海南医学院第二附属医院
网络安全改造项目

项目概述及建设内容

根据现有网络及后续发展情况进行统一规划，按照三级等保建设标准对海南医学院第二附属医院网络安全进行改造，通过改造尽可能地消除或降低信息系统存在的安全风险，进一步提升信息系统的安全水平，建设具有海南医学院第二附属医院特色的信息安全等级保护深度防御体系。

本项目总预算为 439.31 万元，含软硬件设备采购及集成费、工程监理费、等保测评费和可研报告编制评估费，各标段预算分述如下：

1、软硬件设备及材料采购（A 包）：¥4,050,900.00 元

2、信息系统安全等级保护测评服务（B 包）：¥150,000.00 元

3、信息化项目监理服务（C 包）：¥89,100.00 元

本次招标项目金额合计：¥4,290,000.00 元，招标代理费由中标单位支付。

采购需求（A 包 软硬件设备及材料采购）

一、 商务要求

1、交付时间：合同签订后 60 天内。

2、交付地点：用户指定地点。

3、交付方式：免费送至用户指定地点。

4、采购资金的支付方式、时间、条件：

完成全部设备的供货，经甲方确认后，支付合同总金额的 30%，项目完成安装调试，经甲方验收合格后，支付合同总金额的 65%，剩余合同总金额的 5%转为质保金，质保期结束后无息返还。

5、供应商资格要求：见招标公告。

6、验收要求：按标书技术参数和国家行业标准进行验收。

7、售后服务要求：

(1) 投标人或生产厂家须在全国设立服务机构，针对使用过程中出现的故障问题，可以通过电话、网络方式先提供服务，如果解决不了的情况下需要及时赶赴现场提供服务。

(2) 提供不低 3 年的免费保修期，自验收合格之日起算。

(3) 保修期内非采购方人为因素而出现的质量问题，生产厂家负责保修、包换或者包退，并承担修理、调换或退货的实际费用。

(4) 质保期内，设备在使用过程中，如发生非人为故障，投标人或生产厂家须在接到维修通知后半小时内响应，2 小时内给予解决方案并委派技术工程师到达现场维修，提供免费服务。重大问题在 2 个工作日内给予解决方案，若在 2 个工作日内无法及时排除故障，生产厂家免费提供同档次的备用机供院方使用。质保期外，投标人或生产厂家须接到维修通知之后 2 个小时内响应，24 小时提供建议解决方案供采购方选择。

(5) 投标人承诺提供的每一台仪器均是全新的，厂家提供终身有偿维修、保养服务，保修范围外有偿维修，只收成本费。

(6) 投标人或生产厂家负责产品安装系统调试及人员培训。

(7) 投标人或生产厂家负责长期提供技术资料和技术支持。

(8) 生产厂家保修期外需提供终身维护，设备故障维修只收取零配件费用。

(9) 生产厂家须对院方使用人员及设备维修人员进行培训，使用人员能够熟练掌握设备的各项功能和操作，使维修人员能对设备进行日常维护和一般性故障的查找及故障的排除。

8、由于项目实施过程会涉及医院敏感信息，供应商必须提交保密承诺函。

二、 项目需求及建设方案

1.1. 系统功能需求

本期将对海南医学院第二附属医院整体网络进行统一规划，按照满足三级等保要求进行建设，本期海南医学院第二附属医院网络安全系统功能需求如下：

1.结构安全（G3）

本项要求包括：

（1）应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；

（2）应保证网络各个部分的带宽满足业务高峰期需要；

（3）应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；

（4）应绘制与当前运行情况相符的网络拓扑结构图；

（5）应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

（6）应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；

（7）应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

2.访问控制（G3）

本项要求包括：

（1）应在网络边界部署访问控制设备，启用访问控制功能；

（2）应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；

（3）应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；

（4）应在会话处于非活跃一定时间或会话结束后终止网络连接；

（5）应限制网络最大流量数及网络连接数；

（6）重要网段应采取技术手段防止地址欺骗；

（7）应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；

（8）应限制具有拨号访问权限的用户数量。

3.安全审计（G3）

本项要求包括：

（1）应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；

（2）审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

（3）应能够根据记录数据进行分析，并生成审计报表；

（4）应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

4.边界完整性检查（S3）

本项要求包括：

（1）应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；

（2）应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

5.入侵防范（G3）

本项要求包括：

（1）应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；

（2）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

6.恶意代码防范（G3）

本项要求包括：

（1）应在网络边界处对恶意代码进行检测和清除；

（2）应维护恶意代码库的升级和检测系统的更新。

7.网络设备防护（G3）

本项要求包括：

（1）应对登录网络设备的用户进行身份鉴别；

（2）应对网络设备的管理员登录地址进行限制；

（3）网络设备用户的标识应唯一；

（4）主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；

（5）身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

（6）应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

（7）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

（8）应实现设备特权用户的权限分离。

1.2. 网络建设及部署需求

海南医学院第二附属医院无线网络改造需遵循原有网络架构，减少对网络现状的影响，遵循现有安全架构和安全等级保护三级要求，提高网络可用性，主干链路采用冗余热备配置，避免单点故障节点。

（1） 先进性原则

以先进、成熟的网络通信技术进行组网，支持数据、语音和视频图像等应用，采用基于交换的技术代替传统的基于路由的技术，并且能确保网络技术和网络产品在几年内基本满足需求。

（2） 开放性原则

应遵循国际标准，采用大多数厂家支持的标准协议及标准接口，从而为异种机、异种操作系统的互连提供便利和可能。

（3） 可管理性原则

网络建设的一项重要内容是网络管理，网络的建设必须保证网络运行的可管理性。在优秀的网络管理之下，将大大提高网络的运行速率，并可迅速简便地进行网络故障的诊断。

（4） 安全性原则

信息系统安全问题的中心任务是保证信息网络的畅通，确保授权实体经过该网络安全地获取信息，并保证该信息的完整和可靠。网络系统的每一个环节都可能造成安全与可靠性问题。

（5） 灵活性和可扩充性

选择网络拓扑结构的同时还需要考虑将来的发展，由于网络中的设备不是一成不变的，如需要添加或删除一个工作站，对一些设备进行更新换代，或变动设备的位置，因此所选取的网络拓扑结构应该能够容易的进行配置以满足新的需要。

（6） 稳定性和可靠性

可靠性对于一个网络拓扑结构是至关重要的，在局域网中经常发生节点故障或传输介质故障，一个可靠性高的网络拓扑结构除了可以使这些故障对整个网络的影

响尽可能小以外，同时还应具有良好的故障诊断和故障隔离功能。

1.3. 性能需求

1. 接入速率需求

（1） 终端接入区接入速率需求：

终端设备至接入交换机采用千兆速率，接入交换机至汇聚交换机采用千兆速率，汇聚交换机至核心交换机采用万兆速率。

（2） 安全管理区接入速率需求：

安全管理区至网络设备及网络设备至核心交换机采用千兆速率进行连接。

（3） 服务器存储区接入速率需求：

服务器存储区网络设备至核心交换区采用万兆速率进行连接。

（4） DMZ 区接入速率需求：

DMZ 区采用千兆速率进行连接。

（5） 非关键服务器区接入速率需求：

非关键服务器区采用千兆速率进行连接。

（6） 互联网接入区及核心区接入速率需求：

互联网接入区及核心区根据实际业务需要采用不同速率的接入方式。

2. 扩展性需求：

网络系统的扩展性需求是通过在网络结构设计和网络设备选型方面来保证的。网络系统结构设计要适当超出医院当前应用的需求，以便日后在技术上平滑升级。其次，网络结构中不同速率端口配置一定要留有适当的冗余，既有利于日后的网络规模扩展也有利于网络维护。

本期海南医学院第二附属医院网络安全改造网络设备端口在本期使用基础上进行预留，为后期网络扩容预留端口。

3. 吞吐速率

吞吐速率主要由各级交换机的背板交换矩阵的带宽决定的，吞吐速率一般可通过交换机堆叠来扩展交换机的背板带宽。

4. 响应时间

响应时间越短，性能就越好，效率就越高。局域网的响应时间通常为 1ms~2ms，广域网的响应时间为 60ms~1000ms，越高越好。一般的文字工作可以用一般的响应标准，但大容量的文件传输，如视频点播、远程视频教学，响应时候就不能那么高了，那样会对整个网络硬件和服务器的配置要求相当高，会增加成本。

5. 并发用户数支持

并发用户数支持是指某一系统可以承载的同时访问的用户数，并发用户数越多，系统性能越好，配置也就越高档。具体的并发用户支持数需求要看同一时间系统的人数而定，并稍高于实际值。目标用户容量=目标 CPU 容量/每个用户 Web CPU 总成本，目标 CPU 容量=处理器的数量*CPU 的频率定额。

6. 磁盘读写性能

终端用户只用于一个人的磁盘读写，一般的磁盘系统可以满足，但在服务器那端，需要同时支持几百甚至是几千人的访问。目前最新的 SCSI 标准传输速率可达 320Mbps，就需要特定的措施给磁盘系统加速，目前主要通过配制 RAID，通过这种冗余阵列可以把数据同时写在多个磁盘上，来提高速度。

7. 误码率

在局域网中误码率较低（通常为 10-8~10-10）基本可以满足用户的需要，

但在广域网中，通过一般可采用 ADSL、Cable MODEM 甚至是光纤来满足用户的需要。

8. 可用性

可以通过提高系统的稳定性来达到，可采用一些具有自愈能力的设备，也可通过提高网络本身的可靠性，如利用冗余链路连接。

1.4. 安全需求

保密性：采取有效措施保障数据保密性好

完整性：不经授权数据不得修改。

可靠性：数据或有关数据的信息不能有错。

保证网络管理系统正确运行，保护被管理的目标免遭破坏，包括身份鉴别、密钥管理、病毒预防和灾难恢复等。

管理：具有数据备份和恢复的能力，定时更新等，各种服务的管理，如 HTTP、FTP、SMTP、POP3、DNS 服务管理等。

需求类型	要求	备注
保密性	高	防病毒、防攻击
完整性	高	不经授权数据不得修改
可靠性	高	信息正确的传输
数据备份与恢复	较高	暂无
服务管理	一般	如 HTTP、FTP、SMTP 管理等

1.5. 接口需求

根据需要，本期海南医学院第二附属医院需要跟海南医学院进行对接，实现海南医学院对海南医学院第二附属医院的管理，本期海南医学院第二附属医院核心交换机侧应预留相关接口。

1.6. 总体建设方案

1.6.1. 总体框架

为使得《信息系统安全等级保护基本要求》能够进行落地实施建设，通过对等级保护要求的整合分析，结合业界成熟的信息安全体系建设理论，提出了从安全管理、安全保障、区域边界、通信网络、计算环境、应用系统几个层面，进行整体安全设计的思路。

同时考虑以安全管理中心为管理建设重点，形成长治久安的管理核心，以安全服

务为长期服务，共同构建起信息系统整体安全建设框架。

1.6.2. 技术路线

本期海南医学院第二附属医院网络安全改造按照三级等保标准进行建设，新增网络安全设备要符合三级等保建设要求，采用目前最新技术实现对来自内网及外网相关访问的检测、控制、防篡改、日志审计及记录等功能，同时要实现账号的统一管理，数据库、服务器、网络设备账号的集中管理等。

根据三级等保建设标准，本期项目计划在海南医学院第二附属医院网络安全改造中增加以下设备，为整体网络提供安全、高效的保护措施。

1、互联网接入区

新增防火墙、防病毒网关、上网行为审计系统等。

2、DMZ 区

新增防火墙及交换机等设备。

3、安全管理区

新增终端防毒及补丁分发、网页防篡改系统、威胁分析系统、双因子认证系统、日志审计系统、主机加固系统、堡垒机。

4、服务器存储区

新增虚拟化防病毒系统、数据库审计系统、服务器存储区 IPS、服务器存储区防火墙等设备。

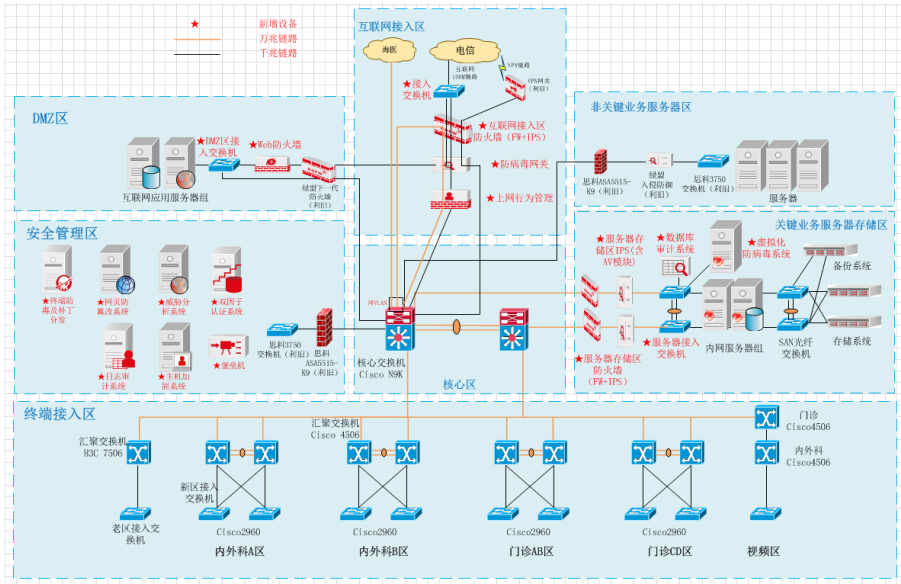
1.7. 基础设施建设

1.7.1. 机房及配套工程建设

本期项目新增设备安装在现有机房机柜内，本期不涉及相关机房及配套工程建设。

1.7.2. 网络拓扑

本期项目安全改造后的网络拓扑图如下所示：



网络拓扑图（本期）

1.8. 安全保障要求

1.8.1. 网络安全设计

本期根据实际安全需求以及信息安全等级保护 3 级的网络安全要求进行建设，网络安全建设方案如下：

1. 网络区域化安全设计。结合“一个中心、三重防护”的安全保障体系及信息安全等级保护的思想，既在一个安全管理中心之下，对安全计算环境，安全通信网络，安全区域边界进行统一防护管理，并对网络系统进行安全区域划分。

2. 将网络划分为互联网接入区、核心区、关键业务服务器存储区、非关键

服务器区、DMZ 区、安全管理区、终端接入区。

3.互联网接入区

（1）新增 1 台接入交换机，实现医院网络对外数据或外部数据访问医院网络的数据交互。

（2）新增 1 台互联网接入区防火墙，实现边界与内网区域的逻辑隔离和访问控制。

（3）新增 1 台防病毒网关,实现对医院整个网络进出口流量进行病毒扫描。

（4）新增 1 台上网行为管理系统，进行身份识别、行为管理、行为分析、应用控制、内容管控、流量管控、非法热点管控、无线网络管理等功能，实现医院全网全终端统一的上网行为的管理、控制与审计。

（5）利旧现网 1 台 VPN 网关设备，实现在外医护人员通过互联网访问医院的相关内部系统。

4.核心区

本期核心区利旧现有 2 台思科 N9K 核心交换机，采用虚拟化方式进行部署，从而提高了核心设备的高可用性，本期只扩容万兆光模块。

5.关键业务服务器存储区

（1）新增 1 台服务器存储区防火墙设备、1 台服务器存储区 IPS 设备，实现边界访问控制，对入侵行为进行主动防范；同时 IPS 设备开启 AV 模块，对恶意代码进行过滤。

