**黑龙江中医药大学第一附属医院**

**网络增值服务平台**

**技术规范书**

(V1.0)

黑龙江中医药大学第一附属医院

2021年10月

# 目录

目录 1

一、总体要求 1

1.1 总述 1

1.2 建议书的文件要求 1

1.3保密条款 4

1.4 知识产权（IPR）/专利权 4

1.5 卖方承诺 4

1.6 工程进度 5

1.7 培训 5

二、工程服务描述及建设目标 6

2.1 建设背景 6

2.2 现状描述 6

2.3 建设目标 8

三、平台设计原则 10

3.1 应用设计 10

3.2 技术设计 10

3.3 性能设计 10

3.4 管理设计 10

3.5 业务安全设计 11

3.6 经济性设计 11

3.7 网络安全性 11

3.8 系统先进性 11

3.9 平台开放性 12

3.10 平台扩展性 12

3.11 设备、网络冗余性 12

3.12 高性能承载 12

3.13 规范化和标准化 12

3.14 分层化网络 12

四、平台规划及功能描述 14

4.1 网络平台升级服务 14

4.1.1 整体网络规划设计 14

4.1.2 整体设计目标 14

4.1.3 网络设计说明 14

4.2 平台安全加固服务 16

4.2.1 VLAN安全设计 16

4.2.2 防网络病毒设计 17

4.2.3 防网络攻击设计 17

4.3 融合虚拟化容灾改造服务 18

4.3.1 融合虚拟化容灾改造设计 18

4.3.2 融合虚拟化容灾设计说明 18

4.4 智慧型医院升级服务 20

4.4.1 智慧型医院技术方案 20

4.4.2 智慧型医院建设目标 20

五、业务服务及性能要求 22

5.1 网络升级服务功能性要求 22

5.1.1 信息化性能要求 22

5.1.2 网络融合性要求 22

5.1.3 网络管理要求 22

5.1.3 稳定、可靠及扩展性要求 22

5.2 网络升级服务性能要求 23

5.2.1 交换性能要求 23

5.2.2 接入性能要求 24

5.3 安全升级服务性能要求 24

5.4 融合虚拟化容灾服务功能性要求 26

5.5.1 建设原则 26

5.5.2 方案达成效果 27

5.5 融合虚拟化容灾服务性能要求 27

5.6要求的业务服务及性能技术参数要求如下： 27

5.7迁移服务 40

六、服务商工作主要内容 43

七、技术培训 44

八、达成效果 45

九、售后服务 46

十、其他 47

# 一、总体要求

## 1.1 总述

1.1.1 本规范书是黑龙江中医药大学附属第一医院（以下简称买方）向为拟建设的网络增值服务平台项目供货商（以下简称卖方）提出的规范书。

1.1.2 卖方如不能满足本规范书中所提到的各项技术要求及业务功能指标，应在建议书中明确提出，否则即认为卖方能够按本文件要求提供服务。

1.1.3 本规范书主要提供黑龙江中医药大学附属第一医院-网络增值服务的总体要求，供卖方编写技术建议书。在满足买方的总体技术要求的情况下，卖方可征得买方的同意，提出适当的修改建议，并陈述理由。若卖方认为买方的技术要求尚不明确或有漏项的地方，请详细加以说明并经双方商定。对规范书内容的澄清及修改将由买方以电子邮件形式发送所有得到规范书的厂家。

1.1.4 黑龙江中医药大学附属第一医院颁发的有关技术规定和行业标准是本规范书不可分割的部分。本规范书未提到的部分应遵从信息产业及工业化部相关文件之规定。

1.1.5 买方有权在签订合同前，根据需要修改本规范书，修改后的最终稿将作为合同附件。在技术谈判的过程中，本文件的有关要求可能出现改动，买方保留对本规范书的解释和修改权。本规范书的修改和解释权属于黑龙江中医药大学附属第一医院。

1.1.6 本技术规范书的文档按版本化管理。在技术谈判过程中不断充实内容，进行版本升级。

1.1.7卖方应在收到本文件20日内，向买方提供中文应答书（含报价服务清单和目录价）、商务报价书（密封件），以及应答书的电子文档（中文OFFICE格式）。

1.1.8卖方如不能满足本规范书中的要求，需要详细说明原因。

## 1.2 建议书的文件要求

结合黑龙江中医药大学附属第一医院-网络增值服务项目建设设计情况建议书至少要对以下对系统建设有重要影响的方面做详细说明：

1. 技术服务设计及实施方案；
2. 技术服务、技术支持及保修；
3. 技术培训；
4. 技术项目文档；

总体描述部分应包含卖方综合情况，卖方应至少提供下列内容：

a) 卖方的背景资料介绍：包括公司成立时间、成立地点、注册资金、银行存款、经营范围、近三年公司的业务收入和利润、企业类型、雇员总数、本地区雇员总数、黑龙江地区的办事机构类型、人员组成和经营范围及具有的相关资质及经营授权，其他需要说明的情况等。

b) 卖方成功实施的与本项目相关成功案例或与主流设备及软件厂商合作经验，卖方需提供项目合同或中选通知书、买方联系人、联系方式等文件作为证明材料，并具体说明案例的项目名称，项目周期，项目规模，合同金额，所参与的软硬件系统概况，项目主要技术难点，自主研发软硬件（如果项目包含）的情况等详细的项目信息，与主流设备及软件厂商合作经验的相关证明材料。

c) 卖方的市场定位、公司目标、业务运作情况，业务发展计划。

d) 卖方的内部组织架构、详细说明网络增值服务平台项目服务人员配置及技术能力、汇报机制。

建议书应答要求：

a) 要求卖方对本规范书所提出各项要求进行逐条逐项答复，首先对实现或满足程度明确做出“满足”、“不满足”、“部分满足”应答。不得使用“明白”、“理解”等词语。

b) 对于本文件中明确要求卖方详细说明或提供其他材料的条款，卖方必须在点对点应答书中详细说明，或者提供详细附件说明而在点对点应答中详细说明参见文档的具体章节或页码。不得简单答复“满足”等，否则视该条款的应答为“不满足”。

c) 对于答复“部分满足”、“不满足”的内容或有不同于本文件相关要求的其他建议的内容，卖方均应逐点给予详细的说明与答复。如果答复“部分满足”，还需要详细说明哪些部分满足，哪些部分不满足，并且详细说明原因。

d) 凡采用“详见”、“参见”方式补充说明的，应指明参见文档的具体章节或页码。

e) 说明与应答矛盾的，以应答为准。

技术建议书其他要求：

1. 服务交付进度安排，详细描述工作任务分解结构、资源安排情况、里程碑时间点（具体到天）及提交物。

2. 分工界面，要求图示并加以说明：

1) 卖方应说明项目中卖方和买方的详细分工界面，包括卖方与其他第三方厂商及买方的工程界面、工作内容及责任划分等。以上说明要求附加图示进一步说明。

2) 卖方在此部分未明确说明的项目相关工作视为卖方独立全权负责。

3. 测试及验收方案，卖方应提供如何配合买方进行验收测试的方案、过程以及评价验收测试是否通过的方法。

4. 本次工程实施建议，卖方对本项目工程实施方面的其他建议。

5. 技术支持、保修、培训和服务承诺，卖方应说明给买方提供的技术文件、技术服务、技术支持、保修及人员培训等的范围和程度：至少包括系统上线后卖方提供的技术支持、售后服务内容、等级、相关服务指标、售后服务组织机构及人员安排情况，并说明培训的内容、人员和时间安排，以及卖方对满足买方提出的新需求在时间上的承诺，（附：保修、维护期为1年）。

6. 交付文档清单，卖方需要提供交付过程中的所有交付文档清单列表，以及交付物提供时间点。

7. 服务功能清单，卖方需要提供为满足甲方需求，提供的所有服务能力数据清单。

8. 其它需要补充的材料，若有其他需要补充的材料，卖方应加以说明并列出详细清单。

## 1.3保密条款

任何一方未经另一方同意不得向任何第三方透露本文档内容，双方一致同意任何一方在任何时候对其持有的有关另一方的事务或其事务运转操作方法等保密信息实行严格保密。除非有信息提供方书面许可，任何一方不得在任何时间向本协议以外的任何第三方披露或提供保密信息（包括但不限于：任何信息提供方不欲公开的观点、发现、发明、公式、程序、计划、图表、模型、参数、数据、标准和专有技术秘密，和/或其中的任何知识产权）的任何内容（本协议另有约定的除外）。除非有信息提供方的书面指示，任何一方不得对保密信息进行拷贝或抄写。

## 1.4 知识产权（IPR）/专利权

自协议生效之日起，对在黑龙江中医药大学附属第一医院-网络增值服务项目工程范围内，与系统相关的由卖方自行开发的所有应用软件产品，卖方应同意上述软件的著作权属于买方或买方关联公司，买方或买方关联公司拥有上述软件及相关文档的所有权、知识产权及解释权。

在未经买方书面允许的情况下，卖方不得以任何方式将上述应用软件产品、文档及或软件的任何数据或程序向买方和买方关联公司以外的任何第三方明示或暗示地披露、提供或以任何方式加以利用。

卖方不得将本工程涉及的任何技术文档、相关的技术规范或技术标准明示或暗示地提供或透露给除买方和买方关联公司以外的任何第三方或以任何方式利用。

## 1.5 卖方承诺

1.5.1在买方书面许可的情况下，如果卖方将本协议项下权利和义务全部或部分转让给任何第三方，卖方应保证该等第三方也遵守本章条款的规定。如果第三方违反或不履行本章条款的规定，均被视为卖方违反本协议。

1.5.2如因卖方违反或不履行本章条款的规定而直接或间接地帮助其他电信运营商也使用了与本协议中的软件产品功能、思路、目标相同或类似的软件产品，买方和/或买方关联公司有权单方解除本协议和/或合同，同时卖方应承担因此给买方和/或买方关联公司造成的全部损失。

1.5.3本章条款可以作为独立的协议在本协议终止或期满后继续有效，有效期为协议生效之日起三年。

## 1.6 工程进度

本项目进度卖方应根据自己提供的方案、软硬件配置、软件运行环境及工程实施的能力，提出详细的项目实施步骤、项目进度时间表、软件设计、开通方案。

## 1.7 培训

卖方应为买方提供技术人员（包括设计、维护及管理人员）技术培训及业务培训，卖方应分别说明培训内容、培训计划和培训人数。

# 二、工程服务描述及建设目标

## 2.1 建设背景

随着网络技术，信息通信领域的长足发展，网络经济，知识经济再不是IT等高科技行业的专利，当今社会信息化进程迅猛发展，网络技术已经对社会、经济和文化各方面产生重大影响，并将改变人们认识世界、思考世界的观点和方法。作为传统行业之一的医疗卫生行业，如何面对网络时代带来的冲击，如何利用网络技术提高医疗卫生行业的管理水平和服务质量，是无法回避的问题。随着信息技术的不断发展和人们对医疗保健水平的要求不断提高，医院信息化建设已经迫在眉睫。

黑龙江中医药大学第一附属医院有意向对目前的接入网和核心网进行全面的升级改造，包括系统层面的虚拟化改造、核心网改造、接入网改造，全面利用先进的网络技术以提高本院的医疗卫生管理水平和医护服务质量。

