标的名称、服务范围、服务要求及服务标准

序号	标的的名称	所属行业	数量及单位	技术要求
一、机房优化改造集成服务				
1	机房空调系统优化改造服务	其他未列明行业	1 项	1.对机房现有机柜、桥架、地板的各类线缆进行梳理、打标签等服务。 2.每季度开展一次机房供配电、防雷、动环等配套设施的巡检维保服务，并对发现的问题进行优化改造。 3.对机房 2 台恒温恒湿机房精密空调每年开展一次清洗、更换雪种、故障配件更换、管线维护等服务，并对空调系统进行优化改造，优化改造后需满足以下要求： （1）总冷量≥12.5kW,显冷量≥11kW，显热比为 0.9,风量≥3000m3/h； （2）输入电压允许波动范围：380～415V±10%。 （3）温度调节范围：+18℃～+32℃； （4）精密空调由直流变频压缩机、EC 风机 、电子膨胀阀等主要部件组成； （5）精密空调可支持制冷量 30%~100%无极调节 ，按需输出冷量，大幅降低能耗； （6）机组应具备不低于 6kV 防雷滤波规格，在极端浪涌条件下更加安全可靠； （7）出厂预充冷媒，30m 以内的内外机连管长度无需添加制冷剂 ； （8）精密空调室外机换热器应采用平直翅片，不能采用开窗翅片，防止积灰脏堵，影响机组性能和可靠性； （9）精密空调控制器应采用 LCD 屏，依托物联网技术实现人机交互功能，支持温湿度曲线显示； （10）具备联动与群控功能，依托物联网技术实现同

				一区域可以将不低于 8 套机组进行统一控制管理； （11）应具有 RS485 接口，对系统进行远程巡检和参数的设置。 4.对机房 2 套供电系统进行优化改造，优化改造后需满足以下要求： （1）主机容量 20kVA，高频在线双变换式，采用 IGBT 整流，功率变换器和系统元件均由 DSP 控制； （2）输出功率因数 0.9； （3）兼容机架式/塔式安装； （4）输入输出制式为单相输入单相输出、三相输入单相输出或三相输入三相输出； （5）输入电压范围应不小于 L-N：80V-280Vac，输入频率范围不小于：40Hz~70Hz； （6）当输入额定电压，满载运行时，设备输入功率因数≥0.99； （7）输出电压稳压精度应小于 L-N：220V±1%。输出频率范围应不超出 50Hz±0.5%(电池逆变工作方式)； （8）整机最高效率不小于 95%； （9）逆变过载能力：5min（105%~125%额度电流），1min（125%~150%额定电流），100ms（≥150%额定电流）； （10）在市电和电池两种状态间切换的时间应为 0ms； （11）保护功能：具有输入频率异常保护功能，电池过压告警和过放电保护功能，高温自动切换旁路保护功能； （12）具有声光告警功能，采用 LCD 屏幕显示，便于操作，通过控制面板设置供电系统的工作电压和工作频率，查看供电系统的工作模式、负载大小、电池容

				量； （13）支持 SNMP、MODBUS、干接点卡扩展。 5.对 2 组供电系统电池组每年开展一次充放电服务，并进行优化改造，优化改造后需满足以下要求： （1）电池组按总负载 15KW 计算，单机配置 1 组 12V100AH 蓄电池，每组 32 节，可实现并机系统后备≥2 小时； （2）电池组蓄电池要求原厂研发生产，非 OEM 或 ODM 产品； （3）每个电池柜可安装 32 节 12V100AH 铅酸蓄电池，含电池内部连接电缆及开关； （4）输出配电箱功率 输入 125A/1P*2.输出 100A/1P*2； （5）开关采用国产品牌，配置防雷器。 6.对消防系统进行优化改造，优化改造后需满足以下要求： （1）对 6 个气瓶组完成 1 次送检、充气服务，并委托第三方对消防系统进行检测及出具报告。 （2）气瓶组容量为：70L 灭火剂瓶组 3 个、40L 灭火剂瓶组 2 个、90L 灭火剂瓶组 1 个。
二、安全服务				
1	网络安全运维服务	软件和信息技术服务业	1 项	通过对采集的数据进行安全分析与安全事件发现，及时感知用户网络系统中的安全事件并提出解决方案。交付成果包括但不限于：基于本地数据和云端威胁情报分析、APT 告警及可疑行为进阶分析、WEB 攻击检测、数据库恶意行为分析、登录动作检测、APT 告警进阶分、安全策略的部署、安全设备的使用等方面。具体服务内容如下： 1. 内部失陷检测服务

				①Webshell 检测，利用流量威胁检测分析服务工具，采用大数据分析技术和高级网络攻防模型，对流量事件进行分析和研判，快速分析出当前 WEB 网站是否已经被恶意者挂了 webshell。并且通过服务，分析出网站其他方面的 web 告警，例如：Webshell：网站 webshell 的数量，以及每个 webshell 的详细信息，例如 webshell 的路径、webshell 的类型、攻击者的来源和入侵者详细的行为（连接数据库信息、文件下载信息、SQL 执行记录、文件编辑、命令执行、文件上传和反弹 shell）等信息。已攻陷的数据库：网站已经被攻陷的数据库的数量，以及其相关的详细信息，包括：数据库的 IP、数据库名称、表名、类型和攻击者 IP 等信息。 ②Redis 检测,通过分析发现内部服务的 Redis 的数量和每个 Redis 的详细情况，包括：时间；源 IP；目的 IP；相关的操作（写文件）；文件名。 ③反弹 shell 检测，全流量威胁检测分析服务通过分析发现内部服务的反弹 shell 的数量和每个反弹 shell 的详细情况，包括：时间；源 IP；目的 IP；反弹执行的命令。 ④针对数据库的恶意操作检测，分析发现数据库的危险操作信息，例如 Drop 数据表等危险操作。并统计出一段时间内数据库危险操作的告警数量和危险数据库操作详细情况，包括：操作的源 IP；数据库所在 IP；数据库类型；操作时间；操作命令（触发条件）。 2.外部攻击检测服务 ①反序列攻击检测，通过分析发现内部服务的反序列攻击行为的数量和每个反序列攻击行为的详细情况，包括：时间；源 IP；目的 IP/端口。