（2）新增 1 台数据库审计系统，对访问数据库的行为进行记录和审计，防止误操作以及对恶意操作进行追溯。

（3）新增 1 套虚拟化防病毒系统，对服务器虚拟化环境提供安全防护。

（4）新增 2 台交换机，实现服务器存储区的数据交互。

6.非关键业务服务器区

利旧现网 1 台思科 ASA5515-K9 防火墙及 1 台绿盟入侵防御设备，为非关键业务服务器区服务器提供安全防护。

7.DMZ 区

（1）新增 1 台 Web 防火墙，利旧现网 1 台防火墙，用于对网站系统进行保护，防止 SQL 注入，挂马等攻击行为。

（2）新增 1 台交换机，实现 DMZ 区的数据交互。

8.安全管理区

（1）利旧现网 1 台 Cisco ASA5515 防火墙，实现边界访问控制。

（2）利旧现网 1 台 Cisco 3750 交换机，实现安全管理区的数据交互。

（3）新增 1 套堡垒机，统一对网络设备、服务器、安全设备进行管理，并对运维管理行为进行审计。

（4）新增 1 套主机加固系统，对系统和应用通过扫描，基于已发布漏洞，和安全选项的相关情况进行综合评估。

（5）新增 1 套日志审计系统，对全网网络设备、服务器、安全设备进行日志集中收集与分析。

（6）新增 1 套双因子认证系统，实现在账号认证基础之上，增加动态密码，实现双重因子认证，从而有效保护用户认证安全。

（7）新增 1 套威胁分析系统，对各类攻击进行检测。

（8）新增 2 套网页防篡改系统，对网站系统进行保护，防止对网站的篡改行为。

（9）新增 1 套终端防毒及补丁分发，实现对终端设备进行病毒防护及补丁管理功能。

9.终端接入区

终端接入区现有汇聚交换机通过万兆链路接入至核心区交换机。

1.8.2. 网络安全防护

1. 网络区域划分

海南医学院第二附属医院应根据医院自身的业务需要，详细、统一进行 VLAN 的规划及 IP 地址资源的分配，尽量细化 VLAN 区域，防止广播风暴的影响蔓延，并应根据整体网络结构特征，进行网络区域的合理划分，而在单位内部根据区域特征进一步细分，如可分为网络通信域、用户域、网络边界域等安全域。

2. 网络边界访问控制

本期海南医学院第二附属医院在关键网络区域的边界处部署防火墙访问控制设备，并建立严格的访问控制策略。

3. 网络入侵防御

本期海南医学院第二附属医院在外网边界处部署防火墙（含 IPS 功能）入侵防御系统，能够实现针对 DDOS 攻击、端口扫描、木马后门攻击、IP 碎片攻击、网络蠕虫攻击等行为的防护。

4. 本期海南医学院第二附属医院部署了主机安全加固系统及上网行为管理系统，对所有主机进行安全漏洞管理及行为监控。

5. 网络准入控制

本期海南医学院第二附属医院部署了上网行为管理系统及堡垒机建立统一的网络准入控制系统，通过制定合理的网络接入控制策略，防止非法的外来电脑接入网络。

1.8.3. 系统安全防护

1. 系统层面双因素认证

海南医学院第二附属医院信息部门应对登录操作系统和数据库系统的用户进行身份标识和鉴别，其中登录用户的身份标识应采用用户名，鉴别方式采用口令。

2. 系统访问控制

海南医学院第二附属医院的应用系统应实现以下访问控制方面的功能：

（1） 应关闭各系统不必要的端口和服务；

（2） 应根据安全策略限制用户访问文件的权限及关闭默认共享；

（3） 数据库系统应限制主体（如用户）对客体（如文件或系统设备、数据库表等）的操作权限（如读、写或执行）；

（4） 应根据管理用户的角色对权限做出标准细致的划分，并分配该角色使用系统或数据库所需的最低权限；

（5） 应为操作系统和数据库系统设置不同特权用户，并合理分离分配特权用户权限；

（6） 应删除系统多余和过期的账户，如 GUEST；

（7） 不允许多人共用一个相同的账户；

（8） 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。

3. 主机防病毒

终端和主机应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

4. 终端安全防护

海南医学院第二附属医院所有终端安全防护工作应遵守以下要求：

（1） 资产信息管理，在线收集、资产配置核查、资产使用情况的在线管理、资产资源利用率；

（2） 终端安全性审查。对终端入网的安全性进行评定，以决定是否达到安全标准；

（3） 补丁管理。建立独立的补丁分发服务器，实现内外的补丁分发；

（4） 终端病毒防护。构建企业级的病毒防护系统，实现病毒库的统一，全网病毒监测和统计。

1.8.4. 应用安全防护

1. 应用层面双因素认证

海南医学院第二附属医院应用系统应实现以下身份认证方面的功能：

（1） 应用系统应具有专用的登录控制模块对登录用户的用户名/密码进行核实；

（2） 应用系统应采用除用户名/密码+数字证书两种鉴别技术来实现身份鉴别；

（3） 应为应用系统中的不同用户分配不同的用户标识即用户名或用户 ID 号，确保身份鉴别信息不被冒用。

2. 应用层面访问控制

海南医学院第二附属医院应用系统应实现以下访问控制方面的功能：

（1） 应用系统和数据库系统开发过程中，应设置必要的访问控制机制，保证用户对信息和应用系统功能的访问遵守已确定的访问控制策略；

（2） 应用系统的访问控制机制应覆盖其所有用户、功能和信息，以及所有的操作行为；

（3） 应根据应用系统的重要性设置访问控制的粒度，一般应用系统应达到访问主体为用户组级，访问客体为功能模块级，重要信息系统应达到访问主体为用户级，访问客体为文件、数据表级；

（4） 应严格限制默认用户的访问权限。

3. 抗抵赖

海南医学院第二附属医院可根据需求建设以下抗抵赖方面的功能：

重要应用系统应采用数字签名等非对称加密技术，保证传输的数据是由确定的用户发送的，没有被篡改破坏且能够在必要时提供发送用户的详细信息；

4. 通信完整性

海南医学院第二附属医院可根据需求建设以下完整性保护功能：

（1） 应用系统中通信双方应利用密码算法对数据进行完整性校验，保证数据在传输过程中不被替换、修改或破坏；

（2） 对完整性检验错误的数据，应予以丢弃，并触发重发机制，恢复出正确的通信数据兵重新发送。

1.8.5. 数据安全防护

本期通过建设数据库审计系统，对访问数据库的行为进行记录和审计，防止误操作以及对恶意操作进行追溯。

1.9. 应急响应与安全审计

海南医学院第二附属医院的重要业务系统应遵守以下安全审计要求：

（1） 应开启系统本身的日志审计功能或部署专业的系统安全审计系统，实现对系统行为、安全事件的审计；

（2） 系统行为审计记录应包括：登录网络时间、离开时间、登录地点、使用网络资源；若是维护人员还应包括维护系统的操作命令记录。

安全事件记录应包括：安全事件发生的时间、导致安全事件产生的使用者、事件的类型及事件造成的结果。

1.10. 计算环境安全设计

1.10.1. 终端安全管理

信息系统内部办公终端安全域和各个子网数据处理的过程中，内部泄密和内部攻击已经成为威胁网络安全应用的最大隐患。在互联网出口处部署上网行为管理实现对终端访问互联网进行限制和保护，达到安全业务访问的目的。同时，可以部署内网安全管理系统的管理主机服务器、控制台、数据库，对各子网终端主机进行统一的管理。

终端安全加固

实现补丁管理，对内网终端计算机补丁状态进行定期检测并自动安装与更新。实现防病毒软件监测，判断终端计算机是否安装了防病毒软件、防病毒软件运行是否正常以及病毒库是否保持最新等情况，并对于未进行防病毒软件部署的主机进行内网接入限制。

终端审计监控

对终端计算机运行的进程进行监控，可限制用户运行某些程序。

1.10.2. 网络防病毒

病毒是对信息系统网络的重大危害，病毒在爆发时将使路由器、3 层交换机、

防火墙等网关设备性能急速下降，并且占用整个网络带宽。

针对病毒的风险，本期通过在互联网区出口处部署防病毒网关设备，实现对整体网络的病毒防护，在关键业务服务器存储区部署虚拟化防病毒系统，实现对关键业务区服务器的防病毒保护，同时部署终端防病毒系统及补丁分发系统，对在网终端设备进行病毒防护及补丁升级。

1.10.3. 日志审计

日志审计是通过集中采集各类系统中的安全事件(如网络攻击、防病毒等)、用户访问记录、系统运行日志、系统运行状态、网络存取日志等各类信息，经过标准化、过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理。仅通过简洁的实时监控界面，用户即可实时动态了解当前整个系统的安全态势，获知异常安全事件和审计违规情况。

本期在网络中统一部署了一套日志审计系统，通过该系统实时采集及分析网络中的各种行为，为分析网络安全性提供了重要的依据。

1.10.4. 数据库审计

针对信息系统核心数据库，本期通过部署数据库审计系统，对用户行为、用户事件及系统状态加以审计，从而把握数据库系统的整体安全。

数据库是核心业务开展过程中最具有战略性的资产，对于信息系统来说通常都保存着重要的机密信息，这些信息需要被保护起来，以防止其他非法者获取。

部署数据库审计系统，可以实现对核心数据库的“系统运行可视化、日常操作可跟踪、安全事件可鉴定”目标，解决数据库所面临的管理层面、技术层面、审计层面的三大风险，以满足不断增长的业务需要。数据库审计系统的目的概括来说主要是三个方面：一是确保数据的完整性；二是让管理者全面了解数据库实际发生的情况；三是在可疑行为发生时可以自动启动预先设置的告警流程，防范数据库风险的发生。

数据库审计系统对于数据库的安全防护功能主要有以下几个方面：

第一：数据库审计系统采用“网络抓包、本地操作审计”组合工作模式，为后续的日常操作跟踪、安全事件鉴定奠定了基础。

数据库审计系统依赖其独特的数据库安全策略库，实现细料度的安全审计，并根据事先对不同业务应用设置的安全策略采取诸如产生告警记录、发送告警邮

件（或短信）、提升风险等级、加入黑名单等响应。同时，数据库审计系统可以提供多视角的审计报告，即根据实时记录的网络访问情况，提供多种安全审计报告，更清晰地了解系统的使用情况以及安全事件的发生情况，并可根据这些安全审计报告进一步修改和完善数据库安全策略库。

第二、当数据库发生危险操作时，可以根据事先的安全策略采取相应的防护措施，并为后续的安全事件责任鉴定提供详细的审计记录。任何有意/无意的越权操作、违规操作等高风险操作行为都将被有效的遏制。真正实现数据库操作的可视化、可跟踪、可追溯。

第三、通过部署数据库审计系统区别出非正常模式的访问造成系统阻塞或宕机。

例如，存在用户以恶意或无意的方式发起对应用前台 WEB 服务（如门户网站）的频繁访问，造成 WEB 服务或后台应用服务、数据库服务的高负载或服务崩溃的可能性，或直接对数据库系统发起拒绝服务攻击。

系统管理员可以通过查看审计日志区分系统的高负载是由于正常的用户访问还是出自个别用户的异常行为，判定是否发生了攻击行为，假如是攻击行为则可以根据客户端 ip 等其它信息确定攻击来源。

第四、及时发现用户对系统敏感数据进行不合理的操作。

部分应用系统的开发商在系统中未提供基本的用户操作审计能力，即记录所有用户的详细操作行为并提供方便的查询功能，即使绝大多数数据库系统也都没有配置用户具体访问行为的记录。通过部署数据库审计系统，设定相应的审计规则。当用户未经授权对敏感信息进行了不合理的操作时，系统管理员或相关负责人便会及时获得相关的告警，以及时控制企业的损失。

1.10.5. 入侵防御系统

本期通过部署入侵检测系统，从而实时侦听网络数据流，寻找网络违规模式和未授权的网络访问尝试。当发现网络违规行为和未授权的网络访问时，网络监控系统能够根据系统安全策略做出反应，包括实时报警、事件登录，或执行用户自定义的安全策略等。入侵检测系统还可以形象地重现操作的过程，可帮助安全管理员发现网络安全的隐患。

1.10.6. 主机加固

信息系统的业务服务器主机及其承载的关键业务系统是信息系统重要的信息资产，主机的安全性很大程度上决定了整个业务系统的机密性、完整性、可用性及可确认性、可鉴别性和可靠性。主机的漏洞和弱点是资产拥有者和攻击者的必争之地，主机的漏洞和弱点代表着风险的可能性和风险的严重性，每年系统新的漏洞和弱点层出不穷，安全事件发生的数量成几何倍增长，而同时安全攻击工具及方法传播速度日益加快，使得主机的安全性遭受着前所未有的挑战。

本期通过部署主机加固系统，根据实际情况制定相应系统的测试方案、加固方案与回退方案，针对不同类型的目标系统，通过打补丁、修改安全配置、增加安全机制等方法，合理加强设备与应用的安全性。安全加固服务能够帮助减少误操作，减小由主机引发的安全隐患的可能性，使得整个信息系统最大可能的安全。

1.11. 应用系统安全要求

1.11.1. 双因素身份认证

内部用户通过 VPN 或专线访问各对应子网的内部服务器，仅仅通过用户名/密码的身份真正方式不够安全，而双因素认证提供了比密码更加安全的新模式，这种网络安全超出了传统意义的静态密码功能。用户要想访问某个特定的数据或信息资源，除了输入一个静态密码，还要输入一个动态的代码。

根据信息系统对双因素认证的需求和应用情况，可将双因素强身份认证系统部署为一个面向各个相关应用系统的统一强身份验证服务，或者和 VPN 接入联合对外部接入用户进行身份认证。所有对重要业务系统的访问均需经过认证系统的强身份验证。

通过双因素的认证机制，每一个用户和一个身份认证令牌进行绑定，大大提高了登陆系统的认证安全级别，避免了用户名+密码 形式的安全风险。

采用双因素认证手段，可以方便地控制用户帐号的状态，如可以通过设置令牌的失效，禁止用户登录关键系统。

通过双因素身份认证的部署，即能满足内部工作人员原有的工作习惯（用户名 + 密码），同时又不会对现有的业务系统造成大规模改造工作，保证在最短的时间内实现内外网系统对用户的加强身份认证。

1.11.2. WEB 应用防护系统

WEB 应用系统承载着很多核心业务，而近年来网络攻击事件大部分都是由 WEB 应用所导致的。而 WEB 的开放性，易用性和 WEB 应用的易于开发性使 WEB 应用的安全问题日益突出。而防火墙只是通过端口限制实现访问控制，但对于 WEB 应用而言，其 HTTP/HTTPS 端口是开放的。因此，防火墙无法检测到 WEB 应用攻击的发生，更谈不上阻止攻击。使得现在 WEB 站点成为攻击者攻击的主要对象，表单篡改、跨站点脚本、命令插入、缓冲区溢出等各种 WEB 安全漏洞不断出现。根据权威网络安全机构的安全威胁报告，WEB 应用正成为最大的安全盲点。因此 WEB 应用安全问题也成为人们关注的网络安全核心问题之一。WEB 安全问题也成为人们关注的核心问题。对于已存在的 WEB 漏洞黑客可在短短几秒到几分钟内完成一次数据窃取、一次木马种植、完成对整个数据库或 WEB 服务器的控制，以至于非常困难做出人为反应。

本期在 DMZ 区互联网应用服务器组处部署 WEB 应用防火墙，从而解决以下问题：

1.防护 WEB 应用层攻击：WEB 应用防火墙可以防护如 SQL 注入、文件注入、命令注入、配置注入、LDAP 注入、跨站脚本等 WEB 攻击行为；

2.协议规范检查：WEB 应用防火墙可以阻断掉不规范的协议，从而障壁未知的攻击；

3.抗扫描：WEB 应用防火墙可以识别扫描行为，从而阻断黑客对 WEB 应用服务的非法扫描；

4.防护敏感信息的泄露：WEB 应用防火墙具备双向内容检测的能力，能识别服务器页面内容的敏感信息，防止敏感信息泄露，如服务器出错信息，数据库连接文件信息，WEB 服务器配置信息，网页中的连续出现的身份证、手机、邮箱等个人信息均可被 WAF 识别并依据策略采取相应的措施；

5.CC 攻击防护：基于 URL 级别的访问频率统计，并通过访问行为建模检测出 CC 攻击的来源，对 CC 攻击者采取限时锁定措施从而有效阻止 CC 攻击行为，该功能还可有效解决因验证码技术落后而导致的口令爆破问题。

1.11.3. 网页系统防篡改

信息系统内拥有众多 B/S 架构的 WEB 应用个系统，WEB 应用的普及使得信息

系统中存在的 WEB 服务器很容易成为不法份子的攻击目标。需要专业的应用系统防篡改工具有效阻止篡改事件的发生，维护 WEB 应用系统的安全。

本期在系统中部署 2 套网页防篡改系统，全面监测 WEB 服务器的页面是否正常。对于突破 WEB 应用防火墙的篡改行为，进行实时监控，确保应用系统的信息安全。一旦发现信息被篡改之后，应用防篡改系统会阻断恶意篡改行为并立刻通知监控中心的管理员。任何恶意篡改痕迹将被实时保留。

