# 网络信息安全整改二期需求调研

## **总体网络架构**

**1.设计原则**

院区网络的核心层交换机承载着整网的内部数据交换，主要任务是把大量来自接入层的数据进行汇聚和集中，承担路由聚合和访问控制的任务。作为整个院区的核心，除了需要考虑性能外，也需要考虑稳定性及可靠性。总体来讲，核心区域设计需要满足以下几个原则：

层次化原则：核心层、汇聚层、接入层，每层功能清晰，架构稳定，易于扩展和维护。

模块化原则：每一个部门一个模块，部门内部调整涉及范围小，定位问题也容易。

可靠性原则：双节点冗余性设计，适当的冗余性提高可靠性。

核心层需要采用全连接结构，保持核心层设备的配置尽量简单，并且和业务部门无关。核心层设备需要具有高带宽、高转发性能。核心设备双机互联，核心汇聚之间建议采用万兆/千兆光纤连接。

**2.网络逻辑架构**

院区网是业务承载网，满足用户、终端与业务系统之间的互联，根据模块化设计的院区，院区网分为院区内部网络和院区外部网络，外部网络主要提供广域网互联、Internet互联、合作伙伴、移动办公、分支互联以及访客的接入。院区内部网络根据逻辑功能主要分为五个模块和两个区域。参见下图：

院区内部网络根据逻辑结构从上往下分为五个层次：

1）院区出口层

院区出口是院区网络到外部公网的边界，院区网的内部用户通过院区出口设备接入到互联网、分支机构以及企业外部用户（包括客户、合作伙伴、远程用户、VPN用户等）也通过院区出口设备接入到内部网络。

2）核心层

核心层负责整个院区网络的高速互联。核心层设计一般要兼顾网络利用率和网络可靠性；需要对网络故障具备快速收敛的能力。

3）汇聚层

汇聚层将众多的接入设备和大量用户经过汇聚后再接入到核心层。汇聚层目的是扩展核心层接入用户的数量。汇聚层通常还作为用户三层网关，承担L2/L3边缘设备的角色，提供用户管理、安全管理等各项跟用户和业务相关的处理。在网络规模较小的情况下，接入和汇聚可以合并，提供两层架构。

4）接入层

负责将各种终端接入到院区网络，通常由以太网交换机组成。当前随着移动终端的普及，无线接入的需求逐渐旺盛。所以院区接入层目前需要考虑有线无线的融合，需要无线AP、AC甚至物联网模块。

5）终端层

包含院区内的各种终端设备，例如PC、笔记本电脑、打印机、传真、POTS话机、手机、摄像头等。

院区网还有包含两个重要的管理区域，一个是运维管理区，另一个是DMZ区。

6）运维管理区

提供对网络、服务器、应用系统进行管理的区域。一般满足FCAPS模型的网络管理，主要包括故障管理、配置管理、性能管理、安全管理等。

7)DMZ区

通常公用服务器部署于该区域，为外部访客（非企业员工）或者远程办公用户提供相应的访问业务（比如Email、Ftp服务器、DNS等），其安全性受到严格控制。

除了以上模块外，院区网络还承担和数据中心互联的功能，满足终端到应用之间的访问权限控制和业务的隔离。

**3.网络物理架构**

该物理拓扑的主要特点有：

• 核心层采用双机部署，具备高可靠性，满足院区业务的高速稳定互联。

• 网络采用分层设计，包括核心层、汇聚层、接入层（汇聚接入根据规模可以合并）。

• 有线无线一体化设计，实现一体化管理、一体化供电。

• 采用网络管理软件管理全网所有网络设备。

• 智能平台同时可以提供用户、终端的接入管理，实现人、设备、业务的智能运维。

#### 信息安全建设

## 本期网络安全建设规划

外网：边界防护增强，vlan划分，无线用户认证；数据泄漏检测；

内网：安全态势平台建设；内网服务器防护。

### 外网规划

#### 区域划分

医院外网划分互联网接入区、核心交换区和终端接入区共三个安全域；通过交换机对各楼层各科室，根据业务的性质与关联性进行vlan划分，增强网络的安全性与稳定性。

#### 互联网行为审计

在互联网接入区以透明串接模式部署上网行为管理，对医院办公外网终端访问互联网的行为进行分析、审计和控制，防止医院内部员工上班时间违规内容或在网上发表违规言论，同时设置日志归并时间为6个月以上，保存至少6个月的访问日志，以便协助公安调查取证。

同时针对于通过无线网络接入外网区域的用户，开启无线接入认证，解决医院无线监控盲区的风险。

#### 网络DLP

在互联网接入区以旁路模式部署网络DLP，对外网区域终端通过网络途径外发或上传的文件进行解析和文档提取，识别敏感数据，依据预先定义的策略，实时响应动作，进而达到对敏感数据防护目的，有效防止数据被非法窃取、访问、和使用。