				②WEB 攻击态势分析，通过流量分析，发现内部服务器受到攻击的总体情况。服务提供 WEB 整体攻击类型的态势分布、每种攻击手段的详细信息和攻击的结果（攻击告警、攻陷和提示）。攻击手段包括但不限于：Webshell；黑产菜刀扫描；Web 漏洞扫描；Struts2 攻击；上传攻击；Sql 注入攻击；信息泄露；网站新增文件。 ③口令爆破攻击检测，提供内部服务器的精准口令爆破等行为的发现，主要包括针对不同服务器每日遭受口令爆破的攻击次数、服务的类型、邮件暴露攻击的详情、远程管理服务爆破攻击的详情和数据库服务爆破攻击的详情。主要的内容包括攻击来源 IP、目的 IP、协议、60 秒内攻击的次数、爆破结果。 3.内部违规检测服务 ①暴露面检测，利用大数据分析工具，分析出当前网络内的非法攻击面的信息，主要包括：攻击面的统计信息：各种开放端口的统计信息；新增攻击面信息；攻击面变更信息；攻击面的详细信息（服务器 IP、端口、服务类型）。 ②非法外联，提供环境内详细的非法外联信息，包括非法外联的目的 IP 物理地址、非法外联事件的历史趋势、以及非法外联事件的详细时间、源 IP、目的 IP、端口等信息。源 IP、目的 IP、端口等信息。 ③恶意 DNS 分析发现，提供内部网络请求的 DNS 监控与分析，并结合云端威胁情报，分析出内部 DNS 的信誉度情况，主要是发现内部存在的恶意 DNS 的请求，并给出详细的信息，包括：请求的时间、源 IP、请求的恶意域名、域名所在物理地址等信息。 ④ACL 梳理，分析出当前网络内现有的所有 IP 的访问

				关系，包括源 IP 到目的 IP 不同端口的访问关系。分析出网络内混乱的 ACL 管控,通过对内部不合理的 ACL 处置，降低环境内受攻击的风险。 ⑤弱口令，通过主动和被动的方式分析发现内部服务器的弱口令的状态，主要报告弱口令总数、被动统计发现的次数、字典匹配发现的次数和主动发现的次数。邮件服务、远程管理服务和数据库服务弱口令的详细信息包括：受影响的账号、弱口令、受影响的服务器、协议和检测到的时间。 ⑥异常登录，可以发现内部服务器的异常登录行为，主要包括：外部登录内部服务器异常详细情况（外部 IP、IP 归属地、内部服务器 IP、协议、访问时间）、异地登录详细情况（用户、常用登录地点、异地登录地点和发现的时间）、非工作时间登录详细情况（来源 IP、IP 归属地、目的 IP、协议和访问时间）等。 ⑦非常规服务分析 全流量威胁检测分析服务提供内部非常规服务的检测和发现，例如远程控制服务、代理服务等。降低内部服务器被攻击的风险和几率。服务包括：RegeoryTunnel 服务检测和发现、HTTP 代理检测和发现、SOCKS 代理检测和发现、Teamview/IRC 检测和发现。详细信息主要包括：连接服务的时间、连接服务的源 IP、连接服务的目的 IP 和服务类型（上述四种服务类型）。 4.事件分析研判溯源服务 ①事件研判，通过发现攻陷事件、WEB 攻击事件、内部异常等信息后，全流量威胁检测分析服务工程师利用网络渗透经验，并结合云端威胁情况，对事件性质是否是真的恶意攻击行为作出判断。并且追溯事件的产

				生原因、以及提出防范和处置建议。 ②事件溯源，利用云端威胁情报和开源社区情况，对一些恶意的攻击事件进行追踪和溯源，帮助找到事件的始作俑者。溯源的主要信息包括攻击者的物理位置、攻击者的行为证据留存和攻击者常用的攻击手段。同时借助工作短信、电话、邮件、移动工作群组将安全事件详情告知给相关电子政务系统的负责人员，并一同协助整改。 5.安全设备的使用与维护：根据工作计划和要求对采购人的网络安全设备进行使用和策略优化调整，具体包括： ①防火墙、WAF、IPS、VPN、上网行为管理与审计、日志管理与审计系统、数据库审计系统、网闸、虚拟化安全管理系统等安全工作的使用操作及安全策略优化。 ②堡垒机的用户建立、策略调整及关键基础设备和核心系统的定期改密。 6.安全加固服务：通过部署对信息系统的安全防护，全面分析用户目前运行的信息系统存在的安全隐患和面临的脆弱性漏洞，有针对性的设置合理的安全策略，从而全面提升系统对 DDOS、SQL 注入、跨站脚本、恶意文件上传、恶意代码、网页篡改等攻击。 7.安全检查：根据采购人的要求，配合采购人完成相关行政监管部门（公安、网信）对采购人关键信息基础设施、网络安全执法检查等网络安全检查。 8.安全制度完善:以 ISO27001 标准、网络安全等保 2.0 基本要求等标准规范为指导，为梧州市信息中心的网络安全管理体系总体方针、安全管理策略进行完善。 9.基础环境安全评估服务：对梧州市电子政务外网资