1.12. 安全服务测试

本项目安全服务应按照以下要求进行服务。

序号	服务名称	服务介绍	输出文档
1	渗透评估测试	结合采用安全评估工具以及专业的安全研究团队人工渗透测试，对应用系统及数据库、虚拟机进行深度安全测试，发现存在的安全漏洞及不安全配置，提供安全评估报告和整改建议。	《渗透测试报告》
2	安全巡检	对业务系统及数据库系统进行定期现场安全巡检，掌握应用系统存在的安全隐患，及时落实修补措施，并提供巡检报告。	《安全巡检报告》
3	安全加固	针对巡检和评估过程中存在安全脆弱点的网络架构、网络设备、操作系统、应用系统和数据库系统，根据安全加固工程师制定的安全加固方案进行现场安全加固，并提供加固报告。	《安全加固报告》
4	应急响应	在发生安全事件后进行 7×24 小时应急响应，快速协助进行系统恢复，尽可能降低安全事件对系统的正常运营所造成的影响，同时对安全事件进行分析，查找事件原因，对其中存在的安全隐患进行规避。	《应急响应报告》
5	安全咨询	以电话、邮件的方式提供可疑事件分析、漏洞信息深入解释、安全建议等包括网站安全在内的各类安全相关问题的咨询。	《安全建议报告》

序号	服务名称	服务介绍	输出文档
6	安全通告	根据目前的信息安全形势，实时提供应用安全相关漏洞的安全通告以及解决方案。	《安全通告》
7	安全培训	现场培训：产品培训及其他项目实施中必要的培训。	《培训材料》
		集中培训：安全技能和安全意识培训，内容由甲方定制。	《培训材料》
8	安全策略分析	分析现有信息安全策略，根据应用系统实际情况，提供适合安全保障需要的安全策略改进建议。	《安全策略建议报告》
9	安全总结报告	经过全面检测、分析、防护和加固，根据系统运行状况，提供系统年度安全报告。	《年度安全报告》

1.13. 部署要求

本期新增设备在网络中具体部署位置如下描述：

1.互联网接入区

（1）本期在互联网接入区部署 1 台接入交换机，实现医院网络对外数据或外部数据访问医院网络的数据交互。

（2）本期在互联网接入区部署 1 台互联网接入区防火墙，实现边界与内网区域的逻辑隔离和访问控制。

（3）本期在互联网接入区部署 1 台防病毒网关，实现对医院整个网络进出口流量进行病毒扫描。

（4）本期在互联网接入区部署 1 台上网行为管理系统，进行身份识别、行为管理、行为分析、应用控制、内容管控、流量管控、非法热点管控、无线网络管理等功能，实现医院全网全终端统一的上网行为的管理、控制与审计。

（5）本期在互联网接入区利旧现网 1 台 VPN 网关设备，实现在外医护人员

通过互联网访问医院的相关内部系统。

2.核心区

本期在核心区利旧现有2台思科N9K核心交换机,采用虚拟化方式进行部署,实现各个区的汇聚接入，由于现有核心交换机万兆光口数量不足，本期需要进行万兆光模块采购。

3.关键业务服务器存储区

（1）本期在关键业务服务器存储区部署2台服务器存储区IPS设备、2台服务器存储区防火墙设备，实现边界访问控制，对入侵行为进行主动防范；同时IPS设备开启AV模块，对恶意代码进行过滤。

（2）本期在关键业务服务器存储区部署1台数据库审计系统，对访问数据库的行为进行记录和审计，防止误操作以及对恶意操作进行追溯。

（3）本期在关键业务服务器存储区部署1台虚拟化防病毒服务器，在虚拟化防病毒服务器上部署虚拟化防病毒系统，对服务器虚拟化环境提供安全防护，同时针对现有3台非虚拟化HIS服务器部署3套服务器防病毒软件。

（4）本期在关键业务服务器存储区部署2台交换机，实现服务器存储区的数据交互。

4.非关键业务服务器区

本期在非关键业务服务器区利旧现网1台思科ASA5515-K9防火墙及1台绿盟入侵防御设备，为该区域服务器提供安全防护。

5.DMZ区

（1）本期在DMZ区部署1台Web防火墙，利旧现网1台防火墙，用于对网站系统进行保护，防止SQL注入，挂马等攻击行为。

（2）本期在 DMZ 区部署 1 台交换机，实现 DMZ 区的数据交互。

6.安全管理区

（1）本期在安全管理区利旧现网 1 台 Cisco ASA5515 防火墙，实现边界访问控制。

（2）本期在安全管理区利旧现网 1 台 Cisco 3750 交换机，实现安全管理区的数据交互。

（3）本期在安全管理区部署 1 套堡垒机，统一对网络设备、服务器、安全设备进行管理，并对运维管理行为进行审计。

（4）本期在安全管理区部署 1 台主机加固服务器，上部署主机加固系统，对系统和应用通过扫描，基于已发布漏洞，和安全选项的相关情况进行综合评估。

（5）本期在安全管理区部署 1 套日志审计系统，对全网网络设备、服务器、安全设备进行日志集中收集与分析。

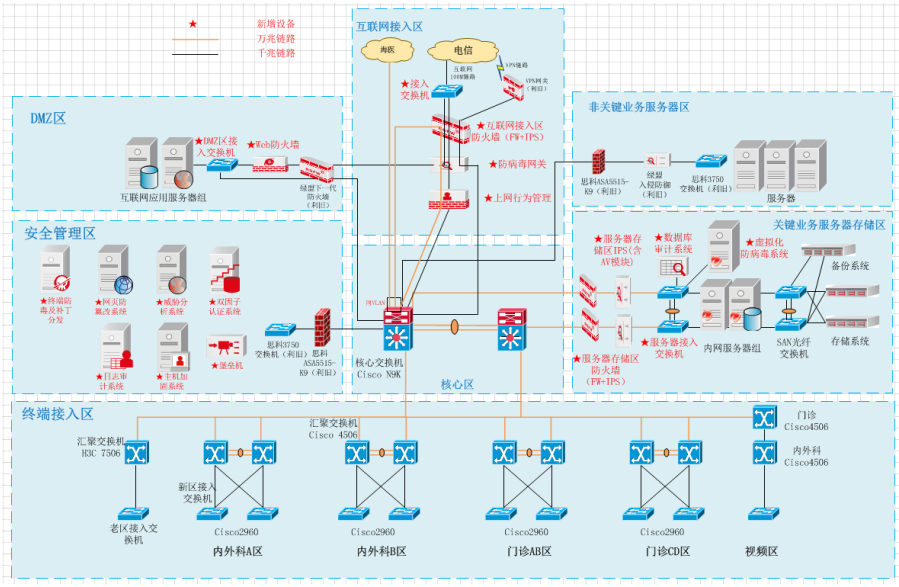
（6）本期在安全管理区部署 1 台双因子认证服务器，上部署双因子认证系统，实现在账号认证基础之上，增加动态密码，实现双重因子认证，从而有效保护用户认证安全。

（7）本期在安全管理区部署 1 套威胁分析系统，对各类攻击进行检测。

（8）本期在安全管理区部署 1 台网页防篡改服务器，上部署网页防篡改系统，对网站系统进行保护，防止对网站的篡改行为。

（9）本期在安全管理区部署 1 台终端防病毒及补丁分发服务器，上部署终端防病毒及补丁分发软件，实现对终端设备进行病毒防护及补丁管理功能。

本期项目改造后网络拓扑图如下所示：



新增设备部署在现有机房中，现有机房空间及电力能够满足项目需要。

1.14. 迁移方案

由于本期网络将进行功能区划分，工程实施过程中会出现服务器的搬迁或改接交换机/防火墙的情况发生。

因此在项目实施过程中，首先要规划好系统的功能，新增设备要首先进行上架安装，进行相关数据的调测，IP 地址的划分等工作，新增设备调测完毕后，需要寻找医院业务量少的时间进行服务器的调整及网络的割接工作，在割接过程中要提前预估好割接过程中出现的问题及风险，做好相关的防范工作，不能因为网络的调整造成医院的正常运营或网络瘫痪。

1.15. 运维方案

1.15.1. 运维服务内容

本项目运维单位为建设单位。运维内容包括服务器或系统平台部署、安装、迁移；运行期间预防巡检、出现的问题排查以及技术支持。

1.15.2. 运维服务提供方式

技术支持与技术服务主要包括电话支持、现场服务等。

1）电话支持

全年 7*24 小时在线电话及传真服务：客户服务工程师在接收到用户通报故障的电话、传真或 Email 后半小时之内将通过电话、传真或电子邮件等方式解决客户在使用过程中遇到的有关系统、服务器和网络的日常操作等方面的问题，并按规范记录存档。

2）现场服务

如通过电话或传真无法排除故障，需要在接到故障电话后 2 小时之内到达现场排除故障。

3）预防性维护

每季度 1 次的系统设备巡检

为保证系统正常运行，运维方对本项目提供周期为每季度 1 次的定期系统预防维护服务，巡检内容包括由专业工程师按周期对系统的使用情况进行了解并进行常规性检查、调试和清理工作，记录系统的运行情况，巡检的目的是帮助您更好地使用产品，提高系统性能，延长使用寿命，并以书面形式提交报告供存档。

三、 设备清单

序号	名 称	技术参数	单位	数量	备注
一	**网络安全改造**				
1	**硬件**				
1.1	互联网区接入交换机	1、▲交换容量≥590GGbps，包转发率≥250Mpps；10/100/1000Base-T 以太网口≥48 个，千兆光口≥4 个，千兆光模块≥4 个； 2、MAC 地址表项≥32K；支持 IPv4 静态路由、RIPv1/v2，支持 IPv6 静态路由、RIPng，支持 OSPFv1/v2，	台	1	

		OSPFv3； 3、支持端口镜像，支持流镜像，支持 802.1X 认证/集中式 MAC 地址认证。 4、最大堆叠台数≥9 台，最大堆叠带宽≥160G，可要求堆叠带宽>=80G，并要求实配接口的基础上额外满配堆叠带宽所需的接口和互联模块 5、支持跨设备链路聚合，单一 IP 管理，分布式弹性路由，支持通过标准以太端口进行堆叠（万兆或 40G 均支持），支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预，支持远程堆叠； 6、要求提供工信部入网证； 7、含 3 年原厂硬件保修。			
1.2	互联网接入区防火墙	详见四、主要设备参数要求。	台	1	需与服务器存储区防火墙的品牌异构，含 3 年特征库升级，3 年原厂设备质保。
1.3	防病毒网关	详见四、主要设备参数要求。	台	1	需与终端防病毒及补丁分发的品牌异构，含 3 年特征库升

					级，3 年原厂设备质保。
1.4	上网行为管理系统	详见四、主要设备参数要求。	台	1	含 3 年特征库升级，3 年原厂设备质保。
1.5	服务器存储区防火墙	详见四、主要设备参数要求。	台	2	需与服务器存储区 IPS 的品牌异构，含 3 年特征库升级，3 年原厂设备质保。
1.6	服务器存储区 IPS	详见四、主要设备参数要求。	台	2	需与服务器存储区防火墙的品牌异构，含 3 年 AV 特征库和 IPS 攻击规则特征库升级，3 年原厂设备质保。
1.7	服务器存储区接入交换机	1、▲交换容量≥750GGbps，包转发率≥300Mpps；10/100/1000Base-T 以太网口≥48 个，1G/10Gbps 速率	台	2	

		SFP+口≥4 个，万兆光模块≥4 个； 2、MAC 地址表项≥90K；支持 IPv4/IPv6 静态路由，RIPv1/v2、/RIPng，OSPFv1/v2、OSPFv3，等价路由，策略路由；支持 N：1 端口镜像，支持 N：4 端口镜像；支持 STP/RSTP/MSTP 协议； 3、最大堆叠台数≥9 台，最大堆叠带宽≥320G;支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预； 4、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。无需软件授权； 5、冗余电源； 6、含 3 年原厂硬件质保。			
1.8	Web 防火墙	详见四、主要设备参数要求。	台	1	含 3 年特征库升级，3 年硬件保修。
1.9	DMZ 区接入交换机	1、▲交换容量≥590GGbps，包转发率≥250Mpps；10/100/1000Base-T 以太网口≥48 个，千兆光口≥4 个，千兆光模块≥4 个； 2、MAC 地址表项≥32K;支持 IPv4 静态路由、RIPv1/v2，支持 IPv6 静态路由、RIPng，支持 OSPFv1/v2，OSPFv3； 3、支持端口镜像，支持流镜像，支持 802.1X 认证/集中式 MAC 地址认证。	台	1	

		4、最大堆叠台数≥9 台，最大堆叠带宽≥160G，可要求堆叠带宽>=80G，并要求实配接口的基础上额外满配堆叠带宽所需的接口和互联模块； 5、支持跨设备链路聚合，单一 IP 管理，分布式弹性路由，支持通过标准以太端口进行堆叠（万兆或 40G 均支持），支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预，支持远程堆叠； 6、要求提供工信部入网证； 7、含 3 年原厂硬件保修。			
1.10	数据库审计系统	详见四、主要设备参数要求。	台	1	
1.11	日志审计系统	详见四、主要设备参数要求。	台	1	
1.12	威胁分析系统	详见四、主要设备参数要求。	台	1	含 3 年特征库升级，3 年硬件保修。
1.13	堡垒机	详见四、主要设备参数要求。	台	1	
1.14	虚拟化防病毒服务器	2 颗 E5 6 核处理器；内存：2*16G ；硬盘：2*600G 10K；配置 Raid 卡，1GB 缓存，支持 RAID 0, 1；网卡：1 张 2 端口千兆网卡；冗余电源；上架导轨；带远程管理卡。	台	1	
1.15	网页防篡改服务器	2 颗 E5 6 核处理器；内存：2*16G ；硬盘：2*600G 10K；配置 Raid 卡，1GB 缓存，支持 RAID 0, 1；网卡：1 张 2 端口千兆网卡；冗余电源；上架导轨；带远程管理卡。	台	1	
1.16	双因子认证服务器	2 颗 E5 6 核处理器；内存：2*16G ；硬盘：2*600G 10K；配置 Raid 卡，	台	1	

		1GB 缓存，支持 RAID 0, 1；网卡：1 张 2 端口千兆网卡；冗余电源；上架导轨；带远程管理卡。			
1.17	主机加固服务器	2 颗 E5 6 核处理器；内存：2*16G ；硬盘：2*600G 10K；配置 Raid 卡，1GB 缓存，支持 RAID 0, 1；网卡：1 张 2 端口千兆网卡；冗余电源；上架导轨；带远程管理卡。	台	1	
1.18	终端防病毒及补丁分发服务器	2 颗 E5 6 核处理器；内存：2*16G ；硬盘：2*600G 10K；配置 Raid 卡，1GB 缓存，支持 RAID 0, 1；网卡：1 张 2 端口千兆网卡；冗余电源；上架导轨；带远程管理卡。	台	1	
1.19	核心交换机光模块	万兆光模块（多模）	个	4	
1.20	核心交换机光模块	万兆光模块（单模）	个	9	
2	**软件**				
2.1	服务器和虚拟化防病毒系统	无限控制台（无服务器，CPU 数量使用上限)详见四、主要设备参数要求。	套	1	需与终端防病毒及补丁分发的品牌异构，含 3 年特征库升级，3 年原厂质保。
2.2		无代理防病毒模块，详见四、主要设备参数要求。	CPU	48	
2.3		服务器防病毒软件,详见四、主要设备参数要求。	套	3	
2.4	终端防病毒及补丁分发	详见四、主要设备参数要求。	点	1500	需与服务器和虚拟化防病毒系统的品牌异构，

					含 3 年特征库升级，3 年原厂质保。
2.5	网页防篡改系统	详见四、主要设备参数要求。	套	2	
2.6	双因子认证系统	1、 用户并发接数≥100 个；设备认证授权数≥500；硬件令牌≥20 个，手机 APP 令牌≥20 个。 2、 实现在账号认证基础之上，增加动态密码，实现双重因子认证，从而有效保护用户认证安全； 3、 提供 Radius 认证模块，包含动态密码认证模块，支持 Windows/Linux 操作系统； 4、 支持与认证服务器联动实现帐号的双重保护支持动态令牌（硬件、手机、短信令牌）； 5、 自服务平台支持用户修改密码，自服务平台支持用户绑定及解绑令牌； 6、 支持第三方接口：提供对外 API 接口，供第三方系统调用增加、删除、修改账号； 7、 认证系统支持多种认证方式并存：硬件令牌、短信令牌、手机 APP 令牌，允许用户绑定多种、多个令牌； 8、 令牌存储安全：手机令牌密钥存储存储在操作系统的安全区，其他程序不可读取，手机令牌 APP 安全保护通过代码混淆后发布，硬件令牌密钥存储存储在 RAM 中，暴力破解导致掉电后密钥销毁，服务器中令牌密钥存储使用 AES +	套	1	

