采购项目需求

一、项目概况

按照国家、省级电子政务外网标准和规范，优化金昌市电子政务外网网络结构，完善链路冗余与网络安全防护，提高网络业务承载能力，为全市各级各部门业务应用、数据传输提供支撑。本项目具体的服务内容为：一是网络接入服务，提供市级城域网服务，提供互联网出口区服务，提供无线网络服务；二是网络安全服务，提供安全运维管理区服务、等保三级服务、售后服务。

二、服务内容及技术要求

序号	服务名称	技术参数	单位	数量
1	市级城域网服务	提供市城域网核心交换服务，实现市级城域网与市级广域网互联；提供城域网边界防火墙服务和接入防火墙服务，满足网络边界保护和访问控制要求。	项	1
2	互联网出口区服务	1.提供互联网出口链路专线接入，链路上联端口必须具备≥1G带宽服务能力，采用光口接入方式直接接入甲方机房。互联网出口上联至运营商网络，必须独享上下对等的光纤专线，不能包含中标方的局域网网内带宽，线路质量稳定可靠，并能很好解决各运营商之间互联互通问题。 2.线路质量稳定可靠，电路可用率≥99.9%;网络平均丢包率≤0.01%，吞吐率100%;传输时延≤20ms，最大延迟≤64ms。 3.互联网出口区要求采用单链路上联至运营商，通过链路负载均衡设备和集中NAT技术方式提供互联网访问服务。要求采用高性能防火墙作为出口的安全隔离设备，隔离互联网和电子政务外网的内部网络，保证跨安全域的访问都能通过防火墙进行控制管理，并能在网络出口处实现入侵防范功能。同时还应该在互联网出口处进行优化控制，保证用户访问选择最优的链路。此外，在互联网出口	项	1

序号	服务名称	技术参数	单位	数量
		处进行流量控制，保证网络发生拥堵的时候优先保护重要的主机。根据公安部等级保护基本要求，所有用户访问互联网需要部署上网行为管理系统，并保存不少于3个月的日志。		
3	无线 网络服务	1.政务外网盲点区域延伸覆盖 使用现在主流的无线控制器 AC+瘦 AP 的无线网络架构进行盲点区域无线网络覆盖，要求该架构下的无线网络由1台无线控制器和5台无线 AP 组成，所有的无线 AP 皆由该控制器进行统一的配置和管理，并提供1条千兆互联网专线。无线 AP 可以通过 PoE 交换机进行远程的 PoE 供电或者选择本地供电，如果采用远程的 PoE 供电，则可以在无线控制器上按照时间进行无线 AP 的开关定时，按照设定好的策略自动定时开关 AP，满足一定的节能需求。通过 AC_无线 AP 方式完成盲点区域补点。 2.VPN 接入服务 VPN 主要用户无线网络服务,建立相对安全的无线网络通道提供特定网络服务的应用，VPN 接入服务具备以下能力： ①吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万； ②支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议； ③支持 NAT66，NAT64，6RD 隧道； ④支持每 IP，每用户的最大连接数限制，防护服务器； ⑤支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维； ⑥支持识别国标 SIP 协议及主流安防厂家的私有协议； ⑦支持全面 NAT 功能，对多种应用层协议支持 ALG 功能，包括 ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS 等； ⑧支持对 HTTPS，POP3S，SMTPS,IMAPS 加密	项	1

