## 采购需求

### 一 产地要求

根据法律法规，本项目采购产品须为中华人民共和国境内（不含港、澳、台）生产或组装。

### 二 采购内容及清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 设备分类 | 序号 | 设备名称 | | 数量 | 单位 |
| 通用硬件 | 1 | 网络部分 | 核心交换机 | 2 | 台 |
| 2 | 万兆光口交换机 | 2 | 台 |
| 3 | 视频网核心扩容 | 1 | 块 |
| 4 | 万兆多模模块 | 200 | 块 |
| 5 | 40km万兆单模 | 4 | 块 |
| 6 | 千兆多模 | 10 | 块 |
| 7 | 48千兆电口板卡 | 1 | 块 |
| 8 | 光口业务板卡 | 1 | 块 |
| 9 | 安全访问平台 | 下一代防火墙设备1 | 2 | 台 |
| 10 | 下一代防火墙设备2 | 2 | 台 |
| 11 | 应用前置服务器 | 1 | 套 |
| 12 | 可信API代理设备（TIP） | 1 | 台 |
| 13 | 可信应用接入代理设备（TAP） | 1 | 台 |
| 14 | 可信代理控制服务设备 | 1 | 台 |
| 15 | 虚拟云桌面一体机设备 | 1 | 套 |
| 16 | 现有数据中心安全体系完善 | 日志采集和存储设备 | 1 | 台 |
| 17 | 数据库审计 | 1 | 台 |
| 18 | 视频专网数据中心安全体系完善 | 下一代防火墙设备 | 3 | 台 |
| 19 | 日志审计配套服务器 | 1 | 台 |
| 20 | 数据库审计 | 1 | 台 |
| 21 | 堡垒主机 | 1 | 台 |
| 安全服务 | 22 | 视频网 | 网络准入控制服务 | 3 | 年 |
| 23 | 终端安全管理服务 | 3 | 年 |
| 24 | 终端水印管理服务 | 3 | 年 |
| 25 | 终端防病毒服务 | 3 | 年 |
| 26 | 网络边界监测服务 | 3 | 年 |
| 27 | 公安网 | 违规外联检测 | 3 | 年 |
| 28 | 安全运营服务 | 安全驻场服务：   1. 安全标准建设 2. 安全合规检查及指导 3. 安全设备运行维护 4. 安全、策略优化   5、配置及备份更新 | 3 | 年 |

### 三 背景及执行标准要求：

3.1项目背景与建设目标

以支撑丽水市公安业务应用访问的安全、可信、合规为目标，以保护数据为核心，采用“零信任”的先进安全理念建立丽水市公安局新一代公安信息网统一安全访问平台，实现访用户的身份可信，确保业务仅对合法用户可见；可结合业务场景和使用环境进行精细化的动态授权；能保护数据安全访问，具备抵御网络攻击的能力，并实现访问过程中用户行为及网络风险的全面发现与审计。

3.2建设依据

3.2.1国家政策

* 1. 《关于加强社会治安防控体系建设的意见》（中办发〔2014〕69号）
  2. 《关于积极推进“互联网+”行动的指导意见》（国发〔2015〕40号）
  3. 《关于印发促进大数据发展行动纲要的通知》（国发〔2015〕50号）
  4. 《国民经济和社会发展第十三个五年规划纲要》（2016年）
  5. 《政务信息资源共享管理暂行办法》（国发〔2016〕51号）
  6. 《关于印发大数据产业发展规划（2016-2020年）的通知》（工信部规〔2016〕412号）
  7. 《“十三五”国家信息化规划》（国发〔2016〕73号）
  8. 《“十三五”平安中国建设规划》（国发〔2017〕30号）
  9. 《政务信息系统整合共享实施方案》（国办发〔2017〕39号）

10.《中华人民共和国网络安全法》

3.2.2行业政策

1. 《关于全面深化公安改革若干重大问题的框架意见》（2015年）
2. 《公安发展“十三五”规划（2016-2020年）》（公发〔2015〕5号）
3. 《关于大力推进基础信息化建设的意见》（公通字〔2015〕18号）
4. 《公安机关信息共享规定》（公通字〔2015〕6号）
5. 《公安云计算建设指导意见》（公科信〔2015〕119号）
6. 《全国公安移动\*\*建设总体技术方案》（公科信〔2016〕79号）
7. 《全国公安装备建设“十三五”规划》（公通自〔2016〕11号）
8. 《关于推进公安信息化发展若干问题的意见》（公通字〔2017〕7号）
9. 《公安信息网安全管理规定（试行）》（公通字〔2017〕8号）

10.《“十三五”公安信息化总体技术架构》（公科信〔2017〕108号）

11.《公安信息化项目建设指南（2018-2020年）》（公安部，2017年9月）

12.《云计算平台框架指南》（公安部，2017年12月）

13.《关于围绕新中国成立70周年安保维稳强化公安大数据智能化建设应用的通知》 （公科信〔2018〕254号）

14.《公安部大数据智能化建设规划设计总体需求书》（公安部，2018年5月）

15.《公安大数据处理技术指南》（公安部，2018年10月）

3.2.3标准规范

1. 《公安大数据安全 总体技术框架》（GA DSJ 300-2019）
2. 《公安大数据安全 安全访问平台技术设计要求》（GA DSJ 350-2019）
3. 《公安大数据安全 零信任体系技术设计要求》（GA/DSJ 351-2019）
4. 《公安大数据安全 安全防护体系技术设计要求》（GA/DSJ 352-2019）
5. 《公安大数据处理 总体技术规范》（（GA/DSJ 200-2019）
6. 《公安大数据处理 数据处理技术要求》（GA/DSJ 220-2019）
7. 《公安大数据处理 数据资源目录管理规程》（GA/DSJ 290-2019）
8. 《新一代公安信息网 网络架构技术要求》（GA/DSJ 400-2019）
9. 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

10.《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

### 四 技术需求

## 4.1硬件采购详细需求

## 4.1.1网络部分

|  |  |  |
| --- | --- | --- |
| **序号** | **设备** | **技术规格要求** |
| 1 | 核心交换机 | 采用高可靠框式交换设备（主控板冗余、交换网板冗余、电源模块冗余、风扇模块冗余），故障时主备倒换毫秒级，关键业务流量不中断转发。要求设备预留足够槽位数量，可以平滑扩容增加单板，支持GE、10GE、40GE、100GE端口平滑扩容。全面支持IPv4/IPv6双协议栈。交换容量512Tbps，包转发率96000Mpps，配置双主控，5个交换网板， 36个万兆光口，4个40G接口，1200W电源4个 |
| 2 | 万兆光口交换机 | 万兆汇聚盒式交换机，24个万兆光口，2个40G万兆光口。2个扩展插槽。模块化冗余电源，模块化冗余风扇 |
| 3 | 视频网核心扩容 | S12500-X 48万兆以太网光接口模块 |
| 4 | 万兆多模模块 | SFP+ 万兆模块(850nm,300m,LC) |
| 5 | 40km万兆单模 | SFP+ 万兆模块(1550nm,40km,LC) |
| 6 | 千兆多模 | 光模块-SFP-GE-多模模块-(850nm,0.55km,LC) |
| 7 | 48千兆电口板卡 | 7506E-X扩容，48端口千兆以太网电接口模块(RJ45) |
| 8 | 光口业务板卡 | 7506E-X扩容，44端口千兆以太网光口(SFP,LC)+4端口万兆以太网光接口模块(SFP+,LC) |

## 4.1.2安全访问平台

|  |  |
| --- | --- |
| **下一代防火墙设备1（2台）** | |
| **指标项** | **技术规格要求** |
| 系统架构 | 为了确保网络数据能够极速稳定转发，系统采用多核架构，硬件设计采用高性能一体化智能安全处理引擎。 |
| 流量镜像功能 | 提供网络端口的流量镜像功能，实现将防火墙经过的全流量数据镜像提供给第三方设备使用。 |
| 性能规格 | 标准3U机架设备,冗余电源。 |
| 至少满足≥8个千兆电口，≥4个万兆光口（含光模块），防火墙本地日志存储空间>=1Tb。 |
| 整机吞吐量≥80Gbps，并发连接数≥900万，每秒新建连接数≥100万。 |
| 基础组网和网络适应能力 | 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； |
| 支持支持通过802.3ad协议、轮询、热备等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余。 |
| ▲所投产品必须支持全面的NAT转换配置，包括包括一对一，一对多，多对一的源、目的地址转换。 |
| 支持DNS透明代理 |
| 支持双机热备和双机负载均衡功能。支持标准VRRP协议，支持路由、透明模式下“主-备”、“主-主”方式部署，设备支持一种多防火墙的负载均衡方法及装置的技术。 |
| 支持基于权重的路由负载均衡，算法支持：源地址目的地址哈希、轮询、源地址哈希、目的地址哈希、源地址轮询、备份、随机、流量均衡、最优链路带宽负载、最优链路带宽备份、时延负载、跳数负载 |
| 支持静态路由，支持策略路由，支持对称路由；支持ISP路由，并支持手动导入；支持动态路由协议RIPv1/v2、OSPF、BGP |
| 要求防火墙支持IPSEC VPN、SSL VPN、PPTP功能。IPSec VPN隧道≥500 |
| 所投产品可直观展示不同风险等级的应用在1天（24小时）或一周（7天）内传输流量的绝对数值及占全网流量的百分比。 |
| 支持IPv6地址配置，支持IPV6手动及自动的IP/MAC探测及绑定，支持IPV6的本地认证；支持IPV6下静态路由及策略路由 |
| 访问控制功能 | 支持基于源目的IP地址、源目的安全域、VLAN ID、MAC地址、时间、用户、地理区域、服务协议及应用等多种方式进行访问控制； |
| 支持一条访问控制策略同时对端口和协议进行管控。 |
| 支持通过一条安全策略配置应用控制、入侵防护、URL过滤、病毒检测、内容过滤、网络行为管理等高级访问控制功能，且无需编辑即可直观审计策略配置。 |
| 能实现对rdp、ssh、telnet、vnc、pcanywhere等各类远程访问控制协议的识别和阻断，要求支持的远程访问控制协议种类在35种以上，。并支持对特定IP的开启例外功能。  能实现对主要种类数据库协议的识别和阻断，要求支持的协议种类超过9种，并支持对特定IP的开启例外功能。 |
| 标准SNMP协议支持 | 要求提供标准SNMP协议支持，允许第三方网管软件对防火墙的CPU、内存、网络流量等性能、可用性等进行监测。 |
| 病毒防护 | 提供病毒查杀和防护功能模块，能够HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；支持对压缩文件进行解压查杀； |
| 支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |
| 病毒库不少于600万种病毒特征，支持病毒库扩充，支持添加特定病毒种类特征。支持病毒云查杀功能。要求提供病毒库来源和名称病毒库，建议以目前国内流行病毒为主。 |
| 应用识别和行为管理 | ▲所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输方式等特征分类 |
| 支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤 |
| 入侵防御 | IPS特征库不少于3000条特征值。 |
| 所投产品的漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息； |
| 支持对拒绝服务、缓冲区溢出、恶意扫描、木马后门、病毒蠕虫、僵尸网络、跨站脚本、SQL注入、WEB攻击等的防御，具备针对DNS、FTP、ICMP、IMAP、SQL、NNTP、POP、SMTP、SNMP等协议类型的入侵检测与防御 |
| 支持对应用层 Flood攻击进行五种处理动作：警告、阻断、普通防护、增强防护及授权服务器防护 ；支持局域网广播防护，支持全局配置的局域网广播防护及基于二层接口的局域网广播防护，可以防止局域网内广播和多播数据包泛滥，保障网络正常通信 |
| 支持基于防护类型及防护级别的预定义IPS模板；基于行业类型特点的预定义URL模板 |
| 内容过滤 | 实现HTTP、FTP、POP3、SMTP、IMAP五种应用协议的双向内容过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义，支持阻断及日志两种处理动作； |
| 安全事件分析和异常感知 | 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破、存在安全风险的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息 |
| 所投设备必须提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素为过滤条件进行数据钻取 |
| 支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为 |
| 所投设备提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL过滤、文件过滤等安全模块检查的日志集中显示 |
| 策略与处置 | 所投设备可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项 |
| 所投产品支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括1天、7天、30天、90天、永久等； |
| 所投产品支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果 |
| 运维管理 | 所投产品支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件 |
| 所投产品需支持加密的WebUI和CLI管理，且支持网页命令行管理（WebUI中内嵌CLI管理界面） |
| 所投产品支持将告警信息以SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、CPU利用率、内存利用率、硬盘利用率、接口带宽利用率等； |
| 威胁感知  系统联动同 | 所投产品支持与网络威胁感知系统联动，将本地终端产生的异常行为、攻击活动等数据上报至网络威胁感知系统，网络威胁感知系统可实时监控网络内的攻击事件并预警可疑的受感染主机，同时支持接收来自网络威胁感知系统推送的情报信息。 |
| 终端安全软件联动 | 所投产品支持与桌面杀毒或终端管理软件联动，实现基于终端健康状态的访问控制；增强防火墙对木马特征的识别能力 |
| 用户登陆认证 | 支持基于web的无客户端方式用户登陆认证；管理页面登陆支持客户端IP地址限定。 |
| 产品要求 | 要求防火墙产品支持IPv6 |