				产和信息系统开展漏洞检测服务，不限系统检测数量。对网络、宿主系统、应用系统和数据库等进行检测和审计，包括网络安全评估、系统、服务器安全评估,及时发现信息系统中存在的漏洞,并对评估中发现的漏洞提供整改建议,及时地消除漏洞的安全风险,并协助运维人员对发现的不合规项进行整改,防范安全事件发生,避免信息系统被非法利用,增强信息系统安全防范能力,保障业务的可持续性。 10.渗透测试服务：通过模拟黑客的攻击方法对系统和网络进行非破坏性质的攻击性测试，目的是模拟侵入系统，以共计工具的使用为辅助，采用可控制的、非破坏性质的渗透测试方法，并在执行过程中把握好每一个步骤的信息输入/输出，获取系统控制权并将入侵过程和细节报告给用户，通过人工渗透测试发现逻辑性更强、更深层次的弱点，找到所存在的安全威胁和风险，帮助用户及时完善安全策略，确保对用户的信息系统不造成破坏性的损害，保证渗透测试前后信息系统的可用性、可靠性保持一致。每年需完成渗透测试的信息系统数量不少于7个。 ▲11.服务期：自合同生效之日起三年。需同时配备不少于1名网络安全专家驻场服务。
2	网络运维服务	软件和信息技术服务业	1项	对梧州市电子政务外网系统进行运行维护服务，具体服务内容如下： 1.统一运维管理中心平台 ①通过RG-RillBMC统一运维监控平台对外网资产运行状态和流量进行监控，包括：设备的CPU利用率，内存利用率，设备板卡状态，线路通断，带宽利用率，路由协议运行状态、路由表等内容。 ②每班次结束编写值班报告，将设备运行状况，网络

				设备性能情况导入值班报告，同时导出互联网接口流量情况、与自治区政务外网广域网接入流量情况以及链路通断情况。 ③通过运维工单管理平台制定、改进各类运维业务处理流程、监管工单处理情况并归档。 ④知识库的建立和完善。 2.应用系统运维 ①DHCP 系统运维：DDI 设备的操纵和使用。监控 DHCP 系统 IP 地址使用情况，避免地址池耗近，保障用户电脑能正常获取 IP 信息。DHCP 系统 IP 地址池的日常备份、应急恢复。新增 IP 地址池、删除 IP 地址池、更改租约时长 ②DNS 域名解析系统运维：DDI 设备的操纵和使用。监控域名解析情况，保障域名服务正常运行。新增域名记录、删除域名记录、更改域名记录。定时备份区域文件。 ③NTP 时间同步系统运维:保障各层次时间服务器正常运行，系统时间在误差范围内；各路由器、交换机、防火墙、业务系统和安全设备配置时间服务器，保证系统时间一致 ④机房视频监控及门禁系统运维：保障视频监控及门禁系统正常运行。定期检查门禁记录，重点检查非正常刷卡记录。定期更改机房门禁密码。 ⑤备份系统运维：保障备份系统正常运行；检查备份计划执行情况；新增备份计划、删除备份内容、还原备份数据。 3.机房运维管理 ①熟悉机房环境监控系统的使用操作，通过环境监控系统实时监控机房环境，保证机房设备在良好的环境

				下运转。 ②机房清洁，每月安排一次专人对机房进行清洁工作，包括地板下桥架清洁、地板清洁、机柜清洁、设备清洁等。 ③对外来人员进出机房进行登记并归档。 ④建立机房设备管理制度执行，每台设备挂上标签标明用途、所属单位、设备责任人。 ⑤对门禁、视频监控系统的正常运行进行管理，对故障设备进行维修或更换处理。对系统发现的异常情况进行及时处理。 4.使用单位的接入服务：梧州市电子政务外网市本级横向与委办接入单位的接入服务，具体包括： ①提供 5×8 小时技术咨询服务； ②协助运营商提供接入技术支持服务，包括配置管理和联调对接。 5.自治区外网对接服务： ①提供 5×8 小时技术咨询服务； ②提供接入技术支持服务，包括配置管理和联调对接。 6.故障排查： ①外网接入单位用户无法访问系统故障定位故障原因及处理； ②外网接入单位用户 VPN 纵向业务故障定位故障原因及处理； ③机房设备发生故障协助定位故障原因及处理； ④统一互联网出口故障协助运营商定位故障原因及处理； ⑤提供接入技术支持服务，包括配置管理和联调对接。 7.巡检服务：为采购人网络提供专业、深入、智能的管家式服务。系统性管理客户、管理客户设备，自动

				收集信息，通过后台嵌入的风险库和问题库，自动化完成风险评估，自动化输出报告，提供专业优化建议。具体包括： ①梧州市政府大楼二楼机房每天进行一次现场巡检，输出巡检报告； ②外网接入单位节点设备每月进行一次远程自动化巡检服务，输出巡检报告； ③重要节点（市政府、市委、红岭大厦）每年度进行一次现场巡检，其他节点抽取 10%比例采样每年度进行一次现场巡检服务。 8.资料收集管理：建立完善的运维服务资料库，保证梧州市电子政务外网运维服务资料文件的完整和安全，便于查找利用，做好文件资料的记录、收集、管理。具体包括： ①单位接入资料； ②IP 地址表； ③设备资产登记； ④故障处理记录； ⑤日常网络数据记录； ⑥产品使用手册； ⑦运维服务内部人员通信录、全市接入点位节点单位及合作厂商、供应商通信录管理。 9.资产管理： ①收集、整理并建立网络设备固定资产资料和配置库并提交给用户； ②整理维护 IP 地址表，包括互联网地址，私网地址、映射地址表，保证充分利用 IP 地址； ③建立、维护并提交全网的网络拓扑图和相关技术说明。梧州市电子政务外网市本级横向与委办接入单位

