**营口市政府采购项目**

**采购需求**

**项目名称：盖州市中心医院服务器、存储、网络安全系统项目采购**

**项目编号：GZC2020-053(1)**

**编制单位：盖州市中心医院**

# 采购需求详细信息

采购人应对招标货物提出详细的数量、技术规格及相关要求。

本部分一般应包含但不限于如下主要内容：

1.交货时间及交货地点

2.付款方式

3.货物名称、数量、货物用途、需实现的功能或者目标，以及为落实政府采购政策需满足的要求

4.技术规格及参数要求、需满足的质量、安全、技术规格、物理特性等要求

5.需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

6.备品备件

7.安装调试

8.技术服务及培训

9.验收标准及方法

10.质量保证和售后服务要求，需满足的服务标准、期限、效率等

服务器存储招标参数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **参数要求** | **数量** | **单位** |
| 1 | 超融合数据库服务器 | 1.★规格：≥2U机架式服务器，可放入42U标准机柜 | 2 | 台 |
| 2.★处理器：英特尔至强金牌系列处理器， CPU数量≥2，单颗处理器核心≥16，主频≥2.3GHZ |
| 3.★内存≥128GB DDR4内存， 内存扩展≥24个内存插槽 |
| 4.支持故障DIMM标识隔离、单颗粒数据纠错（SDDC）、内存巡检、内存地址奇偶检测保护、内存过热调节、内存Rank冗余热备、Socket内的内存镜像 |
| 5.★硬盘≥2\*600GB 10000转 热插拔2.5寸SAS硬盘。 |
| 6.硬盘最大支持的扩展能力≥28块2.5寸硬盘。 |
| 7.RAID功能：配置SAS RAID卡，速率≥12Gb/s，支持RAID0,1,5,6,10，2GB Cache，提供缓存保护套件 |
| 8.★配置网卡≥2个GE电口。≥2个万兆光口(含光模块),配置≥1块双端口16G FC网卡(含光模块)，最大可支持≥10个PCIE 3.0扩展槽位。 |
| 9.★配置冗余电源。 |
| 10.配置冗余风扇。 |
| 11.提供3年原厂商免费维保服务，提供安装调试服务。 |
| 2 | 超融合虚拟化服务器 | 1.★规格：≥2U机架式服务器，可放入42U标准机柜 | 4 | 台 |
| 2.★处理器：英特尔至强金牌系列处理器， CPU数量≥2，单颗处理器核心≥16，主频≥2.3GHZ |
| 3.★内存≥256GB DDR4内存， 内存扩展≥24个内存插槽 |
| 4.支持故障DIMM标识隔离、单颗粒数据纠错（SDDC）、内存巡检、内存地址奇偶检测保护、内存过热调节、内存Rank冗余热备、Socket内的内存镜像 |
| 5.★硬盘≥2\*600GB 10000转 热插拔2.5寸SAS硬盘。 |
| 6.硬盘最大支持的扩展能力≥28块2.5寸硬盘。 |
| 7.RAID功能：配置SAS RAID卡，速率≥12Gb/s，支持RAID0,1,5,6,10，2GB Cache，提供缓存保护套件 |
| 8.★配置网卡≥2个GE电口。≥2个万兆光口(含光模块),配置≥1块双端口16G FC网卡(含光模块)，最大可支持≥10个PCIE 3.0扩展槽位。。 |
| 9.★配置冗余电源。 |
| 10.配置冗余风扇。 |
| 11. 提供3年原厂商免费维保服务，提供安装调试服务。 |
| 3 | 存储 | 1.★实配SAN与NAS统一存储，配置NAS协议（包括NFS和CIFS）、IP SAN和FC SAN协议，不需额外配置NAS网关 | 2 | 台 |
| 2. 配置≥2个控制器，Active-Active；采用2U盘控一体架构 |
