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核心骨干网网络结构，完善链路冗余，避免网络单点故障，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：一是网络专线接入服务，提供市城域网核心节点到市级各部门、单位专线服务以及到金昌市紫金云大数据中心和城市云专线服务，提供互联网出口链路专线接入服务；二是网络安全服务，提供市级城域网边界安全、安全接入区服务、互联网接入区安全服务、安全运维管理区服务以及等保三级服务等；三是运营维护服务，提供市行政中心机房环境优化服务、电子政务外网完善的售后服务和驻场服务。

二、服务内容及技术要求

序号	服务名称	服务要求	单位	数量	备注
一、网络专线接入服务					
1	市城域网核心节点到市级各部门、单位专线服务	1.要求提供市城域网核心节点到市级各部门、单位专线链路及提供使用双芯双向点对点专线接入，链路必须符合接入带宽：市级各部门、单位接入带宽≥500M。 2.要求所有线路独享专线带宽，不得与其它接入用户共享线路及带宽资源。 3.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。 4.专线接入服务质量必须保证采购人现有应用的互通性和兼容性要求，后期根据各单位机构调整和场地搬迁随时调整。	项/年	1	
2	互联网出口专线接入	1.要求提供互联网出口链路专线接入，链路上联端口必须具备≥3G带宽服务能力，具备光口方式直接接入市行政中心机房。 2.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，不能包含供应商的局域网网内带宽，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。 3.互联网接入链路必须独享、不再复用，不得通过接入商缓存、cache等类似设备，且为双向全线速专线，电路可用率≥99.9%；端到端电路丢包率≤0.01%，吞吐率100%；端到端的电路传输时延≤10ms。	项/年	1	

序号	服务名称	服务要求	单位	数量	备注
		4.供应商无故障运行时间≥99.9%。 5.专线接入服务质量必须保证采购人现有应用的互通性和兼容性要求。			
3	市城域网核心节点到金昌市紫金云大数据中心和城市云专线服务	1.要求提供市城域网核心节点到金昌市紫金云数字政府运营指挥中心12芯光纤接入，链路必须符合接入带宽，链路带宽≥1G，后期根据单位机构调整和场地搬迁随时调整； 2.要求提供市城域网核心节点到金昌市城市云服务平台双芯双向专线接入，链路必须符合接入带宽，链路带宽≥10G，后期根据单位机构调整和场地搬迁随时调整； 3.要求所有线路独享专线带宽，不得与其它接入用户共享线路及带宽资源； 4.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； 5.专线接入服务质量必须保证采购人现有应用的互通性和兼容性要求。	项/年	1	
二、网络安全服务					
1	市级城域网边界安全服务	市级城域网与省级广域网互联，以及内部安全域边界提供防火墙服务，实现网络边界保护和访问控制，防火墙开放必需的服务端口，对网络数据进行访问控制，采取有效的边界访问控制策略，提高网络可靠性，提供防火墙双机部署服务，并支持IPv4、IPv6会话信息记录、可溯源。	项/年	1	
2	安全接入区服务	要求本次提供安全接入区服务，提供路由器、防火墙、入侵检测、沙箱、VPN网关、探针等服务内容，实现无线网络接入的安全保护。	项/年	1	
3	互联网接入区安全服务	互联网出口需遵循国家电子政务外网安全规范要求并满足高可用的链路双向负载均衡服务，提供精细化的安全防护和带宽管理服务，提供防火墙、负载均衡设备、链路负载均衡、抗Ddos、探针、汇聚交换机、防病毒网关、入侵防御系统、上网行为管理、网络流量分析系统等安全服务。	项/年	1	

序号	服务名称	服务要求	单位	数量	备注
4	安全运维管理区服务	根据金昌市电子政务外网的安全现状，从安全技术、安全管理、安全运维方面开展建设，打造运营平台化、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体系。按照等级保护三级要求统筹规划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有线网络达到等级保护三级要求，并通过专业机构评测。本次安全体系建设应完善政务技术、管理、运维三大体系建设、提升新型威胁检测能力、打造联动闭环的技术体系。全面解决架构缺乏整体设计、安全架构缺乏协同、技术手段孤岛。完善安全基础设施服务、提升高级威胁检测能力、提升安全体系联动闭环的能力，提供边界防火墙、接入交换机、网络安全态势感知系统、日志审计系统、安全准入平台、网络管理平台、安全管理中心、漏洞扫描系统、僵木蠕检测系统、杀毒软件系统、堡垒机等服务实现电子政务外网的全网威胁可视化、通报预警和统一安全运营能力，并对全市政务新媒体进行安全监测。	项/年	1	
5	等保三级服务	按照等级保护三级要求统筹规划建设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有线网络达到等级保护三级要求，并通过专业机构评测。	项/年	1	
三、运营维护服务					
1	市行政中心机房环境优化服务	优化市行政中心1至6号机房和1号机房监控室基础设施环境，提供完善的维修服务和售后服务，对机房空调系统、UPS供配电系统、监控系统等，作为重点运行维护内容，同时对机房内的其他指标项进行检测，如机房内温度、湿度、消防系统、机房环境、防雷接地等，为电子政务外网运行提供安全稳定的机房环境，主要有以下内容： 1.机房监控设备维护管理：供配电监测系统、空调环境检测系统、门禁设备系统、漏水检测。 2.UPS不间断电源系统维护：负责所有机房UPS的维护、故障诊断检修和器件更换等工作。负责UPS系统、蓄电池的维护保养、一般性故障处理维护、电池充放电管理维护；负责蓄电池配套的电池开关盒、汇流盒、电池架开关盒及连接电缆等的维护、保养、更换。 3.电气配电系统维护：负责所有机房配电柜的器件和柜体维护。器件包括所有柜内切换机构	项/年	1	