## 2.2 现状描述

**2.2.1网络拓扑**

目前黑龙江中医药大学附属第一医院分为内网和外网两部分。如此区分主要考虑到网络安全，要对外网和内网进行物理隔离。

在此基础上，又分为数据核心网、终端接入网和外联网。

内网的数据核心网主要为包括HIS系统在内各个业务核心服务器提供网络接入，同时作为连通各个区域的数据中转核心；

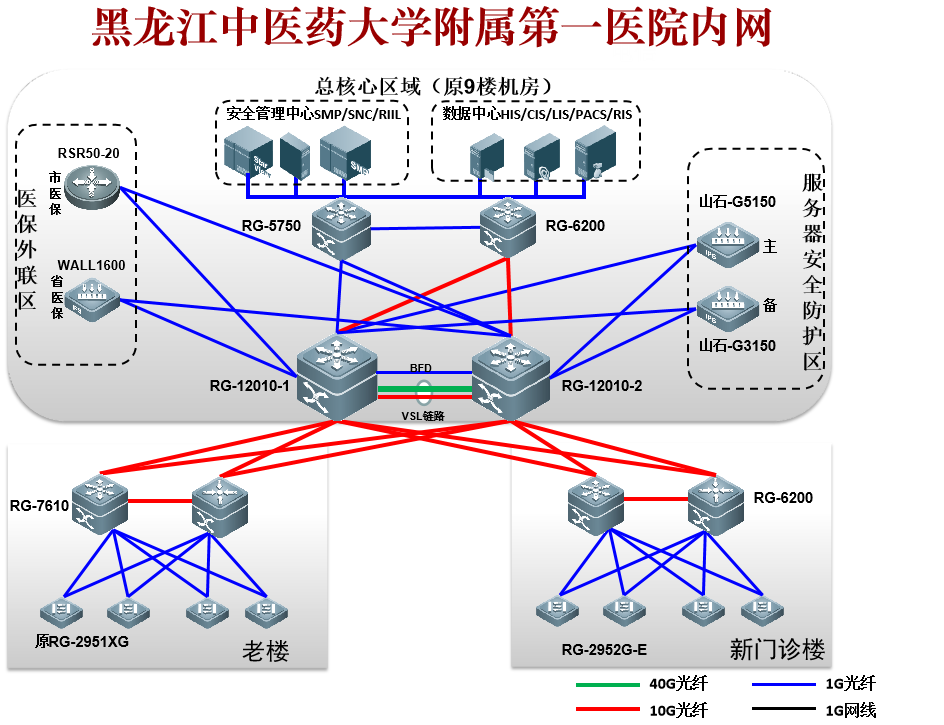
内网的用户接入网主要为医疗、办公终端提供网络接入服务；

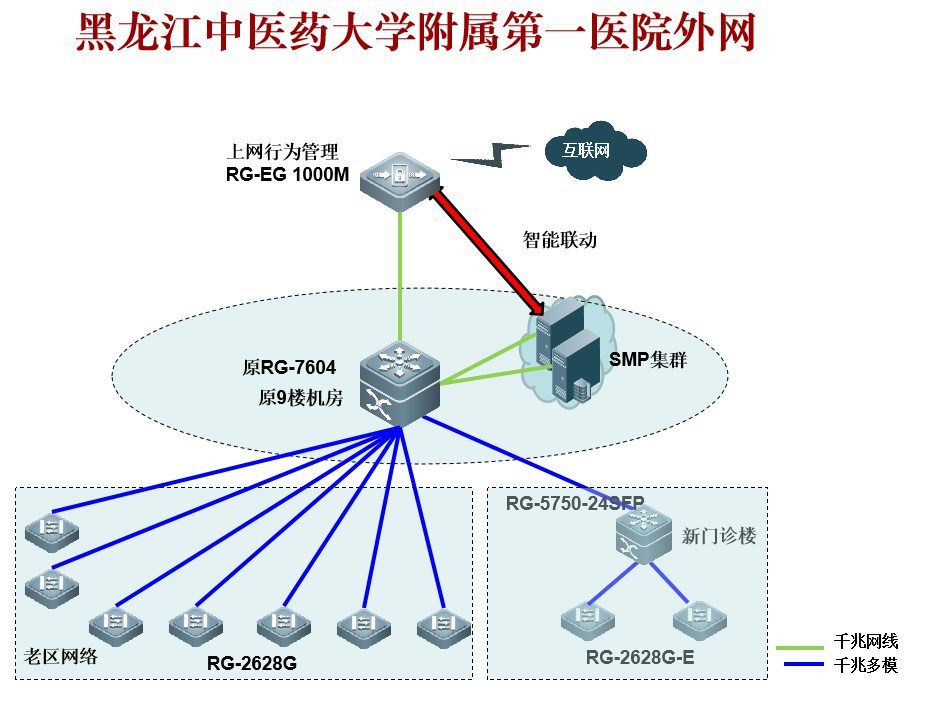
内网外联网主要提供连接其他医疗单位、政府管理部门的网络接口；

外网数据核心网主要为医院提供的互联网服务系统提供服务器接入，同时作为连通格尔该区域的数据中转核心；

外网接入网主要为院内的上网终端提供网络接入服务；

外网的外联网一般指国际互联网接口；





**2.2.2 设施及管理现状**

内网和外网的设备使用年限均超过5年，大量设备存在老化后故障率升高且配件供应存在问题，接入网环境由于非标准化机房，机房内灰尘、温度、湿度均无法达到标准，问题尤为突出。

**2.2.3 内网现状**

内网的骨干核心节点采用的是常规高端交换机，由于年代久远，且内网在组网时核心系统和接入网没有必要的安全边界，存在安全风险；

**2.2.3 外网现状**

外网区域存在单点故障，随着互联网医疗的开展，这将成为今后发展的重要短板；

**2.2.4 当前存在问题**

* 用户目前在用的网络设备8成使用年限超过6年，部分使用年限超过10年，已经超过设备的稳定工作期。设备的稳定性正随着时间流逝严重下滑，影响医院的工作效率。这批设备需要及时更换；
* 园区内传输光缆分批建设且时间很长，其中部分已经损坏难以修复，同时由于近年来院方的基建改动，很多原有线缆沟槽、管道已经无法使用。需要重新规划园区内的光缆槽道，并重新敷设园区内的通信光缆；
* 部分关键节点存在设备单点故障问题，如外网的核心交换机、上网行为管理设施等；
* 网络中缺少对病毒、攻击的预警等安全设施；
* 根据院方对房间的使用规划，部分楼宇汇聚交换机的位置需要迁移到其他楼层（外科楼的汇聚交换机需要从10楼迁移到9楼，相关楼内涉及到楼层交换机的布线全部需要重新敷设）；
* 网络区域之间应增设防火墙系统用以保证关键、核心系统的数据安全；

**2.2.5 智慧医院建设情况**

智慧医院建设目前为空白；

## 2.3 建设目标

平台主要实现以下功能及目标：

* 接入网升级改造——骨干链扩充到40G，并可在今后无缝扩容到100G；
* 核心网升级改造——升级数据中心交换机，提高处理能力和今后的扩容能力；
* 安全升级改造——根据要求提供必要的安全设备确保院方数据安全；
* 融合虚拟化容灾改造——通过升级服务器配置和采购虚拟化软件时间计算、网络、存储资源的虚拟化容灾能力；

# 三、平台设计原则

## 3.1 应用设计

根据卫生部信息化十五规划和医保社保的迫切要求，全国医疗卫生系统从2000年年底开始试点“医院管理信息系统”，实现基于财务的信息管理（门诊划价、收费系统），实现基于医生的辅助治疗，医生工作站、辅助病因分析及治疗建议；实现PACS（影像应用传输系统）基于临床的影像信息管理，分析。还有电子病历、远程医疗、药房管理等。

## 3.2 技术设计

根据应用分析，特定的应用必须要有特定的技术来实现，才能得到预期的应用效果，分析网络的应用，属于集中式应用（客户机/数据中心），网络的数据流量有大约80%集中于网络的主干，所以网络的主干应该是高性能的交换式结构，而且具有较高的系统扩展能力（如端口数量）和新技术应用能力（如万兆、千兆以太网）。关键技术的应用。例如，对于语音和视频应用，交换机系统首先要支持组播技术（IGMP，PIM等）和严格的服务质量管理体系（QoS）。

## 3.3 性能设计

系统的安全高效运行需要系统内的各个设备具有独立的高性能和协同的高性能：

为使网络结构尽量稳定可靠，应采用星型拓扑结构，中心节点与边缘节点间为万兆以太网，服务器以万兆接入中心交换机。

中心交换机应支持无阻塞交换，各种模块支持热插拔，并支持基于板卡智能分布式的基础上实现端口同步级处理等功能。

应用复杂化和多元化，需求网络高带宽，核心层到接入层万兆链路以太网为目标。

## 3.4 管理设计

网络管理能提供流量、状态等多种信息。

网络管理能实施有效的监控。

需要能够对网络设备进行集中的统一管理，自动生成网络拓扑结构，通过颜色变化来区分设备运行情况。

安全策略批量下发，及时调整安全策略，批量对交换机群管理，提高网络安全管理。

## 3.5 业务安全设计

由于病人病历、医保等数据的特殊性，网络系统的安全性成为突出的矛盾，所以，安全性应考虑以下几点：

分层过滤：包括支持链路层的访问控制，传输层的访问控制，网络层（FireWall，IPsec）的访问控制以及应用层的安全控制等。

安全策略管理：

杜绝非法的组播源播放非法的组播信息；

如何有效控制和预防病毒的传播和网络的攻击；

由于各种病毒在被公布前很难防范，网络技术需要能适时的调整安全策略，并在最短的时间内部署到全网，把病毒拒绝在网络之外。

## 3.6 经济性设计

在适当考虑未来发展和先进性能的前提下，以最佳性能/价格为原则。即尽可能采用高档次、低配置、逐步扩展的原则。

## 3.7 网络安全性

网络必须具有良好的安全防范措施和密码保护技术，灵活方便的权限设定和控制机制，使系统具有多种有效手段，防范各种形式对网络的非法入侵和内部攻击，以保证网络的实体安全、网络安全、系统安全和信息安全，有效地保障正常的业务活动和防止内部信息数据不被非法窃取、篡改或泄漏。因此系统应分别针对不同的应用和不同的网络通信环境，采取不同的措施，包括系统安全机制、数据存取的权限控制等。尤其内外网之间要做到物理隔离。

## 3.8 系统先进性

系统设计既要采用先进的概念、技术和方法，又要注意结构、设备、工具的相对先进成熟，整个系统的生命周期应有比较长的时间，可以在信息技术不断发展的今天，在系统建成以后比较长的一段时间内能满足用户需求增长的需要；不但能反映当今的先进水平，而且具有发展潜力，能保证在未来相当长的时间内占主导地位，保证网络建设的领先地位。

## 3.9 平台开放性

采用开放的软硬件平台和数据库管理系统，遵循国际标准化组织提出的开放系统互联的标准，应用软件必须独立于软硬件平台，能集成任何第三方的应用，具有良好的可扩展性、可移植性和互操作性。

## 3.10 平台扩展性

系统必须具有良好的可扩充性，在系统结构、系统容量与技术方案等方面必须具有升级换代的可能，核心设备必须采用模块化的结构，跟踪网络发展的前沿方向，符合网络的发展趋势并具有充分的扩展性。系统建设必须尽量保护现有的软、硬件资源，保证各部门现有的计算机系统的使用，逐步过渡，有效保护用户投资，最终形成一个统一的、一体化的综合网络系统。

## 3.11 设备、网络冗余性

考虑到网络的安全稳定及关键业务不受影响，在线路的设计上我们选择了在服务器区域采用双线路连接到核心，服务器区域是医院网络的核心业务，是我们重点保障的对象，采用双线路后可以保证在任何一根物理连接线出现故障时都可以通过另一条链路连接到核心交换机保证服务器的永续服务。

## 3.12 高性能承载

网络链路和设备具备足够高的数据转发能力，保证各种信息的高质量无阻塞传输；交换系统具有很高的交换容量与多服务支持的能力，保证网络服务的质量。

## 3.13 规范化和标准化

网络体系结构、通信协议及软件的设计和开发必须按照国家或行业标准进行，要模块化、结构化、数据要代码化，以便于信息共享和交流及将来的维护。在系统设计和软件开发时，应用程序必须规范化、模块化和可复用。

## 3.14 分层化网络

为减少网络中各部分的相关性，便于网络的实施及管理，在网络的构建中，从整体上可以将网络划分为核心层、接入层等二个层次。

核心层负责完成网络各汇聚节点之间的互联及完成高效的数据传输、交换、转发及路由分发。

接入层设备提供各种标准接口将数据接入到网络中，完成基本的业务系统之间的隔离和安全性控制、认证管理等功能。

# 四、平台规划及功能描述

## 4.1 网络平台升级服务

### 4.1.1 整体网络规划设计

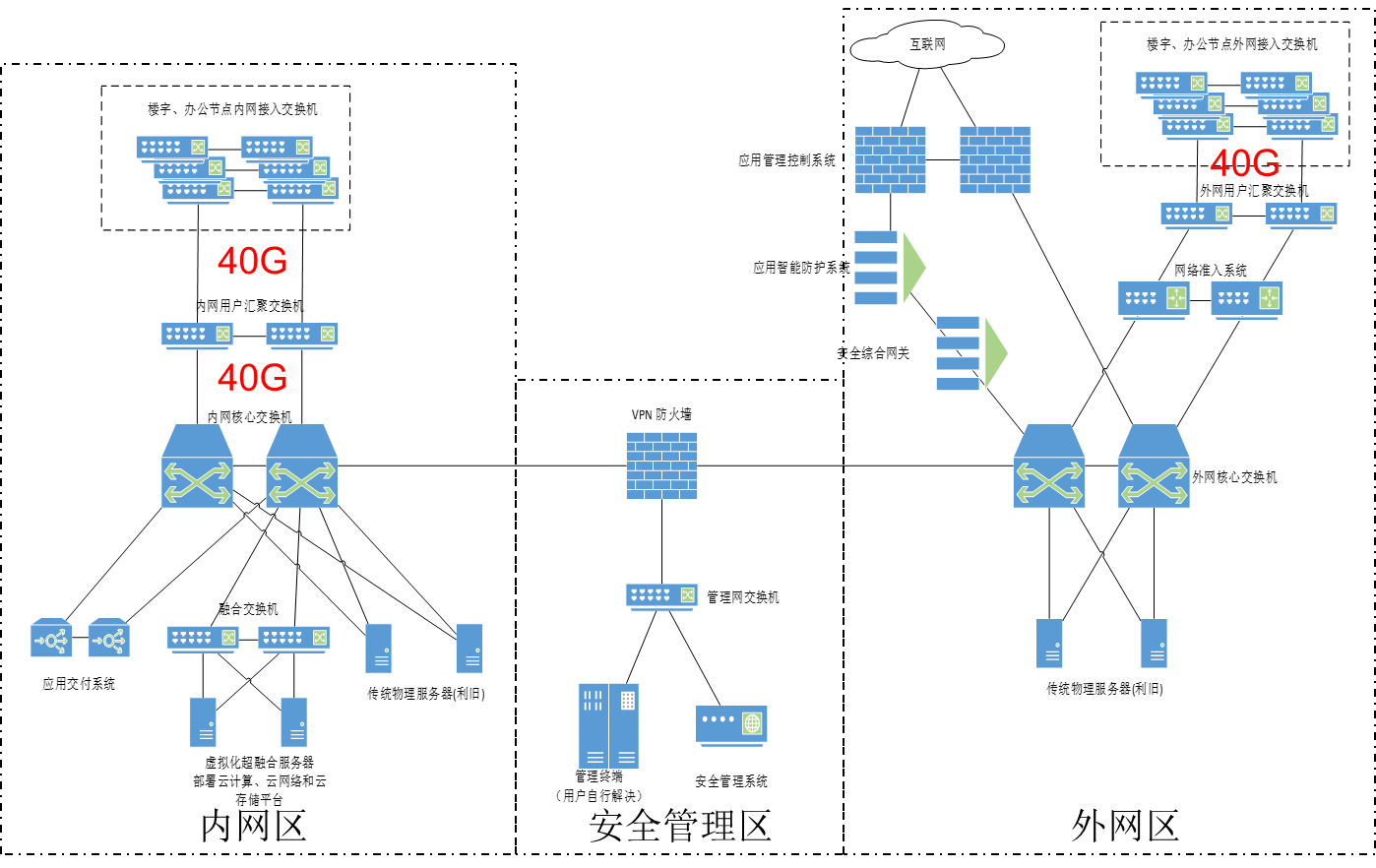


图4.1 整体网络规划设计图

终端管理子平台是由一系列功能互补的子平台及功能模块构成，如下：

### 4.1.2 整体设计目标

重新构架用户内、外网的主体结构并增加安全管理区。内网区域骨干互联从千兆升级到40G级别的互联链路以应对高清医疗图像、视频的实时传输。新增边界安全防护设备应对新的网络威胁。扩容融合计算集群来实现计算、网络和存储的虚拟化。