|  |  |
| --- | --- |
| **代防火墙设备2（2台）** | |
| **指标项** | **技术规格要求** |
| 品牌型号 | ▲要求与防火墙1设备为不同厂商和品牌 |
| 硬件及接口 | 标准机架设备,冗余电源。至少满足≥8个千兆电口，≥4个万兆光口（含光模块），≥2个高速USB2.0接口，≥1个RJ45串口。防火墙本地日志存储空间>=1Tb。 |
| 性能 | 整机吞吐量≥80Gbps，并发连接数≥16,000,000，新建连接数≥1,000,000 |
| 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。 |
| 路由支持 | 支持静态路由，ECMP等价路由，支持RIPv1/v2，OSPFv2/v3，BGP动态路由协议 |
| 基础功能 | 基础功能 访问控制策略支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式；  能够识别应用类型超过1100种，应用识别规则总数超过3000条，支持自定义应用；  支持IPv4／v6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源IP或者目的IP进行连接数控制；  支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制； |
| 内容安全 | 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；  支持采用无特征AI检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测。 |
| 入侵防护 | 为了保证入侵防御系统识别的专业性，要求入侵防护漏洞规则特征库数量在4000条以上，入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号，参考信息和建议的解决方案； |
| 为了避免因黑客暴力破解导致的密码泄露事件，要求设备支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能； |
| 为了帮助管理员及时了解掌握内网所存在的弱密码，避免因这些弱密码导致的系统安全隐患，要求设备具备对常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能； |
| 支持同防火墙访问控制规则进行联动，可以针对检测到的攻击源IP进行联动封锁，支持自定义封锁时间； |
| 为了帮助管理员更好的应对一些突发的热点安全事件，要求设备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； |
| 高级威胁检测 | 支持蜜罐功能，定位感染僵尸网络病毒的真实主机IP地址，提供相关功能相关证明材料； |
| 具备独立的僵尸网络特征库，恶意软件识别特征总数在50万条以上； |
| 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； |
| 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； |
| 病毒防护 | 支持对HTTP，FTP，SMTP，POP3协议进行病毒文件检测； |
| 内置病毒特征数量超过100万； |
| 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，支持包含敏感数据业务的识别，提供相关功能相关证明材料； |
| 为了全面的了解每个业务系统的安全风险及处理办法，要求支持在首页多维度的展示发现的安全威胁，如攻击风险，漏洞风险，终端安全威胁和数据风险等，并支持将所有发现的安全问题进行归类汇总，并针对给出相应的解决方法指引； |
| 高可用性 | 双机支持A/S，A/A方式部署，支持配置同步，会话同步和用户状态同步。 |
| 服务要求 | 承诺中标后根据用户要求能提供样机进行上述功能的逐一测试验证，测试中发现虚假应标的行为，采购人有权单方面解除合同并保留对中标方追究相关责任的权利。 |

|  |  |
| --- | --- |
| **应用前置服务器（1套）** | |
| **指标项** | **技术规格要求** |
| 数量要求 | ▲本项目要求3台超融合虚拟化服务器 |
| 硬件规格 | CPU Hygon5280\*2、内存≥256G、千兆网口≥6个、万兆光口≥2个，冗余双电源；  本项目要求至少配备2块240G SSD硬盘、2块960G SSD硬盘和6块4T的SATA硬盘。 |
| 服务器虚拟化及管理 | ▲本次项目提供6个物理CPU服务器虚拟化管理授权 |
| 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 |
| 虚拟化内核基于开源软件KVM底层开发 |
| 支持虚拟机的无代理备份，能提供至少100个虚拟机的高性能备份功能，支持至少10T的备份数据容量的许可，可将直接将虚拟机备份到磁盘，并支持生成全新虚拟机的方式进行恢复 |
| 支持IO重试，当存储出现故障，导致虚拟机无法读取存储数据时，自动挂起虚拟机，避免业务故障。 |
| 每个虚拟机都可以安装独立的操作系统，为获得良好的兼容性操作系统支持需要包括Windows、 Linux，并且支持国产操作系统包括：红旗linux、中标麒麟、中标普华、深度linux等 |
| 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。 |
| 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。 |
| 支持无代理跨物理主机的虚拟机USB映射，需要使用USB KEY时，无需再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。 |
| 支持在本地管理平台实现对VMware vCenter中的虚拟机备份，并能够在超融合的平台实现VMware虚拟机的启动恢复； |
| 支持双向迁移，可将VMware虚拟机在运行状态下迁移到超融合平台上，也可将超融合平台上的虚拟机在运行状态下迁移到VMware vCenter的集群中，迁移最后阶段业务会中断,可选择自动或手动拉起。 |
| 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 |
| 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。 |
| 支持平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态。 |
| 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。 |
| 支持在管理界面提供基础的命令行功能，通过命令行可以进行基础的排障操作。 |
| 虚拟化的管理平台、可以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 |
| 存储虚拟化 | ▲本次项目提供6个物理CPU存储虚拟化管理授权，要求存储虚拟化授权无容量限制。  支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用License激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能。 |
| 采用分布式架构设计，由多台物理服务器组成分布式存储集群，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。 |
| 支持磁盘坏道检测功能，虚拟存储集群可以对数据盘进行坏道检测，发现坏道后可自动从另外一个副本读取数据，并对坏道数据进行修复。 |
| 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。 |
| 支持多副本冗余功能，支持2个或以上副本，副本互斥地保存在集群的不同节点，当1个或多个主机或者磁盘故障，确保数据依旧正常访问。 |
| 支持数据自动重建机制，当主机或者磁盘故障后，自动利用集群内空闲磁盘空间，将故障数据重新恢复，且重建速度最快可达30min/TB以上，快速恢复副本的完整性和冗余度，确保用户数据的可靠性和安全性。 |
| 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。 |
| 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。 |
| 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。 |
| 支持内存读缓存功能，可以利用物理节点的内存作为读缓存，以提高读性能，实现内存、SSD、HDD三级存储分层 |
| 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。 |
| 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。 |
| 支持存储分卷功能，以物理主机为单位划分为不同的存储卷，如高性能卷，大容量卷，全闪存卷等，可使对存储性能和容量要求不同的业务运行在不同的存储卷上。 |
| 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。 |
| 网络虚拟化 | ▲本次项目提供6个物理CPU服务器虚拟化管理授权 |
| 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。 |
| 提供虚拟机报表功能，可以导出TOPN的虚拟机进行1年以内的性能分析与趋势分析报表。 |
| 分布式防火墙能够基于虚拟机进行3-4层安全防护，以虚拟机为单位的安全策略部署，即使改变虚拟机的IP地址信息，安全策略依然生效。 |
| 分布式防火墙提供实时拦截日志显示，以及支持“数据直通ByPass”功能，方便出现问题快速定位问题。 |
| 通过License激活的方式，实现网络虚拟化功能（支持分布式虚拟交换机、虚拟路由器、虚拟应用防火墙、虚拟化运维堡垒机等功能），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。 |
| 虚拟路由器支持HA功能，当虚拟路由器运行的主机出现故障时，可以实现故障自动恢复，保障业务的高可靠性 |
| 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 |
| 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 |
| 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，并且能够排查到acl策略配置错误等层面，方便快速排查问题保障业务的高连续性； |
| 提供一套持续数据保护CDP软件模块，至少配置5个虚拟机数据保护授权（可按需扩展授权数量），实现和核心业务的数据保护，持续数据保护CDP软件模块需采用无代理的方案，避免对虚拟机的稳定性和性能产生影响。 |