序号	服务名称	服务要求	单位	数量	备注
		模块、空气开关、脱扣控制器、输入输出排、电气监控传感器、电量仪以及配电系统的末端工业连接器、连接线缆、PDU等。 4.机房消防设备维护管理：负责灭火剂的控制装置等的维护以及灭火器药剂的更换。 5.环境监控系统维护：负责所有机房环境监控系统的所有部件、监控平台软件的保养、维护。 6.机房电气系统维护：负责所有机房电器（照明、应急照明、开关、插座）保养、维护。 7.机房环境：清理机房的杂物，将机房物品定置；清洁机房门窗、地面。定期清洁电池室的地面；检查机房所有与外界的空洞是否已严密封堵，严密防鼠；检查机房玻璃、地板、天花板、通气口，墙体表面是否正常，外观是否完好，有否出现老化现象；检查机房是否有漏水现象；检查机房墙壁是否有渗水现象；填写巡检记录，有问题及时报告。 8.空调系统维护：负责所有机房精密空调系统室内外机组的所有部件、空调管线及单独布设的温湿度传感器的保养、维护，并负责两台华为精密空调的保养、维护、维修、更换等。 9.机房供水及排水水路、电路及照明线路的维护管理：水、电路管线及接口的检查。 10.机房基础维护管理：机柜线路的整理、标签检查更换、机房除尘清洁及有关配套的维护管理。 11.机房主机设备维护管理：负责网络设备（路由及交换设备等）的维护、管理、维修、更换等。 12.机房运行维护管理体系建设：完善机房运行维护规范，优化机房运行维护体系。 13.防雷接地维护：定期检查接地系统，防止接地系统腐蚀，确保接地系统连接可靠性，规范接地系统布线，定期测量接地电阻，防止雷击危害。 14.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、应急处置等工作，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，建立协同联动的网络安全监测与通报机制，及时处置安全事件，提升电子政务外网网络安全防护和应急处置能力。 15.将分散在各个机房的动环监测设备统一接			

序号	服务名称	服务要求	单位	数量	备注
		入监控调度中心，设备包括但不限于温湿度传感器、烟雾探测器、门禁系统、UPS电源等，实现全天候24小时的专业化监控，通过集中化、智能化的监测手段，确保机房动力环境系统的稳定运行，提高故障响应速度和处置效率，从而保障整个IT基础设施的可用性和安全性。 16.提供所有机房视频监控维护服务，确保监控系统稳定运行，实时保障行政中心安全，服务涵盖视频监控设备的日常巡检、故障排查、维修更换等，同时提供统一汇聚解决方案，实现监控数据的集中管理和高效分析。 17.提供机房门禁出入记录服务，可实时记录人员出入情况，为机房安全管理提供有力数据支撑，大幅增强机房安全防护能力。 备注：1号机房是指行政中心1#楼1楼101，2号机房是指1#楼负1楼A05，3号机房是指4#楼4楼421，4号机房是指4#楼4楼417，5号机房是指6#楼4楼401，6号机房是指6#楼1楼123，1号机房监控室是指行政中心1#楼1楼103。			
2	电子政务外网完善的售后服务	1.金昌市电子政务外网广域网纵向贯通省市、县的全省统一网络基础平台，提供市、县/区各提供≥2台广域网核心路由器服务，负责开通电子政务外网业务。广域网核心路由器节点具备双核心设备，区/县级通过双链路、≥1000M带宽上联至市广域网核心路由器骨干节点，市级通过双链路、万兆带宽上联至省广域网核心路由器骨干节点，充分保障广域网骨干网络的可靠稳定性。 2.金昌市电子政务外网城域网总体网络架构具备高扩展性的双星型架构，核心路由交换区提供≥2台城域网核心路由器和2台高性能核心交换机服务，负责城域网内互联以及数据路由转发。同时为保证各市级单位接入电子政务外网的便捷性，考虑未来网络灵活扩展性，在每个市级单位及有需求的二级单位提供接入网关服务，用于各部门、单位的接入。 3.安全接入区服务，提供防火墙、入侵检测、沙箱、VPN网关等，实现无线城域网接入的安全保护服务。 4.互联网接入区服务，具备双链路上联至运营商，通过链路负载均衡设备和集中NAT技术方式进行互联网访问。根据等级保护基本要求，电子政务外网互联网出口设备需具备高性能防火墙作为出口的安全隔离设备，隔离互联网	项/年	1	