				城域网接入服务。 ▲10.服务期：自合同生效之日起三年。需同时配备不少于 1 名网络工程师驻场服务。
3	应急响应服务	软件和信息技术服务业	1 项	梧州市政务外网在发生确切的信息安全事件时，提供应急响应技术支持，以年为单位，不限次数，差旅费自理。具体服务内容包括: 1.从安全事件发生在第一时间采取紧急措施,恢复业务到正常服务状态；调查、分析、研判安全事件发生的根源,提供数字证据。 2.服务内容:钓鱼邮件、黑客入侵、APT 攻击、漏洞利用、网络攻击、数据外泄、事件通报、攻击溯源、网站被黑、非法访问、网站挂马、网站暗链、网站篡改等； 3.服务流程初步处置:接到应急响应需求后,现场人员封存现场,保留证据、断绝扩散渠道的建议。现场处置:专家第一时间赶赴现场对安全事件进行日志分析、网络行为分析、应用后门检测等工作。溯源分析:通过大数据资源,对攻击行为进行溯源分析、样本分析、挖掘攻击者行为特点,与本地分析相结合,判定事件类型与影响范围。处置恢复:查明原因、结果、损失后,协助用户方对系统及网络进行安全恢复。 ▲4.服务期：自合同生效之日起三年。
4	应急演练服务	软件和信息技术服务业	1 项	1.梧州市政务外网应急演练服务，组织专业攻防队伍做实战应急演练。 2.网络安全专家根据采购人信息系统实际情况调研并制订攻击演练方案,在采购人现场部署实战演练所需的监测工具,协助采购人搭建互联网攻击演练环境。优选白帽成员在指定时间段内对演练范围内的指定网站进行攻击测试,在安全监测与响应中心由网络安全专

				家与采购人一起监测攻击行为、处理攻击事件,根据整体演习情况形成总结报告。含专业安全服务人员 2 人 2-3 周时间的支持服务。 ▲3.服务期：自合同生效之日起三年。每年开展不少于一次的应急演练服务。
5	安全风险评估及整改服务	软件和信息技术服务业	1 项	对《梧州市电子政务外网系统》做信息安全风险评估服务和商用密码应用评估项目实施服务，具体包括： 1.包含项目的准备及启动、信息系统识别及现状调查、明确等保评估的信息系统范围、制定等保评估工作计划、收集并分析信息系统资料、信息系统安全等级的确定、生成信息系统网络拓扑图、编写定级报告和备案信息。 2.等保管理体系咨询和建设，协助采购人建立网络安全等级保护管理体系。结合等级保护测评报告提出的安全管理体系与等级保护基本要求之间的差距，在信息安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等方面指导并协助建立健全符合相应等级要求的安全管理制度，提交《信息安全等级保护管理制度包》。 3.风险评估：对《梧州市电子政务外网系统》进行风险评估（包括并不限于主机、操作系统、数据库、中间件、网络设备、安全设备），提供该系统的风险评估报告； 4.等级保护现状分析：对信息系统的安全现状进行，分析信息系统保护现状和信息安全等级保护基本要求之间的差距，为通过信息系统等级保护奠定基础。制定用户安全需求分析、安全建设与改建方案的制定、制作原信息系统产品加固方案、测评不符合及部分符合项整改建议、制作新的网络拓扑图、制作安全需求

				分析报告、编制并确认整体信息系统整改方案。 5.项目实施服务，包括设备的系统调试、安全策略配置服务。提供测评期间现场支持服务。 6.根据 GB/T39786-2021《信息安全技术信息系统密码应用基本要求》三级指标要求，从网络和通信安全、设备和计算安全、应用和数据安全、管理制度等层面，对系统进行风险分析，得出系统密码应用需求，编制《密码应用改造方案》，并按照方案进行相关密码应用软硬件包含域名证书，国密浏览器、智能密码钥匙等的部署和实施，并通过商用密码应用安全性评估。 ▲7.服务期：自合同生效之日起三年。每年开展不少于一次的信息安全风险评估服务，需同时提供该系统的风险评估报告。
6	等保测评服务	软件和信息技术服务业	1 项	具有等级保护测评资质的单位对外网《梧州市电子政务外网系统》进行测评服务，通过等保测评。（网络安全等级保护：三级） 基本要求： 1.依据《信息安全等级保护管理办法》（公通字[2007]43 号）和《信息安全技术网络安全等级保护定级指南》（GB/T22240）、《网络安全等级保护基本要求》（GB/T22239-2019）对系统开展安全等级（三级）测评工作，完成现场测评后正式等级测评； 2.上述信息系统的安全等级测评内容应包括技术和管理两大类，其中技术类应包括对安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面的测评，管理类测评应包括对安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等方面的测评，并提出安全整改建议； 3.在等级保护测评过程中，应采用访谈、检查、测试、

				工具扫描等国际国内认可的先进方法和手段进行，并与国家相关规范及标准的要求相符。测评中必须采用专业的国内安全扫描设备及软件产品辅助测评工作的完成。 ▲4.服务期：自合同生效之日起三年。每年需开展一次等保测评服务，并出具符合国家网络安全等级保护管理部门规范要求、公安机关认可的网络安全等级测评报告。
7	商用密码应用安全性评估服务	软件和信息技术服务业	1 项	1.依据 GB/T39786-2021《信息安全技术信息系统密码应用基本要求》三级指标要求，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度等层面，对系统的密码应用情况进行全面测评。 2.根据测评结果编制商用密码应用安全性评估报告，并配合梧州市在广西壮族自治区密码管理局对商用密码应用安全性评估报告进行备案，重点对密码保障系统设计的正确性、合规性、有效性、以及实施计划、应急处置的科学性、可行性等进行审查论证。 3.对在测评中发现的系统安全隐患和风险，提出切实可行的整改建议方案。 ▲4.服务期：自合同生效之日起三年。每年开展一次商用密码应用安全性评估服务，并出具商用密码应用安全性评估报告。
8	安全监测系统服务	软件和信息技术服务业	1 项	1.提供梧州市政务外网安全监测平台。监测范围覆盖城域网、局域网、互联网出口和政务云，具备数据采集、数据分析、态势感知和预警通告等核心功能。 2.功能描述：安全运营平台管理平台，集成大数据分析、APT 分析、风险指标分析、工作流引擎等技术，覆盖资产管理、漏洞管理、关联分析、安全告警、威胁