序号	服务名称	技术参数	单位	数量
		流量代理解密后，并进行内容过滤，审计，安全防护； ⑨支持 HTTP、FTP、SMTP、POP3、IMAP、NFS 等协议的病毒防护； ⑩支持流探针功能，采集网络流量的网络层、传输层和应用层信息，并将采集到的信息发送到网络安全智能分析系统，通过网络安全智能分析系统评估网络中的威胁和 APT 攻击； ⑪支持 Portal 页面定制及调查问卷，进行营销推广； ⑫可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。 3.无线网卡服务 提供≥8张5G 无线网卡,用于远程无线管理和办公使用。		
4	安全运维管理区服务	提供运维管理区边界防火墙服务、安全管控平台服务、高危服务端口安全管控服务、安全风险智能学习服务、系统管理服务、服务器数据非法访问防护服务、系统引导区保护服务、服务器安全自我保护服务、运维终端安全防护服务、数据库审计安全防护服务，实现运营平台化、管理一体化、态势可感知、事件可预警、事故可追溯、技术大融合、安全可闭环的网络安全运维管理。	项	1
5	等保三级服务	按照等级保护三级要求统筹规划优化电子政务外网安全体系，提升安全基础防御能力的水平,金昌市电子政务外网需达到等级保护三级要求，并通过专业机构评测。	项	1

序号	服务名称	技术参数	单位	数量
6	售后服务	提供1人驻场服务，并提供7*24小时全市电子政务外网运维服务，保证全市电子政务外网正常运行。提供全市电子政务外网有线网络各设备设施的日常运行、维护、网络安全保障、应急处置等售后服务工作。供应商负责提供金昌市电子政务外网无线网络服务项目各设备设施的日常运行、维护、网络安全保障、应急处置等工作，供应商应制定各项运行维护规章制度和应急预案，定期开展电子政务外网网络安全风险评估和应急演练，做好日常值班值守、机房和线路巡检、应急处置、故障处理、安全防护及日志记录。	人	1

注：投标供应商须对以上服务内容及技术要求出具完全响应承诺函，此承诺函将作为合同组成部分，若中标人在合同履行过程中未能达到本项目服务内容及技术要求，采购人有权要求整改并延长服务期限、扣款、解除合同并追究违约法律责任。

如未提供此承诺函，将按无效投标处理。

三、商务要求

1、为满足项目服务内容及技术要求，供应商须提供以下清单中（附件一）的软、硬件和数据服务，并在投标文件中提供清单内容响应性的承诺函，此承诺函将作为合同附件的一部分，若中标人在合同履行过程中未能提供以下软、硬件和数据服务，或提供的软、硬件和数据服务无法达到本项目服务内容及技术要求，采购人有权要求整改并延长服务期限、扣款、解除合同并追究违约法律责任。**如未提供此承诺函，将按无效投标处理。**

2、服务期：自签订合同之日起 3 年，合同采取“1+1+1”模式逐年考核签订，采购人根据服务情况进行年度考核，根据考核结果确定是否授予下年度合同。

附件一：

支撑金昌市电子政务外网无线网络服务政府采购服务项目设备参数清单

序号	软硬件名称	技术要求	单位	数量
一、网络接入服务				
（一）市级城域网服务				
1	金昌市城域网核心交换机	1.交换容量≥500Tbps、包转发≥96000Mpps，主控引擎与交换网板物理分离；主控引擎≥2；独立交换网板≥4；整机业务板槽位数≥8； 2.设备支持支持以太网千兆电口、千兆光口、万兆光口、万兆电口、25G端口、40G端口、100G端口； 3.支持VxLAN功能，支持VxLAN二层网关、三层网关，支持BGPEVPN，支持分布式Anycast网关，支持VxLANFabric的自动化部署； 4.支持横向虚拟化技术，将多台设备虚拟为一台，支持长距离集群； 5.支持整机MAC地址≥1M，ARP表项≥256K； 6.支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6； 7.支持SNMPV1/V2/V3、Telnet、RMON、SSHV2； 8.单台配置双主控、双交换网板、双交流电源、万兆光口≥96个、40GE光口≥24个，万兆多模光模块≥10个，万兆单模光模块≥10个、千兆单模光模块≥10个、40G单模光模块（40Km传输距离）≥2个。	台	2
2	防火墙	1.标准机架式1U设备；实配：千兆电口≥12，万兆光口≥12；双交流电源，固态硬盘≥240G；三年IPS、AV、URL、云沙箱特征库升级服务； 2.防火墙吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万； 3.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议； 4.支持NAT66，NAT64，6RD隧道； 5.支持每IP，每用户的最大连接数限制，防护服务器； 6.支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维； 7.支持DNS过滤，提高WEB网页过滤的性能； 8.支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等； 9.支持恶意域名过滤，实现对C&C进行阻断； 10.支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护； 11.要求防火墙具备AI引擎，AI引擎用于恶意C&C流量检测； 12.支持Portal页面定制及调查问卷，进行营销推广；	台	2