序号	服务名称	服务要求	单位	数量	备注
		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≥3个月的日志。因此，互联网出口区域还需部署上网行为管理设备实现对内部用户访问互联网的上网行为进行监控、日志进行记录。 5.提供电子政务外网市广域网核心节点到省广域网核心节点≥10G出口链路专线运维服务、市广域网核心节点到县广域网核心节点专线运维服务及市广域网核心节点到区广域网核心节点主干链路运维服务，并确保线路线路质量稳定可靠。 6.提供7*24小时提供电话或网络报障服务，能够提供包括重大故障及事件预警。如由于线路检修、设备搬迁、工程割接、网络及软件升级等可预见的原因，影响或可能影响市级部门、单位使用该光纤电路接入服务的，应至少提前48小时告知采购人并提供相关预案。在接到市级各部门、单位网络故障申报后，需在4小时内解决，并给予处理报告。 7.支撑金昌市电子政务外网有线网络服务项目设备及设施必须满足附件二相关参数要求。			
3	驻场服务	提供三人以上专属驻场服务团队驻场式服务，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，驻场人员必须能够熟练操作所有设施设备，能及时有效处理各类故障，需为驻场人员购买意外伤害保险等人身保险及社会保险。	项/年	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。

3、驻场服务：提供三人以上专属驻场服务团队驻场式服务，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，驻场人员必须能够熟练操作所有设施设备，能及时有效处理各类故障，需为驻场人员购买意外伤害保险等人身保险及社会保险。

附件 1：

支撑金昌市电子政务外网有线网络服务政府采购服务项目

设备参数清单

序号	设备名称	技术要求	单位	数量	备注
一、网络专线接入服务					
（一）市广域网内容					
1	市广域网核心路由器	提供高性能市广域网核心路由器，需满足：1.设备支持100GE、50GE、40GE、25GE、10GE、GE、FE、E1、POS、CPOS等接口类型；2.支持bras双机热备场景，设备升级其中一台，另一台需能正常工作，用户不下线；3.IPv4、Ipv6路由及转发表容量要求：支持IPv4路由表容量≥25M,IPv6路由表容量≥10M，支持IPv4转发表容量≥4M,IPv6转发表容量≥2M；4.支持独立NAT板卡；支持10G端口支持网络硬切片（FlexE）；5.支持随业务流的检测技术，实现基于IP五元组筛选追踪业务流，进行实时检测，精准定位到故障点，丢包、误码类故障，确保业务性能；6.关键芯片(包括但不限于CPU、NP、TM、TCAM、FIC及交换芯片)具备自研国产化芯片；7.冗余主控，冗余交流电源，≥20个万兆/千兆光接口，交换容量≥130Tbps，转发性能≥25000Mpps；8.支持根据不同的网络服务要求如时延、带宽、安全性和可靠性等来划分切片网络，应对不同的网络应用场景。	台	2	
2	县区广域网核心路由器	提供区县广域网核心路由器，永昌县、金川区各部署≥2台，需满足冗余主控，冗余交流电源，≥20个万兆/千兆光接口；交换容量≥130Tbps；转发性能≥25000Mpps；支持独立NAT板卡；支持10G端口支持网络硬切片（FlexE）。	台	4	
3	广域网万兆单模光模块	提供广域网万兆单模光模块，满足光模块-SFP+-10G-单模模块(1310nm,10km,LC)要求。	个	12	
4	广域网万兆多模光模块	提供广域网万兆多模光模块，满足光模块-SFP+-10G-多模模块(850nm,0.3km,LC)要求。	个	36	
5	广域网千兆单模光模块	提供广域网千兆单模光模块，满足光模块-eSFP-GE-单模模块(1310nm,10km,LC)要求。	个	40	
（二）市级城域网内容					
1	城域网边界防火墙	提供城域网边界防火墙服务做边界隔离连接各区域，需满足≥48个万兆光口，≥6个40G光口，冗余引擎，冗余交流电源；吞吐量≥80Gbps，最大并发连接数2400万，每秒新建连接数≥80万，并提供服务期内免费IPS、AV、URL等特征库升级服务。	台	2	