| 3.★配置系统缓存容量≥64GB，（不含任何性能加速模块或NAS缓存、FlashCache、PAM卡，SSD Cache等），控制器缓存均具备断电保护功能， 在出现电源故障时，可提供充足的电源，将高速缓存内容转储至非易失性内部存储设备上（非通用服务器架构） |
| 4.支持16Gbps FC、8Gbps FC、10Gbps FCoE、1/10Gbps Ethernet |
| 5.★配置≥8个16GB FC主机接口、配置≥12个10GE 万兆光纤主机接口，配置≥8个GE主机接口（提供NAS服务） |
| 6.支持硬盘类型：SSD,SAS,NL-SAS硬盘，并支持混插 |
| 7.★配置硬盘数量≥12\*4000GB 7.2K NL-SAS 3.5寸硬盘 |
| 8. 支持RAID 1、RAID 10、RAID50、RAID 5、RAID6等可选配置 |
| 9. 配置NAS功能，配置NFS、CIFS、多租户、目录配额功能； |
| 10.★配置自动精简配置，结合业务应用，进行空间的预分配，增加业务空间分配的灵活性，保证后续业务平滑扩展 |
| 11.★配置原厂多路径软件 |
| 12.★配置配置快照、克隆功能 |
| 13.★配置阵列双活功能，任意一套设备宕机均不影响上层业务系统运行（业务不中断） |
| 14.支持windows、Linux、Solaris、HP-UX等主流操作系统 |
| 15. 提供3年原厂商免费维保服务，提供安装调试服务。 |
| 16.为了保证存储与服务器的兼容性，存储与超融合服务器同一品牌 |
| 4 | 虚拟化软件 | 1.★本次提供8个CPU的虚拟化软件授权，三年软件升级服务 | 1 | 套 |
| 2. 单个逻辑集群（HA、动态资源均衡资源池）最多支持32 个物理主机； |
| 3.每站点激活虚拟机数最多可达30000 个； |
| 4.每台虚拟机最多可配置虚拟网卡8 块； |
| 5.采用裸金属架构，无需绑定操作系统即可搭建虚拟化平台； |
| 6. 虚拟机之间可以做到隔离保护，其中任何一个虚拟机发生故障都不会影响同一个物理机上的其它虚拟机运行，每个虚拟机上的用户权限只限于本虚拟机之内； |
| 7.虚拟化管理系统节点提供主备冗余方式确保平台的可用性，支持虚拟机部署模式； |
| 8.提供高效的内存调度与保护机制，能够实现内存的过量使用，以保证虚拟平台不会被暂时的物理内存耗尽而崩溃，同时实现虚拟内存可以超过物理内存；支持存储热迁移；支持基于存储空间的存储DRS（Storage Dynamic Resource Scheduler）功能； |
| 9.提供虚拟数据中心（vDC）功能，支持从逻辑上对集群的计算、存储、网络资源按用户或组织进行资源的逻辑配额分配； |
| 10. 支持vDC资源配额操作，创建和管理虚拟机，创建应用，发放服务。支持系统管理员可以将虚拟数据中心划分给具体的组织，实现资源配置。为更高效便捷的管理，统一Portal 可同时管理虚拟软件及物理设备； |
| 11. 为资源更好的利用，支持回收物理机资源，以及强制回收物理机资源； |
| 12. 为更高效便捷的管理，提供基于WEB 的全景维护工具，支持系统配置、业务维护、告警查看、用户管理、许可管理等功能； |
| 13. 为满足业务系统的安全可靠，系统支持“三权分立”的管理运维模式。支持系统管理员、安全管理员、安全审计员的三员角色； |
| 14. 为满足管理系统的安全可靠，管理节点提供主备高可用机制，确保平台的可用性； |
| 5 | 光纤交换机 | ★国内知名品牌，要求与存储同一品牌 | 2 | 台 |
| ★24口FC交换机，8口激活；配置8个16GB FC多模光模块，配上架套件 |
| ★提供安装调试服务 |
| 6 | 交换机 | ★交换容量≥336Gbps | 1 | 台 |
| ★包转发率≥108Mpps |
| ★24个千兆电口，4个万兆SFP+ |