### 4.1.3 网络设计说明

基于医院现有的网络拓扑结构，根据业务保障原则，按照业务系统的不同将网络划分为不同的安全区域。按照“一个中心、三重防护”的设计思路。

通过将不同区域、不同层面的安全保护措施形成持续有效的安全保护体系，落实等级保护各方面的基本要求，最大程度发挥安全措施的保护能力。达到持续保护，不止合规的效果，构建防御+检测+响应的安全能力。

最终实现：满足国家政策要求，增强合规能力，优化医院信息化安全防御及管理；简单交付，大幅降低安全设备采购及运维成本。体现组织利益，让安全建设更简单；持续输送安全能力，改善患者就医体验，提高患者就医满意度，提升医院整体形象和竞争力。

核心网部分按照功能区域分为3个，分别是：管理核心区域、内网核心区域以及外网核心区域。

管理核心区域：该区域由2台管理接入交换机+管理边界防火墙构成。主要承载包括网络管理、数据库管理、主机管理、日志、监控、堡垒机、带外管理、网管监控等网络管理所需的业务系统。该处部署的系统特点是流量和吞吐量保证要求稍低，但是对安全性要求最高。所以从逻辑位置上位于距离互联网、用户终端的最深处。为了便于集中管理，该区域可设置部分与互联网完全断开的PC终端作为监控、告警、管理终端，通过这些终端可以对网络、系统、数据库进行相应的配置，查看安全数据，管理安全设备配置和策略。

内网核心区域：该区域由两台内网核心交换机+内网边界防火墙构成。主要承载院内包括HIS在内的各种业务、办公系统。系统上存储了院方工作的核心数据以及大量病人隐私数据。该区域对性能和稳定性的要求对用户来说都是重中之重，关键节点要具备双机自动容灾功能，且用户在访问该区域数据时需要通过多道安全设备管控，尽力防止病毒、黑客入侵等安全事件发生。

外网核心区域：该区域由两台外网核心交换机+外网边界防火墙构成。主要供医院内用户上网使用以及承载通过互联网面向公众的IT服务（如电子挂号等）。由于需要与互联网连接，为保证安全性，需要具有足够的安全设施并对用户的上网行为加以管控，必要时能够追溯用户上网行为（根据国家对于互联网使用的相关规定）。

## 4.2 平台安全加固服务

### 4.2.1 VLAN安全设计

* **控制广播**

VLAN之间是相互隔离的，所有的广播和多点广播都被限制在一个VLAN的范围内，即一个VLAN产生的广播信息不会被传播到其它的VLAN中，有效地防止了局域网上广播风暴的产生，提供了带宽的利用率。

* **提高安全性**

除了在重要边界部署防火墙、IPS、防病毒网关等设备进行安全控制外。

由于VLAN之间是相互隔离的，因此可将高安全性要求的主机服务器可划分到一个VLAN中，而其它VLAN的用户则不能访问它们。如果VLAN之间要进行通信则必需通过三层交换机才能完成，而三层交换机上具有访问控制（Access-List）以及防火墙等安全控制功能，因此VLAN之间的访问可以通过三层交换机进行控制。

* **提高性能**

通过VLAN的划分，可将需访问同一服务器/服务器组的用户放到同一个VLAN中，这样该VLAN内部的服务器只由本VLAN内的成员访问，其它VLAN的用户不会影响服务器的性能。

* **便于管理**

由于VLAN的划分是逻辑上的，因此用户不再受到物理位置的限制，任意位置的用户可以属于任意一个VLAN，VLAN内的成员可以任意地增加，修改和删除，使得网络管理更加简便易行。VLAN的划分可以有三种方式：By Port、By Protocol、By a User-Defined Value。

* **VLAN Routing**

每一个VLAN 都具有一个标识，不同的VLAN 标识亦不相同，交换机在数据链路层上可以识别不同的VLAN标识，但不能修改该VLAN标识，只有VLAN标识相同的端口才能形成桥接，数据链路层的连接才能建立，因而不同VLAN的设备在数据链路层上是无法连通的。VLAN Routing技术在网络层将VLAN标识进行转换，使得不同的VLAN间可以沟通，而此时基于网络层、传输层甚至应用层的安全控制手段都可运用，诸如Access-list（访问列表限制）等，VLAN Routing 技术使我们获得了对不同VLAN间数据流动的强有力控制。

### 4.2.2 防网络病毒设计

现在网络病毒对网络的冲击影响已经越来越大，如非常猖狂的红色代码（codered）、冲击波（MS Blaster）等网络病毒，所以有必要对网络病毒继续有效的控制。

### 4.2.3 防网络攻击设计

对网络中针对交换机的攻击和必须经过交换机的攻击进行安全加固，如以下几种攻击：

•MAC 攻击

•ARP攻击

•IP/MAC欺骗攻击

•STP攻击

•DoS/DDoS攻击

•IP扫描攻击

•网络设备管理安全

## 4.3 融合虚拟化容灾改造服务

### 4.3.1 融合虚拟化容灾改造设计

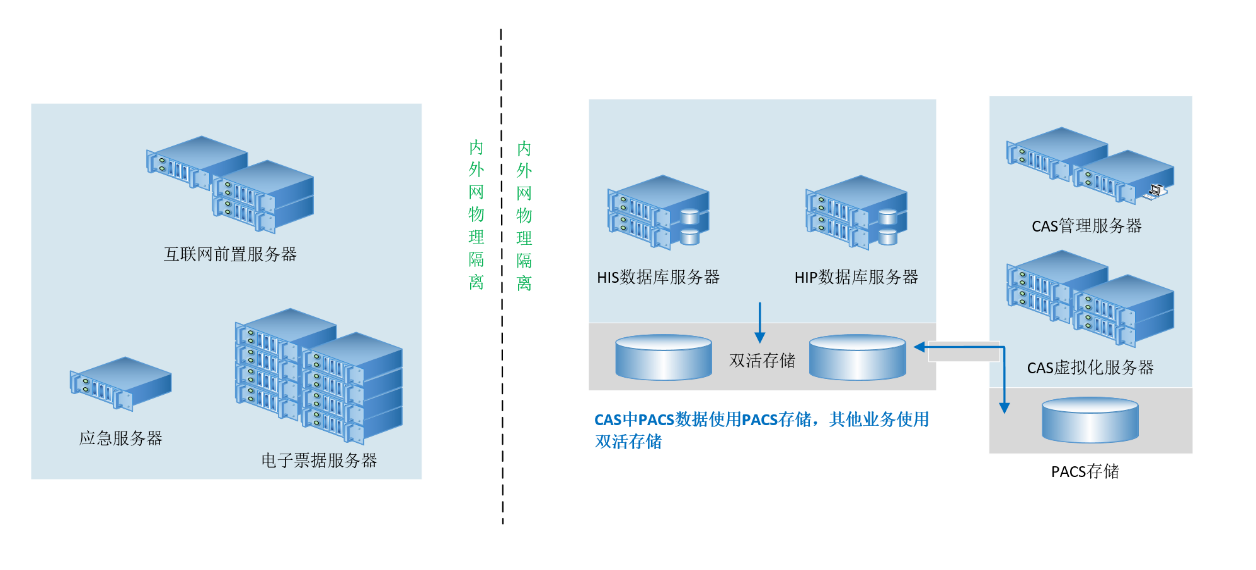


图4.2 改造前情况

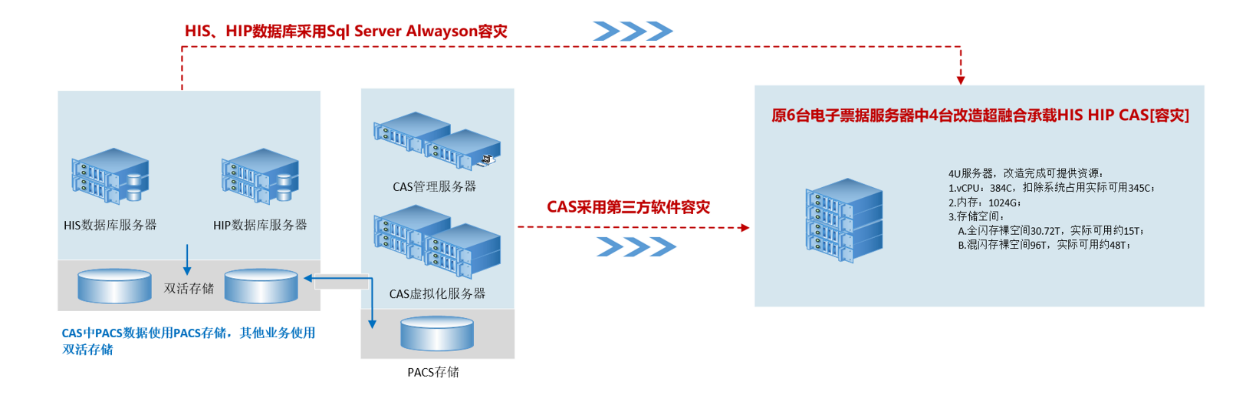


图4.3 改造设计

### 4.3.2 融合虚拟化容灾设计说明

* 容灾数据中心应采用先进的超融合技术进行建设，为业务提供本地化的多副本、备份、持续数据保护（CDP）、故障恢复（HA）、分布式集群的能力，并集成对平台资源使用情况、硬件健康状态的自动化检测机制，保证平台以及平台上的业务能够稳定运行。
* 备数据中心（BBB）按需保存有主数据中心（AAA）上业务的备份，并提供承载业务切换运行所需的计算、存储、网络、安全资源等IT基础架构服务，当主数据中心需要进行计划内维护，或者发生计划外中断时，能够在备数据中心上快速恢复业务；并在主数据中心恢复上线时，将业务从备数据中心快速回迁回来。
* 容灾切换之后，主数据中心的HIS、HIP数据库服务器、CAS平台虚拟机关机，备数据中心上的容灾备机接管业务并提供服务。
* 由于配置了地址转换，在容灾的切换前后，同一个业务在主、备数据中心无须修改IP。