|  |  |
| --- | --- |
| **可信API代理设备（TIP）（1台）** | |
| **指标项** | **技术规格要求** |
| 基本参数 | 冗余电源（支持220V交流及110V-240V直流），CPU：E3-1225v5，内存：8G，1T硬盘,，≥4个万兆光口，≥6个千兆电口， ≥2个扩展槽。支持软件化部署。 |
| 加密吞吐≥5Gbps，最大并发连接数≥50000，RPS≥40000 |
| 标配国密卡，支持SM1、SM2、SM3、SM4国密算法，SM2签名（次/秒）≥12600,SM2验证（次/秒）≥4500,SM2密钥对生成（tps）≥10000，SM1加密/解密≥1Gbps，SM4加密/解密≥4Gbps |
| API资源管理 | 提供了对API名称、API地址、API域名、API方法等应用API资源的统一管理功能 |
| 支持服务名称配置、支持服务地址和服务端口、服务协议配置 |
| 支持访问域名、路径、协议及请求方法配置 |
| API发布管理 | 支持匿名权限发布；支持可信API发布 |
| 根据API业务的重要程度形成可信分并进行授权，提供产品截图 |
| API调用管理 | 提供匿名访问、同步访问、异步回调等多种API调用模式、数据传送方式，提供产品截图。系统具备多核多平台并行安全操作系统，提供计算机软件著作权登记证书 |
| API安全加固 | 支持API调用时间窗口、频率控制，支持API限速，提供产品截图 |
| 支持API调用来源IP ACL控制 |
| 支持API调用熔断机制，提供产品截图 |
| API调用支持请求自定义头字段合法性检测，支持恶意API调用者自动锁定 |
| API动态访问控制 | 具有API动态访问控制功能，提供自主知识产权证明 |
| 与可信访问控制台联动，根据调用环境安全可信分进行动态权限控制，提供产品截图 |
| 三级缓存加速 | 支持三级缓存，提高高频API请求鉴权命中率，提高单机性能。 |
| 支持三级缓存，提高高频API请求命中和转发速率，提高单机性能 |
| 匿名服务 | 支持匿名API业务配置发布及匿名API访问 |
| 可靠性 | 支持3台以上集群部署。 |
| 支持配置统一集群管理中心，管理中心采用APPID、APPKEY进行签名校验。考虑在公安实际环境中运行的稳定性，需提供公安用户3份及以上运行证明文件。 |
| 支持管理消息重复推送，自动执行 |
| 传输安全 | 支持标准TLS1.0/TLS1.1加解密，可禁用SSLv3/v2协议 |
| 支持应用配置HTTP强制转换HTTPS，自动完成HTTP到HTTPS加密服务 |
| 管理TLS加解密算法的强度，自定义RC4-SHA、AES、ADH算法会话协商 |
| 支持国密算法，可选择RSA-SM1-SHA1, RSA-SM4-SHA1, ECC-SM1-SM3, ECC-SM4-SM3算法，提供产品截图 |
| 支持TLS会话自动重协商 |
| 服务器安全防护 | 支持对当前API服务端提供安全防护能力，可对API使用中常见的网络安全攻击进行感知和识别，包括SQL注入，XSS攻击，目录遍历，CC攻击，PHP注入，网站扫描，敏感信息访问，以及异常的访问请求等，提供产品截图 |
| 支持使用黑白名单机制来控制API调用者的访问权限。，提供产品截图 |
| 发现安全攻击时，支持对API请求进行拦截或终止当前会话。，提供产品截图 |
| 日志审计 | 要求拥有高性能的syslog日志处理和存储方法技术，要求提供相关技术文件复印件。提供业务系统前置API详细访问日志、API访问流量统计等信息，并进行日志上报、日志外发，便于实现业务数据的审计、安全风险的分析。  要求设备提供的存储空间支持审计日志本地留存6个月以上，本地磁盘空间无法满足日志容量存储的，要求提供专用的日志存储设备。 |
| 其他要求 | 1、考虑兼容、对接、运维等因素，建议可信代理控制服务能与可信应用接入代理 、可信api代理等产品和组件为同一品牌。 |

|  |  |
| --- | --- |
| **可信应用接入代理设备（TAP）（1台）** | |
| **指标项** | **技术规格要求** |
| 基本参数 | 冗余电源（支持220V交流及110V-240V直流）; ≥1T硬盘;标配≥6个10/100/1000电口，≥4个万兆SFP+光口插槽，≥2个扩展槽。每台TAP支持最大并发用户数≥1000人；TAP支持多台负载； |
| 单向加密吞吐≥1.2Gbps，双向加密吞吐≥2Gbps，最大并发用户数≥1000，每秒新建连接≥7000 |
| 标配国密卡，支持SM1、SM2、SM3、SM4国密算法，SM2签名（次/秒）≥12600,SM2验证（次/秒）≥4500,SM2密钥对生成（tps）≥10000，SM1加密/解密≥1Gbps，SM4加密/解密≥4Gbps |
| 应用资源管理 | 提供对应用名称、应用地址、应用域名、应用协议等应用系统资源的统一管理功能 |
| 支持Web业务登录表单自定义填充 |
| 支持Web业务登出状态自动检测 |
| 支持Web业务URL参数自定义配置 |
| 支持支持外链资源管理及配置 |
| 支持支持动态验证码识别，参数自定义设置及配置，提供产品截图 |
| 应用发布管理 | 支持token传递、消息透传等多种应用发布方式，保证应用系统安全对外发布 |
| 支持令牌传递模式，支持URL、Header、Cookie自定义传递 |
| 支持静态页面接管及定制功能 |
| 应用安全加固 | 支持对用户发起的应用请求的字段的合法性检测功能，提供基于请求内容大小、请求速度、请求的连接数、访问时段进行流量控制，提供基础防爬能力 |
| 支持请求登录/登出URL、参数匹配检测及响应 |
| 支持URL请求、速率、时间段控制 |
| 支持SYN Flood攻击开启，提供产品截图 |
| 应用级动态访问控制 | 具有应用级动态访问控制能力，可进行用户级别的动态访问控制 |
| 支持会话令牌缓存保持，可按小时设置，自动失效 |
| 支持cookie级别的浏览器会话控制，关闭浏览器保持 |
| 支持自动从物理PC获取设备ID，设备ID串安全加密，防伪造 |
| 支持基于风险分的安全策略执行，根据评估结果自动执行放行、阻止、二次认证能力 |
| 考虑兼容、对接、运维等因素，建议可信代理控制服务能与可信应用接入代理 、可信api代理等产品和组件为同一品牌 |
| 传输安全 | 支持标准TLS1.0/TLS1.1加解密，可禁用SSLv3/v2协议 |
| 支持应用配置HTTP强制转换HTTPS，自动完成HTTP到HTTPS加密服务 |
| 管理TLS加解密算法的强度，自定义RC4-SHA、AES、ADH算法会话协商 |
| 支持国密算法，可选择RSA-SM1-SHA1, RSA-SM4-SHA1, ECC-SM1-SM3, ECC-SM4-SM3算法 |
| 支持TLS会话自动重协商 |
| 支持用户登录次数锁定及锁定周期控制 |
| 可靠性 | 支持3台以上集群部署 |
| 支持配置统一集群管理中心，管理中心采用APPID、APPKEY进行签名校验。 |
| 支持管理消息重复推送，自动执行 |
| 应用帐号密码安全 | 支持非对称加密对应用帐号的密码进行安全加解密，密码安全存储、明文不落地 |
| 自动分配公私钥功能，加密帐号密码 |
| 提供公钥导入功能，公私钥分离存放 |
| 解密过程明文不落地，验证签名 |
| 业务零改造 | 提供应用模板，可自定义Header、背景、LOGO、Footer、提示语 |
| 自定义多因子认证项及用户名/密码输入表单，提供产品功能截图 |
| 提供应用适配表单框架，表单元素定位，代填自动触发功能，提供产品功能截图 |
| 日志审计 | 提供终端用户业务访问日志、网络访问流量统计等信息，要求拥有高性能的syslog日志处理和存储方法技术，要求提供相关技术文件复印件。其次能进行日志上报、外发，便于实现业务数据的审计、安全风险的分析。 |