**网络安全设备招标参数**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号：01  产品名称：防火墙（外联边界区）  数量：1套 | | | | |
| 采购文件要求  重要提示：实质性要求及重要指标用★标注，★标注项不得负偏离，如果负偏离，则响应文件无效。非★标注项允许负偏离一条，如果超过一条负偏离，则响应文件无效。 | 响应文件  响应内容 | 偏离程度 | 偏离说明 | 证明资料 |
| ★1.配置要求：机架式结构，配置为6个10/100/1000BASE-T接口，1个单独的管理口，1个万兆SFP+接口； 默认含：病毒防护功能，含1年专业版病毒特征库升级许可；入侵防御功能，含1年攻击规则库升级许可；  ★2.性能要求：防火墙吞吐率：≥10Gbps；并发连接数：≥300万；  3.支持路由、交换、混合、工作模式；  4.支持IPv4/IPv6双栈工作模式并具有IPV6 Ready Phase-2金牌认证；  5.支持静态路由、ISP路由及动态路由协议，支持802.1q模式；支持主流的TRUNK链路封装和解封，支持链路聚合；  6.支持基于源/目的地址、源/目的端口、用户、应用的策略路由，保证关键业务流量通过优质链路转发；  7.支持手动添加绑定，基于IP、接口的动态探测绑定，支持跨三层IP/MAC绑定，IP/MAC绑定表可导入导出；  8.支持一对一SNAT、多对一SNAT、一对一DNAT、双向NAT、NoNAT等多种转换方式，支持IPSEC VPN；  ★9.提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在WEB界面显示检测结果；（需提供功能截图）  10.支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回；  11.一体化访问控制，实现在同一条访问控制策略中配置传统的五元组信息、用户、域名、应用、服务、时间、安全引擎；  ★12.支持基于NTP协议的检测清洗，包括NTP REQUEST FLOOD、NTP REPLY FLOOD等攻击检测，支持基于NTP请求限速、NTP响应限速、源认证、会话认证的防御策略；（需提供功能截图） |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号：02  产品名称：防火墙（应用服务器区）  数量：**2套** | | | | |
| 采购文件要求  **重要提示：**重要提示：实质性要求及重要指标用★标注，★标注项不得负偏离，如果负偏离，则响应文件无效。非★标注项允许负偏离一条，如果超过一条负偏离，则响应文件无效。 | 响应文件  响应内容 | 偏离程度 | 偏离说明 | 证明资料 |
| ★1.配置要求：机架式结构，配置为6个10/100/1000BASE-T接口和2个SFP插槽，支持4个万兆SFP PLUS接口，1个可插拔的扩展槽 ；默认包含应用识别功能，含3年攻击规则库升级许可；  ★2.性能要求：防火墙吞吐率：≥26Gbps；并发连接数：≥800万；  3.支持路由、交换、混合、工作模式；  4.支持IPv4/IPv6双栈工作模式并具有IPV6 Ready Phase-2金牌认证；  5.支持静态路由、ISP路由及动态路由协议，支持802.1q模式；支持主流的TRUNK链路封装和解封，支持链路聚合；  6.支持基于源/目的地址、源/目的端口、用户、应用的策略路由，保证关键业务流量通过优质链路转发；  7.支持手动添加绑定，基于IP、接口的动态探测绑定，支持跨三层IP/MAC绑定，IP/MAC绑定表可导入导出；  8.支持一对一SNAT、多对一SNAT、一对一DNAT、双向NAT、NoNAT等多种转换方式，支持IPSEC VPN；  ★9.提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在WEB界面显示检测结果；（需提供功能截图）  10.支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回；  11.一体化访问控制，实现在同一条访问控制策略中配置传统的五元组信息、用户、域名、应用、服务、时间、安全引擎；  ★12.支持基于NTP协议的检测清洗，包括NTP REQUEST FLOOD、NTP REPLY FLOOD等攻击检测，支持基于NTP请求限速、NTP响应限速、源认证、会话认证的防御策略；（需提供功能截图） |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号：03  产品名称：病毒过滤网关  数量：**1套** | | | | |