### 内网规划

安全平台建设；态势感知平台、威胁探针、资产探针；服务器防火墙规划、终端安全管理系统。

### 区域划分

医院内网划分专网接入区、核心交换区、安全管理区、核心业务区和终端接入区等多个安全域；通过交换机进行vlan划分，防止内网网段混用所带来的的不必要的安全威胁。

### 统一监测平台

在安全管理区按照一体化、标准化、智能化、可视化要求建设一套态势感知系统，通过收集医院网络内的资产、流量、日志、网站等相关的安全数据，经过存储、处理、分析后形成资产态势、风险态势、安全态势及告警，辅助医院信息中心了解整体医院网络安全态势。及时掌握网络安全威胁、风险和隐患，及时监测漏洞、病毒木马、网络攻击情况，及时发现网络安全事件线索，及时预警通报重大网络安全威胁，及时处置安全事件，提升广州医科大学附属肿瘤医院的风险发现能力，加快风险解决速度。

### 内网服务器防护

在医院业务内网的核心业务区1与核心交换区的区域边界部署下一代防火墙。防火墙开启入侵防御功能模块，并提供入侵攻击特证库的自动或手动升级，实时发现和阻止从外部网络发起的网络攻击行为，阻止来自其它网络区域的攻击流量对重要区域造成影响。并记录攻击行为的攻击源IP、攻击类型、攻击目标、攻击时间等，向运维管理人员发送告警信息。