|  |  |
| --- | --- |
| **可信代理控制服务设备（1套）** | |
| **指标项** | **技术规格要求** |
| 基本参数 | 2U机箱;冗余电源（550W）、≥4T硬盘; ≥1 Console口；标配≥4\*千兆电口; ≥4个万兆光口。 |
| 最大并发用户数≥1000，每秒新建连接数≥7000，每秒权限判定数≥3000 |
| 标配国密卡，支持SM1、SM2、SM3、SM4国密算法，SM2签名（次/秒）≥12600,SM2验证（次/秒）≥4500,SM2密钥对生成（tps）≥10000，SM1加密/解密≥1Gbps，SM4加密/解密≥4Gbps |
| 备用设备要求 | ▲为确保系统高可用性和稳定，在5年服务期内，本次项目要求在用户现场提供相同型号的可信代理控制服务备用设备一台，设备产权归原厂商所有。 |
| 可信应用代理集群管理 | 可信应用代理集群的统一管理，统一配置管理维护 |
| 配置管理可信应用代理集群，支持IP、端口、类型，启用/停用配置 |
| 配置管理消息支持自动、手动两种类型分发 |
| 集群消息支持消息签名验证，保障消息传递安全 |
| 消息推送传递失败后，记录状态，支持手动强制同步 |
| 可信API代理集群管理 | 可信应用API代理集群的统一管理，统一配置管理维护 |
| 配置管理可信API代理集群，支持IP、端口、类型，启用/停用配置 |
| 配置管理消息支持自动、手动两种类型分发 |
| 集群消息支持消息签名验证，保障消息传递安全 |
| 消息推送传递失败后，记录状态，支持手动强制同步 |
| OAuth2标准支持 | 支持标准OAuth2，须提供Authorization Code模式 |
| 支持标准OAuth2，提供RestAPI接口服务 |
| 支持标准OAuth2，提供JAVA、PHP、Python、C/C++客户端SDK及Demo |
| OIDC标准支持 | 支持标准OIDC开放身份协议，提供ID\_Token身份令牌服务 |
| 支持标准OIDC开放身份协议，提供RestAPI接口服务 |
| 支持标准OIDC开放身份协议，提供JAVA、PHP、Python、C/C++客户端SDK及Demo |
| XACML标准支持 | 可配置过滤RBAC角色，删减RBAC中不满足属性的权限 |
| 基于属性的扩展授权协议，提供主体、客体授权策略配置 |
| 环境属性配置支持：来源IP、设备系统、系统帐号配置 |
| 可信环境感知：设备可信风险分等级设置 |
| 用户管理 | 提供用户、分组统一管理功能，包括用户信息增删改查用户信息备份导出、状态管理 |
| 单个、批量添加，导入/导出用户及用户组，支持导入导出密码加解密 |
| 支持按组、按用户选择认证服务器 |
| 提供名字、密码、邮箱、电话等属性设置，允许自定义用户属性、扩展字段 |
| 支持强密码校验，首次登录强制修改密码功能 |
| 用户/组可形成1比N归属，支持父组/子组之间继承 |
| 支持用户按认证服务器、组织关系自动分组 |
| 用户状态可设置：允许，锁定、禁止状态控制，支持认证失败次数、属性设定自动锁定用户状态 |
| 资源管理 | 支持API服务/API服务组两级分类资源配置，API组包含API服务列表 |
| 支持API用户、API用户组两级分类资源配置，API用户组支持父组/子组模式 |
| 支持HTTP、HTTPS类WEB应用配置 |
| 配置管理支持密码代填、Token传递、透传模式、代理模式四类WEB应用代理，提供产品功能截图 |
| 支持GET、POST方法设置，支持URLEncoding、JSON、Format格式设置登录格式，支持用户标识URI、用户标识属性提取自定义设置。 |
| 支持SSH、RDP、TELNET、VNC四类运维资源配置管理 |
| 统一提供AppID、访问密钥管理配置，为各类资源提供认证、验签服务接口，提供产品功能截图。 |
| 设备管理 | 提供设备状态、可信风险属性的查询、管理。 |
| 提供终端管理、状态查询功能，可按区域、状态过滤查询 |
| 考虑兼容、对接、运维等因素，建议可信代理控制服务能与可信应用接入代理 、可信api代理等产品和组件为同一品牌。 |
| 授权策略管理 | 支持基于角色的授权策略配置，配置主体、客体角色授权 |
| 支持基于属性的授权策略配置，可为角色授权提供属性条件过滤规则与控制 |
| 提供可信环境风险、用户行为分析、用户环境属性多维度的授权策略统一管理功能 |
| 支持和授权服务联动 | 通过授权服务的应用授权接口、API授权接口、运维授权接口等获取应用、API、运维业务权限列表 |
| 支持权限变更订阅 | 支持订阅授权服务的权限变更服务，以便实时获取最新权限 |
| 授权判定与执行 | 支持为可信应用代理、可信API代理、可信运维代理提供实时的访问权限判定 |
| 代理连接会话管理 | 支持为可信应用代理、可信API代理、可信运维代理提供集中的代理连接会话管理 |
| 用户会话服务 | 提供用户会话自动创建、维护、销毁全生命周期管理 |
| 用户会话状态查询、状态控制功能 |
| 用户会话支持分布式、持久化机制，全局生效，宕机自恢复 |
| 访问令牌服务 | 提供用户令牌、应用令牌、API令牌的申请、颁发、撤销、同步等安全访问控制机制 |
| 支持三级令牌管理：用户、应用、API三级令牌的全生命周期管理 |
| 令牌转换服务：提供OIDC、SAML、OAuch2令牌转换服务 |
| 动态访问控制引擎 | 提供动态策略评估引擎，动态计算用户、行为、风险、环境等安全因子，持续完成用户、设备、应用的可信状态评估 |
| 引擎提供对外RestAPI标准接口，可完成内部、外部授权访问的动态评估 |
| 支持数据库、NoSQL库、策略、设备、用户信息外部资源信息查询 |
| 支持XACML标准、JSON格式，自定义属性、类型引擎决策 |
| 系统具备多核多平台并行安全操作系统。支持硬件或微服务扩展。 |
| 设备属性跨级汇聚 | 支持部、省、市三级的设备属性自动汇聚、上报 |
| 设备可信状态属性自动汇聚 |
| 部级管理可设置、过滤感知部分省、市级风险 |
| 省级管理可设置、过滤感知省级、市级风险 |
| 各级设备可信状态属性可在统一管理平台查询 |
| 可信风险通报 | 风险通报实现将异常信息通报给统一身份与权限管理。异常信息包括：终端异常、违规操作等。支持统一多级式风险感知与通报。 |
| 公安PKI CA证书双向认证 | 支持可信CA导入/导出管理，支持PEM/DER/PCKS7证书格式导入 |
| 支持双向证书认证机制 |
| 提供证书CRL撤销列表、OPCS撤销同步机制 |
| 提供证书过滤、用户/组织关系、用户名+证书多重认证开启功能 |
| RADIUS认证 | 支持监听地址、端口、超时、PAP/CHAP/MS-CHAPv1/MS-CHAPv2协议 |
| 支持NAS配置管理，支持每个NAS配置不同密钥 |
| 支持RADIUS验证多种模式：密码+动态口令、前缀模式、后缀模式、Challenge模式认证 |
| AD认证&LDAP认证 | 支持LDAP认证，支持Client BaseDN设置及认证 |
| 支持LDAP协议的查询、认证指令 |
| 支持Windows IWA统一认证，支持用户通过IWA机制自动认证、免密登录 |
| 其它第三方认证协议 | 支持数据库用户名、密码认证：配置数据库、登录名、表、行列 |
| 支持POP3、SMTP、IMAP三种邮件协议、服务器设置，支持邮件帐号密码认证 |
| 支持HTTP认证：IP、端口、URL、用户、密码及HTTP Response检测认证 |
| 支持短信认证：短信网关设置、单次短信有效时间、发送超时、短信提示模板、验证失败次数配置 |
| 单点登录SSO | 提供单点登录令牌认证服务 |
| 提供SSO共享、不共享配置及策略控制 |
| 支持密码代填、Token验证两类SSO机制 |
| 支持单点登出、登出过程自定义流程控制功能 |
| 可靠性 | 支持3台以上分布式集群。 |
| 统一管理门户，支持用户会话、应用、API多级令牌持久化 |
| 支持统一存储、分布式缓存及状态监控 |
| 支持一键集群自动安装，分布式安装、升级、启停业务 |
| 日志审计 | 要求拥有高性能的syslog日志处理和存储方法技术，要求提供相关技术文件复印件。提供用户登陆日志、用户操作日志、系统运行日志等信息采集、管理及审计，并支持日志服务器上报。  本地存储空间支持审计日志本地留存6个月以上。 |
| 云桌面适配 | 要求支持本次项目云桌面系统联动。 |

|  |  |  |
| --- | --- | --- |
| **虚拟云桌面一体机设备（数量：1套）** | | |
| 招标内容 | **指标项** | **技术规格要求** |
| 资源服务器 | 数量要求 | 要求4台桌面云服务器。 |
| 硬件规格 | CPU Hygon 5280\*2，256G内存， 2\*960 SSD，6\*4T SATA 盘，12盘位，2\*240G系统盘，6个GE接口，2个万兆光口，冗余电源。 |
| 虚拟化软件 | 部署模式 | 提供相关服务器虚拟化与存储虚拟化标准版授权，本项目要求所提供的存储虚拟化授权无容量限制，满足桌面云数据存储空间的扩容需求。  兼容市场上主流x86服务器和存储设备，支持品牌不局限于联想、浪潮，深信服等。无需部署集中管理平台，通过Web方式接入集群主服务器，实现对服务器、虚拟机、网络、存储等进行统一管理。 |
| 部署存储虚拟化之后，可以将服务器直连硬盘组成分布式共享数据存储，构建桌面云提供低成本、高性能的存储方案。要求存储虚拟化和服务器虚拟化采用统一的Web界面进行管理，简化运维。 |
| 功能支持 | 支持服务器端口汇聚技术（管理口、业务口、存储口），将多个网络端口聚合起来，提高网络带宽和容错能力。 |
| 支持集群冗余技术，集群中各主机互为监控，一旦发现某个主机故障，HA机制就会自动触发虚机迁移动作，在另一正常服务器快速拉起、确保VM继续可用。 |
| 支持SSD缓存加速，采用SSD+HDD混合模式，SSD用于缓存热点数据，HDD用于存储个人数据，SSD缓存命中率不低于60%，确保最优用户体验。支持虚拟机集中备份与恢复，可按需选择多个虚拟机或全部虚拟机备份至外置服务器，并可设置备份策略，实现自动化备份。 |
| 支持内存页合并技术，能够有效消除多个虚拟机运行过程中重复只读内存数据，以节省内存使用，提升服务器部署密度。 |
| 支持数据冗余副本技术，每份数据同时写入多台服务器，每次数据变化时自动实时同步，确保磁盘或服务器故障，数据不丢失。 |
| 当磁盘或服务器故障后，桌面业务不中断， IT人员只需要更换新设备，整个数据重建/恢复过程，无需关停机。 |
| 支持全局热备盘技术，管理员可配置在集群中保留多块磁盘作为热备盘，分布在不同主机上，当任何一台主机的任意一块硬盘出现故障后，会自动选择其中1块热备盘进行替换和重建。为满足云桌面扩容需求，要求支持横向/纵向存储扩展，通过新增磁盘或服务器数量，实现桌面云存储空间及性能的扩展。 |
| 桌面云管控系统与云桌面并发用户授权 | 配置要求 | 为了满足不同场景的应用需求，要求每用户授权支持发布个性化桌面、共享式桌面、虚拟应用3种资源类型。本项目提供云桌面功能软件授权，与云桌面管控系统、云桌面服务器虚拟化软件为同一品牌，要求与我局原有桌面云系统组统一集群，统一管理兼容我局现有桌面云控制系统。本次提供100桌面云用户授权。 |
| 用户体验 | 支持WindowsXP、Windows7、Windows10、Windows Server等多种云桌面操作系统,并且支持两种以上的Linux虚拟桌面操作系统，其中要包含国产Linux操作系统，如中标麒麟，银河麒麟。 |
| 云桌面系统要求兼容后续建设的可信代理控制服务系统，配合实现与可信代理控制服务系统联动。 |
| 支持Windows 10优化工具，关闭和禁用不需要的服务、启动项和视觉特效，让桌面运行更流畅。 |
| 支持接入虚拟机时显示开机画面，同时支持在虚拟机上更改分辨率（在桌面右键点击“个性化分辨率”进行设置），保持与普通PC一样的使用方式。 |
| PC（或笔记本）接入虚拟桌面支持通过导航条或快捷键切换为窗口化模式，用户可随意改变窗口大小且分辨率会自动适应。 |
| 支持远程协助功能，管理员在云桌面控制台中可以直接向需要协助的用户发起远程协助，用户桌面无需安装任何辅助软件。 |
| 支持联动关机技术，可以跟使用PC一样，打开操作系统“开始”菜单、点击“关机”按钮，桌面云终端和操作系统将会一体化关闭，没有多余的操作步骤。 |
| 支持视频重定向，包括Media Player、暴风影音等多种本地播放器，以及优酷、土豆、腾讯等多种在线视频网站，要求播放1080P高清视频时，桌面CPU利用率不高于15%。  支持USB外设映射，兼容高拍仪、扫描枪、扫描仪、摄像头、密码小键盘、指纹收集器、身份证读卡器、手写板、打印机、USB-key等不同外设。 |
| 为保证桌面云系统兼容北信源(一机两用)软件，要求桌面云厂家提供和北信源一机两用的兼容性认证报告。 |
| 支持云桌面导航条显示网络状态，支持导航条显示当前终端（瘦终端、PC客户端）与云桌面控制台之间的网络状态，网络状态会以不同的信号格数显示，用户可以实时查看网络状态和时延，当网络状态不佳时在后台进行日志记录，方便管理员进行网络状态查询和维护。 |
| 支持自助快照恢复，当用户自己误操作导致云桌面卡慢、蓝屏、死机或者中病毒的时候，用户通过导航条按钮，可以自助进行系统盘快照还原操作，支持安卓瘦终端、PC客户端。 |
| 客户端连接虚拟桌面无需依赖虚拟机IP，在虚拟机网卡被禁用或被更改IP的情况下，云桌面业务不会中断，这样可以防止因误操作而导致连接中断。 |
| 运维功能 | 支持虚拟机自由分组、支持修改计算机名称、支持根据虚拟机名称、关联用户、用户描述、IP、MAC、所属资源、所属平台等信息搜索虚拟机。 |
| 支持为运行中的云桌面虚拟机进行分组管理和批量设置IP，提升IT人员桌面维护效率。 |
| 支持模板克隆技术，克隆时可指定虚拟机数量、运行位置、存储位置、网口信息、磁盘大小，本项目要求100个虚拟机派时间不超过5分钟。 |
| 支持设置虚拟机开关机计划，一方面可避免并发开机IO风暴问题，另一方面可释放服务器资源。 |
| 支持软件分发，通过创建软件库并关联给虚拟机，实现应用软件、驱动程序的增量式更新，不需要在每个虚拟机执行安装过程，整个分发过程秒级完成，且分发后不会覆盖原虚拟机的个性化配置和自主安装的软件，本项目要求支持应用软件、USB打印机和网络打印机驱动、网页快捷方式和页面控件、办公文件的分发。 |
| 支持为云桌面设置还原模式，在操作系统重启后，除个人数据之外其他内容均还原为初始状态，始终为用户呈现干净可用的桌面环境，降低系统故障率。 |
| 支持外置数据中心报表功能，能够查询一段时间的并发用户会话、用户使用时长、服务器负载情况、存储利用率、存储性能情况等。支持报表导出。 |
| 支持AD域离线认证，在AD域服务器故障离线后，用户依然可以用AD账号认证登录桌面云。 |
| 支持集中分配个人磁盘，并可以指定磁盘空间大小，在空间不足时还可以为用户新增个人磁盘，以满足用户文档存储需求。 |
| 支持控制器、服务器等组件故障后，通过邮件等方式告警。支持管理员给在线用户推送消息和通知，管理员可以根据需求发给指定用户或者发给所有用户。 |
| 要求支持快照技术，当系统故障时可实现故障回滚；同时支持增量保存快照数据，以节省存储空间。 |
| 安全管理 | 支持多种身份认证方式随需组合，至少应包括账号密码、usb-key认证、短信认证、硬件特征绑定、动态口令等5种方式，支持设置首次登录强制修改密码、定时修改密码、图形校验码和软键盘等密码安全策略，以保障认证密码安全性，避免越权访问行为。 |
| 支持在管理组件中内置应用管控技术，实现全方位云桌面管控，在禁止名单中可以通过配置规则禁止指定应用或进程在云桌面中运行，提供功能截图；在允许名单中通过配置规则只允许规则中的应用或进程在云桌面中运行。 |
| 支持客户端安全检测，可根据用户接入的终端类型、操作系统版本、接入IP和时间、软件安装情况等指定访问策略，如客户端不满足安全检测要求则不允许接入，有效保障接入安全性。 |
| 支持文件导出内容审计，开启文件安全导出后，虚拟机通过剪切板、PC设备和USB设备外发文件的操作将被禁止，用户可以使用虚拟机内部的文件导出工具实现文件外发，所有外发的文件内容都可以加密备份到数据中心，以备后续审计使用，可疑的导出行为会产生告警。 |
| 支持USB黑白名单技术，能够精准识别每一款不同类型的外设（包括高拍仪、摄像头、USB光驱、认证key等），并设置放通或者限制策略，提高管控粒度和安全性。 |
| 支持临时权限，管理员为部分用户临时在某个时间段内放通usb和pc剪切板等权限，并在到期后自动回收该权限，保证数据安全。支持用户终端与云桌面平台之间采用VPN隧道传输，实现数据加密，保障外网接入安全。 |
| 要求支持个人盘加密技术，对云桌面个人数据进行加密保存，保障个人隐私安全。 |
| 桌面云控制器内置防火墙，包括设置过滤规则、NAT设置、访问监控、防DOS攻击、QOS上传下载规则等。 |