		13.可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。		
（二）互联网出口区服务				
1	抗DDOS设备	1.实配：千兆光电复用口≥8个，千兆电口≥4个，千兆光口≥4个，万兆光口≥6个，双交流电源，≥20G清洗能力； 2.支持风扇冗余和可插拔更换，当风扇模块出现故障时，可以在设备不断电的情况下，对风扇模块进行更换； 3.直路部署模式，攻击响应延迟<1秒； 4.支持检测设备、清洗设备旁路部署，逐包检测动态引流，支持BGP动态引流，支持PBR回注(策略路由)、二层回注； 5.支持基于源SYN报文比例异常检测防御真实源SYN攻击； 6.支持HTTP应用层Flood/HTTPCC识别及防御，支持HTTPS应用层Flood/HTTPSCC识别及防御，支持DNSQueryFlood识别及防御； 7.支持基于会话检测防御FIN/RSTFlood； 8.系统支持综合报表查询，报表内容包含攻击趋势、流量对比、攻击类型分布、攻击事件TOPN、流量TOPN等，支持报表导出； 9.支持IPv4/IPv6共栈防御。	台	1
2	互联网出口区边界防火墙	1.标准机架式1U设备；实配：千兆电口≥12，万兆光口≥12；双交流电源，固态硬盘≥240G；三年IPS、AV、URL、云沙箱特征库升级服务； 2.防火墙吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万； 3.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议； 4.支持NAT66，NAT64，6RD隧道； 5.支持每IP，每用户的最大连接数限制，防护服务器； 6.支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维； 7.支持DNS过滤，提高WEB网页过滤的性能； 8.支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等； 9.支持恶意域名过滤，实现对C&C进行阻断； 10.支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护； 11.要求防火墙具备AI引擎，AI引擎用于恶意C&C流量检测； 12.支持Portal页面定制及调查问卷，进行营销推广； 13.可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。	台	1
3	互联网出口区接入交换机	1.双主控，双电源，万兆光口≥48个； 2.主控引擎≥2；整机业务板槽位数≥6； 3.交换容量≥70Tbps，包转发率≥57000Mpps； 4.为保证设备散热效果和可靠性，要求设备支持模块化风扇框，	台	1

		可热插拔，独立风扇框数≥2；支持颗粒化电源，整机电源槽位数≥4个； 5.为适应机柜并排部署，设备机箱（包括业务板卡区）采用后出风风道设计； 6.支持独立的硬件监控板卡,控制平面和监控平面物理槽位分离，支持1+1备份，能集中监控风扇、电源等模块，能调节能耗； 7.支持VxLAN功能，支持VxLAN二层网关、三层网关，支持BGPEVPN，支持分布式Anycast网关，支持VxLANFabric的自动化部署； 8.支持整机MAC地址≥512K；支持整机ARP表项≥256K； 9.支持业务板集成AC功能，实现对AP的接入控制和管理，实现对有线无线用户的统一认证管理、用户数据报文的隧道集中转发； 10.支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；支持路由协议多实例； 11.支持真实业务流的实时检测技术，秒级快速故障定位； 12.支持PQ、WRR、DRR、PQ+WRR、PQ+DRR等调度方式； 13.支持SNMPV1/V2/V3、Telnet、RMON、SSHV2，支持通过命令行、中文图形化配置软件等方式进行配置和管理。		
4	上网行为管理	1.实配：千兆电口≥12个，千兆光口≥12个，万兆光口≥4个,硬盘≥2T，交流冗余电源,含集中管理软件,3年特征库升级许可； 2.网络层UDP吞吐量≥39Gbps，应用层HTTP吞吐量≥16Gbps，并发连接数≥500万； 3.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； 4.支持路由和透明模式配置源地址转换、目的地址转换、双向地址转换等； 5.支持4GUSB插卡。支持在4G接口上运行IPSecVPN； 6.支持静态路由、策略路由、动态路由、ISP路由； 7.支持IPv6/v4双栈，支持IPv6安全策略； 8.支持基于全局或链路进行DNS透明代理，支持指定DNS或继承链路DNS配置，针对多链路支持基于优先级、权重、流量算法进行DNS负载； 9.支持基于接口和目的地址进行健康检查，可自定义检查间隔、重试次数等； 10.支持在设备旁路部署时针对违规上网行为进行阻断过滤； 11.支持自定义应用，包括但不限于数据包方向、协议、端口、IP地址、目标域名、关键字识别等维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式； 12.支持智能和快速识别模式配置； 13.针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长；支持使用设备内置公告页面或引用第三方公告页面，支持自定义提醒频率，支持定时发布公告；	台	1