## 4.4 智慧型医院升级服务

### 4.4.1 智慧型医院技术方案

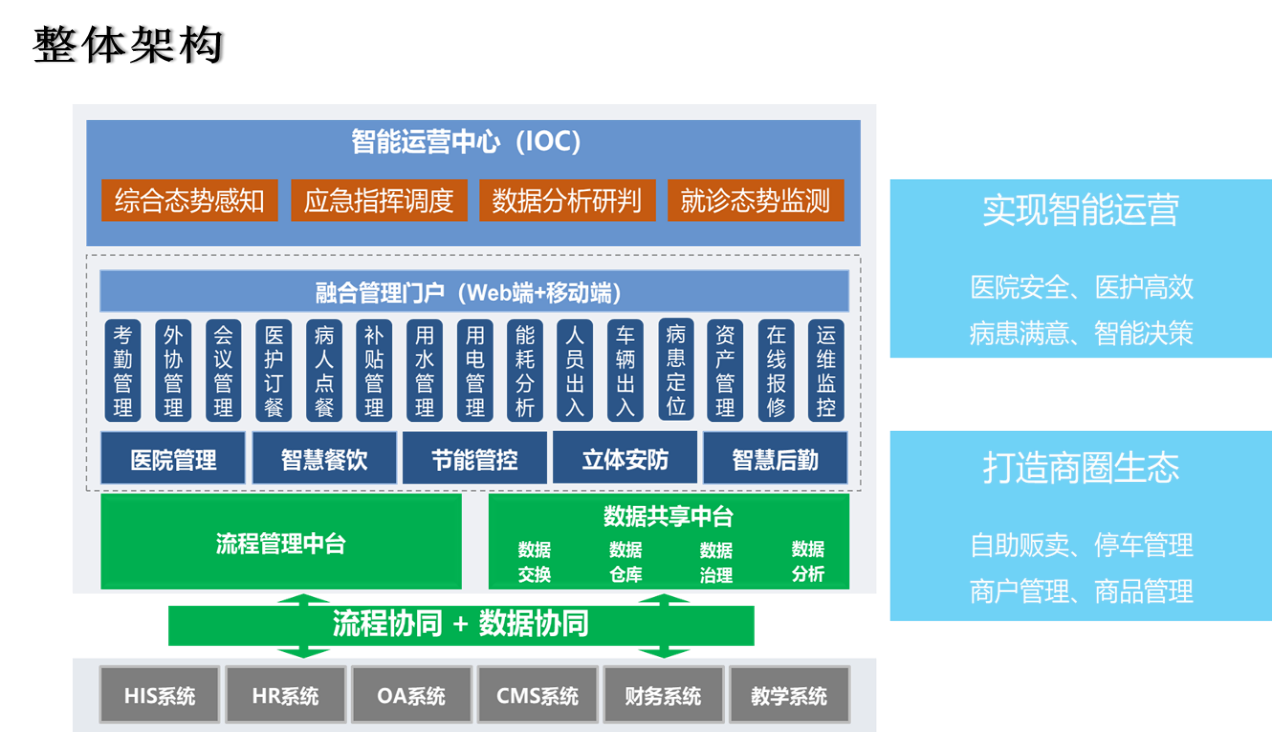


图4.4 智慧型医院整体设计

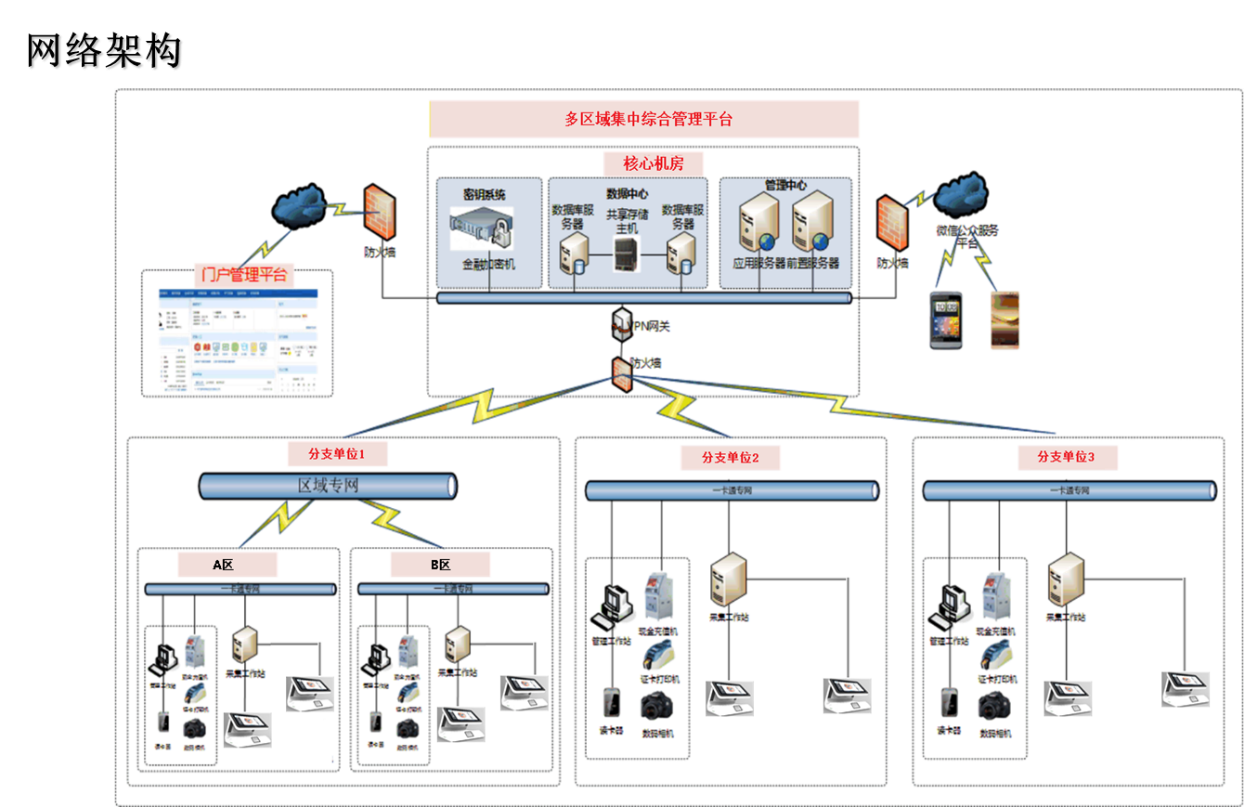


图4.5 智慧型医院网络架构设计

### 4.4.2 智慧型医院建设目标

* **集约化管理平台，实现平台一次建设、分院区复用、告别重复建设。**
* **多区域数据互联，互联互通。**

# 五、业务服务及性能要求

## 5.1 网络升级服务功能性要求

### 5.1.1 信息化性能要求

目前的网络已经不能满足医院日益增长的应用系统对性能和稳定性的需要，尤其是HIS/PACS等系统的对网络高稳定性和数据传输高带宽的需要。因此，网络中心在网络建设中，在网络接入信息点数的同时，需要通过全面的网络建设，在提升网络稳定性的同时，提高医院信息系统的使用性能，同时全面提升医院医疗服务水平。

### 5.1.2 网络融合性要求

本次网络系统建设是在原来的网络系统建设基础上进行全网的网络系统提升,同时,需要将分院网络通过高速的网络链路接入到主院网络系统中,实现医院应用系统的全面融合。

### 5.1.3 网络管理要求

本次外网建设采用可平滑升级至千兆的核心交换机，可通过冗余的方式来保证医院网络的高可靠性，并通过高端三层安全接入交换机，保证了对每个用户的三层业务进行终结，保证了网络区域精细化控制和简单的管理，使院门诊收费、挂号划价、医生工作站等系统能高速稳定的接入主院网络系统中。同时，由于网络设备的不断增加，给网络管理和网络维护带来了一定的难度，需要通过一套网络设备管理系统对整个网络系统内的设备应用情况和链路情况进行全面的查看、监控和管理。

### 5.1.3 稳定、可靠及扩展性要求

通过本次的网络建设,可将核心设备配置冗余管理引擎和冗余电源模块,保证了网络核心设备的高稳定性。同时，核心设备采用万兆路由交换机，提升了整个医院内部网络系统的性能，保证门诊收费、药品划价和门诊药房发药等系统的协调快速、准确运行，减少病人的等待时间，同时预留出今后的扩展空间。

## 5.2 网络升级服务性能要求

### 5.2.1 交换性能要求

聚合组数≥128组，每组成员≥8个，支持跨设备链路聚合，支持对广播、组播、单播报文的均匀分担，支持链路聚合+ECMP情况也可以对报文均匀分担，即等价路由的链路是由聚合链路组成情况下的报文分担。

双引擎快速倒换，主备切换时候板内转发无丢包 ，支持NSF/GR for OSFP/BGP/IS-IS，支持热补丁功能，可在线进行补丁升级，支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由，BFD收敛时间小于50ms，支持IP FRR，满足网络收敛小于50ms。

多虚一技术(N:1)，一虚多技术（1:N）技术配合使用。

支持安全业务插卡FW、IPS、NSM、ACG、LB、SSL VPN。

支持AC板卡，POE，POE+；支持有线无线一体化的终端准入认证。

支持多业务融合板卡，与设备紧耦合无需外部连线，支持部署Windows Server，实现方案与设备一体化部署。

支持L3 VPN，支持VLL，支持VLPS，支持MCE。

支持OPENFLOW。

支持主流的MAC in IP技术，如EVI/EVN/OTV等，实现跨三层网络的二层互联。

支持VxLAN 网关。

支持40G以太网光接口（QSFP+），支持扩展100G以太网光接口 (QSFP28 )；为了简便维护流程，需内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级。

### 5.2.2 接入性能要求

聚合组数≥128组，每组成员≥8个，支持跨设备链路聚合，支持对广播、组播、单播报文的均匀分担，支持链路聚合+ECMP情况也可以对报文均匀分担，即等价路由的链路是由聚合链路组成情况下的报文分担。

双引擎快速倒换，主备切换时候板内转发无丢包 ，支持NSF/GR for OSFP/BGP/IS-IS，支持热补丁功能，可在线进行补丁升级，支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由，BFD收敛时间小于50ms，支持IP FRR，满足网络收敛小于50ms。

多虚一技术(N:1)，一虚多技术（1:N）技术配合使用。

支持安全业务插卡FW、IPS、NSM、ACG、LB、SSL VPN。

支持AC板卡，POE，POE+；支持有线无线一体化的终端准入认证。

支持多业务融合板卡，与设备紧耦合无需外部连线，支持部署Windows Server，实现方案与设备一体化部署。

支持L3 VPN，支持VLL，支持VLPS，支持MCE。

支持OPENFLOW。

支持主流的MAC in IP技术，如EVI/EVN/OTV等，实现跨三层网络的二层互联。

支持VxLAN 网关。

支持40G以太网光接口（QSFP+），支持扩展100G以太网光接口 (QSFP28 )；为了简便维护流程，需内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级。

## 5.3 安全升级服务性能要求

要求满足≥200 SSL VPN用户数。

支持根据访问的国外URL请求进行链路调度，将对应的网站访问请求调度到指定线路，其中设备内置的国外URL网址库不少于900条并支持自动更新，管理员可查看并进行编辑。

支持对不同图片的传输优化技术，在不改变服务器端的图片源文件前提下实现自适应浏览器式的图片转换功能，例如转换为或其他格式，优化加速效果，提升web页面加载速度。

支持首页分析显示接入终端类型、带宽质量分析、实时流量排名、违规访问等行为风险情况，并可以将访问质量差的用户名单以列表形式展示、对单用户进行定向的访问质量检测。

能够与本次项目的安全管理系统进行联动，实现用户同步，以基于用户身份进行威胁分析。

分析系统支持对医院全网资产总览分析，包括资产概览、服务器运行状态、资产统计等，其中资产概览包括一周即将退库资产、全部资产数、核心资产数、资产组数、服务器数、终端数；并可以实现服务器之间的横向访问流量分析，包括TOP5应用流量趋势、TOP5协议趋势，其中服务器视角可展示服务器IP、源IP数量、协议端口TOP10、连接失败数、最大并发，并支持以表格形式导出数据。

从HTTP、DNS、SMTP、FTP、SMB、数据库协议等几十种覆盖黑客攻击和业务常用的网络协议的审计，并从中提取元数据组成相应的XFlow形式（如NetFlow、DnsFlow）传递给平台，便于对应XFlow、文件威胁检测分析引擎进行分析，对这些引擎可实现支持定期自动升级或离线手动升级。

支持针对用户认证的故障进行分析，给出错误详情以及处置建议，支持解密排障，自动检测解密审计不成功原因，包括客户端安装异常、证书安装异常、驱动异常、代理异常等类型，帮助管理员快速配置和修复。

无需安装客户端，通过流量状况检查9款以上主流杀毒软件的运行情况，对不满足检查要求的终端可重定向页面修复。

为建立医院的整体安全框架，快速响应、处置安全风险，要求网络准入系统与安全管理系统之前进行联动，实现接入网络的用户同步。

云计算系统支持虚拟机回收站功能，防止因虚拟机误删除导致数据丢失。

支持识别假死主机并标签化为亚健康主机，通过邮件或短信告警提醒用户进行处理，并限制重要业务在亚健康主机上运行，规避风险。

云计算管理平台支持扩展同一品牌的网络功能虚拟化、虚拟应用防火墙、虚拟应用负载均衡、虚拟数据库审计等功能组件，并支持统一管理，以保障平台的扩展性和兼容性。

支持对oracle、sqlserver、Weblogic数据库及中间件监控，实现对数据库的语句的故障定位排错，执行时延分析。

云存储系统可支持Oracle RAC，支持共享盘，及共享块设备，支持向导式安装，降低部署复杂度。

在3台服务器（E5-2680 v4 CPU，128GB，2块Intel S4600 SSD+6块HDD）硬件配置下，提供至少45万的IOPS。

## 5.4 融合虚拟化容灾服务功能性要求

### 5.5.1 建设原则

1.高性能

充分考虑系统的处理能力，使其整个系统在国内三到五年内保持领先的水平，并具有长足的发展能力，以适应容灾技术的发展。

2.高可靠性

为了进一步增强关键业务数据的抵御灾难能力，所以在设计阶段需要充分考虑其自身的稳定性和可靠性，从而保障关键数据能够持续、稳定的传送到备数据中心。当出现任何问题时都能够通过备份数据得以恢复。

3.可扩展性

当前设计不但应满足当前需要，还需充分考虑业务的发展，同时便于向更新技术的升级与衔接，保护当前投资。

4.可维护性

充分考虑易于管理，易于维护，操作简单，易学，易用，便于进行配置，发现故障。

5.安全性

由于承载的是关键业务系统的数据备份，所以设计需要考虑传输、存放等整个过程中的安全性。

6.高性价比

灾备系统建设首先要从系统的实用性角度出发，满足不同的业务系统的实际需要和前瞻性的同时，选择最高性价比的设计方案。

### 5.5.2 方案达成效果

* 支持业务运行手工灾备切换和业务自动访问切换。
* 应用恢复时间（RTO）：综合业务需要和容灾链路带宽、时延情况最低可达到1s
* 数据恢复时间点（RPO）：根据网络带宽，最低15分钟

## 5.5 融合虚拟化容灾服务性能要求

具备对虚拟机全生命周期管理的能力，可对虚拟机进行开关机、模板部署、克隆、导入导出等操作；具备HA、动态资源调度、蓝屏重启等机制保证业务高可靠；具备对虚拟机资源监控、告警等功能。