		IV 加密存储； 9、 令牌激活方式支持持管理员统一激活、短信激活、邮件激活、帐号密码激活、用户自服务平台等多种方式，自动化令牌发放与回收，统自动管理注销账号的令牌，提供 IT 运维管理的效率。 10、 令牌解绑：支持管理员解绑，单个解绑、批量解绑、筛选解绑（查询过滤后批量解绑、使用模板文件批量解绑）； 11、 手机 APP 令牌优化移动应用安全接入体验-Widget 令牌-通过 Wiget 下拉令牌，并支持 LOGO 自定义； 12、 第三方应用兼容性良好：Cisco、Citrix、华为等厂商的官方合作伙伴，支持 VPN、服务器、数据库、堡垒机、网络设备、虚拟化、WEB 应用等各种应用场景的双因子认证登录，同时支持主流设备的策略下发。 13、 多种数据源无缝集成：除支持 AD、LDAP 等标准帐号源外，还可以从客户自定义系统中（OA、ERP、CRM）同步用户数据； 14、 支持渐进式部署：在大企业中，可通过部署策略定向为不同批次用户逐渐开启双因素认证，避免系统风险。 15、 高级策略：认证时候是否需要动态密码验证，默认所有用户都不需动态密码检验。可针对不通的角色设置是否需要动态密码验证，策略执行顺序自上而下顺序执行； 16、 含 3 年原厂质保。			

2.7	主机加固系统	1、▲支持“操作系统加固”功能，基于操作系统内核加固技术，针对操作系统核心资源，如注册表、网络连接、系统文件、进程等资源进行有效防护； 2、支持细粒度的多种资源客体的强制访问控制，允许多种资源主体类型以不同访问权限对多种资源客体设制访问规则；访问控制资源客体包含文件、进程、服务、磁盘、共享文件、通信端口等，提供强化应用软件安全性证书； 3、支持对各种资源添加敏感标记； 4、支持 Windows、Linux、UNIX,红旗、中标麒麟等全系列操作系统； 5、将非管理员组账户添加到管理员组；禁止在系统目录下对可执行类型文件进行写操作；禁止修改 host 文件；禁止添加启动项；禁止磁盘低级操作；禁止加载没有数字签名的驱动； 6、“登录防护”功能，针对 Windows 及 Linux 操作系统的远程登录进行限制及防护，用户可对“用户名”、“IP 地址范围”、“时间范围”进行具体设置，并通过选择“允许登录”、“禁止登录”等相应的处理方式进行防护； 7、▲支持在网络空间中实现根据不同的应用分别创建出多个虚拟网络应用安全区域，实现应用安全区域与应用安全区域之间的隔	套	1	含 3 个 WINDOWS 或 LINUX 版本授权

		离，用户可将需要保护应用主机，添加进被保护应用对应的安全域内；实现虚拟安全边界的划分需提供截图证明并加盖原厂商章； 8、▲一键式“安全巡检”功能，针对服务器的目录及文件进行全面巡检扫描，对服务器存在的安全隐患进行检查并修复；“服务器安全”主要针对计划任务、账户（登录账户、克隆账户、隐藏账户），实现虚拟安全边界的划分，需提供截图证明并加盖原厂商章； 9、具有系统自身的保护功能，保护系统自身进程不被异常终止、伪造、信息注入； 10、 防止端口扫描，可以防止应用端口被外部扫描器、嗅探工具基于基线扫描检测，拒绝不合法请求； 11、 ▲支持防护日志功能提供对防护过程中所产生的各类日志的查询，包括：系统防护日志、登录防护日志及巡检日志；日志中包含具体时间、日志类别及描述等信息，用户可将日志导出，以便保存、查阅，需提供截图证明并加盖原厂商章； 12、 能够通过应用探针自动识别用户应用类型、版本、漏洞；根据获得的应用相关信息，评估已存在和可能存在的风险；对系统和应用通过扫描，基于已发布漏			

		洞，和安全选项的开关情况进行综合评估。需提供漏洞检测方法及装置专利证书； 13、 支持各功能模块的一键式手动关闭和开启，支持至少三种级别的防护级别控制； 14、 产品具有销售许可证； 15、 ▲符合国家信息系统安全等级保护操作系统安全的三级标准，必须全项通过公安部 GB/T20272-2006 信息安全技术三级认证； 16、 ▲具有国家保密局颁发的涉密产品证书； 17、 具备中华人民共和国国家版权局颁发的计算机软件著作权登记证书； 18、 产品具备国家军队颁发的产品检测通过证书。			

四、 主要设备参数要求

1. 互联网接入区防火墙

产品要求	详细说明
下一代防火墙	1. 整机吞吐量≥16Gbps； 2. 应用层吞吐量≥8Gbps； 3. 并发连接数≥250 万； 4. 每秒新建连接数≥25 万； 5. 设备接口：千兆电口≥6 个，千兆光口≥4 个，万兆光口≥2 个

	（含模块）； 6. 支持 BYPASS； 7. 电源：冗余电源； 8. 尺寸：标准 2U 架构； 9. 部署方式：支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式； 10. 支持根据国家/地区来进行地域访问控制；（需提供相关功能截图证明并加盖厂商公章） 11. 内容安全：内置病毒样本数量超过 200 万； 12. 支持 URL 过滤和文件过滤功能，URL 过滤支持 GET，POST 请求过滤和 HTTPS 网站过滤，文件过滤支持文件上传和下载过滤； 13. 支持针对 SMTP、POP3、IMAP 邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，支持根据邮件附件类型进行文件过滤；（需提供相关功能截图证明并加盖厂商公章） 14. 入侵防护功能：设备具备独立的入侵防护漏洞规则特征库，特征总数在 7000 条以上； 15. ▲可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；（需提供相关功能截图证明并加盖厂商公章） 16. Web 应用安全防护：设备具备独立的 WEB 应用防护识别库，特征总数在 3000 条以上； 17. 支持 Web 漏洞扫描功能，可扫描检测网站是否存在 SQL 注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞； 18. ▲支持对网站黑链进行检测；（需提供相关功能截图证明并加盖厂商公章） 19. 支持 Windows 和 Linux 系统下网页防篡改功能； 20. 僵尸主机检测：支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； 21. 对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告；（需

	提供具备相关云端查杀能力的证明并加盖厂商公章） 22. ▲支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址；（需提供具备相关云端大数据分析能力的证明并加盖厂商公章） 23. 安全可视化：支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别； 24. 支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证； 25. 系统配置管理：支持安全策略一体化配置，通过一条策略既可实现不同安全功能的配置； 26. 厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位；（提供相关证明） 27. ▲信息技术产品安全测评证书（EAL3+）；（提供相关证明）.

2. 防病毒网关

产品要求	详细说明
功能要求	(1) 支持超过 100 种协议支持，如 HTTP/HTTPS/FTP/SMTP/POP3/TFTP/TCP/UDP/NFS/SNMP/ICMP/RTMP/DNS/IRC…
	(2) 支持二至七层全协议应用防火墙、用户及终端管理、应用识别及管理带宽管理及控制、防 DoS/DDoS
	(3) 防已知恶意软件（病毒、木马、蠕虫、后门、加密勒索软件、间谍软件、灰色软件、Rootkits 等）
	(4) APT 防护支持，包括 C&C 违规外联及僵尸网络检测及拦截、支持已知文档漏洞检测及拦截、支持未知文档漏洞及零日文档漏洞检测及拦截
	(5) ▲可与深度威胁发现系统 TDA 联动，获取 APT 增强侦测模块 TDA 侦测到的本地 C&C 黑名单，并阻止 C&C 违规外联（提供截图证明并加盖原厂公章确认）

	(6) 可提交可疑文件、URL、IP 及域对象至 APT 增强定制化沙箱模块 DDAn 做联动分析，并根据 DDAn 的分析结果做进一步处理
	(7) 支持入侵检测及虚拟补丁防护，实现服务器及终端虚拟补丁和主动式主机入侵防御系统，可在漏洞攻击主机之前予以侦测和拦截，防止漏洞利用和 SQL 注入，命令注入，Webshell 攻击，XSS 攻击，CSRF 攻击及主机零日漏洞防护，至少具备 6,000+条虚拟补丁及入侵检测特征库
	(8) 支持 WEB 安全检测及防护，包括不限于如下功能：
	a:URL 信誉检测，包括恶意网站主动实时防御，支持黑白名单
	b:URL 分类过滤（支持自定义 URL 分类）\钓鱼网站检测
	c:▲URL 信誉检测，支持恶意网站主动实时防御、黑白名单（提供截图证明并加盖原厂公章确认）
	d:▲能够对 Web 信誉进行设置，至少包括高、中、低三个级别，设定对 URL 地址的敏感度（提供截图证明并加盖原厂公章确认）
	e:支持本地 URL 信誉检测及云端实时 URL 信誉检测两种检测模式"
	(9) 支持邮件安全检测：
	支持垃圾邮件检测、病毒邮件、恶意邮件检测
	支持邮件黑白名单，支持关键字和正则表达式内容过滤
	支持邮件隔离、带标记转发、记录、清除恶意附件保留邮件正文转发等管理功能"
	(10) ▲具备完善的病毒检测能力，包括 3,000,000+种病毒识别码，每年约新增 750,000+识别码，病毒检测能力通过全球病毒实验室+本地病毒实验室支持，病毒码须为自主研发（须提供官方的证明及病毒码更新地址截图，并加盖原厂公章确认）
	(11) 全球 1300+ 应用程序协议支持,包括不限于如下协议及程序控制：
	点对点 (P2P) 软件控制: Ares,Bittorent,Blubster,eDonkey,Kazaa,Gnutella,Winny,Foxy
	IM 软件登陆及文件控制: AIM,GoggleTalk,MSN,Skype,Yahoo messenger
	网络游戏控制、股票软件控制、流媒體/音频/视频软件控制

	数据库软件控制、文件服务器软件控制、论坛软件控制、邮件软件控制、Microsoft 软件控制、精简客户端软件控制、Web 应用控制、Web 邮件控制、无界,自由门软件控制″
	(12)流量控制功能：支持基于策略（源和用户/目标/通讯类型/时段）的带宽控制、包括上行流量/下行流量的带宽控制、最大带宽限制/最小带宽保证、带宽服务优先级
	(13)针对不同用户分组利用策略分类管理、支持 MS AD 及 Open LDAP 用户认证，支持网页认证及透明认证方式
	(14)部署模式：支持桥接模式、路由模式、监控模式（旁路模式)、混杂模式（桥接+路由）、多路 ISP & WAN 模式，并能支持以虚拟设备的方式部署在 VMWare、FusionShpere、KVM、Xen、Hyper-V 等主流虚拟化平台
	(15)支持中文 Web 界面管理、提供命令行（CLI）配置模式、提供 SSH 远程调试模式、SNMP 管理
	(16)支持自动/手动在线升级，可配置自动升级周期，采用全球病毒码更新源或者本地升级源的设计，降低升级带宽使用
	(17)日志管理功能需提供：安全日志/流量日志/VPN 日志/系统日志/审计日志的查询/打印/导出，可按照时间，协议，威胁类型等查询条件查询日志，提供基于策略（源和用户/目标/通讯类型/时段）的流量日志记录/查询/打印/导出，支持 Syslog 协议，可以实时传输日志到 Syslog 服务器
	(18)报告系统须提供日/周/月图形化报表，以及实时图形化报表，按源用户/源地址生成报告，提供恶意软件/垃圾邮件/入侵防御/Web 信誉服务违例事件安全报告，前 N 个用户违例报告，以及按应用程序/URL 类别/带宽使用等前 N 个通信报告
	(19)通知功能须支持 URL 访问警告通知及 URL 阻止通知，安全信息汇总/监控硬件异常/系统资源警告/预设更新等通知、CPU 阀值/数据分区阀值/硬盘容量阀值/交换内存阀值监视警告等
	(20)安全性要求支持通过加密的 SSL 命令行远程管理以及通过加密的 SSL 访问管理控制台
	(21)硬件可靠性要求系统保证 36 月，下一个工作日提供备机，同时设备支持 Fail Open 功能，在停电与系统出现问题时自动实

	现直通功能、流量过载保护功能；硬件自带液晶屏幕,可快速显示设备硬件故障
产品资质要求	(1) 产品具备 ISCCC 中国信息安全产品认证“防火墙一级”认证
	(2) 产品具备公安部“防火墙一级”销售许可证
	(3) 产品具备公安部“防病毒网关”销售许可证
	(4) 获得国家强制性产品 3C 认证证书
	(5) 提供 5 个 USB 接口，其中 4 个外置 USB 和 1 个内置 USB（提供设备实物图片并加盖原厂公章确认）
厂商资质	(1) 厂商在国内有独立的监控中心
	(2) 厂商可根据用户需求提供高级别的服务承诺，如大客户专署服务、主动式服务、快速响应服务(SLO/SLA)、在线技术支持服务等，可提供 5×8 乃至 7×24 小时的专业防毒服务
	(3)厂商有独立的研发中心
	(4)厂商有独立的病毒响应中心
	(5) 通过中国信息安全评测认证中心的《信息安全服务资质标准》的信息安全服务一级资质认证

3. 上网行为管理系统

产品要求	详细说明
上网行为管理	1. 网络吞吐≥10Gbps； 2. 用户规模≥50000 人； 3. 设备接口：千兆电口≥4 个，千兆光口≥4 个；万兆光口≥2 个 4. 支持 BYPASS； 5. 冗余电源； 6. 尺寸：标准 2U 架构； 7. Web 访问质量检测：针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级；支持以列表形式展示访问质量差的用户名单；支持对单用户进行定向 web 访

	问质量检测；（提供产品界面截图，加盖厂商公章） 8. 用户密码强度：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；可设置密码最小长度；可设置密码必须包括数字或字母或特殊字符；（提供产品界面截图，加盖厂商公章） 9. 应用管理：支持根据标签选择应用，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；支持给每个应用自定义标签；支持根据标签选择一类应用做控制；支持对每一种应用的定义和解释，帮助客户快速定位应用的分类；支持给每一种应用列上图标，易于客户了解应用的特征； 10. 应用识别规则库：设备内置应用识别规则库，支持超过 6000 条应用规则数，支持超过 2800 种以上的应用，1000 种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率；支持根据应用的特征智能识别新更新的应用；支持根据 IP、端口、协议等自定义应用规则；支持根据不同的应用类型或具体的某种应用设置允许或拒绝； 11. SSL 加密内容过滤：针对 SSL 加密的网站、论坛发帖、web 邮箱以及客户端邮箱（如闪电邮）的内容进行关键字过滤； 12. SSL 加密内容审：针对 SSL 加密的网站、论坛发帖、web 邮箱以及客户端邮箱（如闪电邮）的内容进行审计； 13. 应用审计：支持记录 QQ、MSN 等 IM 聊天行为和传文件的内容；支持移动 APP（IOS 和 android）审计（如论坛类、微博类、新闻评论类等；支持金融类应用内容审计如：阿里旺旺、万德（Wind）、路透等应用的聊天内容。 14. ▲加密 SMTP 邮件过滤：支持对加密 HTTPS、SMTP-SSL、SMTP 的邮件进行关键字过滤；（提供产品界面截图） 15. 多终端自绑定：同一个账号，支持与指定数量的多个终端进行自动绑定；（提供产品界面截图,加盖厂商公章） 16. ▲P2P 智能流控：支持通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题。（提供产品界面截图，加盖厂商公章）

	17. 流控黑名单：基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中；（提供产品界面截图，加盖厂商公章） 18. ▲加密证书自动分发　审计 SSL 网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台 PC 单独安装证书的问题（要求提供产品界面截图） 19. ▲所投产品具有国家网络与信息系统安全产品质量监督检测中心《信息技术产品安全分级评估证书-评估保证级 3（EAL3 级）》（提供相关证明） 20. 所投产品获得 IPv6 Ready Phase-2 认证（提供相关证明）