| 采购文件要求  重要提示：实质性要求及重要指标用★标注，★标注项不得负偏离，如果负偏离，则响应文件无效。非★标注项允许负偏离一条，如果超过一条负偏离，则响应文件无效。 | 响应文件  响应内容 | 偏离程度 | 偏离说明 | 证明资料 |
| ★1.配置要求：机架式结构，配置为6个10/100/1000BASE-T接口（支持Bypass）； 默认企业版查杀病毒功能，包括企业版快速扫描防病毒查杀和企业版深度扫描防病毒查杀，含3年企业版病毒库升级服务许可；  ★2.性能要求：整机吞吐率≥4Gbps；最大并发连接数≥300万；病毒检测吞吐率≥1500Mbps；  3.支持IPv4和IPv6双栈协议的病毒扫描和过滤，并具有IPV6 Ready Phase-2金牌认证；  4.要求每种扫描引擎具有独立的病毒库，流行病毒库总数大于600万。  ★5.支持TCP粘合技术，提升病毒检测效率；（需提供功能截图）  6.支持采用邮件地址与IP地址的黑、白名单技术实时检测垃圾邮件并阻止其进入企业网络，为企业节省宝贵的带宽。  7.支持针对“ActiveX”、“Java Applets”及“Script”等控件实施拦截；  ★8.支持实时检测日益泛滥的蠕虫攻击，并对其进行实时阻断，从而有效防止内部网络因遭受蠕虫攻击而陷于瘫痪；（需提供功能截图）  9.支持邮件地址与IP地址的黑、白名单技术实时检测垃圾邮件并阻止其进入企业网络，为企业节省宝贵的带宽；  10.支持对病毒、木马、蠕虫的防御，且支持对压缩数据、加壳病毒的查杀；  11.当病毒突然爆发时，可向网络管理员发送报警信息，支持邮件报警、声音报警、SNMP等报警方式；  12.支持强大的监控功能，可以监控系统资源、网络流量、当前会话数、当前病毒扫描信息等。 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号：04  产品名称：web应用安全防护系统  数量：**1套** | | | | |
| 采购文件要求  重要提示：实质性要求及重要指标用★标注，★标注项不得负偏离，如果负偏离，则响应文件无效。非★标注项允许负偏离一条，如果超过一条负偏离，则响应文件无效。 | 响应文件  响应内容 | 偏离程度 | 偏离说明 | 证明资料 |
| ★1. 配置要求：机架式机构，配置为6个10/100/1000BASE-T接口（支持Bypass）； 默认含3年特征库升级服务，内含SQL注入、XSS、CSRF等WEB攻击防护功能、URL访问控制功能、防盗链功能、WEB漏洞扫描功能、DDOS攻击防护功能、服务器负载均衡功能、报表分析及告警功能；  ★2.性能要求：网络层吞吐≥5G，应用层吞吐800≥Mbps，并发连接≥100万；  3.支持无IP纯透明模式串联部署、旁路监测模式部署、负载均衡模式部署、反向代理模式部署；  4.支持SSL的WEB界面、SSH、Console多种方式管理；  5.支持基于域名和IP的网站防护；支持HTTP/HTTPS站点防护；  ★6.Web界面可以直观查看WAF扩展卡、接口、USB口、管理口、HA口及业务口的运行状态；（需提供功能截图）  7.支持静态路由及策略路由配置；  8.支持IPv4和IPv6双栈协议并具有IPV6 Ready Phase-2金牌认证；  ★9.支持账号策略自定义，支持定义允许最大登录失败次数、密码错误账号锁定时间、最大在线管理员数、对其他非法在线管理员强制下线、防管理员账号暴力破解；（需提供功能截图）  10.支持柱形图方式查看系统中不同资源所占比例；  11.支持最近一小时、一天、三十天等多种条件内攻击源IP攻击次数及攻击分布TOPN的统计；  12.支持操作系统WEB方式升级及命令行等方式的离线升级。 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号：05  产品名称：入侵检测系统  数量：**1套** | | | | |
| 采购文件要求  重要提示：实质性要求及重要指标用★标注，★标注项不得负偏离，如果负偏离，则响应文件无效。非★标注项允许负偏离一条，如果超过一条负偏离，则响应文件无效。 | 响应文件  响应内容 | 偏离程度 | 偏离说明 | 证明资料 |