利用统一的管理平台对虚拟网络设备进行管理和配置。开通后实现”所画即所得“的网络部署，具备全局流量可视化、网络连通性检测等功能。为每个虚拟机提供一个3-4层的分布式防火墙和监控中心以及无限制的虚拟路由器和虚拟交换机，不开通只能创建1个虚拟路由器和2个虚拟交换机。

通过将硬盘资源池化提高资源利用率，利用智能条带化、分层、热点数据预测等技术提高存储性能。开通后支持创建虚拟存储卷，灵活配置存储策略（多副本、QoS等）；具备磁盘故障重建、硬盘亚健康检测等功能。

## 5.6要求的业务服务及性能技术参数要求如下：

|  |  |
| --- | --- |
| **核心部分** | **能力要求** |
| 内网核心交换能力 | （1）交换容量≥512Tbps，包转发率≥96000Mpps；主控板槽位数≥2，业务板槽位数≥8，竖插槽设备，交换网板槽位数≥5；需提供官网链接及截图证明，并加盖投标人公章  （2）实配主控引擎≥2，交换网板数量≥4；  （3）配置≥56个万兆光口，≥24个千兆电口，≥24个千兆光口；配置≥25个万兆单模光模块，≥20个万兆多模光模块，≥10个千兆单模光模块，≥10个千兆多模光模块，≥1根3米SFP+线缆  （4）支持40G高密板卡扩展，支持40G端口≥32个  （5）实际配置≥6个2500W交流电源  （6）正交CLOS架构，支持多级交换架构，能够配置独立的交换网板与独立的主控板，交换网板与主控板硬件槽位分离,需提供官网证明和实物正反面图片，指明槽位物理位置（垂直）关系，并加盖投标人公章  （7）严格前后风道设计，保证设备散热效果  （8）主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔  （9）单槽位能够同时提供千兆光口、千兆电口、万兆光口：且实际可用端口总数≥48，提高槽位利用率和业务可靠性，需提供官网链接及截图证明，并加盖投标人公章  （10）严格前后风道设计，保证设备散热效果  （11）多虚一技术，支持4框虚拟化技术，需提供第三方测试报告关键页证明，并加盖投标人公章  （12）支持多虚一技术和一虚多技术的配合使用  （13）支持Bras功能，能够实现PPPoE、IPoE接入认证方式，PPPoE和IPOE最大上线用户数可达10240个，需提供第三方测试报告关键页证明，并加盖投标人公章  （14）支持融合 AC 功能，无需额外配置单独硬件，在交换机上实现对AP 的接入控制和管理，有线无线用户的统一认证管理，最大 AP上线数量为 12K或配置独立的无线控制器设备，要求无线控制器可管理AP数≥12K，需提供第三方测试报告关键页证明，并加盖投标人公章  （15）★为保障兼容性，本次项目所有交换机设备需要为同一厂商 |
| 服务器区接入交换能力 | （1）交换容量≥307Tbps，包转发率≥57600Mpps；交换网槽位数≥2，业务板槽位数≥6；  （2）配置≥48个万兆光口，≥48个千兆电口，≥4个25G光口；  （3）配置≥30个万兆多模光模块，≥1根3米SFP+线缆  （4）实际配置≥2个650W交流电源  （5）以太网支持千兆电口，千兆光口，万兆光口、万兆电，25G端口、40G端口、100G端口，需提供官网链接及截图证明，并加盖投标人公章  （6）支持双引擎快速倒换，主备切换时候板内转发无丢包 ；  （7）支持 EPON OLT及10G EPON OLT接口，支持10G EPON 功能，支持10G 对称和非对称 ONU，需提供第三方测试报告关键页证明，并加盖投标人公章  （8）支持VXLAN，能够实现VXLAN二三层互通；  （9）支持原生无线 AC 功能：无需独立的AC板卡或带AC功能的接口板，即支持无线AP管理功能，需提供第三方测试报告关键页证明，并加盖投标人公章  （10）支持BFD，能够实现BFD与OSPF/VRRP联动。支持BFD 3ms最小探测间隔测试  （11）支持多虚一技术(N:1)，支持4框虚拟化技术  （12）支持FCoE功能  （13）支持主流的MAC in IP技术，如EVI，实现跨三层网络的二层互联  （14）支持VXLAN，能够实现VXLAN二三层互通  （15）支持BFD，能够实现BFD与OSPF/VRRP联动。支持BFD 3ms最小探测间隔测试  （16）支持内置智能图形化管理功能，能够实现通过图形化界面设备配置及命令一键下发和版本智能升级，需提供第三方测试报告关键页证明，并加盖投标人公章  （17）★为保障兼容性，本次项目所有交换机设备需要为同一厂商 |
| **接入网部分** | **参数要求** |
| 楼宇汇聚交换能力 | （1）交换容量≥25Tbps，包转发率≥1600Mpps；扩展插槽≥2，需提供官网链接及截图证明，并加盖投标人公章  （2）固化≥48个万兆光口，≥2个40G光口；  （3）配置≥4个万兆多模光模块，≥44个万兆单模光模块，≥1根3米SFP+线缆  （4）≥2个250W交流电源，冗余风扇  （5）为了满足不同的上行互联要求，建议所投设备为双插槽设计，可扩展支持万兆光、万兆多速率电、25G、40G等多种类型板卡，需提供官网链接及截图证明，并加盖投标人公章  （5）考虑到园区网络的安全性，要求设备支持安全插卡保障园区的业务安全可靠的运行；  （6）要求支持ERPS功能，并且收敛时间小于50ms；  （7）实现CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作；  （8）支持内置智能图形化管理功能，能够实现通过图形化界面设备配置及命令一键下发和版本智能升级，需提供官网链接及截图证明，并加盖投标人公章  （9）支持802.1ae Macsec安全加密，实现MAC层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验；  （10）★为保障兼容性，本次项目所有交换机设备需要为同一厂商 |
| 用户接入交换能力 | （1）交换容量≥4.3Tbps，包转发率≥166Mpps；  （2）固化≥48个千兆电口，≥4个万兆光口；  （3）配置≥4个万兆单模光模块  （4） 实现ERPS功能，能够快速阻断环路，链路收敛时间≤50ms；  （5）实现CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作；  （6）可配合上端管理设备实现整网拓扑可视，无需再额外配置网管平台，以设备内置及图形化操作的方式，实现对网络的统一运维及管理，需提供官网链接及截图证明，并加盖投标人公章  （7） 支持最多8个端口聚合；支持最多128个聚合组（IRF2）；支持LACP；  （8）设备可与云平台交换机连接管理，支持蓝牙连接管理，需提供第三方测试报告关键页证明，并加盖投标人公章  （9）支持端口休眠，关闭没有应用的端口，节省能源；  （10）★为保障兼容性，本次项目所有交换机设备需要为同一厂商 |
| 用户接入交换能力 | （1）交换容量≥3.3Tbps，包转发率≥126Mpps；  （2）固化≥24个千兆电口，≥4个万兆光口；  （3）配置≥4个万兆单模光模块  （4） 实现ERPS功能，能够快速阻断环路，链路收敛时间≤50ms；  （5）实现CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作；  （6）可配合上端管理设备实现整网拓扑可视，无需再额外配置网管平台，以设备内置及图形化操作的方式，实现对网络的统一运维及管理，需提供官网链接及截图证明，并加盖投标人公章  （7） 支持最多8个端口聚合；支持最多128个聚合组（IRF2）；支持LACP；  （8）设备可与云平台交换机连接管理，支持蓝牙连接管理，需提供第三方测试报告关键页证明，并加盖投标人公章  （9）支持端口休眠，关闭没有应用的端口，节省能源；  （10）★为保障兼容性，本次项目所有交换机设备需要为同一厂商 |
| 网管能力 | （1）软硬一体化设备，硬件一体化专用设备，外观尺寸2U，支持旁路部署； 单路Intel 至强嵌入式CPU ，≥8核，内存≥32G，存储空间不少于1TB，支持RAID1；配置≥2个千兆自适应电口，支持≥4个端口扩展插槽；1+1冗余双电源。配置150点网络设备管理授权  （2）网管平台采取B/S结构，无需在客户端安装任何客户端，采用浏览器即可访问网管平台  （3）要求资源拓扑、告警、性能等功能模块支持多服务器分布式虚拟化部署，可实现负载分担，满足大规模网络环境的统一管理。单套软件可管理的节点数可达15000个  （4）能够对网络中的未知设备、未知端点、未产生流量的端点主动发现。包括但不限于交换机、路由器、防火墙、服务器、PC终端、打印机、摄像头、配电终端、RSU等等。  （5）能够自动识别非法私接、仿冒的端点，并实时告警，告警方式包括但不限于：大屏、短信、邮件、手机APP；同时能够主动将非法端点加入黑名单，阻断非法终端的接入  （6）支持网络管理平台实现设备管理与流量分析联动，如通过点击拓扑某链路可查看该链路的关键应用流量分布、关键用户流量使用等，需提供设备功能截图证明并加盖投标人公章  （7）支持设备面板的显示、定时刷新、面板缩放功能，通过面板管理，网络管理人员可以直观地看到设备、板卡、端口的工作状态；并提供基于设备面板的设备、单板、端口配置功能，需提供设备功能截图证明并加盖投标人公章  （8）支持设备配置集中管理：配置库包括配置文件和配置片断，配置内容可带有参数，在部署时根据设备的差异设置不同的值；配置文件可部署到设备的启动配置或者运行配置；配置片断只能部署到设备的运行配置  （9）支持VLAN拓扑，VLAN拓扑功能以可视的方式对网络中的VLAN资源进行管理，查看拓扑视图中所有设备节点和链路是否允许某个特定VLAN通过，需提供设备功能截图证明并加盖投标人公章  （10）提供多种报表样式，包括普通的行列报表、主/子报表、图形摘要报表、交叉表、TopN和BottomN报表。支持多种图形展示：包括条形图、饼图、曲线图、甘特图、面积图、圆环图、三维梯形图、三维曲面图、XY 散点图、雷达图、气泡图、股票图、漏斗图等  （11）支持超长离线设备自动删除，可设置离线删除时间，需提供设备功能截图证明并加盖投标人公章  （12）支持合规检查功能：通过关联合规策略和待检查的设备，迅速检查出违反合规策略的设备。检查的结果将通过丰富的表现形式进行展现，同时提供修复功能，可以及时解决在网络环境中出现的配置、安全问题。 |