4. 服务器存储区防火墙

产品要求	详细说明
硬件规格	双交流电源；≥12*GE 电口，≥12*SFP 光口，≥4*万兆光口，万兆光模块≥4 个；网络吞吐量≥20Gbps；最大并发连接数≥500 万，每秒新建 HTTP 连接数≥30 万
部署模式	支持路由模式、透明（网桥）模式、混模式，支持将多个物理网口加入一个网桥中；部署模式切换无需重启设备；支持镜像和被镜像；
NAT	支持源地址转换、目的地址转换、双向地址转换、NAT44
4G 支持	▲支持 4G 扩展网卡。支持在 4G 接口上运行 IPSec VPN，提供 web 配置界面截图
安全通信	接口实际配置支持 second IP 地址；每个接口要求支持至少 200 个 second IP。（提供相关截图证明并盖章）
VPN	实际配置支持 IPSecVPN 接入，内置 VPN 硬件协处理器 实际配置支持 DES、3DES、AES 加密算法。（提供相关截图证明并盖章）
SSL 加密内容审计	支持 HTTPS 解密功能，支持管理界面及命令行配置解密策略，包括入接口、源地址对象、目的地址对象、https 对象、域名排除等；支持 HTTPS 域名库，预定义域名以及自定义域名

	▲支持审计 HTTPS 加密邮箱，支持审计主题、内容、附件等，支持本地下载邮件原件。（提供相关截图证明并盖章）
	支持针对 HTTPS 网站、HTTPS 门户搜索等内容进行审计
应用协议识别	▲支持智能和快速识别模式配置。（提供相关截图证明并盖章） 支持日流量限额、时长限额，超过阈值提供弹窗提示且可自定义； 支持流量和时长的月限额（提供相关截图证明并盖章）
防私接路由	支持私接用户的 PPPoE 账号展现（提供相关截图证明并盖章）
用户认证功能	支持 WEB Portal 认证功能，支持本地认证、Radius 认证、LDAP 认证 和 LDAP 用户同步，支持对接 IMC、AAS、SAM 等常见 AAA 服务器，支持配置强制重新认证间隔，支持配置认证通过后重定向 URL，要求本机自身支持短信认证功能，提供 web 界面配置截图
	支持 portal 服务器联动，支持 radius 服务器联动，支持实现 NAS-Identifier(32)在无线场景携带 AC 名字
	支持认证页面自定义
	▲支持微信认证功能，使用微信连 WiFi2.0 接口，限制微信流量放通（pc 和移动端，认证通过放通），支持基于 http 获取 access_token，支持微信内部浏览器 http 弹 portal。强制关注功能（定时检查用户是否关注公众号）。（提供相关截图证明并盖章）
	支持短信认证，登录后方可认证上网
	支持混合认证，支持界面配置选择多种认证方式，用户可根据需要更换认证方式（提供相关截图证明并盖章）
内网资产发现	▲支持内网资产自动发现能力，支持发现资产的操作系统、浏览器、应用、杀毒软件、服务的类型（提供相关截图证明并盖章）
非法外联防护	支持服务器非法外联基线数据自学习的功能，可以自主选择学习时长。支持外联的地址白名单和协议白名单（提供相关截图证明并盖章）
防暴力破解	▲支持防护 telnet、ftp、imap、pop3、smtp、http、oracle、mysql 等协议的暴力破解。支持自定义检测时长和检测阈值。（提供相关截图证明并盖章）
应用缓存	支持文件缓存，支持安卓和 IOS 形式的文件，文件形式不限于视频、APP、文本文件等（提供相关截图证明并盖章）

双机热备	支持双机热备，支持主主模式、主备模式，支持同步配置、会话、运行状态、VPN 状态、特征库，支持配置抢占模式和抢占延时，支持配置 HA 监控接口（提供相关截图证明并盖章）
配置管理	支持通过管理平台进行集中管理，统一升级，下发配置，收集日志
系统维护	web 管理界面支持 Ping、Traceroute、TCP Syn 诊断工具，可支持基于接口、协议、IP 地址、端口、应用进行网络抓包，并可下载导出分析。（提供相关截图证明并盖章） 支持管理员双因子认证
资质证明	通过公安部检测并获得公安部计算机信息系统安全专用产品销售许可证（提供证书复印件并盖章证明）

5. 服务器存储区 IPS

产品要求	详细说明
设备要求	▲提供的产品为 2U，含交流冗余电源模块，2*USB 接口，1*RJ45 串口，2*RJ45 管理口，4 个电口+4 个万兆接口，4 个 SFP 万兆光纤接口模块，1 个接口扩展槽，硬盘容量 1T。吞吐量 5Gbps，网络层吞吐量 14Gbps，应用层吞吐 5Gbps，最大并发 TCP 会话数 400 万，每秒新增 TCP 会话数 12 万。
入侵防护功能	系统应提供覆盖广泛的攻击特征库，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测和阻断，攻击特征库数量至少为 6000 种以上。

批注 [S1]: 笔误，应该是 SFP

	系统须提供对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解等恶意流量的检测和阻断;系统应能够有效抵御 SQL 注入等多种常见的应用层安全威胁。
高级威胁防护	系统应提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为。
	系统应提供关键文件保护功能，能够识别、阻断通过自身的关键文件，以防止非法外传行为。能识别的关键文件类型应包含至少以下几类：文档类如 Excel、PDF、PowerPoint、Word 等，压缩文件类如 CAB、GZIP、RAR、ZIP、JAR 等，图像类如 BMP、GIF、JPEG 等，音频视频类如 MP3、AVI、MKV、MP4、MPEG、WMV 等，脚本类如 BAT、CMD、WSF 等，程序类如 APK、DLL、EXE、JAVA_CLASS 等。
	系统应提供基于信誉的僵尸网络防护能力,具备可以持续升级的信誉库，IPS 通过信誉库内的恶意网站 IP、C&C 服务器地址的信誉值执行相应的防护动作。
沙箱联动	支持提供恶意软件分析服务。
	支持对未知可疑文件统计。
	系统应提供定时自动发送报表功能,支持在指定的时间内将生成的报表以 html、word、excel 等通用格式通过 FTP 或邮件发送给指定的管理员，以减少日常维护工作量。须提供界面截图。
部署模式	系统应支持 IPS 和 IDS 的混合运行模式,同时提供入侵防护和入侵

	检测功能。
产品成熟度证明	投标 IPS 产品应具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》、《计算机软件著作权登记证》，提供有效证书的复印件。

6. Web 防火墙

产品要求	详细说明
资质	产品中国信息安全认证中心《IT 产品信息安全认证证书》 产品具有 EAL3+资质证书
硬件参数	标准 2U 硬件平台，≥2*GE 电管理口，≥4*GE 电业务口（含 2 组硬件 BYPASS 模块），≥4*GE 光业务口，硬盘：≥1T，1*RS232 串口，标准可热插拔电源模块*2；扩展：工作口最大可扩展 12*GE 光/电口
性能参数	应用吞吐量不小于 4000Mbps HTTP 并发连接不小于 30 万 HTTP 新建连接(CPS)不小于 3 万 最大保护站点 32 个
部署方式	透明桥部署：防护口不占用 IP 地址，实现完全透明部署
	端口镜像部署：镜像服务器流量即可实现安全审计和告警
	反向代理部署：可支持代理和路由牵引两种模式，客户端源 IP 可采用透明和非透明两种转发机制，非透明可指定字段进行识别，支持前后端口分离，支持多台 WAF 设备冗余和集群部署，提供界面截图并加盖公司公章
	支持虚拟化部署，支持 KVM、Xen、VMWare 等虚拟机环境，并支持 WAF 镜像导入，需提供第三方测评机构（须是公安部三所、国家保密局、ISCCC 其中一家）的检测报告复印件加盖公章

WEB 服务自发现	▲支持 WEB 站点服务自动侦测功能，支持自动识别 VLAN 信息（提供界面截图并加盖公司公章）
防御功能	能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括 SQL 注入、命令注入 、Cookie 注入、代码注入、LDAP 注入、SSI 注入文件注入等)、跨站请求伪造等应用攻击行为
	内置主流 Webshell 特征库，对上传内容进行检查，防止恶意 Weshell 上传
	WAF 能自动识别扫描器的扫描行为，并智能阻断如 Nikto、Paros proxy、WebScarab、WebInspect、Whisker、libwhisker、Burpsuite、Wikto、Pangolin、Watchfire AppScan 、N-Stealth、Acunetix Web Vulnerability Scanner 等多种扫描器的扫描行为
	内置身份证、银行卡等服务器敏感信息库，对服务器响应敏感内容进行隐藏，并支持自定义，提供界面截图并加盖公司公章
	支持 Cookie 安全机制，支持 Cookie 自学习，防止 Cookie 被篡改和劫持，并支持 Cookie Httponly
智能自学习功能	支持网站自学习建模功能，能通过自学习形成网站 URL 树； 通过自学习能生成安全防护策略；通过自学习能发现参数的名称、类型、匹配频率；可配置匹配到自学习特征后放行；可配置匹配不到自学习特征直接阻断请求；（提供界面截图并加盖公司公章）
智能攻击者锁定	▲支持智能识别攻击者，对网站连接发起攻击的 IP 地址进行自动锁定禁止访问被攻击的网站。可配置攻击者识别策略和算法，可配置攻击者锁定时间，可配置将攻击者直接加入网络黑名单。可展示攻击者发生的时间和攻击者所在的地理位置（提供界面截图并加盖公司公章）
基于时间的访问控制	可基于时间对客户端 IP 进行黑白名单控制。（提供界面截图并加盖公司公章）
防御动作	针对触发安全规则的行为进行阻断并发出告警页面
	告警页面支持重定向至其它 URL
WEB 访问行为合规	▲可实现访问流程的校验，向网站提交表单前必须先访问指定的网页，并等待可配置的时间长度后才能正常提交表单，需提供第三方测评机构（须是公安部三所、国家保密局、ISCCC 其中一家）的检测报

	告复印件加盖公章
CC 防护功能	▲可根据 URL、请求头字段、目标 IP、请求方法等多种组合条件对 CC 攻击进行检测，检测指标为 URL 访问速率和 URL 访问集中度；可根据 IP、IP+URL 和 IP+User_Agent 等算法对客户端进行检测，并支持应用层字段解析和自定义检测字段功能，支持挑战模式，支持基于地址位置的识别，支持对特定的 IP 地址进行 CC 规则白名单放行，支持 CC 慢攻击防护，通过学习业务流量模型，在业务流量异常时开启 CC 防护，并支持启动配置阈值，支持虚拟化部署，支持 KVM、Xen、VMWare 等虚拟机环境，并支持 WAF 镜像导入，需提供第三方测评机构（须是公安部三所、国家保密局、ISCCC 其中一家）的检测报告复印件加盖公章
地图态势分析	▲按地理区域对攻击次数等进行统计，通过地图展示，并在地图上可以指定某一地理区域进行访问控制，阻断此区域 IP 的访问，需提供第三方测评机构（须是公安部三所、国家保密局、ISCCC 其中一家）的检测报告复印件加盖公章
SSL 透明代理	支持 HTTPS 服务器的防护，可支持第三方认证机构颁发的证书链，WEB 应用防火墙前端与后端均为 HTTPS 加密链路，实现 HTTPS 应用系统的防御
	一个保护站点支持上传多个域名证书，提供界面截图并加盖公司公章
	可以选择需要支持的 SSL/TLS 协议版本，提供界面截图并加盖公司公章
移动安全运维	可通过移动端实现设备安全运维监控，APP 具备以下功能：支持查看当前 WAF 的告警数量包括最近 24 小时内以及总的告警数量。支持对攻击的服务器 IP 以及客户端 IP 进行统计。（提供界面截图并加盖公司公章）
智能联动	支持与同品牌的 APT 设备进行联动，对未知威胁流量进行检测和拦截（提供界面截图并加盖公司公章）

7. 数据库审计系统

产品要求	详细说明
硬件指标	审计产品采用专用工控机硬件架构，非普通 PC 服务器， MTBF(平均故障间隔时间)≥65000 小时； ▲系统启动采用 CF 卡加硬盘方式，保证稳定可靠不可篡改。（提供产品图片并盖原厂公章）
	电源模块：具备冗余热插拔双电源；冗余热插拔风扇； 硬盘可用容量：≥1TB*2，支持 RAID1， RAID5 阵列，最大支持扩展到 4T*2。 内存：≥8GB DDR3 1600Mhz； 网络端口：支持监听接口扩展；配备至少 1 个管理口，1 个 HA 口 支持千兆网络环境下的监听能力，标配至少 2 个千兆电口和 2 个千兆光口 支持最大扩展至 4 电 4 光或 8 电或 8 光。 审计性能：能够稳定、流畅地同时支持 8 个数据库数审计能力，不会产生漏审；
部署方式	旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计
	▲支持在目标数据库安装 agent 解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计 提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告
	支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询；
	支持大数据平台部署，具有成熟的大数据 hadoop 平台处理，支持后期无缝扩展大数据版本，支持审计数据外送至大数据平台，检索性能高达 100 亿数据仅需 6-8 秒，存储数据量高达 3000 亿以上，并具有至少提供一个 100 万以上大数据处理合同案例（需提供大数据合同关键页面复印件）
处理能力	吞吐能力：≥2000M，日处理业务操作数：≥4 亿条

	峰值处理能力：≥2 万条/秒；提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告
	审计日志检索能力：≥1500 万条/秒；
协议支持	支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL 等六种主流数据库审计；
	支持 PostgreSQL、Teradata、Cache、人大金仓、达梦、南大通用等数据库审计；
	支持 MongoDB、Hbase 非关系型数据库审计；
	▲支持对 SQL server（2005 及以上版本）数据库采用加密协议通讯，可以通过导入证书的方式实现审计和防护；（需提供功能截图，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告）
	支持对各种协议自动识别编码及在 web 界面手工配置特定编码（提供相关截图证明并盖章）
审计功能	支持数据库操作类、表、视图、索引、存储过程等各种对象的所有 SQL 操作审计；
	▲支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小（提供功能截图证明并盖原厂公章，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告）；
	应对数据库中所有初始化参数的状态进行审计。至少将数据库自身审计的启用和禁用、日志恢复的启动和禁用等信息记入审计日志（提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告）
智能发现	自动识别流量中存在的数据库，也可通过扫描发现网络中的数据库（提供相关截图证明并盖章）；
	▲支持定期自动扫描数据库漏洞和不安全配置，提供漏洞扫描报告；（需提供功能截图并盖原厂公章，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告）
应用关联（三层关联）	支持 B/S 业务系统三层关联审计；（需提供功能截图并盖原厂公章，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告）

	支持 C/S、B/S 三层架构下的真实用户名关联配置
	支持旁路自动学习三层审计关联功能（提供相关截图证明并盖章）；
运维审计	支持与堡垒主机自动关联审计通过 ssh、rdp 等加密协议操作数据库行为（提供产品功能截图，加盖原厂公章，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告证明）；
安全审计	支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义敏感数据掩码规则（提供相关截图证明并盖章）
	内置安全特征库规则不少于 300 条，支持对数据库安全进行检查，如 SQL 注入，缓冲区溢出，数据库漏洞、弱口令等；（提供相关截图证明并盖章）
审计策略	告警查询应支持根据登陆用户、客户端工具名、客户端 IP、规则进行归并分析，能详细展示每类告警占总告警数量百分比，便于告警分析处理；
统计报表	系统提供内置多种报表模板库，内置的报表不少于 35 种，
	支持根据单个数据库或逻辑数据库组生成报表（提供相关截图证明并盖章）
	报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告；
	支持按照源 IP 地址、客户端工具、帐号、告警数等源信息生成报表；
	支持定期自动生成审计报表且以电子邮件方式自动进行发送；（提供相关截图证明并盖章）
	支持报表自定义，自定义的条件不少于 20 个；
模型分析	支持对数据库自动建模及智能对异常行为告警功能；（提供产品功能截图，加盖原厂公章，并提供国家权威检测机构（公安部三所或国家保密科技测评中心）检测报告证明）；
	可通过行为轨迹图方式展示数据库访问行为（提供相关截图证明并盖章）
	可基于账号、IP 地址、访问权限、客户端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警（提供相关截图证明并盖章）
	可以自动对比不同时期的行为模型，以区分其审计日志数趋势、用户、