| ★1.配置要求：机架式结构，配置为6个10/100/1000BASE-T接口；默认含3年攻击知识库升级许可，3年网站知识库升级许可。  ★2.性能要求：整机吞吐率 ≥8Gbps；IDS吞吐率： ≥3Gbps ；最大并发连接数：≥200万。  3.支持直连、路由、VLAN、旁路监听、混合部署等多种接入模式；  4.支持IPv6、IPv6 over IPv4、IPv6和IPv4混合网络，能够在该网络环境中检测出攻击事件，并具有IPV6 Ready Phase-2金牌认证；  5.支持涵盖广泛的攻击特征库、能够针对5000种以上攻击的攻击行为、异常事件，以及网络资源滥用流量，进行检测。  ★6.支持DHCP异常包及DHCP Flood攻击检测；支持ARP异常包及ARP Flood攻击检测；支持CC攻击检测；（需提供功能截图）  7.支持防御包括land、Smurf、Pingofdeath、winnuke、tcp\_sscan、ip\_option、teardrop、targa3、ipspoof、Synflood、Icmpflood、Udpflood、Portscan、ipsweep等在内的DOS/DDOS攻击；  8.支持融合模式匹配、协议分析、异常检测、会话关联分析，逃逸等多种技术，准确识别入侵攻击行为，为用户提供2~7层深度入侵防御；  9.支持DDOS 机器人自学习功能，学习时间可设置；  ★10.支持对网络内的TCP、UDP、其他流量协议占比进行设置及报警；（需提供功能截图）  11.支持DNS异常包及DNS Flood攻击防御，支持DHCP异常包及DHCP Flood攻击防御。 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号：06  产品名称：日志收集与分析系统  数量：**1套** | | | | |
| 采购文件要求  重要提示：实质性要求及重要指标用★标注，★标注项不得负偏离，如果负偏离，则响应文件无效。非★标注项允许负偏离一条，如果超过一条负偏离，则响应文件无效。 | 响应文件  响应内容 | 偏离程度 | 偏离说明 | 证明资料 |
| ★1. 配置要求：机架式结构，配置为1个console口，6个10/100/1000BASE-T接口，存储容量4T。含日志收集、存储、查询、统计分析、告警响应等功能，包含50个日志源授权。  ★2.性能要求：日志处理均值30000EPS，峰值45000EPS；  3.支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志对象的日志数据采集；  4.支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过Agent采集日志数据；  5.支持设备种类清单，提供设备日志外发配置建议指导；  6.支持日志归一化处理，将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者；  7.支持日志备份功能，支持本地备份和FTP备份方式，支持自动备份和手动备份；  ★8.支持对文本类型日志源进行限速采集，匀速采集日志，防止对系统资源产生突发冲击；（需提供功能截图）  9.报表支持基于全国地图、全球地图进行访问源、访问目的追踪；  10.支持自定义统计日志数据形成报表，支持统计分析报表以PDF、word、execl、html等方式导出；支持实时报表、计划报表；  ★11.支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息；（需提供功能截图）  12.支持按照日志源名称、IP地址、日志源类型、接受时间及状态等维度对日志源列表进行排序。 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号：07  产品名称：数据库审计系统  数量：**1套** | | | | |
| 采购文件要求  重要提示：实质性要求及重要指标用★标注，★标注项不得负偏离，如果负偏离，则响应文件无效。非★标注项允许负偏离一条，如果超过一条负偏离，则响应文件无效。 | 响应文件  响应内容 | 偏离程度 | 偏离说明 | 证明资料 |
| ★1. 配置要求：机架式结构型，配置为6个10/100/1000BASE-T接口； 1T存储空间； 默认含3年的攻击库和应用识别库；  ★2.性能要求：审计处理能力≥1Gbps ，峰值SQL处理能力≥6000条/秒；  3.支持B/S管理方式，无需在被审计系统上安装任何代理；  4.支持Oracle数据库、SQL-Server数据库、DB2数据库、Informix数据库、Sybase数据库、MySQL数据库、PostgreSQL、人大金仓kingbase、Cache、南大通用Gbase、达梦数据库审计；  5.支持SQL语法解析器，可分析SQL语句的操作类型，操作对象等信息，同时支持正则与非正则方式；  6.支持SQL操作响应时间的审计,支持Update、Insert、Delete操作返回行数的审计, 支持数据库操作成功、失败的审计；  7.支持其他设备发送的netflow分析能力，支持对netflowV5/V9版本的流量分析；  8.支持以数据库客户端软件名称、数据库名、数据库表名、数据库字段名作为过滤响应条件（非正则表达式方式）的数据库审计策略；  9.支持对接口、传输协议、应用协议、应用协议组、源目的地址、源目的端口进行统计分析，可以多条件组合分析。