|  |  |
| --- | --- |
| **安全及虚拟化部分** | **能力要求** |
| 漏洞扫描能力 | 1、系统漏扫授权IP数≥100，WEB漏扫授权URL数≥20，主机漏扫最大并发IP数≥75。1U设备，内存大小≥8G，硬盘容量≥128GB SSD+ 1TB SATA，单电源，≥6千兆电口+2千兆光口SFP。包含三年硬件质保及软件升级服务。  2、支持全局风险统计时段自定义，展示近3个月、6个月、1年或自定义统计区间的风险分布和详情，时间跨度不限制。  3、支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情。  4、支持从“高危”、“中危”、“低危”、“安全”四个安全级别展示资产的风险分布情况。  5、支持从紧急漏洞的视角展示主机风险，清晰呈现已发生和未发生的紧急漏洞类型，支持以报表形式展示紧急漏洞的风险等级、影响资产数、漏洞数量、最近发现时间，可关联漏洞详情。  6、支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行。  7、资产发现支持并发扫描数量自定义，最大并发扫描IP数为1024。  ★8、支持域管理功能，系统默认内置数据域、终端接入域、运维管理域等九个域，可根据客户实际情况进行自定义管理。（要求提供功能截图并加盖投标人公章）  9、支持白名单管理，自定义匹配与手动两种方式，白名单里的IP允许接入合规自检平台。  ★10、提供检测结果综述分析，按照等保2.0的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况。（要求提供功能截图并加盖投标人公章）  11、系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果支持报表导出的格式包括HTML、WORD、EXCEL等格式。  12、要求漏洞扫描系统支持等保资产登记功能，包括但不限于物理机房、网络设备、安全设备、服务器或存储设备、终端、系统管理软件或平台、业务应用系统或平台、关键数据类型、大数据数据类别、安全相关人员、管理文档、安全文档等12类资产进行资产登记。  13、要求漏洞扫描系统支持域管理功能，系统默认内置数据域、终端接入域、运维管理域等九个域，可根据客户实际情况进行自定义管理。（要求提供功能截图并加盖投标人公章）  14、要求漏洞扫描系统提供检测结果综述分析，按照等保2.0的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况。（要求提供功能截图并加盖投标人公章）  15、要求漏洞扫描系统按“一个中心、三重防护”的架构展示检测结果，每个检测结果呈现具体问题及整改建议，系统支持手动核查确认、整改后重新检测、以及手动导入全局分析和人工核查报告来对测评报告中的结果进行核查确认，其中手动核查确认支持单项核查确认和批量核查确认。（要求提供功能截图并加盖投标人公章）  16、要求设备厂商软件开发必须通过CMMI5级认证，要求提供证书，CMMI官方可查询并提供网站截图。 |
| 业务防护能力 | 1、网络层吞吐量≥25G，应用层吞吐量≥9G，并发连接数≥220万，HTTP新建连接数≥20万，IPSec最大隧道数≥1000，IPSec VPN吞吐量≥450M，IPSec VPN加密速度≥650M。2U设备，内存大小≥8G，硬盘容量≥64G MSATA+1T SATA，冗余电源，≥6千兆电口+2万兆光口SFP+，包含2个万兆光模块，提供至少三年特征库升级服务、产品质保服务和软件升级服务。  2、支持识别HTTP异常，包含HTTP方法过滤、HTTP头部字段Referer、User-Agent等注入检测、Host检测、URL溢出检测、POST实体溢出检测、HTTP头部溢出检测、range字段防护、multipart头部字段异常检测、Content-Type头部字段异常检测。  ★3、支持超过3700种Web应用防护规则。支持防护SQL注入、XSS攻击、网页木马、网站扫描、Webshell、跨站请求伪造（CSRF）、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web漏洞攻击等。  4、支持口令暴力破解防护，至少包含FTP、Web、Weblogic、Zabbix、Wordpress、Tomcat等组件，并支持自定义FTP和Web的爆破阈值设置。  5、支持自定义Web应用防护规则，通过基于正则表达式自定义规则匹配方向、动作、字符串、危险等级、动作、攻击影响、描述等。（需提供产品功能截图证明并加盖投标人公章）  6、支持业务模型学习监督功能，通过智能分析引擎对业务流量进行分析学习，建立用户业务特征模型，解决因WEB应用中因代码不规范和安全检测功能冲突导致的业务误判问题。  7、支持漏洞防扫描，包括404页面检测、WAF规则拦截频率检测、目录访问频率检测、使用不常见的HTTP请求方法、匹配强弱规则扫描、敏感文件扫描等扫描行为特征，支持自定义封锁扫描IP封锁时间、支持隐藏服务器信息。  8、支持网站防篡改功能，支持Windows和Linux双平台操作系统，防止攻击者篡改文件系统。  9、支持Web权限控制，支持自定义文件上传类型过滤，防止通过修改文件后缀名绕过检测。  10、支持受限URL防护，仅允许从自定义的起始页面开始访问网站。  11、支持CC攻击防护，支持自定义来源IP、Referer防CC的次数限制、检测时间和出发阈值，支持特定URL防CC次数限制和检测时间。  ★12、支持针对业务风险汇总，支持展示业务安全状态分布，包括已失陷业务、正在遭受攻击的业务、存在漏洞但暂时未被攻击的业务，以及最近7天内的漏洞风险分布情况。（需提供产品功能截图证明并加盖投标人公章）  13、支持对检测到的攻击行为按照IP地址的地理位置信息进行威胁信息动态投屏展示，实时监测和展示最新的攻击威胁信息。并具备未知威胁检测功能，要求提供未知威胁检测的证书或检测报告。  14、产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。（需提供产品功能截图证明并加盖投标人公章）  15、支持与安全态势感知产品实现联动，Web应用防火墙支持以专属方式对接同品牌态势感知系统，供态势感知系统进行深度关联分析。（需提供产品功能截图证明并加盖投标人公章）  16、要求所投产品具备IT产品信息安全认证证书EAL4增强级，提供有效证书复印件并加盖投标人公章。  17、要求设备厂商软件开发必须通过CMMI5级认证，要求提供证书，CMMI官方可查询并提供网站截图。 |
| 流量采集能力 | 1、吞吐性能≥1Gbps，1U设备，内存大小≥8G，硬盘容量≥64G minisata SSD，单电源，至少6千兆电口+2千兆光口SFP，至少2个万兆光模块，提供至少三年特征库升级服务、三年硬件质保和软件升级服务。  ★2、旁路部署，为保障数据传输的对接，与态势感知平台为同一品牌，支持探针接入单位网络镜像口，每个接口相互独立且不影响。（需提供证明材料并加盖投标人公章）  3、具备主动发送少量探测报文，发现单位潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。  4、支持SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web整站系统漏洞等网站攻击检测。  5、支持对敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤（需提供产品功能截图证明并加盖投标人公章）  6、支持Application漏洞攻击、File漏洞攻击、Scan漏洞攻击、Shellcode漏洞攻击、System漏洞利用攻击、Web Activex等客户端漏洞攻击检测。  7、支持HTTP未知站点下载可执行文件、浏览最近30天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC通信等僵尸网络行为检测。  8、支持包含标准模式、精简模式、高级模式、局域网模式、自定义模式等5种或5种以上类型日志传输模式，适应不同应用场景需求（需提供产品功能截图证明并加盖投标人公章）。  9、支持传输协议审计日志，包括https协议日志、http协议审计日志、DNS协议审计日志、邮件协议审计日志、SMB协议审计日志、、FTP协议审计日志、Telnet协议审计日志、ICMP协议审计日志、LLMNR协议审计日志。  10、支持对单位IP、IP组、服务、端口、访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式。  ★11、内置URL库、IPS漏洞特征识别库、应用识别库、WEB应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。（需提供产品功能截图证明并加盖投标人公章）  12、要求设备厂商软件开发必须通过CMMI5级认证，要求提供证书，CMMI官方可查询并提供网站截图。 |
| 安全管理能力 | 1、存储容量≥14.4T，内存≥64GB，系统盘≥128GB，数据盘≥16TB，标配盘位数≥8，单电源，至少4千兆电口，提供至少三年特征库升级服务、产品质保服务和软件升级服务。  2、支持大屏展示综合安全态势，包括资产态势、脆弱性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势、设备运行态势；支持页面跳转到对应态势大屏，并具备大屏告警能力；  ★3、支持大屏展示业务脆弱性态势，包括漏洞风险态势、漏洞类型TOP5、高危漏洞TOP5、业务总览、脆弱性业务TOP5、实时脆弱性监测（需提供产品功能截图证明并加盖投标人公章）。  4、支持3D地球大屏展示网络攻击态势，包括攻击次数、遭受攻击资产组、攻击源地址、攻击源IP、攻击手段排行、遭受攻击服务器排行；支持境外、境内切换（需提供产品功能截图证明并加盖投标人公章）。  5、支持不同视角展示全网安全态势，包括综合安全态势、分支安全态势、安全事件态势、网络攻击态势、外连风险态势、横向威胁态势、脆弱性态势、资产态势、正常横向访问监控态势、正常外连监控态势、设备运行态势等13个独立的大屏展示功能；支持大屏轮播，可自定义播放顺序（需提供产品功能截图证明并加盖投标人公章）。  6、支持对全网资产总览分析，包括资产概览、服务器运行状态、资产统计，其中资产概览包括7天即将退库资产、全部资产数、核心资产数、资产组数、服务器数、终端数；服务器运行包括服务器离线TOP5、服务器开放端口TOP10、服务器应用TOP5；资产统计包括资产组TOP5、资产来源TOP5、设备类型TOP5、操作系统分布、7天内即将退库资产；  7、支持对资产信息查询、编辑与管理，资产信息包括资产类型，地理位置、责任人、审核状态、主机名、操作系统、域名、服务与端口、应用、制造商、设备型号、厂商序列号、来源设备等。  8、支持流量实时识别与主动扫描资产，可联动扫描器定期或立即扫描资产，支持自定义扫描IP地址、网段、URL。  9、支持北信源、远望科技等第三方资产数据源对接，接入方式支持Webservice、SQL Server等方式，同时可手工导出与导入资产；  ★10、支持检测业务服务器的配置不当，检测内容包括服务器、所属业务、所属分支、配置不当类型、风险等级、发现时间等；支持配置不当类型下钻，展示配置不当详情，提供解决方案和数据包举证，并支持导出配置不当报告（需提供产品功能截图证明并加盖投标人公章）。  11、支持安全域维度展示安全风险，包括安全域列表、安全域评分、事件类型TOP5、IP地址、IP类型、风险等级、关键风险。  12、支持横向威胁分析，包括横向威胁总览、横向攻击、违规访问、可疑行为、风险；其中横向风险总览包括发起横向威胁主机TOP5、遭受横向威胁TOP5、横向威胁类型分布、横向威胁趋势。  13、支持威胁情报关联分析，内置威胁情报数量不少于150W；支持展示威胁情报命中数、今日命中数、命中威胁情报类别TOP10、命中趋势、活跃威胁情报TOP20等。  14、持多维度模糊聚类算法将大量外部攻击日志聚合成少量攻击事件，聚合维度包括攻击IP、攻击地址、攻击目标和目标手法。  15、平台内置挖矿安全知识库，对常见的挖矿如：Bluehero挖矿蠕虫变种、虚拟货币挖矿、EnMiner挖矿病毒、PowerGhost挖矿病毒、DDG挖矿病毒、Docker挖矿、DDG挖矿变种、GroksterMiner挖矿病毒、Linux 挖矿木马、ZombieBoy挖矿木马等提供详细的背景介绍、感染现象、详细分析、相关IOC（MD5、C2、URL）解决方案。（需提供产品功能截图证明并加盖投标人公章）。  16、支持安全检测日志、审计日志、第三方日志存储；日志类型包括漏洞利用攻击、网站攻击、僵尸网络、业务弱点、DOS攻击、邮件安全、文件安全、网络流量、DNS、HTTP、用户、数据库、文件审计、POP3、SMTP、IMAP、LDAP、FTP、Telnet等。  ★17、支持780种以上安全设备、网络设备、DHCP服务器、蜜罐、中间件等设备日志接入，支持syslog、winlogbeat、jdbc、wmi、webservice、ftp、snmp trap等接入方式（需提供产品功能截图证明并加盖投标人公章）。  18、支持溯源快速搜索功能，通过输入攻击者IP和受害者IP即可检索失陷主机溯源结果和攻击者画像信息，其中攻击者画像以攻击者视角整合多源数据，对攻击者的攻击过程、攻击手段、攻击工具、攻击趋势等信息进行展示，以及以时间轴的方式展示攻击者的所有入侵/访问历史痕迹等。  19、弱密码检测技术基于UEBA学习技术（无监督自我学习）提取登陆成功的特征，通过UEBA技术对响应体内容和登录跳转路径进行持续学习训练登录成功特征，包括响应体内容Json、响应体关键字Keyword、响应体MD5值、响应体长度Length、登录跳转路径Location，可实时自动生成学习到的登陆成功规则。（需提供产品功能截图证明并加盖投标人公章）。  20、支持自动化编排响应处置手段，包括联动封锁、访问控制、上网提醒、冻结账号、一键查杀、进程取证，可识别平台已对接的安全设备，自动推荐联动策略（需提供产品功能截图证明并加盖投标人公章）。  21、支持已合规基线管控业务安全，实时监测等保差距项和高风险项，避免策略变更导致不合规，有效应对网监不定期抽查和复测场景。（需提供截图证明并加盖原投标人公章） |
| 互联网防护能力 | 1、网络层吞吐量≥12G，应用层吞吐量≥4.4G，并发连接数≥200万，HTTP新建连接数≥8万，IPSec最大隧道数≥1000，IPSec VPN吞吐量≥250M。1U设备，内存大小≥8G，硬盘容量≥64G minisata SSD，单电源，≥6千兆电口+2千兆光口SFP，提供至少三年特征库升级服务、产品质保服务和软件升级服务。  2、支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求，支持主主、主备两种双机模式部署。  3、具备链路故障检测功能，通过ARP、DNS、PING协议等方式检测目标主机的可达性，确认接口链路是否有效，并可自定义检测频率。  4、支持IPv4／IPv6下NAT地址转换，包括支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT， 支持一对一、一对多、多对一等多种转换方式。  5、支持IPv6环境的应用控制策略设置，能针对IPv6的IP地址、服务端口、区域等条件进行应用访问规则的设置。  6、产品内置应用特征识别库，支持不少于10000种应用规则，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制。  7、支持基于对象、地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。  8、支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。  9、支持TearDrop 攻击、IP数据块分片传输、Land攻击、Smurf攻击、WinNuke攻击、超大ICMP数据攻击等异常报文攻击防护，支持IP协议异常报文和TCP协议异常报文攻击防护。  10、支持对HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP协议进行病毒检测和查杀，支持最大14层的压缩文件查杀。（需提供产品功能截图证明并加盖投标人公章）  ★11、支持与云端联动对未知文件进行检测，在设备界面显示云端检测结果。（需提供产品功能截图证明并加盖投标人公章）  12、具备勒索软件通信防护功能，提供由第三方权威机构关于“勒索软件通信防护”产品功能检测报告并加盖投标人公章。  13、产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则。  14、具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。  ★15、产品支持与本方案中网络防病毒系统联动管理，通过防火墙产品界面完成网络中的网络防病毒系统的安全策略统一管控，实现终端病毒查杀功能。（需提供产品功能截图证明并加盖投标人公章）  16、支持在单条安全策略中可同时启用入侵防御、防病毒、URL过滤、文件过滤。  17、支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。  18、支持针对业务攻击事件汇总，展示攻击事件类型TOP5及当前业务命中的全网实时热点事件，支持通过地图区域颜色深浅展示攻击者的分布与数量。  19、★支持在产品漏洞特征库中以漏洞名称、漏洞ID、漏洞CVE标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，预定义漏洞特征数量超过7650种，并可以支持僵尸主机检测功能，预定义特征库超过110万种，可识别主机的异常外联行为。（需提供产品功能截图证明并加盖投标人公章）  20、产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。（需提供产品功能截图证明并加盖投标人公章）  21、要求所投产品具备IT产品信息安全认证证书EAL4增强级，提供有效证书复印件并加盖投标人公章。 |