	IP 地址、工具、访问权限的差异情况；（提供相关截图证明并盖章）
系统管理	采用 B/S 架构管理，支持中英文两种管理界面（提供相关截图证明并盖章）；
	支持离线手工自动升级，升级数据和配置均需保留
	支持三权分立，系统默认设定系统管理员、规则配置员、审计查看员、操作日志查看员等角色
故障排错	系统内置独立的故障排错系统，可以支持一键导出加密的系统调试日志，支持一键检测服务、许可证、流量等大部分常见常见故障的检测（提供相关截图证明并盖章）
	支持流量分析功能，包括抓包、包内容查看、自动探测 sql 语句等；
产品资质	所有资质必须为数据库审计产品专有的资质，不能是网络审计产品或者综合审计的产品资质。
	具备公安部颁发的《计算机信息系统安全专用产品销售许可证》，数据库安全审计国标-增强级
	要求内置的数据库扫描系统也通过国家相关部门的认证和检测，并获得独立的销售许可、涉密资质
厂家资质	原厂商获得 CSA STAR Tech 认证证书（增强级（Enhanced Level））（提供证书复印件并加盖公章）；
服务要求	提供不少于三年产品原厂商质保服务，提供原厂质保函；
	提供不少于三年的原厂商 7*24 小时上门现场服务支持；
	原厂商工程师实施及提供设备相关的培训，提供原厂产品培训 1 天。

8. 日志审计系统

产品要求	详细说明
品牌要求	产品获得公安部计算机信息系统安全产品销售许可证以及公安部信息安全产品检测中心出具产品检验报告。所提供的产品检验报告须符合《信息安全技术日志分析产品检验规范》，并提供完整的检测报告复印件（行标三级）；

	获得中国信息安全认证中心颁发的《IT 产品信息安全认证证书》，检测标准符合 ISCCC-TR-056-2016《日志采集与分析产品安全技术要求》（提供完整的检测报告复印件并加盖公章）
厂商资质要求	原厂商获得 CSA STAR Tech 认证证书(增强级(Enhanced Level))；（提供证书复印件并加盖公章）
工作模式	独立完成审计日志采集，不依赖于设备或系统自身的日志系统； 审计工作不影响被审计对象的性能、稳定性或日常管理流程； 审计结果存储于独立存储空间； 提供全中文 WEB 管理界面，无需安装任意客户端软件或插件。
硬件规格	≥4 个 100/1000M 自适应电口，≥1 个 console 口 内存：≥16GB，磁盘：≥4T*2 raid1 EPS：≥9000/秒（峰值：12000/秒）；双电源 可扩展项：内存可扩展至 32GB 单个磁盘可扩展至 4T(4 个盘位)，支持 HBA 卡扩展 网口可扩展至 18 个（4 电 4 光、4 电、8 光、2 万兆光） ▲产品采用 CF 卡启动（提供第三方检测报告复印件并加盖公章） 支持审计 200 个日志源；
功能扩展	采用解决方案包上传对产品进行功能扩展，无需要代码开发。(提供相关截图并盖章)
日志收集	支持 Syslog、SNMP Trap、OPSec、FTP 协议日志收集 支持使用代理(Agent)方式提取日志并收集； 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等；设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州,F5,华为,H3C,微软,绿盟,飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），网威，nortel(北

批注 [S2]: 可研方案经专家论证，该位置改为4T*2,这个参数修改漏了。

	电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS 系统日志，Linux/UNIX syslog、IIS、Apache 等； 支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等（提供相关截图并盖章）
日志分析	可以以日志等级进行过滤； 应该可以通过自定义配置将用户不关心的日志过滤掉； 支持对收集到的重复的日志进行自动的聚合归并，减少日志量； 支持可由用户定义和修改的日志的聚合归并逻辑规则； ▲支持基于内存的实时关联分析，跨设备的多事件关联分析；（提供第三方检测报告复印件并加盖公章） 支持自定义条件的事件进行聚合；（提供相关截图并盖章） ▲支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析（三维关联），所有的三维关联算法和准则以 CVE、Bugtraq、OWASP 公开协议和标准为为基础。（提供第三方检测报告复印件并加盖公章）
日志备份	可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比； 支持日志备份自动传送到远程服务器；（提供截图并加盖公章）
日志查询	支持 B/S 模式管理，支持 SSL 加密模式访问； 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询； 极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。
应用性能监控（APM）	▲ 性能监控：通过在目标主机上安装 agent 程序，支持监控目标主机的 CPU 利用率、内存使用率、磁盘使用情况、流量等信息，并支持设置报警阈值。（提供第三方检测报告复印件加盖公章）
脆弱性管理	弱点管理：支持导入安恒明鉴弱点扫描器、绿盟极光扫描器等扫

	描报告，可进行统一检索，并支持计算威胁等级。（提供第三方检测报告复印件加盖公章）
综合查询及报表管理	内置合规性报表 1000+种； 内置 SOX、ISO27001、WEB 安全等解决方案包（提供截图并加盖公章） 内置完善的等级保护合规报表
用户管理	根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义； 系统自带自身管理日志 ★注册用户资产时，提供自动发现识别能力。提供一键式故障排除功能。 提供自助式的升级接口，支持对产品升级、规则升级。（提供截图并加盖公章）

9. 威胁分析系统

产品要求	详细说明
硬件配置	软硬一体化 2U 标准机架式设备；1+1 冗余电源；可用磁盘空间≥1T，带 RAID1；标配千兆管理口*1，HA 口*1，千兆业务电口≥4，千兆业务 SFP 光口≥4
部署方式	▲支持旁路部署和分布式部署，对探测器可以添加、删除，显示探测器版本、状态和 IP，管理中心可实现告警统一管理；可自定义管理中心和探测器之间的数据传输速率、时间、发送目录等参数；（提供相关截图证明并盖章）

自定义配置	管理中心和探测器之间的数据传输速率、时间、发送目录都可自定义
性能规格	**网络层：**2Gbps **应用层：**1Gbps **HTTP 最大并发数:**6 万/秒 **邮件处理数:**140 万封/24 小时；**文件处理能力：**5 万个/24 小时 **综合管理分析：**支持管理节点 10 个
攻击检测	▲支持解析 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、Mysql、MSSQL、DB2、Oracle 等协议报文，提供审计协议类型的端口号配置，可根据需要变更端口号，并支持 LDAP 登录行为识别、VXLAN 镜像流量解析检测及 HTTPS 流量解析能力（提供相关截图证明并盖章）
	▲支持对文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑 IP 白名单、域名白名单、客户端 IP 白名单、服务端 IP 白名单、WEB 风险特征白名单进行设置（提供相关截图证明并盖章）
	可自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等（提供相关截图证明并盖章）
	▲支持对 Telnet、FTP、POP3、SMTP、IMAP 等协议进行弱口令检测（提供相关截图证明并盖章）
	自动学习网络流量中包含的各种可疑 C&C IP/URL，包含各种可能对内网存在影响的 IP 和域名

WEB 攻击检测	支持检测访问 webshell 的行为，包含具体对应的 URL、返回码、返回数据包内容等；自动关联行为分析的详细展现，包含 SQL 注入取数据、表单破解、XSS 测试、目录穿越读取文件、多人访问 Webshell、APT 攻击等
Mail 攻击检测	对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接（提供相关截图证明并盖章）
文件攻击检测	通过分析文件中的二进制代码、文件溢出攻击的代码，分析 APT 攻击中的 0day 攻击
动态沙箱检测	可展示文件中版本信息、段信息、资源信息、导入表、字符串信息、删除文件信息等内容，可展示具体文件的行为，包括所有的注册表行为、进程行为、互斥量、进程运行的函数、返回结果、返回值等信息（提供相关截图证明并盖章）
文件威胁指数	可展示威胁程度最高的文件样本 MD5、威胁指数、传播次数，病毒检测、静态检测和动态检测结果等内容（提供相关截图证明并盖章）
	根据文件传播情况分析受感染主机、接受云端威胁情报、关键威胁行为可视化、回连主机 host 和完整沙箱分析报告（提供相关截图证明并盖章）
管理功能	提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立

	▲支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、同步验证、信息收集等功能。（提供相关截图证明并盖章）
	支持对设备的 CPU、内存等状态进行监控，并在设备界面中进行展示
日志报表	支持同时发送多人、单条发送、发送统计等高级告警功能（提供相关截图证明并盖章）
	报表能够支持 WORD、PDF 等格式导出；
	▲审计数据保留策略应至少满足天数和百分比两个控制参数，支持 web 界面可配置，且恢复数据不影响正常的审计功能。对审计日志可自动备份并加密，必须导入设备才能进行恢复查看，并可自动释放磁盘空间。（提供相关截图证明并盖章）
资质证书	销售许可证（必须是 APT 安全检测类）
	具有国家保密科技中心颁发的《恶意代码检测系统》涉密信息系统检测证书
	提供证明具备国际领先水平的第三方权威机构检测报告（误报率低于 3%，无背景流量情况下检出率不低于 98%，有背景流量情况下检出率不低于 97%）

10. 堡垒机

产品要求	**详细说明**

硬件配置	2U 机型，含冗余电源模块，2*USB,1*RJ45 串口，1*GE 管理口，6*GE 电口，1 个接口扩展槽位，2T SATA 硬盘。可管理对象数量≥1000 个，实配管理对象授权≥500 个；图形操作并发数≥600 个，字符操作并发数≥800 个；可通过应用发布的方式进行协议扩展，无需定制即可支持其他通用及专有的运维客户端程序。含 3 年原厂硬件质保。

11. 服务器和虚拟化防病毒系统

产品要求	**详细说明**
数量要求	提供至少 48 个物理 CPU 的原厂授权许可和统一的集中控管平台
管理控制台要求	能够在一个管理控制台上管理多个异构虚拟化安全策略。可以在一个管理控制台中同时管理如下虚拟化平台的安全策略：
	- Vmware
	- Citrix
	- 华三 CAS
	- 华为 Fusionsphere
	- KVM
功能要求	▲产品要求提供完整的主机安全防护，同时支持实体服务器防御和虚拟服务器的主机防御，包括防火墙、防病毒、完整性监控、虚拟补丁技术、日志审计等功能；在虚拟化环境中，除日志审计模块，其余模块要求和虚拟化环境以无代理方式集成，不需要在每台虚拟机上安装客户端，以便减少对物理机的资源占用；主机整体资源与搭载虚拟机数量无直接关系；虚拟资源消耗不会随虚拟机数量成长，提供截图证明并加盖原厂公章确认。
	▲产品可扩展防火墙功能，不依赖分布式交换机可以无代理运行，并且可集中控管防火墙策略，策略定制可以针对 IP,Mac 地址或通讯端口，可保护所有基于 IP 通讯协议（TCP、 UDP、 ICMP 等）和所有框架类型（IP、ARP 等）。提供截图证明并加盖原厂公章确认。
	▲产品必须具有 DPI(深度内容检测)功能，不依赖分布式交换机可

	以无代理运行,必须可以同时保护操作系统和应用服务（数据库，Web，DHCP 等），提供截图证明并加盖原厂公章确认。
	▲产品必须具有操作系统虚拟补丁功能，不依赖分布式交换机可以无代理运行,在服务器尚无安装补丁前，提供针对此补丁攻击的防护能力。
	具备特征库更新功能，实时追踪并保护最新动态威胁：提供自动扫描功能，针对服务器弱点、漏洞进行安全检测并自动形成防护，产品必须能够防御应用层攻击、SQL Injection 及 Cross-site 跨网站程序代码改写的攻击。
	产品必须提供包含攻击来源、攻击时间及试图利用什么方式进行攻击等必要信息，并在事件发生时，立即自动通知管理员。
	产品必须可以和 VMSafe 集成并提供集成管理功能，支持无代理方式,不需要在每台虚拟机上安装,只需在虚拟化环境底层安装即可,对每个虚拟机没有资源占用。
	产品可以通过在整个虚拟环境中安装单一拷贝来达到保护所有虚拟环境中 Guest OS 和应用的功能。
	产品必须和虚拟化环境的 WMotion,Storage VMotion 以及 HA 集成,能够自动感知和保护虚拟环境的变更和迁移。
	▲产品可扩展完整性监控，能够监控操作系统和关键应用包括注册表项、关键目录、特定目录变更，以防范恶意修改，提供截图证明加盖原厂公章确认。
	产品可扩展支持对主机的日志审计，包括收集和分析操作系统和应用程序日志中的安全事件 ；协助遵循规范(PCI DSS 10.6) 优化识别埋在多个日志项下的重要安全事件； 将事件转至 SIEM 系统或中央日志服务器，做关联性分析、报告和归档； 侦测可疑行为、收集数据中心的安全事件和管理操作,并使用 OSSEC 语法来建立高级规则。提供截图证明加盖原厂公章确认。
	产品必须具有集中控管的功能，能够统一的管理和配置，并且日志能够统一的在集中控管平台上呈现。
操作系统支持	Microsoft Windows 2000 (32 位） ， XP (32 /64 位） ,Vista (32/64 位） , Windows 7; Windows Server 2003 (32/64 位)， Windows Server 2008 (32/64 位） , 主流各类 linux 和 UNIX 操作系统

虚拟化系统支持	支持基于 VMware6.0& 6.5 NSX 虚拟化平台底层的无代理安全防护功能，而非在每台虚拟机中部署安全软件实现防护功能
	今后可扩展支持华三，华为，微软， Citrix，等主流虚拟化平台的无代理安全防护。
	可以用有代理模式支持 Docker，Container
应用防护支持	1. 产品必须可以保护以下类型数据库服务器,Oracle, MySQL, Microsoft SQL Server, Ingres。
	2. 产品必须可以保护以下类型邮件服务器，Microsoft Exchange Server, Merak, IBM Lotus Domino, Mdaemon, Ipswitch, Imail, MailEnable Professional。
	3. 产品必须可以保护以下类型文件服务器，Ipswitch, War FTP Daemon, Allied Telesis。
	4. 产品必须可以保护以下类型备份服务器，Computer Associates, Symantec, EMC。
	5. 产品必须可以保护以下类型存储服务器，Symantec, Veritas。
原厂资质和服务要求	1. ▲厂家在国内具有独立的病毒研发和响应中心，投标时提供证明材料，并原厂盖章确认。
	2. ▲厂商已通过 ISO 20K 的质量体系认证，投标时提供证明材料，并原厂盖章确认。
	3. 厂商参加国家级活动和提供网络安全保障工作，并获得中央网信办感谢信两次以上（提供证明材料）
	4. 国家计算机病毒应急处理中心技术支持单位（提供证明材料）
	5. 厂商可根据用户需求提供高级别的服务承诺，如大客户专署服务、主动式服务、快速响应服务、在线技术支持服务等，可提供 5×8 乃至 7×24 小时的专业防毒服务。
其他要求	投标商不得随意扩大所投产品的技术功能及性能，以官网公布的资料为准；技术偏离表需逐条应答，签订合同前需提供功能性测试。

12. 终端防病毒及补丁分发

产品要求	详细说明
系统管理	控制中心：采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能；
	客户端提供控制中心管理所需的相关数据信息，通讯可选择非明文方式； 客户端执行最终的木马病毒查杀、漏洞修复等安全操作；
	产品支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行； 要求客户端程序具备自保功能，避免被恶意篡改
	支持服务器、PC的同台管理；至少支持Windows Server 2003、2008、2012 三个版本操作系统平台的杀毒防护与漏洞管理；至少支持3个以上Linux服务器版本并且可以和Windows统一管理；
资产管理	按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；可监控CPU温度、硬盘温度和主板温度
	支持终端软、硬件变更审计，资产清单报表；
	支持统计指定分组或全网的终端扫描数、终端管理软件安装数、未安装终端数及安装率
	支持自动发现设备的IP-MAC地址的绑定（提供产品界面截图）
	支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件（提供产品界面截图）
	▲支持正版软件的正版序列号的读取功能，确保软件正版化。（提供功能截图，并加盖公司公章）
日志报表	展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表； 展示全网终端病毒库日期比例，可方便的查看全网终端病毒库的情况
	展示指定时间段内指定终端修复漏洞，病毒查杀，木马查杀的情况
	要求支持邮件报警，可以设定多种触发条件，满足条件后自动发送