				感知、安全监控、报告管理、工单管理、系统管理等功能，从资产运营、威胁感知、风险管理、处置响应的层面支持网络安全运营的业务开展、统计分析、态势展示； 3.授权：管理≥1000 个资产； 4.期限：含三年软件维保及策略库升级服务。 ▲5.需与广西壮族自治区政务外网安全监测平台建设对接。
9	安全培训	软件和信息技术服务业	1 项	1.针对采购人信息技术相关工作人员，提供不同层级的网络安全、信息安全、数据安全等内容开展安全培训。包括安全管理体系的设计、安全管理的执行、安全意识、安全攻防知识等。 2.针对采购人普通工作人员，提供安全意识培训。 ▲3.服务期：自合同生效之日起三年。培训频率为每季度 1 次，培训内容由采购人决定。
三、集成服务				
1	网络集成服务	软件和信息技术服务业	1 项	1.梧州市电子政务外网网络集成服务： （1）远程技术支持 要求提供 7×24 小时人工热线服务，为采购人提供售后技术问题咨询、受理采购人故障申报、硬件报修服务请求、提供服务投诉及建议通道。 问题咨询：要求对采购人提出的所有咨询问题在 1 个工作日内进行及时有效的解答。 故障报修：故障申报及硬件报修需给出具体解决时限。 用户投诉：服务投诉及建议需在 3 个工作日内提供反馈信息及处理结果。 （2）远程问题处理 应用故障：工程师在 30 分钟内提供远程支持，进行问题分析、信息收集、故障诊断和排查，提供合理的解

				决方案，并配合用户实施。对于疑难问题需升级至专家团队进行远程支持。应用类故障要求在最短时间内恢复业务，必要时提供临时解决方案，并在 2 个工作日内给出详细故障报告。 设备故障：工程师在 30 分钟内提供临时解决方案，并进入“备件先行”流程。要求在 2 个工作日内给出详细故障报告。 （3）在线技术支持 要求提供专业的技术支持网站，可在线下载系列产品技术资料、最新产品配置手册、方案实施一本通、技术指导书、产品培训视频等信息，采购人可访问网站并下载相关资料。 （4）软件更新支持 需向采购人提供主机版本软件及修复补丁，并完成软件升级实施方案。软件要求主机版本及补丁软件经过实际应用环境充分验证，升级后能够确保主机版本的持续稳定运行。为保证升级后设备的稳定运行，需由原厂工程师现场升级安装并持续观察 2 个工作日，设备稳定运行后完成软件升级。 （5）备件先行服务 当核心交换机设备出现故障时，要求 5*9 小时内受理，下一个工作日发出备件，备件及运送免费，并负责安装调试上线并恢复业务，以满足采购人的运维需求。 （6）现场问题处理 远程受理采购人提出的问题/故障请求时，通过远程技术支持不能有效解决的设备问题，将安排技术支持工程师按照服务等级规定时间（5*9 小时*NBD）内前往采购人现场，现场协助采购人进行故障分析和诊断、制定故障恢复方案，并协助现场排除故障。

				（7）具体需购买集成服务的清单见附件 1《网络集成服务清单》； ▲（8）服务期：自合同生效之日起三年。
2	安全集成服务	软件和信息技术服务业	1 项	1.梧州市电子政务外网安全集成服务： （1）硬件质保服务 设备返修服务 投标人提供的设备发生软件故障或新机交付验收合格后超过 90 天后发生硬件故障的情况下，须提供返厂维修服务，最长维修周期不超过 10 个工作日（若有特殊情况不能保证时间，将提前向采购人说明）。 维修备机服务 投标人提供的产品交付验收合格后发生硬件故障需要返厂维修，若收到货后 10 个工作日未能维修完毕，须根据采购人的需求，向采购人提供同型号或高型号备机，等到故障机维修完毕后收回备机。 （2）远程技术支持服务 服务方式：免费热线，远程协助，邮件支持，在线客服 ▲服务时限：自合同生效之日起三年 服务内容：当采购人在使用设备遇到疑问或问题时可以通过远程基础支持服务得到有效的技术支持，快速解决问题 服务结果：通过电话、远程、邮件等方式解决设备使用过程中遇到的问题 （3）现场技术支持服务 服务方式：现场支持 ▲服务时限：自合同生效之日起三年 服务内容：远程排查仍然无法解决的，定位是设备本身故障导致的，提供现场支持

				服务结果：现场解决采购人问题或定位设备需返厂维修 （4）软件升级服务 服务方式：软件版本升级 ▲服务时限：自合同生效之日起三年 服务内容：采购人与原厂确认版本升级不影响现有采购人使用情况下进行系统版本升级 服务结果：设备升级后将会获得新版本的新增功能或功能优化 （5）特征库更新服务 服务方式：特征库更新，提供数据安全平台解决方案 ▲服务时限：自合同生效之日起三年 服务内容：设备可定期自动更新相应的特征库信息 服务结果：更新特征库后，将会提高设备相应的检测识别能力 （6）远程技术支持方式 方式：电话支持、远程技术支持 联系方式：须提供服务热线电话 支持时间说明：7*24 小时 （7）具体需购买集成服务的清单见附件 2《安全集成服务清单》
3	设备系统集成服务	软件和信息技术服务业	1 项	1.满足本项目与之相关的周边设备、线材及相关配件； 2.对所有施工材料包干/根据采购人实际要求布线； 3.电信级熔接保证所有熔接点稳定运行； 4.面向采购人的新建网络、扩容、改造工程，由有经验的工程师开展设备的软件调试工作，保障设备部署满足采购人网络建设或改造需求。 ▲5.服务期：自合同生效之日起三年。
4	网络运维服务系统	软件	1 项	1.提供梧州市电子政务外网系统的网络运维服务系统

