# 技术标准和服务要求

## 一、技术要求

### （一）具体技术指标要求

#### 1. 专线边界防火墙

| 分类 | 安全控制点 | 等级保护安全要求 |
| --- | --- | --- |
| 安全区域边界 | 边界防护 | 在网络边界是否部署访问控制设备并启用访问控制策略； |
| | | 设备配置信息是否指定端口进行跨越边界的网络通信，指定端口是否配置并启用了安全策略。 |
| | 入侵防御 | 核查是否能够检测到以下攻击行为：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；<br>核查相关系统或设备的规则库版本是否已更新到最新版本<br>核查相关系统或设备配置信息或安全策略是否能够覆盖网络所有关键节点。 |
| | 恶意代码防范 | 核查关键网络节点处是否部署防恶意代码产品等技术措施；<br>核查防恶意代码产品运行是否正常，恶意代码库是否已经更新到最新。 |

#### 2. 堡垒机

| 分类 | 安全控制点 | 等级保护安全要求 |
| --- | --- | --- |
| 安全区域边界 | 安全审计 | a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| 安全计算环境 | 身份鉴别 | c)当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； |
| | | d)应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。 |
| | 安全审计 | a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| | | b)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； |
| | | c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； |
| | | d)应对审计进程进行保护，防止未经授权的中断。 |
| | 入侵防范 | c)应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。 |
| 安全管理中心 | 系统管理 | a)应保证系统管理员通过管理工具或平台进行系统管理操作，并对这些操作进行审计； |

| | | |
|---|---|---|
| | | b)应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、资源配置、加载和启动、运行的异常处理、数据和设备的备份与恢复等。 |
| | 审计管理 | a)应保证审计管理员通过管理工具或平台进行安全审计操作，并对这些操作进行审计； |
| | | b)应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 |
| | 安全管理 | a)应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； |
| | | b)应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。 |
| | 集中管控 | b)应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； |
| | | c)应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测。 |

3. 日志审计系统

| 分类 | 安全控制点 | 等级保护安全要求 |
|---|---|---|
| 安全区域边界 | 安全审计 | a)应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| | | b)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； |
| | | c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
| 安全计算环境 | 安全审计 | a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| | | b)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； |
| | | c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； |
| | | d)应对审计进程进行保护，防止未经授权的中断。 |
| 安全管理中心 | 审计管理 | a)应保证审计管理员通过管理工具或平台进行安全审计操作，并对这些操作进行审计； |
| | | b)应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 |
| | 集中管控 | d)应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。 |

## 4. 数据中心边界防火墙

| 分类 | 安全控制点 | 等级保护安全要求 |
| --- | --- | --- |
| 安全区域边界 | 访问控制 | e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制； |
| | 入侵防范 | a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； |
| | | b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； |
| | | d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。 |
| | 恶意代码和垃圾邮件防范 | a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新。 |
| 安全计算环境 | 入侵防范 | d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； |
| | | e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； |
| | | f) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。 |

## 5. 网闸

| 分类 | 安全控制点 | 基本要求 |
| --- | --- | --- |
| 安全通信网络 | 网络架构 | c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； |
| | | d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段。 |
| 安全区域边界 | 边界防护 | a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； |
| | | b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制； |
| | | c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制； |
| | | d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 |
| | 访问控制 | a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； |
| | | b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； |
| | | c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； |
| | | d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； |
| | | e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。 |

## 6. 上网行为管理

| 分类 | 安全控制点 | 安全要求（三级） |
| --- | --- | --- |
| 安全区域边界 | 边界防护 | b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制； |
| | | c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制； |
| | | d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。 |
| 安全计算环境 | 身份鉴别 | c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； |
| | 入侵防范 | c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。 |

## 7. 数据库审计

| 分类 | 安全控制点 | 等级保护安全要求 |
| --- | --- | --- |
| 安全管理中心 | 审计管理 | a) 应保证审计管理员通过管理工具或平台进行安全审计操作，并对这些操作进行审计； |
| | | b) 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。 |
| | 集中管控 | d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求。 |

## 8. 漏洞扫描

| 分类 | 安全控制点 | 基本要求 |
| --- | --- | --- |
| 安全计算环境 | 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； |
| | | b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。 |
| | 访问控制 | b）应重命名或删除默认账户，修改默认账户的默认口令； |
| | 入侵防范 | b）应关闭不需要的系统服务、默认共享和高危端口； |
| | | c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； |
| | | e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 |
| 安全管理机构 | 审核和检查 | a）应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。 |

| | | |
|---|---|---|
| 安全建设管理 | 测试验收 | b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。 |
| 安全运维管理 | 漏洞和风险管理 | a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补； |
| | | b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。 |
| | 配置管理 | b）应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。 |