## 4.1.3现有数据中心安全体系完善

|  |  |
| --- | --- |
| 日志采集和存储设备（1台） | |
| **指标项** | **技术规格要求** |
| 硬件规格 | 标准1U机架，要求配置≥6个10/100/1000M Base-T电口(RJ45)（1个管理口，5个侦听口），另有2个端口扩展槽位，支持万兆光纤插槽，1个Console口 。 |
| 自带存储 | 内置存储总容量≥4TB，支持外接存储设备。产品要求支持SOC产品的硬盘减震技术 |
| 日志审计  性能要求 | 事件采集性能：峰值可达到10000EPS  事件分析性能：每秒实时关联分析3000EPS  事件入库性能：峰值可达到10000EPS |
| 使用模式 | 界面100%都是B/S模式，无需安装客户端，WEB浏览器访问管理中心，浏览器端无需安装Java运行环境。支持chrome浏览。 |
| 管理范围 | 能够对IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计，最大支持 1000个日志源事件采集。 |
| 审计对象 | 支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防DDOS攻击，Web应用防火墙、等）配置日志、运行日志、告警日志等；  支持审计各种主机操作系统（包括Windows,Solaris, Linux, AIX, HP-UX,UNIX,AS400）配置日志、运行日志、告警日志等；  支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等；  支持审计各种中间件（tomcat、apache、webshpere、 weblogic等）配置日志、运行日志、告警日志等；  支持各种应用各种应用系统（邮件，Web，FTP，Telnet、等）配置日志、运行日志、告警日志等；  以及用户自己的业务系统的日志、事件、告警等安全信息进行全面的审计。 |
| 资产管理 | 按照设备资产重要程度和管理域的方式组织设备资产，提供便捷的添加、修改、删除、查询与统计功能；  支持资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需设备资产的信息，并对资产进行关键度赋值；  支持自定义资产属性；  支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。 |
| 日志归一化 | 支持采集一化后的日志和保留原始日志，方便用户对关键日志快速定位，和事后取证；系统具备一种大规模事件处理的规则群组系统及处理方法技术，为避免虚假应标  日志收集后进行字段和安全等级的归一化处理，系统归一化字段不少于50个字段,并至少有8个可自定义字段。  系统提供灵活简单的归一化方式,对系统新增的日志类型只需修改配置文件即可支持,不需修改系统程序。 |
| 实时监视 | 支持实时的日志滚动显示，可通过雷达图等直观显示目前日志量和日志详细信息。  支持对实时展示的字段进行选择，调整字段顺序，修改显示字段别名。  双击单条日志显示详细信息，支持左右布局和上下布局。  支持自定义实时监视场景，提供可视化规则编辑视图，对关注的事件进行实时展示。  支持鼠标放在日志对应字段上界面可悬浮提示资产信息和常用端口信息。 |
| 实时分析 | 可对收集的日志进行分类实时分析和统计，从而快速识别安全事故；  分析统计结果支持柱图、饼图、曲线图等形式并自动实时刷新，图表数据支持数据下钻；  支持统计分析的时长设定，分析结果支持导出报表PDF，HTML，RTF,XLS,PNG,DOCX,XLSX；  支持自定义实时分析场景，提供可视化规则编辑视图，根据实际业务编写分析规则；  用户在实时监视的过程中如果发现某条事件的相关属性需要持续予以关注，可以将该事件分配到黑白名单中；  支持对于关联事件进行追溯，查看导致该关联事件的所有原始事件。 |
| 报表管理 | 提供丰富的报表管理功能，根据时间、数据类型等生成报表，提供打印、导出以及邮件送达等服务；直观地为管理员提供决策和分析的数据基础，帮助管理员掌握网络及业务系统的状况。报表可以保存为html，excel，文本，pdf等多种格式。  提供自定义报表，用户可根据自身需要进行定制。报表可根据设置自动运行,调度生成日报、周报和月报。 |
| 备份归档 | 支持按周期的方式选择备份，支持原始日志与分析后日志分离，支持历史日志恢复导入；  当磁盘空间日志存储量达到一定百分比时可设定为删除磁盘中的历史日志或接收的日志不再入库，并进行告警； |

|  |  |
| --- | --- |
| **数据库审计（数量：1台）** | |
| **指标项** | **技术规格要求** |
| 硬件规格 | 接口配置 6个千兆电口，硬盘存储>=4TB，内存>=8GB ，单电源，可支持1个扩展插槽，支持液晶屏，峰值事件处理能力不低于12000条语句/秒，日志存储最低5亿条 |
| 部署方式 | 可通过端口镜像（SPAN）或者分流器（TAP）模式旁路部署或Agent插件方式部署。 |
| 审计功能 | 支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用Gbase、Caché、REDIS；  支持旁路阻断功能（非串联方式）。阻断两种模式，宽松模式：对单一会话危险操作阻断；严格模式：源IP操作的所有请求直接阻断；  支持端口重定向审计，在服务器端口变化动态协商为其他端口时同样能精确审计；  支持白名单管理，根据白名单（条件为IP/MAC/数据库账户/审计对象/操作语句）定义规则进行应用层过滤；  可监控发现未知仿冒进程工具访问数据库，如通过非法第三方工具连接数据库进行风险操作的行为；可监控权限滥用行为，对超出用户权限范围的操作，可根据IP、MAC等五元组实时监控；  支持对SQL注入、跨脚本攻击、grant语句进行提权行为的审计，支持数据库嵌套、函数、脚本访问以及返回内容等审计；绑定变量：可审计通过隐藏用户名的绑定变量，动静态变量方式访问数据库，如：Varchar、Nvar char、int、short int、tinyint、bigint、float、guid、datetime、datetime2、image、Nvar char等；  支持B/S架构Http应用三层审计，可提取包括应用系统的人员工号（账号）的身份信息，精确定位到人，并可获取XML返回结果。支持C/S架构COM、COM+、DCOM组件的三层审计，可提取应用层工号（账号）的身份信息，精确定位到人；支持框架：tomcat、apache、weblogic、jboss；  全面支持后关系型数据库Cache的审计，包括terminal、portal、studio、Sqlmanager、MedTrak等工具访问的审计，Portal可审计Sql语句、查询Global变量以及二者的返回内容，Terminal可审计M语句及返回内容，MedTrak可审计工号、操作报表以及二者的返回内容，studio可审计到编译、代码更改等操作，Sqlmanager可审计数据库账号和操作的sql语句。 |
| 审计策略 | 审计策略支持18种以上分项响应条件；可支持数据库操作命令（包括select、create等14个命令）；语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、应用账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端MAC、客户端IP、客户端端口、客户端进程名、会话ID、关键字、时间（含开始结束日期）等；  支持重复操作的统计规则，一定时间内重复某项操作达到设定的统计次数，则触发审计告警。 |
| 审计查询 | 支持全数据库检索，检索效率高达亿条数据秒级响应；  可根据包括时间范围、风险级别、保护对象、操作类型、进程名、应用账号、关键字、规则类型、规则名、规则组名、操作系统主机名、操作系统用户名、客户端MAC、客户端端口、服务器端口、数据库名、语句长度、语句回应、语句执行时间、返回行数、返回结果、处理状态、会话ID、记录编号等二十种条件进行精细化查询。 |
| 风险评估 | 支持对指定时间段风险数据按不同维度进行统计排行，统计维度包括:风险最多的类型、触发风险最多的保护对象、触发风险最多的IP、触发风险最多数据库账户、触发风险最多应用账户、触发风险最多工具。 |
| 实时监控 | 提供用户界面告警、Syslog告警、SNMP告警、邮件告警、短信系统、短信猫告警等六种方式；  可实时监控检索模块、解析模块、规则模块、消息中心和入库模块是否正常工作，方便系统维护；  可实时监控系统解析速率、匹配速率、入库速率和当前的会话个数的具体数值。 |
| 系统管理与防护 | 用户管理支持三权分立，系统提供了审计管理员、系统管理员、安全管理员分权的用户体系；  备份数据支持弹性180天的时间，可上传至FTP服务器，或者其他网络转存方式备份日志信息；  系统本身具备访问防火墙，对于系统的异常访问可对账号进行强制下线管理，能有效防范非法IP地址、防范暴力破解登录用户密码（能够对连续失败登陆进行自动锁定，锁定时间可设置）、设置系统黑白名单等安全功能。 |