	集成	和信息技术服务业		集成（包含有线网络运维服务系统集成及 5G 网络运维服务系统集成）。 ▲2.服务期：自合同生效之日起三年。
四、线路租赁服务				
1	互联网出口线路 1	软件和信息技术服务业	1 条	▲1.光口接口，上下行速率≥3Gbit/s，提供 1 个 C 类地址； ▲2.线路要求必须有物联双路由保护，租赁周期 3 年；
2	互联网出口线路 2	软件和信息技术服务业	1 条	▲1.光口接口，上下行速率≥1Gbit/s，提供 1 个 C 类地址； ▲2.线路要求必须有物联双路由保护，租赁周期 3 年； ▲3.互联网出口线路 2 使用的运营商不得与互联网出口线路 1 同为一家。
3	互联网出口线路 3	软件和信息技术服务业	1 条	▲1.网口接口，上下行速率≥200Mbit/s，全链路的传输设备要求支持 IPv6； ▲2.线路要求必须有物联双路由保护，租赁周期 3 年；
4	城域网横向电路 1	软件和信息技术服务业	2 条	▲1.光口接口，上下行速率≥2000Mbit/s，线路类型为采用裸光纤或 MSTP、SDH、OTN 等基于硬管道技术的传输电路， ▲2.不接受基于网络层的电路和虚拟通道电路，所需传输及配套设备由投标人提供；租赁周期 3 年；
5	城域网横向电路 2	软件和信息技术服	27 条	▲1.网口接口，上下行速率≥200Mbit/s，线路类型为采用裸光纤或 MSTP、SDH、OTN 等基于硬管道技术的传输电路， ▲2.不接受基于网络层的电路和虚拟通道电路，所需

		务业		传输及配套设备由投标人提供；租赁周期 3 年；
6	城域网横向电路 3	软件和信息技术服务业	163 条	▲1.网口接口，上下行速率≥100Mbit/s，线路类型为采用裸光纤或 MSTP、SDH、OTN 等基于硬管道技术的传输电路， ▲2.不接受基于网络层的电路和虚拟通道电路，所需传输及配套设备由投标人提供；租赁周期 3 年；
7	城域网横向电路 4	软件和信息技术服务业	73 条	▲1.网口接口，上下行速率≥50Mbit/s，线路类型为采用裸光纤或 MSTP、SDH、OTN 等基于硬管道技术的传输电路， ▲2.不接受基于网络层的电路和虚拟通道电路，所需传输及配套设备由投标人提供；租赁周期 3 年；
8	城域网横向电路 5	软件和信息技术服务业	3 条	▲1.网口接口，上下行速率≥20Mbit/s，线路类型为采用裸光纤或 MSTP、SDH、OTN 等基于硬管道技术的传输电路， ▲2.不接受基于网络层的电路和虚拟通道电路，所需传输及配套设备由投标人提供；租赁周期 3 年；
9	城域网横向电路 6	软件和信息技术服务业	5 条	▲1.网口接口，上下行速率≥10Mbit/s，线路类型为采用裸光纤或 MSTP、SDH、OTN 等基于硬管道技术的传输电路， ▲2.不接受基于网络层的电路和虚拟通道电路，所需传输及配套设备由投标人提供；租赁周期 3 年；
10	5G 快线备用线路服务	软件和信息技术服务业	1 套	▲1.配套提供 5G 工业网关用于交付流量使用。 2.5G 网关需采用贴片卡的方式。 3.提供管理平台和小程序，管理平台和小程序共用一个账号密码，管理平台和小程序的功能如下： （1）管理平台： 5G 网关管理：能够查看 5G 工业网关在线状态、IMEI、ICCID、IMSI 等信息，具备对 5G 网关 WiFi 远程配置的功能和基于 MAC 地址的黑白名单功能，支持远程重启，

				信号强度监控，设备列表导出，支持固件升级，具备DNN远程配置功能，能够查询流量使用情况。 5G卡管理：能够查看5G卡的卡状态、激活时间、本月流量详情，能够操作5G卡的状态变更（例如激活）。 （2）小程序： 5G工业网关信息:能够查看配套5G工业网关的ICCID、MSISDN、当前网络制式、设备型号、设备状态、流量使用情况、信号强度等信息，能够通过扫配套5G工业网关的IMEI条码来快速查询该设备相关信息。 5G卡信息：能够查看5G卡的卡状态、激活时间、本月流量详情。 ●4.配套5G工业网关支持完整性保护/祖冲之加密算法正确功能/SRB/DRB以及支持加解密/祖冲之加密算法的正确功能/SRB/DRB。
11	接入路由器	租赁和商务服务业	20台	▲1.固化三层千兆电口≥2个，固化三层千兆光口≥1个，二层千兆以太LAN口（电口）数量≥4个，满足上述要求后实际剩余可扩展槽位≥2； ▲2.包转发率≥1Mpps； 3.配置USB接口，SD卡接口可用于零配置上线，多功能复FUNC键（一键复位，一键升级）； 4.无风扇设计，降低噪音、提高设备可靠性 5.支持并实配支持L2TP、IPSecVPN、GREVPN、DMVPN功能； 6.为便于设备管理，要求路由器面板提供多功能复原键，便于紧急情况的设备状态恢复； 7.支持静态路由、RIPv1/v2、OSPF、BGP4等路由协议； 8.支持IGMP、PIM-SM、PIM-DM、DVMRP等组播协议 9.支持Telnet、SNMP、CLI等网络管理功能； 10.支持状态防火墙功能；