| 互联网接入区应用管理控制能力 | 1、网络层吞吐量（大包）≥8Gb，应用层吞吐量≥1.1Gb，带宽性能≥750Mb，IPSEC VPN加密性能≥150Mb，支持用户数≥5000，包转发率≥108Kpps，每秒新建连接数≥12000，最大并发连接数≥500000。1U设备，内存大小≥4G，硬盘容量≥1T SATA，单电源，≥6千兆电口+2万兆光口SFP+。提供至少三年特征库升级服务、产品质保服务和软件升级服务。  2、支持网关、网桥、旁路部署模式，支持网桥模式，以透明方式串接在网络中；支持电口bypass；必须支持多路桥接功能，最多可支持32组网桥模式；  3、支持DNS透明代理，能够基于用户、域名、目标DNS，指定代理策略生效，代理策略可以设置为：重定向至DNS服务器、解析为IP、丢弃、重定向至制定线路；  ★4、设备内置应用识别规则库，支持超过10000条应用规则数，支持超过6500种以上的应用，并保持每月更新至少2次，保证应用识别的准确率，支持标签化选择管理应用，并可以提供应用的定义和解释帮助标签化管理，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类。（需提供产品功能截图证明并加盖投标人公章）  5、支持首页分析显示接入用户人数、终端类型、认证方式；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况；  6、实时提供用户流量排名、应用流量排名、所有线路应用流速趋势、流量管理状态、连接监控信息；  7、提供图形化排障工具，便于管理员排查策略错误等故障;  8、具备用户密码安全性功能，可设置用户密码置密码最小长度，可设置密码必须包括数字或字母或特殊字符，可设置用户密码不能等于用户名，新密码不能与旧密码相同;  9、支持为用户添加自定义属性（职位、临时项目组、邮件组等），能够根据用户属性自动归类并可以针对用户属性配置上网权限策略、流控策略，审计策略等;  10、支持认证页面分权分域管理。启用后，普通管理员只能看到自己有权限的页面，其他管理员页面不可见。 系统管理员可以将某个页面授权给指定的普通管理员管理;  ★11、支持radius、AD、POP3、Proxy、PPPOE、 H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作，可强制指定用户、指定IP段的用户必须使用单点登录。（需提供产品功能截图证明并加盖投标人公章）  12、支持通过OAuth认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证；用户通过企业微信、MOA、钉钉认证上线，本地会创建与认证服务器上对应的用户组，用户会上线到对应创建的组；（需提供产品功能截图证明并加盖投标人公章）  13、支持终端分类可视功能，对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等，支持查看终端类型，以及终端详细信息（厂商，系统，端口等），支持查看终端类型分布;  14、支持检查终端是否运行指定经常，对不满足检查要求的终端可弹窗提示、禁止上网，可强制中止违规进程；  15、支持非法外联检查与外联管控功能，支持检查终端是否使用非法网关（可设置合法网关白名单），对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户。支持设置终端访问地址白名单和黑名单，写入终端防火墙ACL策略，实现强访问管控。（需提供产品功能截图证明并加盖投标人公章）  16、支持审计用户的Webmail邮件外发行为，支持webmail形式发送的附件审计，并能精准到原始邮件。  17、支持加密邮件过滤功能，支持对加密HTTPS、SMTP-SSL、SMTP的邮件进行关键字过滤，基于关键字、发件人地址等识别和过滤使用邮件客户端外发SSL加密邮件的行为。（需提供产品功能截图证明并加盖投标人公章）  18、支持Teamviewer、向日葵、Anydesk、RDP的远程应用的外发文件审计，（需提供产品功能截图证明并加盖投标人公章）  19、支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义。（需提供产品功能截图证明并加盖投标人公章）  20、要求上网行为管理是国家标准《信息安全技术信息系统安全审计产品 技术要求和测试评价方法》的主要起草单位，提供证书复印件并加盖投标人公章。 |
| 外网应用区应用智能防护能力 | 1.1U含交流双电源，2\*USB接口，1\*RJ45串口，1\*RJ45管理口，4\*GE电口(Bypass)。1个接口扩展槽位,最大支持8路防护。  2.网络吞吐量≥3G  3.事务处理能力（TPS≥0000  4.支持设备集中管理能力，包括策略集中下发、设备集中监控、批量升级等，满足大规模部署环境  5.支持对SSL（HTTPS）加密会话进行分析。  6.支持对HTTP协议的异常元素、异常参数、非法编码和解码的灵活控制与处理。（提供截图证明文件）  7.支持针对主流Web服务器及插件的已知漏洞防护。Web服务器应覆盖主流服务器：apache、tomcat、lighttpd、NGINX、IIS等；插件应覆盖：dedecms、phpmuadmin、PHPWind、shopex、discuz、echsop、vbulletin、wordpress等。  8.支持对注入、XSS、SSI指令、Webshell防护、路径穿越及远程文件包含的攻击防护。（提供截图证明文件）  9.支持CSRF（跨站请求伪造）防护。  10.支持爬虫防护，实现对100种以上的爬虫特征进行识别和阻断，防止页面因爬虫而引起信息泄露等问题。  11.支持盗链防护，有效识别网页盗链行为，避免用户网页资源被滥用。  12.支持扫描防护，应至少包括阈值告警、请求量统计、应答分布统计等防护手段  13.支持URL ACL。对多种HTTP方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE等。  14.支持TCP Flood防护和HTTP Flood防护，并说明HTTP Flood防护的检测算法。  15.支持XML防护，包括XML基础校验、Schema校验以及SOAP校验。（提供截图证明文件）  16.支持基于五元组（源IP地址、目的IP地址、源端口、目的源口、协议类型）及接口的网络防火墙功能。（提供截图证明文件）  17.产品厂家具备国家信息安全测评信息安全服务资质证书-安全工程类（三级>二级>一级），（提供相关证明材料）  18.产品厂家具备微软MAPP计划合作伙伴。（提供相关证明材料） |
| 专网接入区安全综合网关能力 | 1.1U机型，含交流单电源，1\*RJ45串口，1\*RJ45管理口，2\*USB接口，6\*GE电口（Bypass）,4\*SFP光口，2个接口扩展槽位，256G固态硬盘，1T机械硬盘  2.系统吞吐≥4Gbps  3.最大并发≥200万  4.每秒新建会话≥5万  5.支持虚拟线、二层透明、路由、混合、旁路监听、PPPoE等接入方式，适应各种网络环境需求。  6.支持IPMAC绑定，支持手动和自动探测绑定  7.支持基于策略的双向NAT、动态/静态NAT、端口PAT。  8.支持应用过滤器，至少支持4个维度进行过滤，比如：应用类别、实现技术、风险等级、标签，请截图证明  9.可自定义操作系统、浏览器、杀毒软件的风险等级，并支持预置风险等级。可提供截图  10.可为每个内网主机生成风险指数，通过数字直观展示内网主机的风险状态。可提供截图  11.在事件关联分析中，可以设置自定义应用、目的IP、源IP，即使不在TOPN里面，同样可以进行统计及数据挖掘，请截图证明  12.支持基于IPv6的访问控制，并可灵活配置。  13.支持对1500+ 种应用平台及2200+种的应用进行识别和控制，至少支持5大类，比如：商业系统、协作应用、一般网络应用、媒体等及28子类，比如：认证服务、数据库、ERP-CRM、软件更新、电子邮件、VOIP视频、游戏等；支持自定义应用；  14.web服务器防护模板规则数量需要超过2000条  15.支持对入侵规则库的分类组织和管理，包括：攻击手段/技术/流行度/危险度/服务类型  16.支持木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的查杀  17.支持文件名称、类型及病毒名称的白名单，请截图证明；  18.可支持以文件扫描方式查杀病毒，请截图证明；  19.产品厂家具备国家信息安全测评信息安全服务资质证书-安全工程类（三级>二级>一级），（提供相关证明材料）  20.产品厂家具备微软MAPP计划合作伙伴。（提供相关证明材料） |
| 云计算能力 | ★1、要求与云存储系统和云网络系统为相同品牌，要求能够兼容医院现有服务器，云计算系统采用分布式管理架构，去中心化，管理平台不依赖于某一个虚拟机或物理机部署，采用分布式架构保障平台更可靠；（需提供产品功能截图证明并加盖投标人公章）  2、虚拟化的管理平台、可以支持扩展同一品牌的存储虚拟化、网络功能虚拟化、虚拟应用防火墙、虚拟应用交付、SSL VPN软件、数据库审计软件等功能组件的，并支持统一管理，以保障平台的扩展性和兼容性；  3、支持创建虚拟机的时候批量指定IP地址和虚拟机的hostname，支持编辑已经创建的虚拟机的IP地址和hostname；  4、支持对平台虚拟机的精细化权限管理，可根据单个虚拟机开关机、打开控制台、删除等操作设定不同的权限，管理员也可以根据用户需求合理分配权限；  5、支持虚拟机卡死及蓝屏的检测功能并实现自动重启，无需人工干预，减少运维工作量；  6、虚拟机资源告警项支持虚拟机CPU利用率、内存利用率，虚拟机单网口链接session数过高，并检测异常状态持续时间，支持检测虚拟机镜像文件损坏，备份失败，虚拟机与外部网络不通的监控告警，用户可自定义告警项并支持通过邮件和短信进行告警；  7、主机资源告警项支持主机CPU利用率、主机内存利用率，主机交换分区利用率，主机CPU温度异常，主机网口丢包率，并检测异常状态持续时间；支持主机网关不通，主机网口掉线，主机离线，数据通信口不通的监控告警，用户可自定义告警项并支持通过邮件和短信进行告警；  8、支持设置告警类型（紧急和普通）、告警内容（集群、主机、虚拟机、CPU、内存、磁盘），针对告警信息平台可自动给出告警处理建议，同时支持将告警信息以短信和邮件方式发送给管理员；  9、支持以EXCEL表格的方式导出虚拟机的配置信息，包括名称、IP、CPU内存磁盘配置、使用率信息；  10、支持在线的带存储的虚拟机迁移功能，可以在不停机状态下和非共享存储的环境中，实现虚拟机在集群内的不同物理机上迁移，保障业务连续性；  ★11、为避免主机假死导致系列问题发生，支持识别假死主机并标签化为亚健康主机，通过邮件或短信告警提醒用户进行处理，并限制重要业务在亚健康主机上运行，规避风险。（需提供产品功能截图证明并加盖投标人公章）  12、支持无代理跨物理主机的虚拟机USB映射，需要使用USB KEY时，无需在虚拟机上安装客户端插件，且虚拟机迁移到其它物理主机后，仍能正常使用迁移前所在物理主机上的USB资源，对于业务的自适应能力、使用便捷性更佳；（需提供产品功能截图证明并加盖投标人公章）  13、支持一键还原已删除的虚拟机，可恢复30天内已删除的虚拟。（需提供产品功能截图证明并加盖投标人公章）  14、具有合理的内存调度机制，支持内存回收机制，实现虚拟化平台内存资源的动态复用，并支持手动设置内存超配机制，能够实现内存的过量使用，保证内存资源的充分利用；  15、支持配置集群动态资源调度功能，系统支持自动评估物理主机的负载情况，当物理主机负载过高时，自动将该物理主机上的虚拟机迁移到其他负载较低的主机上，确保业务持续高效运行和集群主机负载均衡；  16、支持配置动态资源扩展功能，系统支持自动评估虚拟机的性能，当虚拟机性能不足时自动为虚拟机添加CPU和内存资源，确保业务持续高效运行；  17、支持虚拟机的HA功能,当物理服务器发生故障时，该物理服务器上的所有虚拟机，可以在集群之内的其它物理服务器上重新启动，保障业务连续性；  18、虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的IP地址、MAC地址等；  19、为保障云平台的领先性和成熟度，云平台厂商需入围2016 X86服务器虚拟化魔力象限，提供证明材料。  20、超融合软件通过数据中心联盟颁发的云计算超融合架构可信评估证书，提供证书复印件。  21、要求能够提供三年软件升级服务，提供原厂售后服务承诺函。 |
| 云网络能力 | ★1、要求与云存储系统和云计算系统为相同品牌，要求能够兼容医院现有服务器，通过License激活的方式，实现网络虚拟化功能（分布式虚拟交换机、虚拟路由器、虚拟应用防火墙、虚拟应用负载均衡），支持Vxlan网络和现有的Vlan网络对接，实现虚拟化平台与原有网络的兼容性；  ★2、支持对oracle、sqlserver、Weblogic数据库及中间件监控，实现对数据库的语句的故障定位排错，执行时延分析；（需提供产品功能截图证明并加盖投标人公章）  3、在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个平台虚拟设备实现统一的管理，提升运维管理的工作效率；（需提供产品功能截图证明并加盖投标人公章）  4、主动探测业务系统，实时监控业务可用性，监控策略包括HTTP、FTP、POP3、SMTP、自定义端口协议等，当业务出现故障时，通过多种方式（短信、邮箱）告知管理员进行排障；  5、支持链路聚合，为网络中的每个虚拟机提供内置的网络故障切换和负载均衡能力，实现更高的硬件可用性和容错能力；  6、可以支持手动指定路由器运行在固定的物理主机上，可以自动将路由器规划到高性能和高网络吞吐的物理主机上；  7、为满足用户使用ipv6地址的需求，支持为虚拟机配置ipv6地址，并可通过ipv6地址访问该业务；  8、主动探测业务系统，实时监控业务可用性，监控策略包括HTTP、FTP、POP3、SMTP、自定义端口协议等，当业务出现故障时，通过多种方式（短信、邮箱）告知管理员进行排障（需提供产品功能截图证明并加盖投标人公章）  9、分布式防火墙基于监测虚机IP地址和端口进行东西向流量隔离控制，并提供实时拦截日志，以及支持“数据直通ByPass”功能，方便出现问题快速定位问题；  10、提供虚拟路由器、虚拟交换机等设备的连通性探测功能，方便在虚拟化环境中，进行相应的故障排除和恢复，能够定位到出现故障的虚拟网络设备，方便快速排查问题保障业务的高连续性；  11、支持大屏展示便于客户直观查看虚拟化资源池的使用情况和健康状态，包括集群资源情况，各主机资源使用情况，存储资源池的IO次数、IO速率、IO时延、存储命中率、主机命中率，以及集群故障与告警，支持Top 5主机CPU和内存利用率、Top 5虚拟机CPU和内存利用率信息大屏展示等。（需提供产品功能截图证明并加盖投标人公章）  12、考虑云网络系统及云平台自身的安全能力，要求系统厂商为国家级网络安全应急服务支撑单位，提供网站查询截图。 |
| 云存储能力 | ★1、要求与云计算系统和云网络系统为相同品牌，要求能够兼容医院现有服务器，全自动化的分布式存储配置，和虚拟化平台紧密耦合，为虚拟机提供存储资源；（需提供产品功能截图证明并加盖投标人公章）  2、采用分布式的软件定义存储架构，在通用x86服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点；通过新增物理服务器可以实现存储容量和性能的横向扩展（Scale-Out架构），扩容过程保证业务零中断；  3、支持多种存储配置；磁盘预分配根据业务需求分配固定的物理存储空间、磁盘精简分配根据应用实际写需要时才分配相应的物理存储空间，磁盘动态分配机制根据业务动态需求分配存储资源，实现预分配的高性能和提高磁盘利用率；  4、支持为虚拟磁盘配置不同的存储策略以满足特定场景的需求, 如系统盘和数据盘选择高性能策略, 备份盘选择低性能策略；  5、支持标准的iSCSI协议，允许外部物理主机或应用通过标准的iSCSI接口访问虚拟存储，实现Server SAN和IP SAN的融合，能够使存储资源的利用率发挥到最大价值，在iSCSI接入场景下支持内部负载均衡和高可用；  ★6、支持数据重建优先级调整，在故障数据重新恢复时，可由用户指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性；（需提供产品功能截图证明并加盖投标人公章）  7、支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中IO性能占用导致对业务的性能造成影响；  8、在可视化的WEB管理平台上，可以查看虚拟分布式存储对应的容量大小、容量使用率、实时的IOPS读写次数、IOPS读写数据量等信息，方便为IT管理做为有效的决策依据；  9、支持数据分层，提供好的读写性能，并支持对重要虚拟机提供性能保护；  10、支持条带化功能，实现分布式raid0的性能提升效果，并且支持以虚拟磁盘为单位设置不同的条带数；（需提供产品功能截图证明并加盖投标人公章）  11、为了便于部署关键业务系统，虚拟存储可支持Oracle RAC，支持共享盘，及共享块设备，支持向导式安装，降低部署复杂度；（需提供产品功能截图证明并加盖投标人公章）  12、支持存储分卷功能，以物理主机为单位划分为不同的存储卷，可将集群内全闪存的节点组成一个高性能存储池，满足高性能应用需求，将混闪节点组成一个大容量存储池，满足低性能大容量应用需求；所有类型不同性能磁盘均可支持分区，包含SSD，SAS，SATA，NL-SAS等；  13、支持单节点的一块或多块缓存盘（SSD）拔出后，集群内所有的虚拟机正常运行未出现中断，其中一台虚拟机硬盘拔出前后磁盘读写（IO）性能少幅下降，或几乎没有下降；  14、支持针对虚拟机或虚拟磁盘设置数据分布策略，当采用副本聚合策略时，可以保证以性能优先为原则，实现IO本地读效果，当采用副本散列策略时，可以保证虚拟机以分布均匀优先为原则，打散分布均匀在各物理主机上；  15、支持对虚拟机或虚拟磁盘设置不同的缓存QoS能力，区分出高性能虚拟机、普通性能虚拟机和低性能虚拟机；（需提供产品功能截图证明并加盖投标人公章）  16、支持IO读写SSD Cache功能，提升存储性能，支持写Cache的节点故障保障，当节点故障或宕机时，写Cache内的数据不丢失；  17、支持磁盘亚健康监测，包括PCIE SSD寿命告警、硬盘卡、慢的检测和告警、IO错误告警、RAID卡错误告警等，支持邮件和短信告警；  ★18、支持坏道修复功能，发现坏道后，主动修复坏道区域的数据，及时恢复数据副本的冗余性；当硬盘的坏道数过多，系统能自动将该盘的数据迁移至其他健康的硬盘上，保障数据的安全。（需提供产品功能截图证明并加盖投标人公章） |