支持流量趋势分析、支持流量分析的下钻与上卷；  10.支持与防火墙等设备联动阻断攻击行为。支持Syslog告警、SNMP trap告警、邮件告警；  11.支持审计数据管理功能，可根据时间或磁盘空间状况实现对审计数据的自动备份、删除；  12.支持频率趋势图、概率统计图、饼图方式进行报表展现，并可导出统计结果报表；  ★13.支持历史版本回退功能，系统内建历史版本库不少于3个；（需提供功能截图）  ★14.支持系统管理员IP黑白名单，对于无权访问的IP可以隐藏设备自身IP地址；（需提供功能截图）  15.支持IPv6、IPv6 over IPv4、IPv6和IPv4混合网络，能够在该网络环境中检测出攻击事件，并具有IPV6 Ready Phase-2金牌认证。 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号：08  产品名称：运维安全审计系统（堡垒机）  数量：**1套** | | | | |
| 采购文件要求  重要提示：实质性要求及重要指标用★标注，★标注项不得负偏离，如果负偏离，则响应文件无效。非★标注项允许负偏离一条，如果超过一条负偏离，则响应文件无效。 | 响应文件  响应内容 | 偏离程度 | 偏离说明 | 证明资料 |
| ★1. 配置要求：机架式结构，配置为6个10/100/1000BASE-T接口，1T存储空间，；  ★2. 支持50个主机/设备许可，用户数不限制；  3.支持旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构，不改变运维人员的运维习惯；  4.支持完整的用户帐号生命周期管理，实现帐号的创建、维护、修改、删除的集中管理；自定义用户类型，基于针对用户类型进行用户地址策略；  5.支持提供系统内部操作审计，包括管理员和运维用户的登录、登出、对系统的配置操作、账号属性修改等系统管理操作；  6.支持对unix资源、网络资源、windows资源、数据库资源、中间件资源进行密码变更；密码变更可以根据密码策略的要求进行变更，变更的密码符合密码策略中关于密码强度的要求；  7.图形资源访问时，支持键盘、剪切板、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、文件传输记录的指定位置开始回放；  8.支持AD域抽取功能，可以将AD域内帐号作为自然人帐号来存储；  9.为提高设备的安全性，能够不采用标准的协议端口，平台支持FTP、telnet、ssh、远程桌面等协议服务端口变更；  ★10.采用动作流方式代填，将单条动作转换为一系列操作并代替人工输入，无需定制即可对各类资源实现代填和审计；（需提供功能截图）  ★11.具有配置向导功能，快速教会客户部署实施；（需提供功能截图）  12.支持日志数据的外置存储备份，支持NFS和windows文件共享协议，远程审计存储和本地存储对审计员透明；  13.支持SSH、TELNET、FTP、SFTP、VNC、XWINDOW、WINDOWS文件共享等协议。其中，SSH协议代理支持SecureCRT软件的Session Clone及Send To All等复杂的功能；  14.支持自定义角色。角色可按照组节点进行定义，从而实现分层分级管理模式。角色权限细粒度高，可自由组合；  15.支持配置成可访问时间段方式，也可以配置成不可访问时间段方式。配置时间段时可以配置日期和小时；  16.支持配置访问失败几次锁定，也可以配置锁定后多长时间解锁。 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号：09  产品名称：业务融合集中管控平台  数量：**1套** | | | | |
| 采购文件要求  重要提示：实质性要求及重要指标用★标注，★标注项不得负偏离，如果负偏离，则响应文件无效。非★标注项允许负偏离一条，如果超过一条负偏离，则响应文件无效。 | 响应文件  响应内容 | 偏离程度 | 偏离说明 | 证明资料 |
| ★1.配置要求：机架式结构，配置为2个万兆SFP plus接口、4个10/100/1000BASE-T接口；  ★2.支持对医院HIS系统、虚拟化、超融合进行集中管理，针对CIS、LIS、EMR、PACS、RIS、CAD等业务可用性监测、业务数据精细指标监测、性能监测；  3.支持对Cisco、Juniper、Foundry、F5、IBM、Brocade、Microsoft、华为、中兴、华三、戴尔、联想、锐捷、烽火、天融信、深信服等主流设备厂商进行监控、管理；  4.支持对Windows Server 2008、Windows Server 2003、Centos linux、Redhatlinux、Suselinux、红旗linux、HP-Unix、Aix、Solaris、其它Windows、Linux、Unix等操作系统进行监控、管理；  5.