				11.产品支持 IPV6/IPV4； ●12.支持国密局 SM1 加密算法。 13.租赁周期：自合同生效之日起三年。
五	**互联网服务接入区配套设施租赁服务**	**租赁和商务服务业**	**1 项**	**1.租赁周期：自合同生效之日起三年。 2.租赁设备清单详见以下《互联网服务接入区配套设施租赁服务租赁设备清单及设备技术要求一览表》**
互联网服务接入区配套设施租赁服务租赁设备清单及设备技术要求一览表				
序号	**设备名称**	**数量及单位**	**技术要求**	
1	分布式拒绝服务攻击防护系统	2 台	▲1.标准机架式 1U 设备，冗余双电源，冗余风扇 3+1，1 个 Console 接口，1 个 MGMT 接口，1 个 USB 3.0 接口，内置 Bypass 插卡； ▲2.接口：≥8*GE COMBO ，≥4*GE RJ45 ，≥4*GE SFP ，≥6*10GE SFP+； ▲3.支持对 SYN Flood、SYN-ACK Flood、ACK Flood、FIN Flood、RST Flood、TCP Malformed、TCP 链接耗尽、TCP Fragment Flood、UDP Flood、UDP Fragment Flood、ICMP Flood 等常见网络层泛洪攻击识别及防御，支持各类 TCP 反射、UDP 反射攻击的识别和阻断； 4.支持 HTTP 应用层 Flood/HTTP CC 识别及防御，支持 HTTPS 应用层 Flood/HTTPS CC 识别及防御，支持 DNS Query Flood 识别及防御。 5.严格前后风道； 6.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； 7.直路部署模式，攻击响应延迟<1 秒； ●8.支持基于行为分析防御针对 WEB、APP 的 HTTP CC/大资源高频请求攻击；	

			●9.系统支持 DDoS 攻击智能化自动防御，防御全程自动化，无需人工干预； 10.支持通过集中的管理平台实现多台防御设备集中管理、性能监控，支持基于业务划分防护对象，定义防御策略，提供精细化防护，支持业务动态流量基线学习，支持攻击告警、攻击详情、清洗前后流量对比集中展示，支持抓包取证，首页实时监控至少支持攻击告警、设备入出流量对比、设备 CPU 利用率、IP 流量 TOPN 等； 11.支持 SYN 首包丢弃功能防御虚假源 SYN Flood； 12.支持基于错误序列号和正确序列号的源挑战认证防御虚假源 SYN Flood； 13.支持基于会话行为检测防御 UDP Flood； 14.支持基于源 SYN 报文限速防御真实源 SYN 攻击； 15.支持 SYN-ACK 首包丢弃防御虚假源 SYN-ACK Flood； 16.支持基于 UDP 协议自定义过滤规则对 UDP Flood 及 UDP 分片进行限速防御，可配置的字段包括源 IP、目的 IP、源端口、目的端口、报文长度、报文载荷等； 17.支持基于会话限速和限流防御 UDP Flood 及 UDP 分片； 18.支持基于限速防御 ICMP Flood 及 ICMP 分片； 19.支持 IPV4/IPV6 共栈防御。
2	出口路由器	2 台	▲1.设备性能：整机最大支持交换容量≥320Gbps，最大支持包转发性能≥60Mpps； ▲2. 硬件架构：全框宽主控板槽位数≥2 个，可拔插电源槽位数≥2 个，业务板槽位数≥8 个（主控、风扇、电源、其他扣卡等槽位不及入业务槽位之内），单槽位最大带宽≥10Gbps； 3.设备配置：配置主控板≥1，万兆三层路由 SFP+光口≥14 个，千兆三层路由电口≥10 个，千兆 combo 口≥4 个，交流电源模块≥2 个； 4.转发架构：支持多核 CPU 处理器和 NP 芯片架构；

			●5.芯片自主化：设备关键芯片（包括但不限于CPU、NP芯片）为国产芯片； 6.整机高度:适应现有机柜空间要求，整机高度≤3U； ●7.热插拔：为便于运维管理和安全，业务板卡须支持热插拔，无需配置命令等辅助操作； 8.应用安全：设备可扩展支持IPS、URL过滤和应用识别功能； 9.基础功能：支持DHCP server/client/relay，PPPoE server/client，NAT，子接口管理等 10.局域网协议：支持IEEE 802.1P，IEEE 802.1Q，IEEE 802.3 ，VLAN管VLAN聚合，MAC管理，STP/RSTP/ MSTP，SEP等； 11.无线局域网（AC）:支持AP设备管理(AC发现/AP接入/AP管理)，CAPWAP协议，WLAN 用户管理，WLAN射频管理（802.11a/b/g/n/ac），WLAN QoS（WMM），WLAN 安全（WEP/WPA/WPA2/密钥管理）； 12.IPv4单播路由：支持静态路由，策略路由，动态路由协议：RIP、OSPF、BGP、IS-IS； 13.IPv6单播路由：支持静态路由，路由策略， RIPng，OSPFv3，IS-ISv6，BGP4+； 14.IPv6基本功能：支持IPv6 ND，IPv6 PMTU，IPv6 FIB，IPv6 ACL，ICMPv6，DNSv6，DHCPv6； 15.IPV6隧道：支持手工隧道，自动隧道，GRE隧道，6over4隧道，6to4，ISATAP； 16.组播路由：支持组播协议：IGMP V1/V2/V3， PIM SM，PIM DM，MSDP，MBGP，IPv6 PIM，MLD； 17.MPLS：支持LDP，MPLS L3 VPN，VLL，PWE3，静态LSP，动态LSP，MPLS TE，IP FRR，LDP FRR，TE FRR； 18.VPN：支持IPsec VPN，GRE VPN，DSVPN，A2A VPN，L2TP VPN，L2TPv3 VPN，VxLAN； 19.QoS：支持Diffserv模式，MPLS QoS，优先级映射，流量监管