## 4.1.4视频专网数据中心安全体系完善：

|  |  |
| --- | --- |
| **下一代防火墙设备（3台）** | |
| **指标项** | **技术规格要求** |
| 性能规格 | 标准机架设备,冗余电源。 |
| 至少满足≥8个千兆电口，≥4个万兆光口（含光模块），防火墙本地日志存储空间>=1Tb。 |
| 整机吞吐量≥80Gbps，并发连接数≥900万，每秒新建连接数≥100万。 |
| 基础组网和网络适应能力 | 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式； |
| 支持支持通过802.3ad协议、轮询、热备等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余。 |
| 所投产品必须支持全面的NAT转换配置，包括包括一对一，一对多，多对一的源、目的地址转换 |
| 支持DNS透明代理 |
| 支持双机热备和双机负载均衡功能。支持标准VRRP协议，支持路由、透明模式下“主-备”、“主-主”方式部署，设备支持一种多防火墙的负载均衡方法及装置的技术。 |
| 支持基于权重的路由负载均衡，算法支持：源地址目的地址哈希、轮询、源地址哈希、目的地址哈希、源地址轮询、备份、随机、流量均衡、最优链路带宽负载、最优链路带宽备份、时延负载、跳数负载 |
| 支持静态路由，支持策略路由，支持对称路由；支持ISP路由，并支持手动导入；支持动态路由协议RIPv1/v2、OSPF、BGP |
| 要求防火墙支持IPSEC VPN、SSL VPN、PPTP功能。IPSec VPN隧道≥500 |
| 所投产品可直观展示不同风险等级的应用在1天（24小时）或一周（7天）内传输流量的绝对数值及占全网流量的百分比。 |
| 支持IPv6地址配置，支持IPV6手动及自动的IP/MAC探测及绑定，支持IPV6的本地认证；支持IPV6下静态路由及策略路由 |
| 访问控制功能 | 支持基于源目的IP地址、源目的安全域、VLAN ID、MAC地址、时间、用户、地理区域、服务协议及应用等多种方式进行访问控制； |
| 支持一条访问控制策略同时对端口和协议进行管控。 |
| 支持通过一条安全策略配置应用控制、入侵防护、URL过滤、病毒检测、内容过滤、网络行为管理等高级访问控制功能，且无需编辑即可直观审计策略配置。 |
| 能实现对rdp、ssh、telnet、vnc、pcanywhere等各类远程访问控制协议的识别和阻断，要求支持的远程访问控制协议种类在35种以上，。并支持对特定IP的开启例外功能。  能实现对主要种类数据库协议的识别和阻断，要求支持的协议种类超过9种，。并支持对特定IP的开启例外功能。 |
| 标准SNMP协议支持 | 要求提供标准SNMP协议支持，允许第三方网管软件对防火墙的CPU、内存、网络流量等性能、可用性等进行监测。 |
| 病毒防护 | 提供病毒查杀和防护功能模块，能够HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；支持对压缩文件进行解压查杀； |
| 支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀 |
| 病毒库不少于600万种病毒特征，支持病毒库扩充，支持添加特定病毒种类特征。支持病毒云查杀功能。要求提供病毒库来源和名称病毒库，建议以目前国内流行病毒为主。 |
| 应用识别和行为管理 | 所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输方式等特征分类 |
| 支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤 |
| 入侵防御 | IPS特征库不少于3000条特征值。 |
| 所投产品的漏洞防护特征库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息； |
| 支持对拒绝服务、缓冲区溢出、恶意扫描、木马后门、病毒蠕虫、僵尸网络、跨站脚本、SQL注入、WEB攻击等的防御，具备针对DNS、FTP、ICMP、IMAP、SQL、NNTP、POP、SMTP、SNMP等协议类型的入侵检测与防御 |
| 支持对应用层 Flood攻击进行五种处理动作：警告、阻断、普通防护、增强防护及授权服务器防护 ；支持局域网广播防护，支持全局配置的局域网广播防护及基于二层接口的局域网广播防护，可以防止局域网内广播和多播数据包泛滥，保障网络正常通信 |
| 支持基于防护类型及防护级别的预定义IPS模板；基于行业类型特点的预定义URL模板 |
| 内容过滤 | 实现HTTP、FTP、POP3、SMTP、IMAP五种应用协议的双向内容过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义，支持阻断及日志两种处理动作； |
| 安全事件分析和异常感知 | 支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破、存在安全风险的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息 |
| 所投设备必须提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素为过滤条件进行数据钻取 |
| 支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为 |
| 所投设备提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL过滤、文件过滤等安全模块检查的日志集中显示 |
| 策略与处置 | 所投设备可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项 |
| 所投产品支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括1天、7天、30天、90天、永久等； |
| 所投产品支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果 |
| 运维管理 | 所投产品支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件 |
| 所投产品必须支持加密的WebUI和CLI管理，且支持网页命令行管理（WebUI中内嵌CLI管理界面） |
| 所投产品支持将告警信息以SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、CPU利用率、内存利用率、硬盘利用率、接口带宽利用率等； |
| 威胁感知  系统联动同 | 所投产品支持与网络威胁感知系统联动，将本地终端产生的异常行为、攻击活动等数据上报至网络威胁感知系统，网络威胁感知系统可实时监控网络内的攻击事件并预警可疑的受感染主机，同时支持接收来自网络威胁感知系统推送的情报信息。 |
| 终端安全软件联动 | 所投产品支持与桌面杀毒或终端管理软件联动，实现基于终端健康状态的访问控制；增强防火墙对木马特征的识别能力 |
| 用户登陆认证 | 支持基于web的无客户端方式用户登陆认证；管理页面登陆支持客户端IP地址限定。 |
| 产品要求 | 所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（万兆三级），或防火墙（万兆增强级）销售许可证。 |
| 要求防火墙产品支持IPv6 |
|  |  |
| **日志审计配套服务器（1台）** | |
| **指标项** | **技术规格要求** |
| 硬件规格 | Xeon E5 2.0GHz 以上CPU，≥16G内存，千兆网口≥2个、硬盘≥6\*8TB硬盘,≥800个日志源接入授权 |
| 日志审计  性能要求 | 事件采集性能：峰值可达到10000EPS  事件分析性能：每秒实时关联分析3000EPS  事件入库性能：峰值可达到10000EPS |
| 使用模式 | 界面100%都是B/S模式，无需安装客户端，WEB浏览器访问管理中心，浏览器端无需安装Java运行环境。支持chrome浏览。 |
| 管理范围 | 能够对IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计，最大支持 1000个日志源事件采集。 |
| 审计对象 | 支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防DDOS攻击，Web应用防火墙、等）配置日志、运行日志、告警日志等；  支持审计各种主机操作系统（包括Windows,Solaris, Linux, AIX, HP-UX,UNIX,AS400）配置日志、运行日志、告警日志等；  支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等；  支持审计各种中间件（tomcat、apache、webshpere、 weblogic等）配置日志、运行日志、告警日志等；  支持各种应用各种应用系统（邮件，Web，FTP，Telnet、等）配置日志、运行日志、告警日志等；  以及用户自己的业务系统的日志、事件、告警等安全信息进行全面的审计。 |
| 资产管理 | 按照设备资产重要程度和管理域的方式组织设备资产，提供便捷的添加、修改、删除、查询与统计功能；  支持资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需设备资产的信息，并对资产进行关键度赋值；  支持自定义资产属性；  支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。 |
| 日志归一化 | 支持采集一化后的日志和保留原始日志，方便用户对关键日志快速定位，和事后取证；系统具备一种大规模事件处理的规则群组系统及处理方法技术，为避免虚假应标，投标时要求提供国家知识产权局出具的相关证明文件复印件或检测报告。  日志收集后进行字段和安全等级的归一化处理，系统归一化字段不少于50个字段,并至少有8个可自定义字段。  系统提供灵活简单的归一化方式,对系统新增的日志类型只需修改配置文件即可支持,不需修改系统程序。 |
| 实时监视 | 支持实时的日志滚动显示，可通过雷达图等直观显示目前日志量和日志详细信息。  支持对实时展示的字段进行选择，调整字段顺序，修改显示字段别名。  双击单条日志显示详细信息，支持左右布局和上下布局。  支持自定义实时监视场景，提供可视化规则编辑视图，对关注的事件进行实时展示。  支持鼠标放在日志对应字段上界面可悬浮提示资产信息和常用端口信息。 |
| 实时分析 | 可对收集的日志进行分类实时分析和统计，从而快速识别安全事故；  分析统计结果支持柱图、饼图、曲线图等形式并自动实时刷新，图表数据支持数据下钻；  支持统计分析的时长设定，分析结果支持导出报表PDF，HTML，RTF,XLS,PNG,DOCX,XLSX；  支持自定义实时分析场景，提供可视化规则编辑视图，根据实际业务编写分析规则；  用户在实时监视的过程中如果发现某条事件的相关属性需要持续予以关注，可以将该事件分配到黑白名单中；  支持对于关联事件进行追溯，查看导致该关联事件的所有原始事件。 |
| 报表管理 | 提供丰富的报表管理功能，根据时间、数据类型等生成报表，提供打印、导出以及邮件送达等服务；直观地为管理员提供决策和分析的数据基础，帮助管理员掌握网络及业务系统的状况。报表可以保存为html，excel，文本，pdf等多种格式。  提供自定义报表，用户可根据自身需要进行定制。报表可根据设置自动运行,调度生成日报、周报和月报。 |
| 备份归档 | 支持按周期的方式选择备份，支持原始日志与分析后日志分离，支持历史日志恢复导入；  当磁盘空间日志存储量达到一定百分比时可设定为删除磁盘中的历史日志或接收的日志不再入库，并进行告警； |