	邮件到相关人。邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等
设备联动	▲支持与上网行为管理、VPN产品联动，达到网关边界联动防御效果（提供产品界面截图）
病毒、恶意代码、木马防护	支持内存实时监控查毒，能够自动隔离感染而暂时无法修复的文件；
	支持抢先加载防毒，在系统未加载前启动文件监控，通常情况下不必重启到安全模式也能清除病毒；
	支持文件、引导区、内存、注册表、服务、进程、进出文件、目录、压缩文件、网页等恶意代码、恶意样本查杀
	支持电子邮件内文件检测，可清除隐藏于电子邮件计算机病毒和恶性程序；
	支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置（提供功能截图，并加盖公司公章）
	支持U盘等移动磁盘设备和电脑硬盘间文件传输检测； 支持局域网共享文件传输检测；
	能够实时检测和拦截攻击行为，包括改写系统关键文件、修改注册表关键键值、感染移动存储介质、创建系统账号
	要求能够自定义时间、自定义扫描频率，自定义扫描类型，对终端进行定时查毒，并且可以自定义查杀病毒后的处理方式自定义；
	支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件；
	文件被加入白名单，客户端不再查杀，加入黑名单，客户端不可执行此文件；（提供功能截图，并加盖公司公章）
	要求支持通过数字签名或者文件名的方式分别显示文件，方便管理员管理全网终端上报的文件；（提供功能截图，并加盖公司公章）
	支持按病毒、木马、终端等维度统计全网病毒感染状况；
	要求支持对网内未知文件云查询的控制，可以选择直接连接互联网云查询中心查询；
	要求上报文件至少包括:文件名称、发现时间、鉴定结果、文件大小、数字签名和文件所属源计算机等信息
	要求能够支持漏洞利用防御，尤其对通过文件漏洞（尤其是0day漏

批注 [S3]: 这个不能明确 NGFW，NGFW 是某品牌的防火墙，建议去除 NGWF 字样

	洞）的攻击行为进行有效检测与防御；（提供功能截图，并加盖公司公章）
	可对备份区、隔离区的文件进行有效管理。能够对单个、指定的文件和全部文件，进行文件的删除、恢复等多项管理措施。
	▲对敲诈者病毒提供防护机制，同时可提供相关解密工具，解密工具为自主研发；（提供功能截图，并加盖公司公章）
	要求产品具备本地多引擎查杀能力，且引擎可配置；（提供功能截图，并加盖公司公章）
	要求支持服务器端病毒库的定时更新和手动更新两种升级模式。
	要求支持客户端升级时对网络带宽的保护，可以设定服务器端最大升级带宽。（提供截图，并加盖单位公章）
补丁分发与漏洞修复	要求产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型；
	支持漏洞修复影响文档编辑时提醒功能；
	支持补丁下载安装顺序设置,可以有效节省漏洞修复时间与减少CPU占用；
	支持自定义补丁排除名单，防止终端打补丁后造成系统或业务进程崩溃；
	▲终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁（要求提供截图）；
	▲产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能（要求提供截图）
	▲要求产品生产公司具备面向微软官方级别漏洞发现能力（提供2014年至今少20个以上微软漏洞发现案例,提供微软官方确认链接）
	▲产品具备漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端P2P补丁分发加速,有效节省外网带宽资源（要求提供截图）
产品资质	提供公安部颁发的《计算机信息系统安全专用产品销售许可证》。
	提供《国家信息安全产品安全测评证书EAL2》。

13. 网页防篡改系统

产品要求	详细说明
基本要求	针对 Windows 和 Linux 操作系统的 Web 服务器，实现文件防篡改、文件恢复等核心功能；具有防篡改行为发生时即刻阻断，篡改行为无法执行的工作；网页篡改防护系统发生故障时不影响网站系统正常运行；防护利用 WEB Shell 等进行的文件非法上传、SQL 注入、跨站攻击。含 3 年原厂质保。

采购需求（B 包 信息系统安全等级保护测评服务）

一、商务要求

1、在中华人民共和国注册的、具有独立承担民事责任能力的法人（提供营业执照副本复印件、组织机构代码证复印件、税务登记证复印件或工商营业执照三证合一复印件）；
2、投标人应具有海南省信息系统安全等级保护协调小组办公室或国家信息安全等级保护工作协调小组办公室颁发的信息安全等级保护测评机构推荐证书（提供资质证书复印件加盖公章）；
3、交付时间：订合同后 60 个日历天内交付测评报告；
4、交付地点：用户指定地点；
5、交付方式：免费送至用户指定地点；
6、投标人在参加政府采购活动前三年内，在经营活动中没有重大违法记录声明函；
7、本项目不接受联合投标；
8、本项目不允许分包、转包；
9、供应商资格要求：见招标公告；
10、由于项目实施过程会涉及医院敏感信息，测评单位必须提交保密承诺函；

11、付款方式：完成合同约定的信息系统安全等级保护测评，并交付测评报告，经甲方验收合格后，按合同约定全额支付。

二、项目需求

2.1 测评内容

1、对用户的信息系统进行摸底、分析和梳理，提出详细的测评方案及完成系统备案工作。

2、逐一对信息系统进行安全等级保护测评，测评的内容包括但不限于以下内容：

（1）安全技术测评：包括物理安全、网络安全、主机系统安全、应用安全和数据备份及恢复等五个方面的安全测评；

（2）安全管理测评：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全测评。

3、完成测评工作后，提出整改方案；最后出具符合等保要求的网络安全保护等级测评报告，并协助用户完成网络安全保护等级备案工作。

2.2 项目输出(包括但不限于以下内容)

（1）信息系统定级相关文件和报告；

（2）信息系统测评报告及整改建议；

（3）网络安全整改设计方案。

2.3 测评对象描述

序号	被测系统名称	安全等级	被测系统描述
1.	HIS 系统	三级	HIS 系统即为医院管理信息系统，覆盖医院所有业务和业务全过程，业务包括：病案信息，医嘱信息，病人住、转、出院信息，血液信息，用药信息，财务信息，医疗统计信息，医保数据和医院分析决策信息等
2.	LIS 系统	二级	LIS 系统即为检验信息系统是协助检验科完成日常检验工作的计算机应用程序。其主要任务是协助检验师对检验申请单及标本进行预处理，检验数据的自动采集或直接录入，检验数据处理、检验报告的审核，检验报告的查询、打印等。系统应包括检验仪器、检验项目维护等功能。实验室信息系统可减轻检验人员的工作强度，提高工作效率，并使检验信息存储和管理更加简捷、完善
3.	PACS 系统	二级	PACS 系统即为影像归档和通信系统，主要的任务就是把日常产生的各种医学影像（CT、DR、MR 等设备产生的图像）通过各种接口（模拟，DICOM，网络）以数字化的方式海量保存起来，当需要的时候在一定的授权下能够很快的调回使用，同时增加一些辅助诊断管理功能。它在各种影像设备间传输数据和组织存储数据具有重要作用。

2.4 测评服务步骤

信息系统等级保护测评过程需按照《信息系统安全等级保护测评过程指南》

开展工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

2.4.1 测评准备活动

测评准备工作包括编制项目启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
项目启动	1.组建测评项目组	向用户提交《项目计划书》《提供资料清单》
	2.编制《项目计划书》	
	3.确定测评委托单位应提供的资料	
信息收集分析	定级报告及整改方案分析	《系统基本情况分析报告》
	1.整理调查表单	
	2.发放调查表单给测评委托单位	
	3.协助测评委托单位填写调查表	
	4.收回调查结果	
	5.分析调查	
工具和表单准备	1.调试测评工具	确定测评工具（测评工具清单）《现场测评授权书》《测评结果记录表》《文档交接单》
	2.模拟被测系统搭建测评环境	
	3.模拟测评	
	4.准备打印表单	

2.4.2 方案编制活动

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出成果
一、测评对象确认	识别被测系统等级 识别被测系统的整体结构 识别被测系统的边界 识别被测系统的网络区域 识别被测系统的重要节点和业务应用 确定测评对象	《测评方案》的测评对象部分
二、测评指标确定	识别被测系统业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	选择对应等级的安全要求作为测评指标	
	就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标	
三、工具测试点确定	确定工具测试的测评对象 选择测试路径 确定测试工具的接入点	《测评方案》的测试工具接入点部分
四、测试内容确定	识别每个测评对象的测评指标	《测评方案》的单项测评实施和系统测评实施部分
	识别每个测评对象对应的每个测试指标的测试方法	
五、测评指导书开发	从已有的测评指导书中选择与测评对象对应的手册	《测评方案》的测评实施手册部分
	针对没有现成测评指导书的测评对象，开发新的测评指导书	
六、测评方案编制	描述测评项目基本情况和工作依据	向用户提交《测评方案》
	描述被测系统的整体结构、边界和网络区域	
	描述被测系统的重要节点和业务应用	
	描述测评指标	
	描述测评对象	
	描述测评内容和方法	

2.4.3 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，然后依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出
1.现场测评准备	现场测评授权书签署	会议记录、确认的授权委托书、更新后的测评计划和测评方案
	召开现场测评启动会	
	双方确认测评方案	
	双方确认配合人员、环境等资源	
	确认信息系统已经备份	
	测评方案、结构记录表格等资料更新	
2.现场测评和结构记录	依据测评指导书实施测评	访谈结果：技术安全和管理安全测评的测评结果记录或录音 文档审查结果：管理安全测评的测评结果记录 配置检查结果： 技术安全测评的网络、主机、应用测评结果记录表格 工具测试结果：技术安全测评的网络、主机、应用测评结果记录，工具测试完成后
	记录测评获取的证据、资料等信息	
	汇总测评记录，如果需要，实施补充测评	
3.结果确认和资料归还	召开现场测评结束会	
	测评委托单位确认测评过程中获取的证据和资料的正确性，并签字认可	

	测评人员归还借阅的各种资料	的电子输出记录，备份的测试结果文件 实地察看结果：技术安全测评的物理安全和管理安全测评结果记录 测评结果确认： 现场核查中发现的问题汇总、证据和证据源记录、被测单位的书面认可文件

2.4.4 报告分析及编制活动

在现场测评工作结束后，应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项主要任务。

详细要求见下表：

工作内容	工作详细任务	工作依据（模版）
1.单项测评结果判定	分析测评项所对抗威胁的存在情况	等级测评报告的单项测评结果部分
	分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较	
	综合判定单个测评项的测评结果	
2.单元测评结果判定	汇总每个测评对象在每个测评单元的单项测评结果	等级测评报告的单项测评结果汇总分析部

	判定每个测评对象的单元测评结果	分
3.整体测评	分析不符合和部分符合的测评项与其他测评项（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况	等级测评报告的系统整体测评分析部分
	分析被测系统整体结构的安全性对结果的影响情况	
4.风险分析	整体测评后的单项测评结果再次汇总	等级测评报告的风险分析部分
	分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性	
	分析威胁利用安全问题后造成的影响程度	
	为被测系统面临的风险进行赋值	
	评价风险分析结果	
5.等级测评结论形成	统计再次汇总后的单项测评结果为部分符合和不符合项的项数	等级测评报告的等级测评结论部分
	形成等级测评结论	
6.测评报告编制	概述测评项目情况	等级测评报告 提交用户
	描述被测系统情况	
	描述测评范围和方法	
	描述整体测评情况	
	汇总测评结果	
	描述风险情况	
	给出等级测评结论和整改建议	

三、项目服务要求

3.1 项目实施要求

项目实施过程中，投标人应遵循国家标准、行业标准。

在项目实施中投标人须做到：

1. 本项目的项目经理必须具有1年以上的等保测评服务项目管理经验；其中，本项目成员中至少有2人具备信息安全等级保护中级测评师资格；
2. 提供完整的系统实施方案和项目实施管理办法；
3. 提供详细的项目实施方案和计划进度说明书；
4. 项目实施完成后提供可靠的后期技术服务工作；
5. 严格按照双方确定的计划进度保质保量完成工作；
6. 规范项目实施过程中的文档管理。

3.2 项目验收要求

中标人必须提供给业主详细的项目验收方案。

3.2.1 验收组织

成立由业主、中标人以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

3.2.2 验收标准

1. 标准化：项目验收最关键的指标，应确保测评过程符合国家标准规范；
2. 系统稳定性：在测评过程中应确保软硬件环境的稳定性、运行正常；
3. 系统文档：验收文档是否齐全、规范、准确、详细；
4. 系统可操作性：交付成果清晰、通俗易懂。

3.3 售后服务要求

对于评估中发现的应用系统、主机和网络设备漏洞，投标方应提供项目验收后一年内的跟踪服务，对本次评估范围内的问题提供远程或现场技术咨询，对于

漏洞的修补、问题的排除给出建议和指导。

采购需求（C包 信息化项目监理服务）

一、 商务要求

1、交付时间：本项目监理服务周期自签订合同之日起，至建设项目完成竣工验收。
2、项目监理地点：用户指定地点。
3、在中华人民共和国注册的、具有独立承担民事责任能力的法人（提供营业执照副本复印件、组织机构代码证复印件、税务登记证复印件或工商营业执照三证合一复印件）；
4、投标人在参加政府采购活动前三年内，在经营活动中没有重大违法记录声明函；
5、投标人必须具备有效期内的信息系统工程监理乙级（含）及以上资质；
6、投标人必须具备有中国合格评定国家认可委员会（CNAS）颁发的实验室认可资质；
7、供应商资格要求：见招标公告；
8、本项目不接受联合投标；
9、本项目不允许分包、转包；
10、采购资金的支付方式、时间、条件：
按合同完成本项目的监理工作并交付项目建设过程的监理资料，经甲方验收合格后，按合同约定全额支付。
11、供应商资格要求：见招标公告。
12、由于项目实施过程会涉及医院敏感信息，监理单位必须提交保密承诺函。

二、监理技术要求

2.1 监理范围

重点对项目建设过程中设备/材料的采购、设备安装调试、系统集成、软件

开发及应用技术培训、试运行、测试、验收等全过程进行监督管理，从硬件监理、软件监理、系统集成监理等三个方面梳理该项目建设的工程监理应如何通过切实有效方式、方法、手段达到建设方所要求的深度、广度，最终实现工程监理的目标。实现对质量、进度、经费、变更的控制及合同管理和文档管理。当工程质量或工期出现问题或严重偏离计划时，应及时指出，并提出对策建议，同时督促承建单位尽快采取措施。

2.2 监理目标控制方案

以工程建设合同、监理委托合同、国家（GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》）及有关法规、技术规范与标准、项目建设单位需求为依据，通过专业的控制手段，协助建设单位全面地进行技术咨询和技术监督，对工程全过程进行监督、管理、指导、评价，并采取相应的组织措施、技术措施、经济措施和合同措施，确保建设行为合法、合理、科学、经济，使建设进度、投资、质量达到建设合同规定的目标。

1)、监理质量目标控制

监理质量目标控制是监理技术服务的核心所在，也是监理单位综合实力的最好反映，所以做好监理质量目标控制方案，确保本项目建设质量能达到建设单位要求的质量目标。确保本项目建设质量达到工程合同中规定的功能、技术参数等目标。

确保工程建设中的设备和各个节点满足相关国家(GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》)、地方或行业质量标准和技术标准，按照承建合同要求进行基于总体方案的细化设计、开发、安装、调试和运行；系统集成和软件开发过程涉及用户需求调研分析、概要设计、详细设计、系统实现、系统测试和系统运行等比较复杂、制约因素多的工作内容，应该成为质量控制的重点；深化设计方案的确定、开发平台选定，也要进行充分论证。要求监理在整个工程实施过程中做好对工程质量的事前控制，事中监督和事后评估，以确保工程质量合格。

投标人应针对本项目建设中软硬件设备采购、设备安装调试、系统集成、软

件开发、工程培训等提出工程监理的质量控制原则、方法、措施、工作流程和目标。

2)、监理进度目标控制

确保本项目按合同规定的工期完工。

依据合同所约定的工期目标，在确保质量和安全的原则下，采用动态的控制方法，对进度进行主动控制，确保项目按规定的工期完工。

通过对本项目概要设计的分析、研究，提出针对本项目建设的、有代表性的信息工程监理进度控制的主要原则、方法、内容、措施、工作流程和目标。

3)、监理投资目标控制

协助用户控制本项目建设总投资在项目预算及审计范围内，减少项目建设中的额外开支。以项目建设方和承建单位实际签订的合同金额为准，确保项目费用控制在合同规定的范围内。在项目建设中，合理减少项目变更，保护建设单位的经济利益。

2.3 工程监理重点难点分析

投标人应根据本项目建设的特点，从实际出发分析本项目监理工作的重点、难点，并根据分析的结果制定相应的监理工作规划、对策和策略，以便日后有针对性的开展建设工程的监理服务工作。