表1**网络信息安全整改二期采购内容**

| **序号** | **产品**  **名称** | **功能参数** | **数量** |
| --- | --- | --- | --- |
| 1 | 上网行为管理 | 功能概述：上网行为管理能对网络中的网络社区、P2P/IM带宽滥用、网络游戏、炒股、网络多媒体、非法网站访问等行为进行精细化识别和控制。利用智能流控、智能阻断、智能路由等技术，配合创新的社交网络行为管理功能、清晰易管理的日志分析等功能，可以提供业界最全面和完善的上网行为管理解决方案。从而保障网络关键应用和服务的带宽，对网络流量、用户上网行为进行深入分析与全面的审计。支持超过60天以上的保存时间，满足公安部82号令。  技术参数：2U,6个千兆电口， 2个千兆光口,冗余电源,2个扩展槽位,带宽性能500M，网络吞吐量1.5G，最大并发连接数>100万，推荐用户数：3000人，硬件3年原厂保修 | 1套 |
| 2 | 网络DLP:数据防泄漏系统 | 功能概述：系统是独立网关类产品，可以对敏感数据实施事中、事后全面保护与审计和对网络传输协议SMTP、http/https、FTP、SMB等，以及RESTful接口传输数据进行抓取，基于深度内容识别技术，通过定义关键字、指纹库、数据标识符、权重词典、机器聚类等多种敏感数据规则，对传输数据进行监测，对违规传输行为作出告警、审计、阻断、审批等响应。  技术参数：1U,6个千兆电口、2个千兆光口，1个管理口2个扩展槽位,7层最大检测吞吐率：200Mbps，硬件3年原厂保修 | 1套 |
| 3 | 边界网闸：安全隔离与信息交换系统 | 功能概述：基于国产化硬件平台和国产操作系统自主设计开发的网络安全产品。该系统采用“2+1”系统架构，包括内外网代理主机和自主研发的FPGA专用隔离硬件，对信息流进行协议剥离、落地还原、内容过滤、病毒查杀处理并结合访问控制、安全审计等安全防护机制，有效阻挡黑客入侵、恶意代码和病毒渗透，防止内部机密信息的泄露，实现网间安全隔离和数据摆渡。  技术参数：2U,内外端机双侧液晶屏； 内端机6个10/100/1000Base-T接口，1个扩展槽位，含1个MGMT口； 外端机6个10/100/1000Base-T接口，1个扩展槽位，含1个HA口；网络吞吐量：450Mbps； 并发连接数：8万；内外端机各1TB硬盘。可扩展WebFilter过滤模块，防病毒模块，硬件3年原厂保修 | 1套 |
| 1 | 服务器防火墙：服务器安全管理系统 | 功能概述：融入了AI驱动一体化智能检测引擎，并集WAF、僵木蠕、ADS、HTTPS流量检测、高级威胁防护、异常行为分析、DLP等多个安全模块于一身，联动云管端多个网元，最终为用户提供融入AI单点防御、多元智慧协同、云检测赋能的智能、主动、安全“零”死角的综合防护。服务器安全管理系统同时提供资产梳理、暴露面梳理、风险发现、威胁监测、病毒查杀、等保合规基线、系统加固、溯源分析等全面的安全能力,在服务器端形成、事中控制、事后溯源的一体化防护体系。全面覆盖服务器资产梳理、暴露面梳理、漏洞检测、病毒查杀、勒索病毒防护、等保合规服务器微隔离、日常运维等。  技术参数：1U,8电口2光口2万兆接口2个扩展槽位,液晶显示屏，防火墙吞吐8G，并发连接220万 默认包含应用识别功能；可扩展IPSecVPN、SSL VPN模块；支持扩展IPS入侵防御、WAF、僵木蠕、URL过滤及AV防病毒功能，硬件3年原厂保修 | 1套 |
| 2 | 网络准入控制系统（内网） | （1）每秒事务数（TPS)：≥3000（次/秒），最大吞吐量：≥8Gbps；应用层吞吐量≥4G  （2）最大支持终端同时在线数≥2000；  （3)系统部署简单，支持旁路或串联部署，支持命令行与B/S模式管理，提供系统首页图形化展示功能，可展示设备面板状态、CPU状态、内存状态、硬盘状态、在线用户、报警统计等信息；  (4)支持802.1X、Portal、透明网关、策略路由等多种准入模式选择，单设备情况下可进行混合准入模式应用；  (5)支持准入设备黑/白名单管理，可根据所应用的不同准入模式，设置黑/白名单终端IP、MAC、协议、端口、VLAN号等信息，以便针对该名单中设备进行入网控制；  (6)支持资产管理功能，可管理不同类型入网资产；提供交换机网络设备管理功能，可查看交换机设备接口状态、主机连接等详细信息。对入网资产可发现、可审批入网。（7）主机包含3年基本维保服务。 | 1套 |
| 3 | 威胁探针：僵尸网络木马和蠕虫监测处置系统 | 功能概述：威胁探针集合了攻击检测、僵木蠕检测、DDoS检测、恶意程序检测、APT检测、WEB安全检测、虚拟沙箱、元数据提取、流量分析九大功能，即九合一全流量检测探针。该产品通过深度解析网络流量，结合特征匹配、异常行为分析、威胁情报、机器学习、虚拟沙箱等技术，实现迅速、精准识别网络中各种已知和未知威胁。威胁探针全面的威胁监测能力，让网络安全状态一目了然，提升风险应对。  技术参数：2U,6个千兆电口，4个千兆光口,冗余电源,5个扩展槽位,最大并发连接数：150W，综合威胁检测能力：3000Mbps，硬件3年原厂保修，默认含： 打包升级许可，包含攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库、URL分类库。 | 1套 |
| 4 | 资产探针：脆弱性扫描管理系统 | 功能概述：系统集成了系统漏洞、Web漏洞、数据库漏洞、弱口令的发现能力，可以高效、全方位的检测网络中的各类脆弱性风险，并可生成风险分析报告和修补建议，满足不同用户的多样化需求。  技术参数：1U,6个千兆电口，1个扩展插槽1个扩展槽位,40个域名扫描 任务不限制IP数量； 并发扫描40个IP地址； 并发扫描5个系统扫描任务； 并发扫描3个web任务 | 1套 |
| 5 | 态势感知：态势分析与安全运营系统 | 功能概述：态势感知平台系统为用户提供集中安全态势监视能力。系统应用大数据技术架构，能够实现全网海量数据规模的安全信息的采集和集中存储，在此基础上对数据进行综合处理和关联分析，从资产态势、运行态势、攻击态势、漏洞态势、风险态势和威胁态势六大维度，为用户展示面向全网业务资产防护的安全态势，帮助用户感知隐患和威胁，进而为安全运维提供决策支撑。态势感知平台可灵活的对接用户网络中的安全设备或安全子系统， 实现各类型多厂商安全监测防护资源的整合，通过对接，态势感知系统可覆盖全网攻击行为信息、资产及业务脆弱性信息、异常流量信息、威胁情报及未知威胁等信息呈现，形成被攻击对象和攻击源识别、脆弱性识别、攻击过程及影响分析、安全风险态势等在内的多视角全方位的态势感知。  技术参数：2U,6个千兆电口， 4个千兆光口,冗余电源,存储8TB，内存64G，硬件3年原厂保修。  默认包含1个License，默认带一次安装、一次使用培训及一年远程故障支持服务。 | 1套 |
| 三、其他 | | | |
| 1 | 重点防病毒信息安全软件 | 对单位现有使用的杀毒软件原有功能进行原厂维保续期，续期的维保时间为3年，同时增加客户端200个点 | 1项 |
| 2 | 服务器防病毒信息安全软件 | 对单位现有使用的杀毒软件原有功能进行原厂维保续期进行原厂维保续期，续期的维保时间为3年，要求如下：服务器客户端要求：支持WINDOWS服务器的防病毒、补丁管理功能等，同时增加客户端60个点。 | 1项 |
| 3 | VPN设备 | （1）1U,6个千兆电口， 2个千兆光口,单电源,2个扩展槽位,IPSEC吞吐率：1Gbps IPSEC VPN隧道数：10000 SSL吞吐率：600Mbps SSL并发用户数：4000 最大管理用户数：15000  （2）默认含1500个SSL VPN的客户端许可；移动端人脸识别认证功能模块；PC端可信接入模块、短信认证模块；  （3）支持自有DDNS动态域名注册，支持使用域名进行动态寻址，支持使用域名进行隧道定义及协商，支持使用域名进行集中认证和管理；  （4）符合国密局制定的《IPSEC VPN技术规范》，支持国家商用密码算法SM2、SM3、SM4。 | 1套 |
| 四、系统集成服务 | | | |
| 1 | 系统集成服务 | 系统集成服务要求：要求集成商提供信息安全专业技术人员按我院网络信息安全规划结合现状提供集成实施方案；充分一期安全加固的设备，完成集成安装部署服务；根据医院需求完成网络安全一期相关设备的策略优化工作。 | 1项 |