9. 备份一体机

| 分类 | 安全控制点 | 等级保护安全要求 |
|---|---|---|
| 安全计算环境 | 数据备份恢复 | 应提供重要数据的本地数据备份与恢复功能； |
| | | 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； |
| | | c)应提供重要数据处理系统的热几余，保证系统的高可用性。 |

10. 配套核心网络设备

围绕院内网的核心交换区域和数据中心区域，配套建设核心交换机双备份冗余架构，实现热机互备容灾机制，避免因单一设备故障引起的网络整体瘫痪，短时间无法恢复影响业务正常开展。

11. 等保测评服务

项目建设基本完成后，需配合医院进行网络机房物理和环境安全规范措施，完善网络安全机构和人员岗位管理、安全制度和应急预案等保测评项目内容，组织进行医院网络信息安全等保测评相关工作，直至等保 2.0 三级顺利通过评级达标。

（二）样品要求（若没有，可不写）

（三）实施人员要求（若没有，可不写）

（四）生产及安装调试等要求

中标方提供安装、调试。

（五）供货、安装周期及交货地点要求

1、合同生效后，中标方在120日内完成安装及调试。

2、中标方提供设备的各项技术性能指标必须达到合同和技术文件规定的要求。

3、交货地点：甘肃省酒泉市。

**二、服务要求**

（一）售后质保培训等要求

1.免费质保期为项目验收之日起1年内，超过1年后质保由双方另行约定。

2.项目实施期间或实施结束后，供应商需对相关使用者进行免费的技术操作培训。

3.供应商提供项目质保期间，项目软硬件设备、仪器、系统等因故障、损坏等原因影响业务运行的，需在15分钟内提供电话指导服务，协助排查故障问题；1小时内无法自行解决的，供应商需委派技术人员在故障发生2小时内，提供上门服务。

（二）保密要求

甲、乙双方在采购和履行合同过程中所获悉的对方属于保密的内容，甲乙双方均有保密义务。

（三）报价要求

人民币96万元（含税）。

（四）其他项目个性化要求

报价企业应当具备服务履约能力，在履约环节不得转包和违法分

包，一经发现存在转包和违法分包行为，转包和违法分包的相关企业均将受到相关处罚。

**三、投标（报价）人资质要求**

（一）资质要求

1.符合《中华人民共和国政府采购法》第二十二条资格条件。

2.具备有独立承担民事责任的能力；

3.具有良好的商业信誉和健全的财务会计制度；

4.具有履行合同所必需的设备和专业技术能力；

5.有依法缴纳税收和社会保障资金的良好记录；

6.参加政府采购活动前3年内，在经营活动中没有重大违法记录；

7.法律、行政法规规定的其他条件。

（二）投标人需准备资料要求（若没有，可不写）

**四、验收、付款及其他内容**

（一）验收方式

（一）验收方式

安装调试完毕后，由供应商提交书面验收申请，甲方成立项目验收小组，由组成员现场核查验收并形成书面验收报告。

（二）付款方式

项目验收完成后30日内支付95%合同款，验收合格一年后30日内支付5%质保金。

（三）现场踏勘等信息（若没有，可不写）

（四）其他信息

# 医院网络信息安全等级保护项目技术参数

| 序号 | 名称 | 单位 | 数量 | 参数类别 | 参数要求 | |
|---|---|---|---|---|---|---|
| 1 | 专线边界防火墙 | 台 | 2 | 性能参数 | 整机吞吐量 | ≥9Gbps |
| | | | | | 网络层吞吐量 | ≥9Gbps |
| | | | | | 应用层吞吐量 | ≥4Gbps |
| | | | | | 最大并发连接数 | ≥400万 |
| | | | | | 每秒新建连接数 | ≥10万 |
| | | | | 硬件参数 | 内存 | ≥8G |
| | | | | | 硬盘容量 | ≥128G SSD |
| | | | | | 电口 | ≥6个千兆电口 |
| | | | | | 光口 | ≥2个万兆光口（带模块） |
| | | | | 功能参数 | 国产化要求 | 设备需采用国产化芯片与国产化操作系统（提供证明材料并加盖厂商公章）。 |
| | | | | | 1、支持对服务器漏洞扫描攻击者ip进行封锁（提供证明材料并加盖厂商公章）。<br>2、要支持 Cookie 攻击防护功能。(所投产品需提供经国家权威机构认可的检测机构出具的且关于“Cookie 攻击防护”功能项的产品检测报告并加盖厂商公章)。<br>3、要做到对策略生命周期管理功能的支持。对安全策略修改的时间、原因以及变更类型进行统一的管理，以利于策略的运维和管理。(需提供功能截图并加盖厂商公章)。<br>4、产品内置≥13000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则（需提供产品功能截图证明并加盖厂商公章）。<br>5、产品支持联动云端智能运营平台，支持流量日志分析、事件聚合，微信告警、联动处置等主要功能。<br>6、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）。 | |