序号	设备名称	技术要求	单位	数量	备注
2	城域网核心路由器	提供城域网核心路由器实现核心层全冗余和高速连接，确保核心层稳定可靠高效地运行，城域网核心路由器需满足冗余主控，冗余交流电源，冗余主控，冗余交流电源，≥20个万兆/千兆光接口，≥6个40/100G光口；交换容量≥130Tbps；转发性能≥25000Mpps；支持独立NAT板卡；支持≥10G端口支持网络硬切片（FlexE）。	台	2	
3	城域网核心交换机	提供城域网核心交换机上联城域网核心路由器，需满足：1.冗余主控、冗余交换网板、冗余交流电源，≥96个万兆/千兆光口，≥12个不少于40G光口，≥4根不少于3米高速堆叠电缆；交换容量≥500Tbps，包转发率≥96000Mpps；3.支持独立的硬件监控模块,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；4.支持整机MAC地址≥1M,支持ARP表项≥384K;5.支持IPv4路由转发表FIB规格≥3M，支持Ipv6路由转发表FIB规格≥1M；6.支持硬件BFD/OAM，3.3ms稳定均匀发包检测，提高设备的可靠性；7.支持真实业务流的实时检测技术，实现对IP网络的精确丢包监控和快速故障定界能力。	台	2	
4	市级城域网探针	提供市级城域网探针旁挂城域网边界防火墙，需满足6G检测能力，≥16个千兆电口，≥6个千兆光口，≥6个万兆光口，交流供电，≥1T硬盘，≥4个万兆多模光模块，并提供服务期内免费威胁防护服务。	台	1	
5	市级各部门、单位接入防火墙	提供市级各部门、单位接入防火墙，需满足：1.≥12个千兆电口+8个千兆光口+4个万兆光口，冗余交流电源，≥240G固态硬盘，吞吐量≥20Gbps，并发连接数≥800万，每秒新建连接数≥20万，并提供服务期内免费威胁防护（IPS、URL、AV，云沙箱检测功能）功能授权；2.支持每IP，每用户的最大连接数限制，防护服务器；3.支持DNS过滤，提高WEB网页过滤的性能；4.支持恶意域名过滤，实现对C&C进行阻断；5.要求防火墙具备AI引擎，AI引擎用于恶意C&C流量检测；6.支持Portal页面定制及调查问卷。	台	2	
6	市级各部门、单位接入汇聚交换机	提供市级各部门、单位接入汇聚交换机，需满足：1.≥48个万兆/千兆光口+240个千兆光口，冗余交流电源，4根高速堆叠电缆，交换容量≥85Tbps，包转发率≥57600Mpps；2.支持真实业务流的实时检测技术，秒级快速故障定位；3.支持硬件BFD/OAM，3.3ms稳定均匀发包检测，提高设备的可靠性。	台	2	
7	市级各部门、单位接入探针	提供市级各部门、单位接入探针旁挂市级各部门、单位接入防火墙，需满足6G检测能力，≥16个千兆电口，≥6个千兆光口，≥6个万兆光口，交流供电，≥1T硬盘，≥4个万兆多模光模块，并提供服务期内免费威胁防护服务。	台	1	

序号	设备名称	技术要求	单位	数量	备注
8	59段市级各部门、单位接入交换机	为市级各部门、单位提供59段接入交换机，需满足1.≥48个千兆光口，≥4个万兆光口（非复用接口），交流供电，≥48个千兆单模光模块，≥4个万兆多模光模块；2.交换容量≥2.72Tbps，包转发率≥780Mpps；3.支持MAC地址规格≥32K；4.支持Ipv4路由FIB表≥8K，Ipv6路由FIB表≥4K。	台	1	
9	市级各部门、单位接入网关	提供市级各部门、单位接入网关，需满足≥5个千兆电口+4个千兆光口，交流供电，整机交换容量≥20Gbps，转发性能≥9Mpps。	台	200	
10	市行政中心楼层接入交换机	提供市行政中心楼层接入交换机，需满足1.≥48个千兆电口+4个千兆光口（非复用接口），交流供电；2.交换容量≥400Gbps，包转发率≥80Mpps；3.支持MAC地址≥32K，支持ARP表项≥4K。	台	30	
11	市级城域网40G单模光模块	提供市级城域网40G单模光模块，需满足40GBase-ER4光模块-QSFP+-40G-单模模块(1310nm,40km,LC)要求。	个	12	
12	市级城域网40G多模光模块	提供市级城域网40G多模光模块20个，需满足40GBase-eSR4光模块-QSFP+-40G-多模模块(850nm,0.3km,MPO)(可对接4个SFP+)要求。	个	20	
13	市级城域网万兆单模光模块	提供市级城域网万兆单模光模块，需满足光模块-SFP+-10G-单模模块(1310nm,10km,LC)要求。	个	24	
14	市级城域网万兆多模光模块	提供市级城域网万兆多模光模块，需满足光模块-SFP+-10G-多模模块(850nm,0.3km,LC)要求。	个	60	
15	市级城域网千兆单模光模块	提供市级城域网千兆单模光模块，需满足光模块-eSFP-GE-单模模块(1310nm,10km,LC)要求。	个	500	
16	市级城域网千兆多模光模块	提供市级城域网千兆多模光模块，需满足光模块-eSFP-GE-多模模块(850nm,0.55km,LC)要求。	个	80	
二、网络安全服务					
（一）安全接入区内容					
1	安全接入区路由器	提供安全接入区路由器，需满足1.双主控，双交流电源，≥10个万兆/千兆光接口+10个千兆光接口；2.支持交换容量≥110Tbps,支持包转发率≥14000Mpps;3.设备支持100GE、50GE、40GE、25GE、10GE、GE、FE、E1、POS、CPOS等接口类型；4.支持MACSec加密技术；5.10G端口支持网络硬切片（FlexE）。	台	2	
2	安全接入区防火墙	提供安全接入区防火墙，需满足≥12个千兆电口+8个千兆光口+4个万兆光口，冗余交流电源；≥240G固态硬盘，吞吐量≥20Gbps，并发连接数≥800万，每秒新建连接数≥20万，并提供服务期内免费威胁防护（IPS、URL、AV，云沙箱检测功能）功能授权。	台	2	