		14.支持IPsecVPN冷备份技术，指定VPN主备链路，当主链路存活时，备链路不接受不发送报文，避免主备链路同时收发包来回路径不一致导致业务中断的情况； 15.支持单用户全天行为分析报表，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息。		
5	堡垒机	1.设备高度：1U，交流单电源，4GCF卡，2TSATA硬盘，8G内存，4*GE电口，2*USB接口，1*RJ45串口，1*GE管理口，1个接口扩展槽。缺省授权管理200台设备； 2.为了运维人员登录安全，支持自动登录、手工登录、半自动登录、密钥登录方式； 3.为了运维人员运维方便，支持自动填写特权密码，从普通管理模式进入到特权模式，提供对部分配置操作进行向导式配置界面； 4.除用户身份认证外，对特定目标设备访问还需要高级管理员授权才能访问。授权审批方式支持web和手机APP审批两种方式，手机APP上进行登录授权审批，金库授权审批，工单审批三种审批模式，方便随时随地进行审批工作，支持手机APP上进行运维监控，包括设备信息推送，系统告警监控两种数据； 5.要求支持孤儿账号功能，能够提供对各从账号的运维使用率的分析功能，当发现使用率异常的从账号，对相关管理员采取告警、记录及通知操作； 6.支持第三方客户端实现SSH、RDP、VNC、X11、Telnet、SFTP、FTP协议自动、手动登录运维设备，并实现审计功能。	台	1
6	全流量安全监测	1.可管理路由器数量≥20台，含12万flows/s授权许可。引擎模块，2U，含交流冗余电源模块，8GCF卡，2T硬盘，32G内存，2*USB接口，1*RJ45串口，2*GE管理口，4个100/1000M以太网电口，3个网络接口卡扩展插槽。2个万兆SFPP插槽（不含光纤接口模块），支持万兆多模光纤接口模块、万兆单模光纤接口模块； 2.设备支持IPv4/IPv6环境下的异常流量检测功能； 3.支持的数据分析格式至少包括sflowv4/v5、netflowv5/v9、netstreamv5、flexiblenetflow、ipfix； 4.支持自定义攻击特征进行检测和告警； 5.支持从外网到内网异常流量检测，支持从内网到外网异常流量检测； 6.支持检测阈值自动学习，支持学习时间、学习对象预先指定，同时支持学习阈值自动配置与手动配置功能； 7.针对不同防护对象，支持设置不同的异常流量检测参数和牵引策略； 8.支持对自定义的IP域范围检测入域流量超常和出域流量超常； 9.支持对指定时间范围的告警阈值进行抬升/降低，避免因业务流量正常波动带来误报和漏报；	台	1