# 医院网络信息安全等级保护项目技术参数

| 序号 | 名称 | 单位 | 数量 | 参数类别 | 参数要求 | |
|---|---|---|---|---|---|---|
| 2 | 堡垒机 | 台 | 1 | 性能参数 | 管理点数 | ≥50 |
| | | | | | 图形运维最大并发数 | ≥50 |
| | | | | | 字符运维最大并发数 | ≥100 |
| | | | | 硬件参数 | 内存 | ≥16G |
| | | | | | 硬盘容量 | ≥64GB+1T |
| | | | | | 电口 | ≥6个千兆电口 |
| | | | | | 光口 | ≥4个千兆光口（带模块） |
| | | | | 功能参数 | 国产化要求 | 设备需采用国产化芯片与国产化操作系统（提供证明材料并加盖厂商公章）。 |
| | | | | | 1、运维授权:支持在授权基础上自定义访问审批流程，可设置多级审批人，审批通过才可最终发起运维操作，需提供功能截图并加盖厂商公章。<br>2、用户管理:支持动作流配置，通过动作流配置既可实现应用接入又可以实现单点登录和审计接入。支持丰富的认证方式，包括但不限于口令认证、数字证书认证、AD域认证、Radius认证等认证方式。并且支持各种认证方式和口令进行组合认证。 | |

# 医院网络信息安全等级保护项目技术参数

| 序号 | 名称 | 单位 | 数量 | 参数类别 | 参数要求 | |
|---|---|---|---|---|---|---|
| 3 | 日志审计系统 | 台 | 1 | 性能参数 | 每秒日志处理能力 | ≥2500条/秒 |
| | | | | | 日志存储能力 | ≥128GB+4T |
| | | | | | 默认包含主机审计许可证书数量 | ≥100 |
| | | | | 硬件参数 | 内存 | ≥16G |
| | | | | | 硬盘容量 | ≥128GB+4T |
| | | | | | 电口 | ≥6个千兆电口 |
| | | | | | 光口 | ≥2个万兆光口（带模块） |
| | | | | 功能参数 | 国产化要求 | 设备需采用国产化芯片与国产化操作系统（提供证明材料并加盖厂商公章）。 |
| | | | | | 1、支持过滤无用日志，减少发送到服务器的安全事件数，减少对网络带宽和数据库存储空间的占用。支持日志批量转发，可以转发到第三方平台，支持转发原始日志和已解析日志的两种日志。需提供功能截图并加盖厂商公章<br>2、支持进行内置关联分析规则，关联分析规则数量不少于350条。实时监控系统日志传输率和日志留存的合规性，要求产品可对首页进行自定义。需提供功能截图并加盖厂商公章 | |

# 医院网络信息安全等级保护项目技术参数

| 序号 | 名称 | 单位 | 数量 | 参数类别 | 参数要求 | |
|---|---|---|---|---|---|---|
| 4 | 数据中心防火墙 | 台 | 2 | 性能参数 | 整机吞吐量 | ≥9Gbps |
| | | | | | 网络层吞吐量 | ≥9Gbps |
| | | | | | 应用层吞吐量 | ≥4Gbps |
| | | | | | 最大并发连接数 | ≥400万 |
| | | | | | 每秒新建连接数 | ≥10万 |
| | | | | 硬件参数 | 内存 | ≥8G |
| | | | | | 硬盘容量 | ≥128G SSD |
| | | | | | 电口 | ≥6个千兆电口 |
| | | | | | 光口 | ≥2个万兆光口（带模块） |
| | | | | 功能参数 | 国产化要求 | 设备需采用国产化芯片与国产化操作系统（提供证明材料并加盖厂商公章）。 |
| | | | | | 1、支持对服务器漏洞扫描攻击者ip进行封锁（提供证明材料并加盖厂商公章）。<br>2、要支持 Cookie 攻击防护功能。（所投产品需提供经国家权威机构认可的检测机构出具的且关于“Cookie 攻击防护”功能项的产品检测报告并加盖厂商公章）。<br>3、要做到对策略生命周期管理功能的支持。对安全策略修改的时间、原因以及变更类型进行统一的管理，以利于策略的运维和管理。（需提供功能截图并加盖厂商公章）。<br>4、产品内置≥13000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。（需提供产品功能截图证明并加盖厂商公章）。<br>5、产品支持联动云端智能运营平台，支持流量日志分析、事件聚合，微信告警、联动处置等主要功能。 | |