|  |  |
| --- | --- |
| **数据库审计（数量：1台）** | |
| **指标项** | **技术规格要求** |
| 硬件规格 | 接口配置 6个千兆电口，硬盘存储>=4TB，内存>=8GB ，单电源，可支持1个扩展插槽，支持液晶屏，峰值事件处理能力不低于12000条语句/秒，日志存储最低5亿条 |
| 部署方式 | 可通过端口镜像（SPAN）或者分流器（TAP）模式旁路部署或Agent插件方式部署。 |
| 审计功能 | 支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用Gbase、Caché、REDIS；  支持旁路阻断功能（非串联方式）。阻断两种模式，宽松模式：对单一会话危险操作阻断；严格模式：源IP操作的所有请求直接阻断；  支持端口重定向审计，在服务器端口变化动态协商为其他端口时同样能精确审计；  支持白名单管理，根据白名单（条件为IP/MAC/数据库账户/审计对象/操作语句）定义规则进行应用层过滤；  可监控发现未知仿冒进程工具访问数据库，如通过非法第三方工具连接数据库进行风险操作的行为；可监控权限滥用行为，对超出用户权限范围的操作，可根据IP、MAC等五元组实时监控；  支持对SQL注入、跨脚本攻击、grant语句进行提权行为的审计，支持数据库嵌套、函数、脚本访问以及返回内容等审计；绑定变量：可审计通过隐藏用户名的绑定变量，动静态变量方式访问数据库，如：Varchar、Nvar char、int、short int、tinyint、bigint、float、guid、datetime、datetime2、image、Nvar char等；  支持B/S架构Http应用三层审计，可提取包括应用系统的人员工号（账号）的身份信息，精确定位到人，并可获取XML返回结果。支持C/S架构COM、COM+、DCOM组件的三层审计，可提取应用层工号（账号）的身份信息，精确定位到人；支持框架：tomcat、apache、weblogic、jboss；  全面支持后关系型数据库Cache的审计，包括terminal、portal、studio、Sqlmanager、MedTrak等工具访问的审计，Portal可审计Sql语句、查询Global变量以及二者的返回内容，Terminal可审计M语句及返回内容，MedTrak可审计工号、操作报表以及二者的返回内容，studio可审计到编译、代码更改等操作，Sqlmanager可审计数据库账号和操作的sql语句。 |
| 审计策略 | 审计策略支持18种以上分项响应条件；可支持数据库操作命令（包括select、create等14个命令）；语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、应用账户、服务器端口、客户端操作系统主机名、客户端操作系统用户名、客户端MAC、客户端IP、客户端端口、客户端进程名、会话ID、关键字、时间（含开始结束日期）等；  支持重复操作的统计规则，一定时间内重复某项操作达到设定的统计次数，则触发审计告警。 |
| 审计查询 | 支持全数据库检索，检索效率高达亿条数据秒级响应；  可根据包括时间范围、风险级别、保护对象、操作类型、进程名、应用账号、关键字、规则类型、规则名、规则组名、操作系统主机名、操作系统用户名、客户端MAC、客户端端口、服务器端口、数据库名、语句长度、语句回应、语句执行时间、返回行数、返回结果、处理状态、会话ID、记录编号等二十种条件进行精细化查询。 |
| 风险评估 | 支持对指定时间段风险数据按不同维度进行统计排行，统计维度包括:风险最多的类型、触发风险最多的保护对象、触发风险最多的IP、触发风险最多数据库账户、触发风险最多应用账户、触发风险最多工具。 |
| 实时监控 | 提供用户界面告警、Syslog告警、SNMP告警、邮件告警、短信系统、短信猫告警等六种方式；  可实时监控检索模块、解析模块、规则模块、消息中心和入库模块是否正常工作，方便系统维护；  可实时监控系统解析速率、匹配速率、入库速率和当前的会话个数的具体数值。 |
| 系统管理与防护 | 用户管理支持三权分立，系统提供了审计管理员、系统管理员、安全管理员分权的用户体系；  备份数据支持弹性180天的时间，可上传至FTP服务器，或者其他网络转存方式备份日志信息；  系统本身具备访问防火墙，对于系统的异常访问可对账号进行强制下线管理，能有效防范非法IP地址、防范暴力破解登录用户密码（能够对连续失败登陆进行自动锁定，锁定时间可设置）、设置系统黑白名单等安全功能。 |
|  |  |
| **堡垒主机（数量：1台）** | |
| **指标项** | **技术规格要求** |
| 硬件规格 | 2 U设备，采用专用硬件平台和安全操作系统， 软硬件一体化；  提供6个千兆电口，支持2个可扩展插槽，内置≥4 T硬盘，冗余电源；  支持液晶屏显示：接口IP，以及CPU、内存、硬盘的使用率等；  图形会话并发连接数≥150；  字符会话并发连接数≥400；  配置≥500个运维资源授权许可。 |
| 部署方式 | 支持物理旁路，逻辑串联模式，不影响原有网络架构；  支持HA双机热备、支持跨地域、跨数据中心，多层次部署 |
| 资源管理 | 支持SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin等协议；  支持Linux/Unix、Windows、H3C、Huawei、Cisco等系统；  支持图形、字符，混合协议下的批量登录；  通过应用发布实现对MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client、Radmin、dbisql等应用程序/客户端的扩展支持；  支持云主机资源批量添加，包括阿里云、百度云、华为云、腾讯云、Ucloud、AWS、Azure云平台的资源；  不限操作客户端系统类型，无需安装任何客户端插件，使用H5即可直接运维windows、Linux、网络设备等资源（提供相关功能的界面截图）；  支持以云盘形式在堡垒机上存储常用文件，实现操作端、堡垒机、目标服务器三者之间文件共享并进行审计 |
| 用户管理 | 支持本地、RADIUS和AD域等认证方式；  支持动态令牌、USBKEY、手机令牌、手机短信等多因子认证；  支持按IP黑白名单、访问时间段限制用户访问堡垒机；  支持按功能模块自定义角色权限，便于管理。 |
| 访问控制 | 支持按用户、账户组设置多对多的资源访问授权，用户组和账户组内的新增成员自动继承授权关系；  预制Linux主机和网络设备的基本命令，支持正则表达式和通配符方式设置匹配规则，自定义命令黑白名单；  支持对MySQL和Oracle数据库的访问操作控制，可基于库、表、命令实现对数据库操作的细粒度访问控制。 |
| 操作记录 | 支持用户水印功能，避免数据泄露无法追责；  支持对运维操作中的详细操作命令、步骤、以及双人授权、协同用户、剪切板拷贝行为进行记录，并可以通过关键字搜索定位回放，审计日志内容支持导出；  系统内置多种运维、系统报表模板，支持按日、周、月为周期，自动生成Word、HTML、Excel和PDF格式报表；  支持数据库命令级审计，数据库支持类型包括：DB2、MySQL、Oracle、SQL Server等；  支持以图形、字符方式双重审计，完整详细还原操作记录。 |
| 访问和命令控制 | 支持访问控制策略，可配双人授权，针对核心设备需要管理员现场审批才能操作；  预制Linux主机和网络设备的基本命令，支持正则表达式和通配符方式设置匹配规则，自定义命令黑白名单；  支持对MySQL和Oracle数据库的访问操作控制，可基于库、表、命令实现对数据库操作的细粒度访问控制。 |
| 系统设置 | 支持登录失败次数锁死设置 ；  支持内置OpenVPN客户端、实现异地资源管理；  支持网盘功能，可以自定义网盘总空间和每用户使用空间；  支持自定义系统事件的告警等级及方式，例如邮件、手机短信（内置短信网关）通知及Syslog日志外发；  支持web和SSH登录无操作超时设置；  支绑定堡垒机用户公钥，实现客户端访问堡垒机免密码登录持；  支持查看用户所属角色的权限范围，包含系统登录日志、系统操作日志和资源登录日志；  支持页面展示系统负载、内核、内存、网卡、路由表、ARP信息、磁盘使用信息等状态信息  支持web页面上ping、traceroute、telnet诊断工具；  支持web页面上修改对外提供服务的端口； |
|  |  |