序号	设备名称	技术要求	单位	数量	备注
3	安全接入区VPN设备	提供安全接入区VPN设备，需满足≥12个千兆电口+12个万兆光口+2个40G光口，冗余交流电源，≥240G固态硬盘，提供服务期内免费特征库升级服务，并发SSLVPN≥2000用户，吞吐量≥30Gbps，并发连接数≥1200万，每秒新建连接数≥40万。	台	2	
4	安全接入区探针	提供安全接入区探针，需满足3G检测能力，≥16个千兆电口，≥6个千兆光口，≥6个万兆光口，交流供电，≥1T硬盘，≥4个万兆多模光模块，并提供服务期内免费威胁防护服务。	台	1	
5	安全接入区入侵防御	提供安全接入区入侵防御，需满足≥8个千兆COMBO+4个千兆电口+10个万兆光口，冗余交流电源，IPS检测吞吐量≥18Gbps，每秒新建连接数≥50万，并发连接数≥2000，并提供服务期内免费特征库升级服务License。	台	1	
6	安全接入区沙箱	提供安全接入区沙箱，含配套服务器，冗余电源，≥8个千兆电（1个千兆管理接口、3个千兆备用接口、4个千兆监听接口）+2*10GE光口；高性能APT威胁检测系统，可以精确识别未知恶意文件渗透和C&C恶意外联。通过直接还原网络流量并提取文件或依靠下一代防火墙提取的文件，在虚拟的环境内进行分析，实现对未知恶意文件的检测。	台	1	
7	安全接入区万兆多模光模块	提供安全接入区万兆多模光模块，需满足光模块-SFP+-10G-多模模块(850nm,0.3km,LC)要求。	个	30	
8	安全接入区千兆单模光模块	提供安全接入区千兆单模光模块，需满足光模块-eSFP-GE-单模模块(1310nm,10km,LC)要求。	个	6	
（二）互联网接入区内容					
1	互联网接入区链路负载均衡	1.提供互联网接入区链路负载均衡，需满足：1.≥14个千兆电口，≥8个千兆光口，≥8个万兆光口，≥480G固态硬盘，冗余交流电源，L4吞吐量≥40Gbps，4层新建≥60W，7层新建≥65W，并发会话数≥2000万；2.支持基于管理员自定义的时间计划来配置出站访问的链路调度策略；3.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；4.通过ICMP、TCP、DNS等方式，检验SNAT地址池中的地址有效性，避免出口SNAT池中地址被意外封杀后仍然被使用造成网络访问中断；5.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；6.支持基于TCP、HTTP的被动健康检查，通过监控链路中的重置、重传、错误应答码等信息判断服务器的健康状态；7.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；8.支持中文界面管理，支持具备命令行，而非Linux命令，对设备进行功能配置。	台	2	
2	互联网接入区抗Ddos设备	提供互联网接入区抗Ddos设备，需满足≥8个千兆combo口+6个万兆光口，冗余电源，≥20G流量清洗能力，含配套服务器；实时防御流量型攻击和应用层攻击。	台	2	

序号	设备名称	技术要求	单位	数量	备注
3	互联网出口防火墙	提供互联网出口防火墙，需满足≥12个千兆电口+12个万兆光口+2个40GE光口，冗余交流电源，≥240G固态硬盘，吞吐量≥40Gbps，并发连接数≥1200万，每秒新建连接数≥40万，并提供服务期内免费IPS、AV、URL、云沙箱等特征库升级服务。	台	2	
4	互联网接入区汇聚交换机	提供互联网接入区汇聚交换机，需满足≥24个万兆光口+24个千兆光口，冗余主控，冗余交流电源，1根万兆堆叠线缆；交换容量≥18Tbps，包转发率≥26000Mpps。	台	2	
5	互联网接入区探针	提供互联网接入区探针，需满足≥6G检测能力；≥16个千兆电口，≥6个千兆光口，≥6个万兆光口，交流供电，≥1T硬盘，≥4个万兆多模光模块，提供服务期内免费威胁防护服务。	台	1	
6	互联网接入区防病毒网关	1.提供互联网接入区防病毒网关服务，含显示屏，冗余电源，≥4个万兆光口，≥4个千兆光口，≥6个千兆电口（含光模块），网络层吞吐≥20G，防病毒吞吐≥12G，最大并发会话数≥400万，每秒新增会话数≥20万，对利用HTTP、SMTP、POP3、FTP、IM等多种协议进行传播的病毒进行扫描，完成对木马病毒、蠕虫病毒、宏病毒、脚本病毒等的查杀，同时支持多线程并发控制、深层次压缩文件杀毒、病毒白名单等功能，提供服务期内免费特征库升级；2.策略匹配时有极高的匹配效率，并经过相关机构的检测证明，基本信息只需统一匹配一次，不用每个上层策略都匹配一次，提高网络数据流的转发、规则匹配的性能；3.支持对1600+种应用平台及2500+种的应用进行识别和控制，至少支持5大类，比如：商业系统、协作应用、一般网络应用、媒体等及≥28子类，比如：认证服务、数据库、ERP-CRM、软件更新、电子邮件、VOIP视频、游戏等。	台	2	
7	互联网接入区入侵防御系统	提供互联网接入区入侵防御系统服务，需满足≥8个千兆COMBO+4个千兆电口+10个万兆光，冗余交流电源，IPS检测吞吐量≥18Gbps，每秒新建连接数≥50万，并发连接数≥2000，提供服务期内免费特征库升级服务License。	台	1	
8	互联网接入区上网行为管理	提供互联网接入区上网行为管理，需满足≥12个千兆电口+12个千兆光口，含1对Bypass，≥4个万兆光口，≥1T硬盘，包含管理软件；冗余交流电源；网络吞吐量≥40Gbps，应用性能≥5Gbps，最大并发连接数≥1000万，最大用户数≥20000。提供服务期内免费特征库升级许可。	台	1	
9	互联网接入区网络流量分析系统	提供互联网接入区网络流量分析系统，需满足1.冗余电源，机架式设备，含液晶屏，接口≥4千兆电口+4千兆光口+2万兆光口，吞吐量≥5G，并发≥300万，异常流量的检测、流量统计分析等，提供服务期内免费版本与特征库升级许可；2.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；3.配置空路由牵引时，每个BGP支持配置≥5个community名称，用于多出口场景下实现空路由。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；4.攻击事件支持对Top源IP、Top端口、Top接口、Top协议、Top源AS、Top源子网以及TOPtcpflag进行监控数据呈现。	套	1	