# 医院网络信息安全等级保护项目技术参数

| 序号 | 名称 | 单位 | 数量 | 参数类别 | 参数要求 | |
|---|---|---|---|---|---|---|
| 5 | 网闸 | 台 | 1 | 性能参数 | 整机吞吐量 | ≥300M |
| | | | | | 最大并发连接数 | ≥9万 |
| | | | | 硬件参数 | 内存 | ≥16G |
| | | | | | 硬盘容量 | ≥960G |
| | | | | | 电口 | ≥6个千兆电口 |
| | | | | 功能参数 | 1、支持非标准应用协议以及IP、SMTP、POP3、MULTICAST、网络协议等。支持基于FTP、NFS、SFTP、Samba等方式的文件同步；支持Oracle、SQLServer、DB2、MySql及国产达梦、人大金仓等主流同构异构数据库同步功能。支持国际主流视频控制协议SIP、RTMP、GB28181。需提供功能截图并加盖厂商公章。<br>2、支持双机热备，主设备出现故障时，从设备迅速接替工作，保证业务持续性。需提供功能截图并加盖厂商公章。 | |

# 医院网络信息安全等级保护项目技术参数

| 序号 | 名称 | 单位 | 数量 | 参数类别 | 参数要求 | |
|---|---|---|---|---|---|---|
| 6 | 上网行为管理 | 台 | 2 | 性能参数 | 整机吞吐量 | ≥5G |
| | | | | | 网络层吞吐量 | ≥5G |
| | | | | | 应用层吞吐量 | ≥750Mb |
| | | | | | 带宽性能 | ≥500M |
| | | | | | 最大并发连接数 | ≥50万 |
| | | | | | 每秒新建连接数 | ≥10000 |
| | | | | 硬件参数 | 内存 | ≥8G |
| | | | | | 硬盘容量 | ≥960G |
| | | | | | 电口 | ≥6个千兆电口 |
| | | | | | 光口 | ≥2个万兆光口（带模块） |
| | | | | 功能参数 | 国产化要求 | 设备需采用国产化芯片与国产化操作系统（提供证明材料并加盖厂商公章）。 |
| | | | | | 1、支持远程应用的外发附件审计,包括但不限于Teamviewer、向日葵、Anydesk、RDP；支持外发截屏，当用户外发附件时，会自动截取外发时刻的屏幕，并记录到文件审计日志；支持Windows终端打印文件行为和打印文件内容的审计。支持Windows桌面水印，支持设置水印的内容、透明度、密度，水印效果预览，离线时继续生效。需提供功能截图并加盖厂商公章。<br>2、支持自定义测试地址，检查终端是否能PING通，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；需提供功能截图并加盖厂商公章。<br>3、支持与专网边界防火墙、数据中心防火墙实现认证联动，可以转发用户认证信息到专网边界防火墙，实现单点登录，为保障联动效果要求所投上网行为管理与专网边界防火墙、数据中心防火墙为同品牌。（提供产品界面截图并加盖厂商公章及投标商同品牌承诺函并加盖投标商公章）。 | |

# 医院网络信息安全等级保护项目技术参数

| 序号 | 名称 | 单位 | 数量 | 参数类别 | 参数要求 | |
|---|---|---|---|---|---|---|
| 7 | 数据库审计 | 台 | 1 | 性能参数 | 整机吞吐量 | ≥1.5G |
| | | | | | 数据库审计实例授权 | ≥30 |
| | | | | | SQL处理性能 | ≥30000条/秒 |
| | | | | 硬件参数 | 内存 | ≥8G |
| | | | | | 硬盘容量 | ≥128G SSD+4T SATA |
| | | | | | 电口 | ≥6个千兆电口 |
| | | | | 功能参数 | 国产化要求 | 设备需采用国产化芯片与国产化操作系统（提供证明材料并加盖厂商公章）。 |
| | | | | | 1、支持IPv6网络，具备对非关系型数据库的支持，支持监控已添加的Agent的运行情况，支持模糊化处理，保护数据安全，防止数据泄密。（需提供功能截图并加盖厂商公章）。<br>2、以动态曲线的形式展示用户，源头ip，操作类型以及操作对象。（需提供功能截图并加盖厂商公章）。 | |