		10.支持威胁情报查询，在设备界面查询攻击源IP的地理位置、开放端口、关联域名、ASN及安全信息等； 11.支持自定义或根据告警详情定义BGPFlowspec规则并发送给路由器进行流量过滤； 12.管理界面友好、易用性强，支持集中管理、本地管理、远程管理等多种管理方式，并能实时显示攻击事件、流量、系统运行状况等信息； 13.配置空路由牵引时，每个BGP至少支持配置5个community名称，用于多出口场景下实现空路由； 14.支持配置路由邻居，支持配置RemoteAS、NeighborIP，并支持NTA与FlowspecBGP邻居路由器之间加密码认证； 15.提供完善的日志管理功能，包括日查询、删除、备份、生成报表等操作，而且要支持自定义报表、自动生成报表等功能。		
7	链路负载均衡	1.40Gbps吞吐，1U机型，14*10/100/1000M电口，8*千兆SFP插槽，8*万兆SFPP插槽，4*可选扩展插槽，5*风扇，480GB硬盘模块*2，双电源； 2.支持Vlan、QinQ、STP、MSTP等二层协议，满足二层的区域隔离以及链路冗余，支持RIP、OSPF、BGP等路由协议以及各自的IPv6版本； 3.支持多种链路检测方法，能够通过ICMP、UDP、TCP、FTP、DNS、HTTP、RADIUS、SSL、HTTPS、TCPhalf-open、SNMP-DCA、RADIUS-ACCOUNT等方式监控链路的连通性； 4.支持轮询、加权轮询、最小连接、加权最小连接、随机、源地址HASH、目的地址HASH、源地址端口HASH、静态就近性、动态就近性、带宽算法、最大带宽算法、本地优先级、基于ISP选路等链路调度算法； 5.支持基于ToS、五元组条件（源IP地址，源端口，目的IP地址，目的端口，传输层协议号）来配置出站访问的链路调度策略； 6.支持基于应用协议的智能选路，能识别主流互联网应用如P2P、微信、网银，进行调度； 7.支持基于域名的流量调度，针对特定网站选择指定的链路转发； 8.ISP地址库支持自动升级功能，使设备的ISP地址库保持在最新状态，保证流量调度的准确性； 9.支持主备部署，支持两台设备统一管理，配置只配置一遍，配置自动同步、设备间会话实时同步； 10.支持IPv6基础特性及IPv6的负载均衡，满足今后IPv6网络的升级,可以通过负载均衡设备进行网站发布的NAT64转换，以及IPv6站点的负载。	台	1
（三）无线网络服务				
1	VPN	1.吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万；	台	1

		2.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议； 3.支持NAT66，NAT64，6RD隧道； 4.支持每IP，每用户的最大连接数限制，防护服务器； 5.支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维； 6.支持识别国标SIP协议及主流安防厂家的私有协议； 7.支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等； 8.支持对HTTPS，POP3S，SMTPS,IMAPS加密流量代理解密后，并进行内容过滤，审计，安全防护； 9.支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护； 10.支持流探针功能，采集网络流量的网络层、传输层和应用层信息，并将采集到的信息发送到网络安全智能分析系统，通过网络安全智能分析系统评估网络中的威胁和APT攻击； 11.支持Portal页面定制及调查问卷，进行营销推广； 12.可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。		
2	AC	提供主流的无线控制器AC+瘦AP的无线网络架构进行盲点区域无线网络覆盖，该架构下的无线网络由无线控制器和多台无线AP组成，所有的无线AP皆由该控制器进行统一的配置和管理。	台	1
3	AP	1.采用最新一代支持802.11acWave2协议，单个AP同时具备二个射频，一个射频支持2.4GHz频段，一个射频支持5GHz频段； 2.不低于2个10/100/1000Mbps，整机协商速率不低于1000Mbps，一台AP覆盖范围30米，满足应用需求； 3.每射频最大接入用户数：512（整机最大接入用户数1024）。	台	5
4	无线上网卡	提供5G无线网卡，用于远程无线管理和办公使用。	张	8
二、网络安全服务				
（一）安全运维管理区服务				
1	安全运维管理区边界防火墙	1.标准机架式1U设备；实配：千兆电口≥12，万兆光口≥12；双交流电源，固态硬盘≥240G；三年IPS、AV、URL、云沙箱特征库升级服务； 2.防火墙吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万； 3.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议； 4.支持NAT66，NAT64，6RD隧道； 5.支持每IP，每用户的最大连接数限制，防护服务器； 6.支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维； 7.支持DNS过滤，提高WEB网页过滤的性能； 8.支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等；	台	1