序号	设备名称	技术要求	单位	数量	备注
10	互联网接入区万兆多模光模块	提供互联网接入区万兆多模光模块，满足光模块-SFP+-10G-多模模块(850nm,0.3km,LC)要求。	个	40	
11	互联网接入区千兆单模光模块	提供互联网接入区千兆单模光模块，满足光模块-eSFP-GE-单模模块(1310nm,10km,LC)要求。	个	8	
12	互联网接入区千兆多模光模块	提供互联网接入区千兆多模光模块，满足光模块-eSFP-GE-多模模块(850nm,0.55km,LC)要求。	个	10	
（三）安全运维管理区内容					
1	安全运维管理区边界防火墙	提供安全运维管理区边界防火墙，需满足≥12个千兆电口+12个万兆/千兆光口+2个40GE光口，冗余交流电源；≥240G固态硬盘；吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万，提供服务期内免费IPS、AV、URL、云沙箱等特征库升级服务。	台	2	
2	安全运维管理区接入交换机	提供安全运维管理区接入交换机，需满足≥96个万兆光口，冗余主控,冗余交流电源,4根高速堆叠电缆;交换容量≥85Tbps，包转发率≥26000Mpps。	台	2	
3	安全运维管理区网络安全态势感知系统	提供安全运维管理区网络安全态势感知系统服务，含服务器，冗余电源，≥10Gbps流量处理能力；具备最新大数据分析和智能学习技术，从海量数据中提取关键信息，通过多维度风险评估，具备大数据分析方法关联单点异常行为，从而还原出APT攻击链，准确识别和防御APT攻击，能够对攻击链进行可视化呈现、展示全网安全态势、提供威胁报表等，展示资源侦查、外部渗透、命令与控制、内部扩散、数据外发等APT攻击过程，感知全网威胁态势、攻击路径、高危资产等信息，帮助快速掌控全网威胁，感知全网威胁态势，避免核心信息资产损失。提供全市政务新媒体安全监测服务。	套	1	
4	安全运维管理区日志审计系统	提供安全运维管理区日志审计系统，需满足：1.含服务器，冗余电源，≥6个千兆电口，≥4个千兆光口，≥1个console口，≥3*4T硬盘；≥200日志源，提供服务期内免费维保服务与特征库升级license；2.系统应支持规则自适应日志接入，应支持将新接收的日志信息与系统内置规则、自定义规则进行匹配，完成自动接入;3.系统应能够对主机日志展开深度分析，分析场景包括但不限于登录情况、用户核心文件/文件夹监控、敏感操作及异常外联;4.系统应提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源IP信息.	套	1	
5	安全运维管理区安全准入平	提供安全运维管理区安全准入平台，含配套服务器，≥3000个接入终端管理授权；网络管理控制系统，是集管理、控制、分析和AI智能功能于一体的网络自动化与智能化平台。	套	1	