## 4.2安全服务

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 大类 | 序号 | 产品名 | 服务内容 | 软硬件 | 服务年限 |
| 视频网 | 1 | 网络准入控制服务 | 网络准入控制：根据实际需求，可选择在重点部位部署安全准入设备，建立重点、敏感前端安全管控机制。根据网络环境，支持多种形式的安全准入手段，如：PC客户端注册模式、网络摄像机（IPC）协议识别或指纹识别模式，其他哑终端的IP、MAC绑定模式等，并对合法设备纳入资产库，对非法设备进行告警和阻断，避免非摄像机资源、非授权PC设备及非法终端资源连入公安视频专网。提供对公安视频专网中攻击流量的检测能力，包括非法访问、入侵攻击、木马病毒传播行为等，能够对前端摄像头的弱口令进行检测，对视频服务器应用层防护，实现对网络中非法恶意行为的有效识别和管理；提供6万点授权数。 | 服务 | 3年 |
| 2 | 终端安全管理服务 | 实现对公安视频专网中终端电脑的统一安全。终端管理系统以内网终端计算机为管理对象，通过“终端准入控制、终端安全控制、桌面合规管理、终端泄密控制、终端审计和终端防泄密”多维管理，全面提升内网安全防护能力和合规管理水平，帮助用户构建起安全可信的合规内网；提供800点授权数。 | 服务 | 3年 |
| 3 | 终端水印管理服务 | 显示于用户计算机桌面上，不会遮挡应用程序窗口，只有在显示桌面的时候显示水印内容，用于显示保密原则、工作注意事项，宣传标语等。显示于打印机输出的结果文件上，用于对于打印文件需要加载水印的用户场景。在编辑文档电子版的时候不受影响。水印只显示于应用软件区域，可随应用软件界面大小变化而变化，不影响其他应用程序显示。用于用户只想保护特定数据的场景，例如只保护word里边的数据，效果为打开word的时候，只在word区域显示水印，防止word内容被拍照；提供800点授权数。 | 服务 | 3年 |
| 4 | 终端防病毒服务 | 实现病毒传播的防护、木马的查杀、病毒特征库的升级等；提供800点授权数。 | 服务 | 3年 |
| 5 | 网络边界监测服务 | 网络监测系统通过流量镜像、流量劫持、主动探测扫描方式发现视频专网内部存在违规行为；提供6万点授权数。 | 服务 | 3年 |
| 公安网 | 6 | 违规外联检测 | 违规外联包含了网络状态监测、实时抓包分析、定时外联监测及通信防火墙等功能组件。通过这一系列组件的无缝协同工作，达到第一时间发现外联行为并进行防护目的。防护方式可提供终端提醒、通信阻断、强制关机、关机并需管理员解锁等手段。 | 服务 | 3年 |
| 安全运营服务 | 7 | 安全驻场服务 | 提供专人进行现场的驻场服务，驻场人员服务内容包含下属基础运营服务以及安全事件响应服务。详见7.1---7.5项内容。本次项目需提供一个专门驻场人员进行现场的驻场服务，相关人员需经过用户单位现场面试通过后方可进驻项目现场，驻场人员服务内容要求如下： | 服务 | 3年 |
| 7.1 | 安全标准建设 | 结合丽水市公安现状以及未来安全合规及监管的实际需求出发，围绕着安全管理、安全技术、安全运营形成自己的安全标准规范用来指导建设、管理、运营工作的开展。制订安全管理要求、安全技术标准、安全运营标准 | 服务 | 3年 |
| 7.2 | 安全合规检查及指导 | 协助丽水市公安开展安全管理工作，针对不同技术活动参照相应的标准规范开展，并对各业务单位的重要系统进行安全建设和整改指导、定期开展网络安全情况及能力建设情况检查。按照上级主管单位要求开展安全工作。 | 服务 | 3年 |
| 7.3 | 安全设备运行维护 | 对安全设备运行状态进行监测，每月对网络设备（路由器、交换机等）、安全设备（防火墙、日志审计系统、堡垒机等）、服务器设备等进行至少一次巡检查看设备运行状态，查看系统运行状态、运行日志、故障告警、规则库更新时间等。巡检采用远程登录和本地检查的方式进行。在出现设备故障时快熟处理及时恢复，保障安全设备的可用性、实效性。每月提供一次安全设备运行维护服务。 | 服务 | 3年 |
| 7.4 | 安全、策略优化 | 结合实际业务安全需求，对现有各网络边界防火墙等安全策略；网络设备的路由策略等进行差距分析，发现策略缺失、策略冗余、策略未废止等问题，并制定相应工作方案开展策略优化工作，内容包括：访问控制策略优化、安全防护策略优化、行为审计策略优化等，通过安全策略优化完善策略可用性，提升防护能力。针对所有需要安全策略优化的安全设备输出安全策略优化报告。每月提供一次安全策略优化服务。 | 服务 | 3年 |
| 7.5 | 配置及备份更新 | 对系统内运行的网络设备（路由器、交换机等）、安全设备（防火墙、日志审计系统、堡垒机等）进行相关配置文件、策略文件进行定期备份，定期根据厂家系统更新情况及时对安全设备进行软件及规则库及版本更新，保证安全设备的稳定运行。每月提供一次配置及备份更新服务。 | 服务 | 3年 |
| 7.6 | 安全事件监控分析 | 安全服务人员日常对安全防护设备、安全管理平台、安全监测系统等类型的安全设备进行查看，对所产生的告警信息结合公安网、视频网资产进行分析，结合外部威胁情报数据分析验证告警的真实性、影响范围及程度，经过分析验证后给出相应的解决方案，通报给相应的用户协助用户进行整改，整改后进行验证，对于重大安全事件驻场人员请求二线专家进行响应快速处置。每月提供一次安全事件监控分析服务。 | 服务 | 3年 |
| 7.7 | 安全通报服务 | 建立安全通告机制，对出现的安全问题、威胁情报信息等进行全面传达，定期通告以邮件形式向用户通告业内安全态势、重要系统漏洞及补丁信息等。非定期通告对于紧急重大类漏洞信息，将以最快时间通过邮件或电话向客户告知漏洞危害、影响范围及应对方案等信息。对于公安网、视频网上系统发现的安全事件及漏洞、威胁等快速通告相应单位负责人。 | 服务 | 3年 |
| 7.8 | 全网安全态势监测预警分析 | 安全服务工程师针通过专用威胁检测分析工具，针对视频网及公安信息网所采集的全流量网络数据，进行资产梳理和攻击面分析，利用威胁情报数据，利用采集到的安全大数据并采用专业攻防思路构建分析模型，提供内部失陷主机、外部攻击、内部违规和内部风险等关键信息安全问题的周期性的检测、发现和响应服务。提升主动应对安全威胁能力，在信息安全方面构建最后一道防线。主要包括内部失陷主机检测、外部攻击检测、内部攻击检测、内部违规检测和事件分析研判溯源四大类服务。深度风险分析服务结合公安网、视频网实际情况，周期性的开展工作，提供交付成果全流量风险分析报告。每季度提供一次深度风险分析服务，输出分析报告及整改建议。 | 服务 | 3年 |
| 7.9 | 应急响应处置 | 基于公安网、视频网发生安全事件开展应急响应，实施安全事件检测、安全事件抑制、安全事件根除、安全事件恢复、安全事件总结，与其他相关单位形成协调联动机制，增强应急技术能力，健全应急响应机制。安全事件处置完成，系统得到恢复。找到安全事件发生原因并提供安全解决方案。提供重大安全事件应急响应报告。 | 服务 | 3年 |
| 7.10 | 系统安全评估 | 针对重点系统，采用各种手段模拟真实的安全攻击，从而发现黑客入侵信息系统的潜在可能途径。渗透测试工作以人工渗透为主，辅助以攻击工具的使用。主要的渗透测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、云服务客户端攻击、中间人攻击、web脚本渗透、B/S或C/S应用程序测试等。 | 服务 | 3年 |

### 五 商务要求

5.1 质保要求**：**采购需求文件中无特别说明的，所有软硬件产品要求提供原厂五年质保，硬盘损坏不返还，价格包含用户所需的所有的软件相关授权或license数量,授权时间不低于5年。并需在合同签订后提供原厂质保服务承诺函（加盖原厂公章）。本次招标要求万兆防火墙功能模块全开。承诺函需承诺质保期内软硬件质保，且提供最新的软件版本及特征库等升级服务。硬件设备和商品化软件维保期、定制化软件维保期从项目验收合格之日算起。

5.2售后项目维护计划及响应情况：

5.2.1要求服务工作人员对工作中涉及到的用户的数据、文件等任何资料进行保密。因工作人员的行为造成泄密等问题由中标单位承担相应的责任；

5.2.2对于出现紧急故障情况，中标方应承诺商务时间30分钟内响应，一般故障2小时内响应，4小时内到达现场，重大故障1小时内响应，2小时内到现场服务，4个小时内解决问题；不能修复的，12小时内提供备品、备件或备机等措施，以保证用户的正常使用。

5.3 付款方式：合同签订且收到供应商缴纳的履约保证金后，支付合同首付款30%，终验后支付40%，终验合格后每满一年，支付10%，维护期分3年。

5.4 培训要求：

中标人应安排技术人员对用户进行培训或技术指导。

培训人数不少于3人，次数不少于2次，培训时间不少于4小时。

培训内容主要为本项目采购的各软硬件产品，培训目标要求使用户能够独立进行日常管理和维护。

对于投标文件中不合理培训内容及费用，用户在项目实际实施中不予执行的，在项目决算时对相关费用予以审减。

5.5 备品备件及耗材要求：

1.按照采购需求文件要求提供备品备件。

2.采购需求文件中未明确说明的，备品备件种类和数量由投标商根据所投产品自行确定。

5.6其他：

5.6.1系统集成项目组实施人员能力

投标人项目组负责人应当具有高级工程师资格（或具有PMP、CISSP、CISA、CISAW、CISP、CISP-PTE等资质证书）。项目组成员2人以上具备CISP证书或高级工程师资格。

项目实施期间（设备到货后起，项目验收止），投标供应商提供一名固定的有经验驻场技术人员，全程联系并会同厂商工程师进行软硬件安装实施、系统部署和调试配置等工作，同时由该工程师联系和协助处理后续项目相关的细节技术问题。

提供以上人员证书复印件、有效社保记录并加盖公章，并承诺项目相关工程师在服务期内可随时响应并到现场解决采购方的实际技术问题。（须提供近一年社保证明）。

5.6.2知识产权等相关要求

本项目中如存在定制开发软件产品，相关知识产权归丽水市公安局与项目承建单位共同拥有，其中丽水市公安局占51%，项目承建单位占49%。定制开发软件的源代码必须遵循标准和规范，并无条件提交给我局；接口必须遵循标准和规范，向下部署的、在公安网上运行的非涉密信息系统必须无条件开放所有接口，项目承建单位有义务配合信息中心做好有关信息共享工作，若未能做到以上要求项目承建单位需承担相应责任。

### 六 工期及供货地点要求

**▲**6.1 工期要求：

合同签订后1个月内完成项目中涉及的所有软硬件设备交货，货物送达丽水市公安局信息中心机房。

软硬件设备完成安装部署和调试工作后，进行初步验收，初步验收后进行为期3个月的试运行，试运行结束后由承建单位申请终验。

6.2 供货（安装）地点要求：丽水市公安局

### 七 安装、调试、验收要求

7.1 安装要求：按照国标或行业规范要求；

7.2 调试要求：要按国标或行业规范要求；

7.3 验收要求：在设备到货时须提供相对应的产品检测报告；

7.3.1本项目安装、调试完成后，接到承建单位书面验收申请且经监理单位确认后7个工作日内组织验收。

### 八 其他

8.1本项目所涉及的安装数量，招标时确认数量不一定准确时，按其中标单价和实际工程量结算。税收、人工费、安装费等一切与之相关的所有费用都需包含在报价中。

8.2本项目排名第一的中标候选人未注册成为“浙江省政府采购供应商”的，采购代理机构将暂缓发布中标通知书，由此造成的不利影响自行承担。

8.3 有关“浙江省政府采购供应商”注册事宜可向采购代理机构咨询，联系人：朱中豪，联系电话：0578—2292117。