		9.支持恶意域名过滤，实现对C&C进行阻断； 10.支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护； 11.要求防火墙具备AI引擎，AI引擎用于恶意C&C流量检测； 12.支持Portal页面定制及调查问卷，进行营销推广； 13.可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。		
2	安全运维管理区接入交换机	1.双主控，双电源，万兆光口≥48个； 2.主控引擎≥2；整机业务板槽位数≥6； 3.交换容量≥70Tbps，包转发率≥57000Mpps； 4.为保证设备散热效果和可靠性，要求设备支持模块化风扇框，可热插拔，独立风扇框数≥2；支持颗粒化电源，整机电源槽位数≥4个； 5.为适应机柜并排部署，设备机箱（包括业务板卡区）采用后出风风道设计； 6.支持独立的硬件监控板卡,控制平面和监控平面物理槽位分离，支持1+1备份，能集中监控风扇、电源等模块，能调节能耗； 7.支持VxLAN功能,支持VxLAN二层网关、三层网关,支持BGPEVPN,支持分布式Anycast网关，支持VxLANFabric的自动化部署； 8.支持整机MAC地址≥512K；支持整机ARP表项≥256K； 9.支持业务板集成AC功能，实现对AP的接入控制和管理，实现对有线无线用户的统一认证管理、用户数据报文的隧道集中转发； 10.支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；支持路由协议多实例； 11.支持真实业务流的实时检测技术，秒级快速故障定位； 12.支持PQ、WRR、DRR、PQ+WRR、PQ+DRR等调度方式； 13.支持硬件BFD/OAM，3.3ms稳定均匀发包检测，提高设备的可靠性； 14.支持SNMPV1/V2/V3、Telnet、RMON、SSHV2，支持通过命令行、中文图形化配置软件等方式进行配置和管理。	台	1
3	应用服务器	1.国产设备，2U机架式服务器，非OEM产品，具有自主知识产权； 2.配置2颗英特尔至强处理器（主频2.4GHz，核数12）； 3.配置128GDDR4内存，可支持至少24个内存插槽； 4.配置2*480GBSSD硬盘，1000GB以上的SAS硬盘，支持热插拔SAS/SATA/SSD硬盘，可支持配置8块2.5inch托架的SATA/SAS硬盘，最大支持28块2.5寸硬盘； 5.支持双MiniSSD硬盘可做RAID1,可安装操作系统,hypervisor,虚拟化软件等； 6.配置1块SR430C-M1G(LSI3108)SAS/SATARAID卡，支持RAID0,1,提供Raid状态迁移，Raid配置记忆，自诊断，WEB远程设置等功能； 7.配置2*GE+2*10GE网口以太网卡； 8.配置2块900W双冗余电源，支持电源热插拔； 9.可管理和维护性:①集成系统管理处理器支持：自动服务器重	台	1