序号	设备名称	技术要求	单位	数量	备注
	台				
6	安全运维管理区网络管理平台	提供安全运维管理区网络管理平台，需满足：1.配套服务器，≥700个网络设备管理，提供交换机、防火墙等多种设备的统一管理，支持多厂商设备统一视图、资源，拓扑、故障、性能以及智能配置功能；2.场景化模版建网，支持快速复制到其他站点，满足小型网络不同的行业场景；3.支持内置CA服务器，满足企业CA运维管理，如个人证书颁布、挂失和过期处理，该个人证书可以作为网络准入认证身份源；4.支持用户业务随行，将用户和IP解耦，帐号即用户，根据用户登录条件（5W1H）授权安全组，基于UCL的策略矩阵，实现用户权限互访限制，满足随时随地接入网络业务权限一致。	套	1	
7	安全运维管理区安全管理中心	提供安全运维管理区安全管理中心，含机架式硬件设备，冗余交流电源，≥4千兆光口+4千兆电口，≥3*2T硬盘，可管理设备≥500台，日志处理性能≥12000条/秒；链接短信告警平台，实现日志统计告警结果短信通知，进行设备状态监控、设备管理、设备升级、策略下发、日志查询、报表统计、虚拟化设备集中授权等功能。	套	1	
8	安全运维管理区漏洞扫描系统	提供安全运维管理区漏洞扫描系统，需满足1.≥6个千兆电口+4个千兆光口，内存≥8G，硬盘≥1T，并发扫描数≥150个IP地址，最大扫描速度≥2000ip/h，最大并发任务数≥50，支持多路扫描，满足在复杂环境中部署的要求，支持不同网段同时检测的需求；2.支持授权IP数无限；3.发现信息系统存在的安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。支持分布式部署，提供服务期内免费特征库升级服务；4.为了漏洞扫描检测漏洞的全面性，支持检测的漏洞数大于250000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq标准。	套	1	
9	僵木蠕检测系统	提供僵木蠕检测系统，检测通过网页、电子邮件或文件共享方式试图进入企业网络的病毒、蠕虫、木马，以及高级恶意软件、APT威胁和勒索软件，冗余电源，≥4个万兆光口+4个千兆光口+4个千兆电口（含光模块），网络吞吐量≥5Gbps，最大并发连接数≥500W，文件处理数≥12万/天，硬盘≥1TBSATA，通过行为特征库检测引擎、流式病毒检测引擎、静态文件分析引擎、动态沙箱检测引擎、威胁情报等多种技术手段，实现了对恶意样本文件的还原、检测、保存、上报以及特征分发等全部能力；提供服务期内免费特征库升级服务。	套	1	
10	安全运维管理区杀毒软件系统	提供安全运维管理区杀毒软件系统，含配套服务器，杀毒软件客户端授权2000个终端授权，提供服务期内免费特征库升级。	套	1	

序号	设备名称	技术要求	单位	数量	备注
11	安全运维管理区堡垒机	提供安全运维管理区堡垒机，需满足：1.具备液晶屏，≥4个千兆电口，≥2TSATA硬盘，1个网络接口扩展槽，字符并发会话数≥300，图形并发会话数≥700，可管理设备数≥200台，系统对运维人员维护过程进行全面跟踪、控制、记录、回放，支持细粒度配置运维人员的访问权限，实时阻断违规、越权的访问行为，同时提供维护人员操作的全过程的记录与报告，实现运维过程的事前预防、事中控制、事后审计的严格管控；2.具有用户角色权限自定义功能，可对用户进行细粒度权限划分，可细分用户录入管理员，设备录入管理员，设备账号管理员，运维权限管理员，运维审批管理员，运维审计管理员，普通运维人员和审计员（提供配置界面截图证明并加盖公章）；3.支持划分多级组织架构（至少10个层级），不同层级有独立的用户管理，用户角色管理，资产管理，密码管理、策略管理、审计管理的权限角色，支持不同角色相互组合（提供配置界面截图证明并加盖公章）；4.用户登录堡垒机支持多种认证方式，包括本地静态密码认证、LDAP认证、RADIUS认证、USBKEY认证、PIN+软件OTP、短信认证、企微认证、钉钉认证、OAuth2.0等身份认证方式；支持可知因素和不可知因素的双因素认证；5.支持可通过参数配置开启或关闭字符、图形、文件等协议运维行为审计，但不影响对应协议的会话审计，防范涉密运维行为泄露。	台	1	
12	安全运维管理区运维笔记本电脑	提供安全运维管理区运维笔记本电脑，需满足≥14.2英寸显示屏，正版≥Windows10专业版，≥16G内存，≥512G固态硬盘，CPU≥i5-12500H四核处理器（含鼠标、键盘）。	台	1	
13	安全运维管理区二合一电脑	提供安全运维管理区运维笔记本平板二合一电脑，需满足≥13英寸显示屏，正版≥Windows10专业版，≥16G内存，≥256G固态硬盘，CPU≥i5-1135G7四核处理器（含鼠标、键盘、触控笔）。	台	2	
14	安全运维管理区运维终端	提供安全运维管理区运维终端，需满足i5-9400F及以上处理器，内存≥8G，硬盘≥256GSSD+1TSATA硬盘，≥2G独显，≥23英寸显示器。	台	3	
15	安全运维管理区运维平板电脑	提供安全运维管理区运维平板电脑，需满足≥10.8英寸显示屏，≥8G内存，≥256G存储容量。	台	3	
16	安全运维管理区会议平板电脑	提供安全运维管理区运维平板电脑，需满足≥11英寸显示屏，≥12G内存，≥256G存储容量。	台	1	
17	安全运维管理区KVM	提供安全运维管理区KVM，需满足屏幕规格≥19英寸，接口数≥16口；网卡≥1个RJ-45；连接线VGA线。	台	2	
18	安全运维	提供安全运维管理区万兆多模光模块，需满足光模块	个	50	