# 医院网络信息安全等级保护项目技术参数

| 序号 | 名称 | 单位 | 数量 | 参数类别 | 参数要求 | |
|---|---|---|---|---|---|---|
| 8 | 漏洞扫描 | 台 | 1 | 性能参数 | 地址扫描授权 | ≥1000 |
| | | | | | 系统漏扫授权IP数 | ≥1000 |
| | | | | | WEB漏扫授权URL数 | ≥200 |
| | | | | 硬件参数 | 内存 | ≥32G |
| | | | | | 硬盘容量 | ≥128G SSD+4T SATA |
| | | | | | 电口 | ≥4个千兆电口 |
| | | | | | 光口 | ≥4个千兆光口+2个万兆光口（带模块） |
| | | | | 功能参数 | 国产化要求 | 设备需采用国产化芯片与国产化操作系统（提供证明材料并加盖厂商公章）。 |
| | | | | | 1、合规自检：支持域管理功能，可根据客户实际情况进行自定义管理。按“一个中心、三重防护”架构展示检测结果给出整改建议。提供功能截图并加盖厂商公章。<br>2、系统扫描：支持系统漏洞、WEB漏洞、基线配置和弱口令的扫描和分析，并可生成包含这些扫描结果的综合报表。弱口令扫描支持任务的两种执行方式：立即执行和指定时间执行。支持ping、curl、traceroute、dig、nmap等工具，检测的漏洞数大于22000条。提供功能截图并加盖厂商公章。 | |

# 医院网络信息安全等级保护项目技术参数

| 序号 | 名称 | 单位 | 数量 | 参数类别 | 参数要求 | |
|---|---|---|---|---|---|---|
| 9 | 备份一体机 | 台 | 1 | 硬件参数 | 内存 | ≥128G |
| | | | | | 系统盘 | ≥480G |
| | | | | | 数据盘 | ≥24T |
| | | | | | 标配盘位数 | ≥12 |
| | | | | | 电源 | 冗余电源 |
| | | | | | 电口 | ≥4个千兆电口 |
| | | | | | 光口 | ≥2个万兆光口（带模块） |
| | | | | 功能参数 | 国产化要求 | 设备需采用国产化芯片与国产化操作系统（提供证明材料并加盖厂商公章）。 |
| | | | | | 1、支持Oracle数据库多通道备份策略，提高数据库备份效率需，提供功能截图并加盖厂商公章。<br>2、支持Windows、Linux下全量、增量、差异等文件备份方式，支持加密传输，提高传输的安全性；支持配置15分钟滚动备份任务，支持指定时间段进行限速备份限速策略；支持重复数据删除及压缩功能。 | |

# 医院网络信息安全等级保护项目技术参数

| 序号 | 名称 | 单位 | 数量 | 参数类别 | 参数要求 | |
|---|---|---|---|---|---|---|
| 10 | 核心交换机 | 台 | 2 | 性能参数 | 交换容量 | ≥2.4Tbps |
| | | | | | 包转发率 | ≥780Mpps |
| | | | | 硬件参数 | 光口 | ≥4个千兆电口+16个千兆光口+4个万兆光口（带模块）或≥12千兆电口+12个万兆光口（带模块） |
| | | | | | 国产化要求 | 设备需为国产品牌 |
| | | | | 功能参数 | 1、支持跨设备链路聚合技术，通过将两台物理设备在转发层面虚拟成一台设备来实现跨设备链路聚合，保持控制层面互相独立，提升至设备级可靠性。<br>2、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，全局配置及网管口配置，设备升级备份、监控及设备故障替换，组网拓扑可视及管理、设备列表展示等功能。<br>3、支持1588V2功能，满足网络设备间高精度时间同步需求。 | |

# 医院网络信息安全等级保护项目技术参数

| 序号 | 名称 | 单位 | 数量 | 参数类别 | 参数要求 | |
|---|---|---|---|---|---|---|
| 11 | 等保测评服务 | 项 | 1 | | 网络安全等级保护三级测评，符合质量检测标准 | 网络安全等级保护三级测评，符合质量检测标准。 |