（一）项目组织及总体技术方案的质量控制

1、协助审查项目建设方的投标书、合同及实施方案；

2、在技术上、经济上、性能上和风险上进行分析和评估，为采购人提供建议；

3、协助审查项目建设方提交的组织实施方案和项目计划等相关文档；

4、协助审查项目建设方的工程质量保证计划及质量控制体系；

5、参与制定项目质量控制的关键节点及关键路径。

（二）项目质量控制

1、组织措施：建立质量管理系统，完善职责分工及有关质量监督制度，落实质量控制责任。

2、系统集成质量控制

审核系统总集成方案；

对采购的硬件设备及网络环境的综合质量进行检验、测试和验收；

参与制定系统验收大纲；

对设备安装、调试进行验收；

对系统进行总体验收。

3、人员培训的质量控制

协助审查并确认培训计划，审定培训大纲；

监督审查建设方实施其培训计划，并征求采购人的意见反馈；

监督审查考核工作，评估培训效果；

协助审核并确认培训总结报告。

4、文档、资料的质量控制

监督审查建设方提供的设备型号、数量、到货时间以及设备的技术资料、系统集成和软件安装在实施过程中所有相关文件的标准性和规范化，在各项目验收时，应监督项目建设方提交符合规定的成套资料，包括印刷本和电子版。

对监理项目实施过程中的文档进行标准化、规范化管理，在监理项目验收时，应提交符合规定的监理项目的成套资料，包括印刷本和电子版。

（三）进度协调控制

1、组织措施：建立进度控制协调制度，落实进度控制责任。

2、编制项目控制进度计划：编制项目总进度计划和网络图。按各子系统实

际情况进行编制，包括系统建设开工、设备的采购、设备的安装调试、软件的编制、试运行等各方面内容，做到既要保证各子系统、各阶段目标的顺利实现，又要保证项目间、阶段间的衔接、统一和协调。

3、审查各子系统建设方编制的工作进度计划：分析系统建设进度计划是否能满足合同工期及系统建设总进度计划的要求，特别要对照上阶段计划工程量完成情况进行审查，对为完成系统建设进度计划所采取的措施是否恰当、设备能否满足要求、管理上有无缺陷进行审查。要根据建设方所能提供的人员及设备性能复核、计算设备能力和人员安排是否满足要求等，分析判断计划是否能落实，审查建设方提出的设备供应计划能否落实。如发现供应计划未落实，应及时报告采购人，要求建设方采取应急措施满足系统建设的需求。

4、系统建设进度的现场检查：随时或定期、全面地对进度计划的执行情况跟踪检查，发现问题及时采取有效措施加以解决。加强系统建设准备工作的检查，在工程项目或部分工序实施前，对情况进行检查，要加强检查设备、人员安排、各项措施的落实情况，确保准备工作符合要求，不影响后续工程的进行。

5、进度计划的分析与调整：要保证建设进度与计划进度一致，经常对计划进度与实际进度进行比较分析，发现实际进度与计划进度不符时，即出现进度偏差时，首先分析原因，分析偏差对后续工作的影响程度，并及时通知建设方采取措施，向建设方提出要求和修改计划的指令。

（四）投资控制

1、组织措施：建立健全项目管理组织，完善职责分工及有关质量项目管理制度，落实投资控制的责任。

2、审查设计图纸和文件，审查建设方的施工组织设计和各项技术措施，深

入了解设计意图，在保证系统建设质量和安全的前提下尽可能优化设计。

3、严格督促建设方按合同实施，严格控制合同外项目的增加，协助采购人严格控制设计变更，制定设计变更增加工作量的报批制度；及时了解系统建设情况，协调好各方矛盾，减少索赔事件的发生。对发生的事件严格按合同及法律条款进行处理，认真进行索赔调解。

（五）合同管理

合同管理是加快系统建设进度、降低系统建设造价、保证系统建设质量的有效途径之一。通过合同管理，可以督促建设方在各个阶段按照合同要求保证设备、人员的配备及投入，保证各阶段目标按合同实施，减少索赔事件，控制系统建设结算等。具体要求如下：

1、以合同为依据，本着“实事求是、公正”的原则，合情合理地处理合同执行过程中的各种争议。

2、分析、跟踪和检查合同执行情况，确保项目建设方按时履约。

3、对合同的工期的延误和延期进行审核确认。

4、对合同变更、索赔等事宜进行审核确认。

5、根据合同约定，审核项目建设方的支付申请。

6、建立合同目录、编码和档案。

7、合同管理坚持标准化、程序化，如设计变更、延期、索赔、计量支付等应规定出固定格式和报表。合同价款的增减要有依据，合同外项目增加要严格审批制度。重大合同管理问题的处理，如大的变更、索赔、复杂的技术问题等，组成专门小组进行研究。不符合实际情况的合同条款及时向采购人报告，尽早处理，以免造成损失。

（六）信息、工程文档管理

在项目管理过程中，为了实现对进度、质量、投资的有效控制，处理有关合同管理中的各种问题，监理方需要收集各种有用的信息。信息的来源主要包括采购人文件、设计图纸和文件、建设方的文件、建设现场的现场记录（或项目管理日志）、会议记录、验收情况及备忘录等等。其中项目管理日志是进行信息管理的一个最重要的方面。项目管理日志主要包括当天的工作项目和工作内容、投入的人力和设备运行情况、计划的完成情况及进度情况、停工和返工及窝工情况。信息管理主要措施要求如下：

1、制定详细的信息收集、整理、汇总、分析、传递和利用制度，力求信息管理的标准化和制度化。由专人负责系统建设信息的收集、分类、整理储存及传递工作。信息传递以文字为主，统一编号，利用计算机进行管理，力求信息管理的高效、迅速、及时和准确，为系统建设提供及时有用的信息和决策依据。

2、在项目实施过程中做好工程监理日记和工程大事记。

3、做好双方合同、技术建设方案、测试文档、验收报告等各类往来文件的存档。

4、建立必要的会议、例会制度，整理好会议纪要，并监督会议有关事项的执行情况。

5、立足于建设现场，加强动态信息管理，对现场的信息进行详细记录和分析，做到以文字为基础，以数据说明问题。根据收集到的信息与合同进行比较，督促建设方的人员和设备到位，促使承包商按合同完成各项目标，从而实现对进度、质量、投资的控制。

6、建立完整的各项报表制度，规范各种适合本项目的报表。定期将各种报

表、信息分类汇总，及时向采购人及有关各方报送。

7、监理项目验收时，应提交符合规定的有关工程的成套资料，包括印刷本和电子版。

（七）日常监理

1. 掌握监理范围内涉及的各种技术及相关标准；

2. 安排足够的监理人员，按工程需要派驻相应的专业人员进行项目监理，至少保证 1 名专职信息系统监理工程师在现场，随时为采购人提供服务，总监理工程师必需专职于本项目；

3. 制定工程管理的组织机构方案并协助采购人组建相关机构，并提供相关培训；

4. 熟悉了解项目的业务需求，协助采购人对项目的目标、范围和功能进行界定，参与并协助项目的设计方案交底审核工作；

5. 建立健全科学合理的会议制度，并予以贯彻落实；

6. 建立健全科学合理的文档管理制度，制订开发过程中产生的各类文档制作、管理规范，并予以贯彻落实；

7. 与采购方一起制定评审机制，在工程实施全过程中随时关注隐患苗头，如发现将会导致工程失败的情况出现时，应及时启动评审机制，组织专家对工程实施情况进行评审，对评审不合格的，应向采购方提出终止合同意见。此外，还应组织定期评审（阶段性评审、里程碑评审、验收评审），对评审结果为优的，提出奖励意见，评审不合格的，则向采购方提出处理意见；

2.4 工程各阶段的监理规划、实施

投标人应对本项目从设计施工到项目竣工验收阶段制定一整套工程监理的工作流程，并叙述各阶段主要监理工作内容。

本项目监理工作主要分为设备/材料采购、施工阶段、验收阶段、质保期阶段等。

⑴、设备/材料采购监理

建设项目由承包单位承担设备/材料采购任务，工程监理单位在设备/材料采购阶段监理工作主要有：

- ✧ 审核承包单位的设备采购计划和设备采购清单；
- ✧ 订货进货验证；
- ✧ 组织到货验收；
- ✧ 鉴定、设备移交等；

⑵、施工阶段监理

1、开工前的监理

1) 审核施工设计方案：开工前，由监理单位组织实施方案的审核，内容包括设计交底，了解需求、质量要求，依据设计招标文件，审核总体设计方案和有关的技术合同附件，以避免因设计失误造成实施的障碍；

2) 审核实施方案的合法性、合理性、与设计方案的符合性；

3) 审批施工组织设计：对施工单位的实施工作准备情况进行和监督；

4) 审核施工进度计划：对施工单位的施工进度计划进行评估和审查；

5) 审核实施人员：确认施工方提交的实施人员与实际工作人员的一致性，如有变更，则要求叙述其原因；

6) 审核《软件项目开发计划》。

2、施工准备阶段的监理

1) 审批开工申请，确定开工日期；

2) 了解承包商设备订单的定购和运输情况；

3) 了解施工条件准备情况；

4) 了解承建单位实施前期的人员组织、施工设备到位情况；

5） 编制各个子项目监理细则；

6） 签发开工令。

3、施工阶段的监理

1） 审核软件开发各个阶段文件；

2） 协助采购人组织软件开发阶段评审；

3） 材料、硬件设备、系统软件的供货计划的审核；

4） 材料、硬件设备、系统软件的进场、开箱和检验；

5） 促使项目中所使用的产品和服务符合合同及国家相关法律法规和标准；

6） 对施工各个阶段的安装工艺进行检查；

7） 审核项目各个阶段进度计划；

8） 督促、检查承建单位进度执行情况；

9） 审查项目变更，提出监理意见；

10） 审查承建单位阶段款支付申请，提出监理意见；

11） 按周（月、旬）定期报告项目情况；

12） 组织召开项目例会和专项会议。

4、试运行阶段的监理

1） 协助建设方确认项目进入试运行；

2） 监查系统的调试和试运行情况，记录系统试运行数据；

3） 进行试运行期系统检测或测试，做出检测或测试报告；

4） 对试运行期间系统出现的质量问题进行记录，并责成有关单位解决。解决问题后，进行二次监测；

5） 进行试运行时间核算；

6） 协助业主确认试运行通过。

⑶、验收阶段监理

1、验收阶段

1）对承建单位在试运行阶段出现的问题的整改情况进行监督和复查；

2）监督检查承建单位作好用户培训工作，检查用户文档；

3）组织系统初步验收；

4）审查承建单位提交的竣工文档；

5）参与项目竣工验收；

6）竣工资料收集整理齐全并装订，签署验收报告；

7）审核项目结算；

8）审查承建单位阶段款支付申请，提出监理意见；

9）向建设单位提交监理工作总结；

10） 将所有的监理材料汇总，编制监理业务手册，提交采购人；

11） 系统验收完毕进入保修阶段的审核与签发移交证书。

2、项目移交阶段

1） 系统的设计方案、设计图纸和竣工资料的全部移交；

2） 设备、软件、材料等的验收文档核实；

3） 施工文档的移交；

4） 竣工文档的移交；

5） 项目的整体移交。

⑷、质保期阶段监理

监理单位承诺依据委托监理合同约定的工程质量保修期规定的时间、范围和内容开展工作主要有：

1） 定期对项目进行回访，协助解决技术问题；

2） 对项目建设单位提出的质量缺陷进行检查和记录；

3） 对质量缺陷原因进行调查分析并确定责任归属；

4） 检查承建单位质保期履约情况，督促执行；

5） 审查承建单位阶段款支付申请，提出监理意见。

投标人应根据上述监理工作内容（但不局限于上述内容），分别制定详细的监理工作流程，使本项目的监理工作流程化、制度化。

2.5 监理工作要求

1、监理工作制度要求

根据本项目的特色，本项目要求以现场监理为主要方式进行，在施工现场主

要监理人员必须具备所从事监理业务的专业技术和类似系统经验，并具有丰富的项目管理经验。监理工作必须由具有相应资质和职称的人员来担任。本次监理项目实行总监理工程师负责制。监理公司应建立项目监理小组，负责整个项目的全程监理工作，本项目必须配备不少于 1 名的现场专业工程师。监理人员的确定和变更，须事先经业主方同意。监理人员必须奉公守法，具有高度的责任心。

2、监理项目组织要求

工程监理组织形式应根据工程项目的特点、工程项目承包模式、业主委托的任务以及监理单位自身情况而确定，结构形式的选择应考虑有利于项目合同管理、有利于目标控控制、有利于决策指挥、有利于信息沟通。

要求投标人在报价方案中要明确工程监理的各项运作，包括监理人员的相关资料、职能分配、监理组织的构成及工作流程、各项监理工作的相关负责人等。

3、监理信息管理要求

投标人应制定有关本项目信息管理流程，规范各方文档并负责整理记录归档业主单位与承建单位来往的文件、合同、协议及会议记录等各种文档，并定期以监理月（周/季）报形式提交业主。包括下列监理工作：

1）做好监理日记及工程大事记；

2）做好合同批复等各类往来文件的批复和存档；

3）做好项目协调会、技术专题会等各项会议纪要；

4）管理好实施期间的各类、各方技术文档；

5）做好项目周报；

6）做好监理建议书、监理通知书存档；

7）阶段性项目总结。

投标人应针对项目特点，制定相应的信息分类表、信息流程图、信息管理表格、信息管理工作流程与措施，同时要求采用先进的项目信息管理软件对项目信息进行综合管理。

4、监理合同管理要求

本项目建设过程中会与承建单位签订各种合同，投标人应该针对项目特点制定合同从草案到签署的管理工作流程与措施，规范合同管理，并在具体项目合同执行时进行下列监理工作：

1）跟踪检查合同的执行情况，确保承建单位按时履约；

2）对合同工期的延误和延期进行审核确认；

3）对合同变更、索赔等事宜进行审核确认；

4）对合同终止进行审核确认；

5）根据合同约定，审核承建单位提交的支付申请，签发付款凭证。

要求对项目合同进行合理的管理，以完善整个项目建设的过程。

三、监理服务准则

遵照国家 GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》的规定，以“守法、诚信、公正、科学”的准则执业，维护建设方与承建方的合法权益。具体应做到：

1） 执行有关项目建设的法律、法规、规范、标准和制度，履行监理合同规定的义务和职责。

2） 不收受被监理单位的任何礼金。

3） 不泄漏所监理项目各方认为需要保密的事项。

4） 遵守国家的法律和政府的有关条例、规定和办法等。

5） 坚持公正的立场，独立、公正地处理有关各方的争议。

6） 坚持科学的态度和实事求是的原则。

7） 在坚持按监理合同的规定向建设单位提供技术服务的同时，帮助被监理者完成起担负的建设任务。

8） 不泄漏所监理的项目需保密的事项。

四、监理依据

1）国家 GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》和海南省有关信息系统项目建设和监理管理规范；

2）建设单位与承建单位签订的承包工程合同

3）建设单位与监理单位签订的委托监理合同

4）本工程招标书、招标过程文件、各中标商的投标书

5）国家有关合同、招投标、政府采购的法律法规

6）部颁、地方政府的信息工程、信息工程监理的管理办法和规定

7）建设工程和信息工程相关的国家、行业标准和规范

8）建设工程和信息工程技术监督、工程验收规范

9）与工程相关的技术资料

10）其他与本项目适用的法律、法规和标准

11）国家、地方及行业相关的技术标准

五、安全保密要求

本项目要求投标人制定一整套工程监理安全保密制度，确定工程保密责任人，同时要求投标人：

1） 按照国家、省、市的有关法规文件规定，要求监理履行保密责任，并与建设单位签订保密协议；

2） 监理单位各级组织严格履行保密职责；

3） 按照公司内部保密规定开展监理工作。

六、监理验收要求

1）审核监理方应提交的各类监理文档和最终监理总结报告，综合评估监理方在系统开发进度、质量把关、重难点问题解决、项目投资等方面的监理情况。只有文档齐全，系统开发工作中没有出现重大质量事故才予验收。

2）本监理工作的最终验收由委托方组织。

七、其它要求

1.监理总工程师

1）具有信息系统监理师资格证书；

2）5 年以上监理或项目管理经验。

2.监理工程师

1）具有信息系统监理师资格证书资格；

3.项目管理及施工组织

投标人须提供详尽的监理技术方案，包括但不限于施工组织部署、项目管理目标、施工准备、进度控制、质量管理、验收方法等内容。