【华为S5735S-L24T4X-A】设备来进行部署。

## 3.3、接入层

接入层的主要功能是完成用户流量的接入和隔离，它直接面向用户，我们在接入层设计上主张使用性能价格比高的设备。因为是考虑到为每个病房都提供网络，所以是根据楼层的数量来确定设备数量，这里选用【华为S1730S-S24T4S-A】设备来进行部署。

## 3.4、网络安全设备

**传统防火墙**：部署于网络边界，是内部网络和外部网络之间的连接桥梁，同时对进出网络边界的数据进行保护，防止恶意入侵、恶意[代码](https://baike.baidu.com/item/%E4%BB%A3%E7%A0%81/86048" \t "https://baike.baidu.com/item/%E9%98%B2%E7%81%AB%E5%A2%99%E6%8A%80%E6%9C%AF/_blank)的传播等，保障内部网络数据的安全，我们这里选择部署的是【华为USG6525E】

**下一代防火墙**：在防火墙的基础上，增加了全面应对应用层威胁的功能，是一种高性能防火墙，我们这里选择部署的是【深信服—AF1210】

**安全感知平台与探针**：这里我们采用的深信服的【STP】和【STA】

* **安全感知平台(SIP)**: 负责收集汇总探针、防火墙等各类安全组件数据，通过人工智能、大数据技术，精准检测威胁、全局可视风险、快速闭环处置。
* **潜伏威胁探针(STA)**: 旁路部署在关键网络节点，镜像交换机流量，对全流量进行检测，提取有效数据上报给SIP。

**上网行为管理**：上网行为管理是指帮助互联网用户控制和管理对互联网的使用。其包括对网页访问过滤、上网隐私保护、网络应用控制、带宽流量管理、信息收发审计、用户行为分析等。这里我们采用的深信服的【上网行为管理AC】

**入侵防御系统**：帮助用户定位各种网络威胁， 以及违反安全策略的流量，并提供详实、有效的指导措施，进而实现防护 - 检测 - 响应一体化的解决方案。这里我们选用的是启明星辰的【天清入侵防御系统】。

**漏洞扫描系统**：基于漏洞数据库，通过扫描等手段对指定的远程或者本地[计算机系统](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%B3%BB%E7%BB%9F/7210959" \t "https://baike.baidu.com/item/%E6%BC%8F%E6%B4%9E%E6%89%AB%E6%8F%8F/_blank)的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为。这里我们选用的是奇安信的【漏洞扫描系统】

上述所选的设备都是市面上较先进的设备，以此来保证先进性及可扩充性。

# 总结

1、此套方案使用了双层保护机制，在入口处建立起第一道防御，针对重要的区域，建立第二道防御。

2、划分出不同的区域，根据区域内部信息的重要性以及机密性，给每个区域都配置相应的防护措施。

3、将公众网络跟内网直接隔离开，在节省了成本的同时也杜绝了横向攻击等相关威胁。