序号	设备名称	技术要求	单位	数量	备注
	管理区万兆多模光模块	-SFP+-10G-多模模块(850nm,0.3km,LC)要求。			
三、运营维护服务-市行政中心机房环境优化内容					
1	UPS主机	模块化在线式双变换式主机，配置≥3个不少于50KVA功率模块（2+1），支持热插拔，冗余控制模块，具备集中旁路方式，旁路模块支持热插拔。	台	1	
2	锂电池机柜（主柜）	电池模组具备模块化设计，支持可插拔，且支持靠墙、背靠背安装；电池柜内单个电池模块故障，剩下电池模块支持串联后继续运行，不影响业务；整机满足抗震≥8级烈度；锂电柜配备≥7寸的LCD屏幕，且锂电柜可监控并显示单体电芯温度、电压、SOH/SOC等数据、电池模块数据、电池柜数据、系统数据。	个	1	
3	锂电池机柜（辅柜）	电池模组具备模块化设计，支持可插拔，且支持靠墙、背靠背安装；电池柜内单个电池模块故障，剩下电池模块支持串联后继续运行，不影响业务；整机满足抗震≥8级烈度。	个	3	
4	电池储能模块	≥64V,≥40Ah；电池柜内单个电池模块故障，剩下电池模块支持串联后继续运行，不影响业务；电芯具备过放电、过充电、外部短路、挤压、重物冲击、机械冲击、加热、跌落等可靠性测试；电芯具备针刺测试。	个	56	
5	市电输入柜	主路输入（不低于以下配置）：630A，带自动切换开关，400A维修旁路。主路输出1路400A/3P，2路250A/3P，2路160A/3P，4路40A/3P,4路16A/1P。	个	1	
6	UPS输出柜	主路输入（不低于以下配置）：2*400A，≥400A维修旁路。主路输出2路250A/3P，2路160A/3P。	个	1	
7	配电柜	支持两路市电输入；具有防雷开关或防雷器故障指示的微动开关，以便远程监控防雷状态。≥2个63A/3Pups输出空开，≥14个40A/3P机柜电源空开，≥2个40A/3P空调电源空开。	个	1	6号楼汇聚机房
8	UPS主机	UPS主机容量≥20kVA，高频在线双变换式UPS，具备≥IGBT整流，功率变换器和系统元件均由DSP控制。输出功率因数≥0.9。输入额定电压，满载运行时，UPS设备输入功率因数应≥0.99。整机最高效率≥95%。逆变过载能力≥5分钟（125%额度电流），1分钟（150%额定电流）。具有声光告警功能，具备LCD屏幕显示，便于操作，界面显示输出，市电模式，负载容量，电池模式，电池容量，市电，逆变，旁路，故障状态。支持风扇故障预警、电容器故障预警、电池故障预警。支持电池组共用，电池节数32-40节可调。防雷能力：交流输入端满足5kA防雷和6kV防浪涌。	台	1	6号楼汇聚机房
9	蓄电池	阀控式密封免维护铅酸蓄电池，≥12V，≥100AH。	只	32	6号楼汇聚机房
10	电池柜	配套电池柜。	个	1	6号楼汇聚机房

序号	设备名称	技术要求	单位	数量	备注
11	精密空调	风冷级精密空调，上送风，总冷量≥13KW，风冷量≥11KW，风量≥3000m^3/h，具备R410A制冷剂；具备低功耗加湿系统，加湿量2kg/h；室内机具备高效工业用直流变频涡旋压缩机；EC风机；蒸发器具备“V”型；室外机风机驱动具备变频调速器；精密空调具备电子膨胀阀。	台	2	
12	动力环境管理系统	机架式服务器：CPU主频≥2.0GHz，核数≥16Core；DDR4内存≥32GB；硬盘≥2*1200GBSAS2.5“HDD；Raid卡；双网卡，每块网卡≥4*GE电口；冗余交流电源软件平台：统一动力环境管理平台，实现对配电、UPS、精密空调、视频监控、温湿度、烟雾、水浸等设备和环境进行集中监控和管理；基于Web的远程管理功能，通过短信、Email告警方式，实现机房安全无人职守；要求系统软件具备B/S架构，服务器具备Linux操作系统；客户端软件基于IE浏览器；数据中心管理系统具备高安全设计，着重对操作系统、数据库、管理软件进行加固，可有效防御窃听、伪造、篡改、越权访问、病毒、网络入侵等危害动作，避免管理系统服务器成为用户网络中的安全短板，并提供3种以上主流杀毒软件的扫描报告。系统应提供南向集成接口，可支持接入各个监控子系统，支持的接口类型必须包括但不限于：SNMP、Modbus-TCP、电信C接口、BACnet、跨平台的API接口。系统须具有开放性，要求支持的接口协议包括但不限于：Webservice、API、SNMP、Modbus、BACnet、电信C接口。短信猫，网络制式：支持4G，5G，无线GPRS-48Kbp，USB供电，移动APP运维。	套	1	
13	动力环境采集器	用于非标信号的采集处理，转化为SNMP协议上传到服务器处理，采集器支持Web访问。	台	5	
14	交换机	≥24个10/100/1000Base-T太网端口，4≥个复用的千兆ComboSFP，≥4个万兆SFP+，PoE+，冗余交流电源。	台	5	