		启、风扇监视和控制、电源监控、温度监控、启动/关闭、按序重启、本地固件更新、错误日志，可通过可视化工具提供系统未来状况的可视显示；②具有图形管理界面及其他高级管理功能；③配置独立的远程管理控制端口，支持远程监控图形界面,可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、虚拟软驱、虚拟光驱等操作。		
4	应用服务器	1.国产设备，2U机架式服务器，非OEM产品，具有自主知识产权； 2.配置2颗英特尔至强处理器（主频2.4GHz，核数12）； 3.配置64GDDR4内存，可支持至少24个内存插槽； 4.配置2*480GBSSD硬盘，2200GB以上的SAS硬盘，支持热插拔SAS/SATA/SSD硬盘，可支持配置8块2.5inch托架的SATA/SAS硬盘，最大支持28块2.5寸硬盘； 5.支持双MiniSSD硬盘可做RAID1,可安装操作系统,hypervisor,虚拟化软件等； 6.配置1块SR430C-M1G(LSI3108)SAS/SATARAID卡，支持RAID0,1,提供Raid状态迁移，Raid配置记忆，自诊断，WEB远程设置等功能； 7.配置2*GE+2*10GE网口以太网卡； 8.配置2块900W双冗余电源，支持电源热插拔； 9.可管理和维护性:①集成系统管理处理器支持：自动服务器重启、风扇监视和控制、电源监控、温度监控、启动/关闭、按序重启、本地固件更新、错误日志，可通过可视化工具提供系统未来状况的可视显示；②具有图形管理界面及其他高级管理功能；③配置独立的远程管理控制端口，支持远程监控图形界面,可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、虚拟软驱、虚拟光驱等操作。	台	1
5	安全管控平台模块	1.数据安全防护系统的基础承载平台； 2.最大支持400个服务器安全软件授权； 3.支持VMWare、KVM、Xen等主流虚拟化技术。	套	1
6	高危服务端口安全管控模块	1.通过端口控制限制对服务器的访问； 2.支持VMWare、KVM、Xen等主流虚拟化技术。	套	1
7	安全风险智能学习模块	1.自动学习被保护数据的操作访问行为，禁止恶意程序的启动和运行； 2.支持VMWare、KVM、Xen等主流虚拟化技术。	套	1
8	系统管理模块	1.提供B/S方式管理界面。支持系统管理员、安全管理员和日志管理员权限三权分立，支持进行统一的策略配置和软件版本升级，支持终端安全策略管理； 2.支持VMWare、KVM、Xen等主流虚拟化技术。	套	1
9	服务器数据非法访问防护模块	1.对被保护数据进行非法操作防护； 2.支持windowsServer和LinuxServer主流内核版本。	套	140

10	系统引导区保护模块	1.对操作系统引导区进行保护，阻断勒索病毒攻击引导区导致系统引导失败，业务受损； 2.支持windowsServer和LinuxServer主流内核版本。	套	140
11	服务器安全自我保护模块	1.支持自我保护功能； 2.支持windowsServer和LinuxServer主流内核版本。	套	140
12	运维终端安全防护模块	1.对下载到本地的数据实现透明加解密，非授权环境无法使用，授权环境使用无感知； 2.支持外发数据审批电子流，并集成密码认证、权限控制、截屏录屏等多项管控技术，制作成外发文件； 3.监控终端行为，阻断采用系统原生或第三方截屏录屏工具的数据窃取行为； 4.完善的自我保护能力，抵御恶意卸载、恶意关闭、病毒加密； 5.支持windows系列操作系统。	套	140
13	数据库审计安全防护模块	1.支持数据库：Oracle、MySQL、SQLserver、DB2、Sybase、Informix、Teradata、PostgreSQL、Cache； 2.支持数据库：达梦、南大通用、人大金仓、神通、浪潮KDB、湖南上容； 3.支持大数据平台非关系型数据库：Hive、HBase、MongoDB等； 4.支持对日志进行细粒度解析，支持数据库操作(DML)、对象管理(DDL)、控制(DCL)等操作语句的审计，解析后的日志记录至少包括访问发生时间、客户端IP地址、客户端MAC、终端程序、访问账号、访问数据库名、操作表名、SQL语句、数据库响应时间以及返回结果等关键信息； 5.三层关联审计，实现用户、主机、SQL操作三层关联分析，精确定位具体操作人员； 6.支持智能定义高危动作识别，实现对数据库的高危动作的阻断； 7.支持SYSLOG、SNMPTRAP、邮件、FTP等多种事件告警和提示方式； 8.支持对SQL语句操作类型统计、事件类型统计、风险级别统计、流量统计，同时按在线用户、客户端IP、会话、模板数等支持在线信息统计，并生成多种专业报表； 9.支持SQL语句进行拼接功能，能够完整解析与审计超长SQL语句（超过1460字节），屏蔽逃逸审计通道。	套	1