★注：支持与黑龙江中医药大学第一附属医院现有云管理系统进行对接，应答人提供云管理系统厂商针对该项目对接授权，不提供视为无效投标。

## 5.7迁移服务

1. 外科楼九层设备迁移服务：负责原有机架拆卸、负责在新机架上安装、负责运输。包括核心交换设备；网络防火墙设备、无线控制器设备、入侵防御设备、行为管理设备、路由器设备、存储设备、IBM小型机设备、服务器设备、KVM设备等；设备迁移到应用机房后进行单系统调试与全系统联调，确保用户单位各项业务正常运行，提供相关必要的保障措施。
2. 门诊楼负一层设备迁移服务：负责原有机架拆卸、负责在新机架上安装、负责运输。包括存储设备、路由器设备、网络防火墙设备、网络交换设备、服务器等；设备迁移到应用机房后进行单系统调试与全系统联调，确保用户单位各项业务正常运行，提供相关必要的保障措施。
3. 规培楼三层机房内UPS设备维护服务：80KVA UPS电源检测及维护，电气专业技术人员针对设备安全进行检测，需要采用专用设备仪表进行；保障设备的日常安全使用。
4. 规培楼三层机房内空调设备维护服务：机房恒温恒湿专用空调检测及维护，空调专业技术人员针对设备安全进行检测，需要采用专用设备仪表进行；保障设备的日常安全使用。
5. 规培楼三层机房环境监控维护服务：机房动环系统检测及维护，专业技术人员针对设备系统进行检测，需要采用专用设备仪表进行；针对机房内的电力供给、输送进行维护服务；针对机房设备的运行情况进行维护服务；针对机房温度、湿度、漏水等模拟参数进行监测服务；
6. 规培楼三层机房视频监控维护服务：机房视频监控维护，专业技术人员针对设备系统进行检测，需要采用专用设备仪表进行；针对视频监控区域、监控存储等应用进行维护服务；
7. 门诊楼负一层监控视频网络基础迁移服务：视频系统设备迁移服务，包括硬盘录像机、 阵列、网络交换机，监控网络安全加固，监控核心交换机、汇聚交换机迁移服务；ODF架、机柜安装、监控设备组网规划、测试服务，单机调试及联网调试服务；
8. 门诊楼负一层有线电视系统设备迁移维护服务：视频编解码器24套；机顶盒24套等，全院有线电视整体优化服务：有线电视机房内设备、全院病房终端线路优化、主干分支线路优化，有线电视光传输机(发射端、接收端)；
9. 弱电间网络机柜维护整理服务：全院弱电间线路整理，原有机柜内线缆整理、捆邦；清除不用线缆，规划交换机线序等，确保网络正常运行；
10. 网络链路测试服务：信息网络链路测试、缕清各系统的网络路由并做好基础电子资料；确保用户单位各项业务正常运行，提供相关必要的保障措施。
11. 机房维护服务：维护机房内各基础设施服务，包括但不限于防静电地板维护、不锈钢玻璃隔断玻璃隔断维护、防火门维护、机柜金属支架维护、UPS电源设备维护等；机房电气维护：包括但不限于配电柜至列头电缆维护、机架设备电缆维护、照明线路维护、UPS主机维护、弱电系统维护等；微模块机房组维护：包括但不限于对原有模块重新拆除、变动布局位置、调试；服务时确保用户单位各项业务正常运行，提供相关必要的保障措施。外科楼十层机房清场设备服务：外科楼10层机房UPS及电池拆除外运：电池规格：100AH电池，共计64块负责电池拆卸、搬运；需要提供汽车运输；UPS规格：80KVA，负责电池拆卸、搬运；需要提供汽车运输；
12. 其他要求：各应用服务器和数据库服务器,各应用系统终端应不需要修改任何配置(包括 IP 地 址)。

服务实施前做好设备配置及数据备份工作。服务实施前将现有应用系统进行数据备份，避免由于设备搬迁过程中故障导致数据受损；对于使用内置磁盘的系统，增加备份份数，保障数据的完整性和可靠性。网络设备方面，搬迁前应完成对搬迁设备IOS及配置文件的备份。

服务实施后做好测试验证工作，以保证应用系统在搬迁后快速恢复正常运行。

应用系统服务控制指标要求描述如下：

网络中断时间控制在24小时内 ；

业务系统分为核心业务系统和非核心业务系统，核心业务系统停机时间控制在12小时内，非核心业务系统停机时间控制在 24 小时内；

相关数据库系统情况（停机 24 小时内）；

# 六、服务商工作主要内容

负责协调各参与方最终制定平台总体建设方案、软件系统方案以及工程进度安排，并负责协调各参与方将上述方案付诸实施。其具体工作主要包括：

--网络总体建设方案、软件系统方案及工程进度的制定：形成详尽、系统的方案文档；

--组织、协调、指导各系统/设备提供商有序完成全网系统、软硬件调整步骤，并确保软件平台建设之后的稳定运行。

--协调各系统/设备提供商完成全网相关协议的全部参数统一调整，并确保在平台应用后稳定运行；

--完成全网安全、软件平台策略的拟订，并协调各系统/设备提供商完成各自负责设备的部署工作；

--全网联调测试：负责全网联调测试方案的拟订，负责完成全网建设、软件部署、协议功能的连通性、稳定性、安全性测试以及运行高效性；

# 七、技术培训

为了使买方能够在项目验收后有能力运营构建的平台。需要对买方指定人员进行平台的使用方法进行培训。同时，有能力协助买方对平台完成良好运营。现场培训买方的维护人员的具体数量、时间、地点由双方商定。卖方应免费提供具体的人员培训计划，课程安排以及师资。具体要求如下：

1、网络构架培训（使买方人员可以对构建的平台有全局的了解，便于在平台运营过程中可以快速定位故障，并在进行业务变更时选择正确的设备进行调整）。

2、软件使用培训（使买方人员可以根据业务需要对软件中的功能设置进行常规调整）。

# 八、达成效果

随着信息系统的升级，带来如下效果提升：

* 提高系统数据整体安全性，避免因数据丢失导致的公共事件发生
* 平滑的提供更大的存储空间
* 提供更快的数据响应速度
* 提供更大的数据吞吐能力
* 提供灵活的资源调配能力（包括服务器和存储）

并且，可解决如下问题：

* 如何解决应用系统和数据容量迅速增长带来的问题：
* 利用率降低
* 成本不断增加
* 管理越来越复杂等
* 如何满足关键应用系统的业务连续性要求
* 关键系统高性能
* 关键服务不停顿
* 关键数据不丢失

# 九、售后服务

在合同签订后，卖方在合同规定时间范围内完成环境搭建。所采用的设备、复材性能参数要求全部满足上问的描述。在实施完成后买方按照要求对环境进行检查，如出现工艺、参数不达标情况，要求在规定期限内完成整改。完全通过验收后开始计算服务时间。

服务期限内，买家可以自行对基础设施进行配置调整，卖家需要提供相关技术支持。

服务期限内，基础服务设备如出现非外力造成的损坏，卖家需要在规定的时间内进行响应、处理。处理时限和相关定义如下：

故障处理时限要求：

|  |  |  |  |
| --- | --- | --- | --- |
| **故障等级** | **响应时间** | **服务方式** | **恢复通信时间** |
| 一级故障 | 立即响应 | 2小时内到达现场，同时提供24小时电话热线 | 6小时内恢复 |
| 二级故障 | 立即响应 | 2小时内到达现场，同时提供24小时电话热线 | 10小时内恢复 |
| 三级故障 | 6小时内响应 | 24小时到达现场，同时提供24小时电话热线 | 24小时内恢复 |
| 四级故障 | 10小时内响应 | 48小时到达现场，或提供24小时电话热线，买方有权选择 | 48小时内恢复 |

故障级别定义：

|  |  |
| --- | --- |
| **一级故障** | 因设备故障造成的整个系统瘫痪。 |
| **二级故障** | 因设备故障严重影响系统运行。 |
| **三级故障** | 因设备故障影响系统的效率，系统仍然可以运行。 |
| **四级故障** | 不影响业务的设备及管理功能故障。 |

# 十、其他

若卖方提供的软件服务某些部分不能完全符合本技术规范书要求时，卖方应提出符合本技术规范的承诺和时限。

当买方有新建议，而本规范又尚未包括或和本规范不符时，则应符合买方新建议的要求；对于买方尚未有标准的，而本规范又未提及的部分，卖方提出其标准，留待双方认可后执行。

本次应标厂商如若存在与其它厂家的合作关系，请澄清双方职责分工，就服务内容、工程实施等内容做详尽的责任分工界面，合作的下放厂商应针对在本工程所担任的角色分工，出具相关资质证明。

在保修期内，本系统须无条件遵循黑龙江中医药大学附属第一医院最新颁布的技术规范和业务规范。亦即在保修期内，若遇黑龙江中医药大学附属第一医院颁布新的技术规范和业务规范，商应及时给予免费升级，以保证本系统的技术和业务规范符合集团公司的要求。

合同文本采用黑龙江中医药大学附属第一医院合同范本，如果合同文本中与本规范不一致的内容，买方有选择权。

卖方承诺遵守《黑龙江中医药大学附属第一医院通用网络与信息安全责任条款》和《保密协议》。

本技术规范书最终解释权归黑龙江中医药大学附属第一医院所有。