支持对Oracle、SqlServer、DB2、Mysql、PostgreSQL、Tomcat、Weblogic、Jboss、Websphere等应用进行监控、管理；  6.支持对FTP、DHCP、DNS、Http、Https、POP3、SMTP、ICMP、LDAP、URL等协议进行实时监控与管理；  7.支持主动从多个方面监控网络设备，能实时监控设备网口、电口、光接口的状态。包括端口可用性、端口性能数据、端口故障、链路问题都能实时掌控。支持直接在操作界面真实展现设备的机架图、面板图，并能方便的配置和自定义机架图和面板图；  ★8.支持一拖N上网检测，防止私架局域网，如发现可将IP自动加入黑名单阻断上网，阻断时间可自定义；（需提供功能截图）  9.可以自动发现发现全网的主机/服务器，也支持手工添加和删除主机/服务器。系统能主动监控主机/服务器的在线状态，对主机/服务器资源如：CPU、磁盘、内存、网络接口、系统进程等进行性能采集。并可以设定监视器指标对资源进行实时监控，如监控某个服务器上的应用连接详细情况，实时在线访问改业务应用的客户端数量、IP地址、上传/下载流量大小等等信息；  10.能自动发现物理主机或虚拟化服务器的虚拟化系统，包括虚拟机服务器和虚拟机工作站，管理服务器和虚拟化之间的关系。并能监控虚拟机载体和其资源池的各种性能指标如 CPU 负载、内存使用率、系统进程、磁盘空间等性能；  11.支持自动发现、搜索网络设备，并识别设备类型和厂商型号，生成设备的面板图和加载设备资源，如：板卡、端口、CPU、内存、磁盘等，并发现设备之间的链路关系。通过自动化发现设备并自动识别设备间的链路关系，自动生成拓扑图，简化用户操作，提升管理效率；  12.支持 LLDP、STP、CDP 技术、邻居路由、端口转发表、等物理拓扑发现技术自动识别聚合链路工业环网等。展示设备之间的链路、运行状态、流量性能数据智能识别链路关系，通过直观的拓扑图进行展现；  13.支持多种告警机制，自定义配置告警阀值，支持快速标示已经执行操作的告警，迅速定位告警设备。全面采集设备资源、应用、服务等告警信息。可将告警信息数据按照时间、资源、性能类型等多种维度以图表等形式展现。 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号：10  产品名称：安全隔离与信息交换系统  数量：**1套** | | | | |
| 采购文件要求  重要提示：实质性要求及重要指标用★标注，★标注项不得负偏离，如果负偏离，则响应文件无效。非★标注项允许负偏离一条，如果超过一条负偏离，则响应文件无效。 | 响应文件  响应内容 | 偏离程度 | 偏离说明 | 证明资料 |
| ★1. 配置要求：机架式结构，内外端机双侧液晶屏，各1TB硬盘； 内端机4个10/100/1000Base-T接口，1个扩展槽位； 外端机4个10/100/1000Base-T接口，1个扩展槽位； 标准配置包含安全浏览模块、文件传输模块、文件同步模块、邮件访问模块、VOIP访问模块、数据库访问模块、数据库同步模块、自定义访问模块、数据中心模块。  ★2. 性能要求：网络吞吐量≥600Mbps；并发连接数：≥7万；  3.支持50种以上文件类型特征识别，非扩展名过滤，包括可执行文件、文本文件、压缩文件、图片文件、多媒体文件等，支持上下行方向过滤单独控制，支持允许、阻断、告警三种处理方式；  4.支持基于单一域名的黑白名单访问控制，支持基于URL分类地址库的访问控制，支持允许、阻断、告警三种处理方式；  5.支持IP地址、端口、时间以及基于源用户身份的访问控制策略；  6.支持IPV4\IPV6双栈IP+MAC绑定功能，支持基于物理接口和IP网段的IP+MAC主动探测，支持IP、MAC信息查询功能；  7.支持多种主流数据库系统如：ORACLE、SQLSERVER、MYSQL、达梦数据库的同步；  ★8.支持自动读取数据库表名和字段名，无需手动录入表名和字段名，降低配置复杂度；（需提供功能截图）  9.支持威胁统计监控，以图表形式实时展现内外端机TOP20的病毒防御威胁事件统计排名；  10.支持本地认证功能和外部认证功能，外部认证支持Radius、Ldap、Tacacs等类型的认证服务器；  ★11.支持连接保护功能，基于源和目的IP地址的并发连接数和新建连接数控制，并可以手动设置相关阈值，超过阈值后可选限制和警告两种处理方式；（需提供功能截图）  12.内置VOIP安全模块，内置VOIP安全引擎，支持主被叫用户黑名单的控制。 |  |  |  |  |

1、交货/交付时间：合同签订后30个工作日。

2、交货/交付地点：盖州市中心医院指定地点

3、付款方式及条件：验收合格后支付合同总价款95%.余款5%作为质保金，一年后无息返还。