			（CAR），流量整形，拥塞避免，拥塞管理，HQoS，MQC（流分类，流行为，流策略），端口三级调度和三级整形（Hierarchical QoS），WLAN QoS，FR QoS，智能应用控制（SAC）； 20.安全：支持 ACLv4/v6，基于域的状态防火墙，802.1x 认证，MAC 认证，Portal 认证，AAA，RADIUS，HWTACACS，PKI，广播风暴抑制，ARP 安全，ICMP 防攻击，URPF，CPCAR，黑名单，攻击源追踪，国密算法，上网行为管理。
3	SDN 交换机	2 台	▲1.交换容量≥4.8Tbps ，包转发率≥2000Mpps，端口交换容量≥2.56Tbps； ▲2.1/10GE SFP+端口≥48 个（可通过命令行将接口配置为 10G 或 1G 速率），40/100GE QSFP28 端口≥8 个，冗余交流电源，提供不少于 1 根 100GE 高速堆叠线缆； ●3.M-LAG（或 vPC 或 DRNI）支持一致性检查、维护模式无损升级、协议认证等功能； ●4.支持 MAC 漂移联动端口 error-down； 5.支持数据面故障快速自愈 DPFR； 6.支持 VRRP、VRRP 负载分担、BFD for VRRP ●7.支持 MacSec 国密算法； 8.支持弱安全协议/算法查询与安全增强； 9.支持 IFIT 随流检测功能； 10.支持配置回滚； 11.支持全网路径探测； 12.端口侧面板和电源侧面板都配备系统运行状态灯和远程运维 ID 指示灯（现场定位用指示灯，运维人员可远程控制 ID 灯开启和关闭）； 13.支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议。
4	出口防火墙	2 台	▲1.防火墙吞吐量≥50Gbps，最大并发连接数≥2000 万，每秒新建连接数≥50 万 ； ▲2.实配：千兆 Combo 接口≥8，千兆电口≥4，万兆光口≥10,2

			个交流电源，1 个固态硬盘-960GB-SATA，SSL VPN 授权数 100； 3.IPS 吞吐量≥18Gbps,IPSec VPN 吞吐量≥30Gbps,SSL VPN 吞吐量≥3Gbps； 4.IPSec VPN 隧道数≥20000，SSL VPN 并发在线用户数≥5000； 5.防火墙转发时延≤18μs； 6.配置 3 年 IPS、AV 特征库升级服务和 URL 远程查询升级服务授权； 7.支持 2 条万兆光 Bypass 链路； ●8.产品采用自主研发的关键芯片(CPU)； 9.严格前后风道； 10.支持设备的 WEB 管理页面中直接打开 CLI 控制命令； 11.支持基于源 IP/目的 IP，服务类型，应用类型，安全域，时间段等字段进行安全策略规则的配置； 12.支持一条安全策略中同时配置 ipv4 和 ipv6 地址； 13.支持安全策略阻断时设备发送反馈报文快速断开连接，如针对 TCP 报文反馈 reset 报文，针对 UDP 和 ICMP 报文反馈 ICMP 不可达报文； 14.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议； ●15.支持 SRv6 协议； 16.策略路由支持的匹配条件：源 IP/目的 IP，服务类型，应用类型，用户(组)，入接口，DSCP 优先级； 17.支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议； 18.支持 IPv6 over IPv4 隧道，6RD 隧道； 19.支持每 IP 的最大连接数限制，防护服务器；
5	入侵防御设备	2 台	▲1.网络层吐量≥15Gbps，网络层并发连接数≥1000 万，网络层每秒新建连接数≥25 万； ▲2.IPS 检测吞吐量≥10Gbps，IPS 最大并发连接数≥50 万，IPS 每秒新建连接数≥32000；

			▲3.实配：千兆 Combo 接口≥8，千兆电口≥4，千兆光口≥4，万兆光口≥6，配置 SSD 硬盘≥960G，可插拔电源模块≥2 个，提供 IPS 特征库升级服务≥36 个月； 4.具备不少于 2 个扩展插槽，支持 Bypass 功能和接口； 5.标准机架式 1U 设备； 6.配置 1 个电源；配置 2 个风扇，形成 1+1 冗余备份； ●7.产品采用自主研发的关键芯片(CPU)； 8.当风扇模块出现故障时，在设备不断电的情况下，对风扇模块进行更换；为了避免设备过热，要求更换风扇模块所用的时间控制在 1 分钟内； 9.支持冗余电源，要求设备安装了两块电源模块时，其中的一块可以进行热插拔； 10.单台设备必须支持 IDS/IPS 混合部署方式，实现部分接口旁路检测，部分接口对直路防护，设备支持单臂部署方式，可以旁挂在二层或者三层设备上进行入侵防御； 11.配置入侵防护功能模块；能够防范各种应用层攻击，包括但不限于：后门程序，木马程序，间谍软件，蠕虫，僵尸主机，异常代码，协议异常，扫描，可疑行为审计类等； 12.支持上亿数量级的变种病毒库； 13.系统预定义入侵防御签名库数量不得少于 20000 条且具备 CVE 和 CNNVD 编号的签名条目数不得少于 11000，支持用户自定义签名规则，支持正则表达式 14.模块应包括对 P2P，IM，网络游戏，炒股软件，语音聊天工具，流媒体，常用邮件以及远程控制软件等的识别和控制； 15.支持不少于 6000 种的应用识别能力； 16.支持 SYNFlood、SYNACK、UDPFlood 等 DDoS 防护，支持 HTTPFlood、HTTPSFlood 等应用层 DDoS 防护； ●17.系统支持除了基于攻击事件本身进行严重级别划分，还可以根据攻击与资产相关性关联进行风险级别定义，协助管理员关注

			实际环境中需要紧急处理的安全告警，提升安全事件响应效率。 18.支持对 VLAN、IPv4、MPLS、GRE、IPv6、IPv4 over IPv6、IPv6 over IPv4 报文的入侵检测。	
六	**安全管理中心区(运维中心)配套设施租赁服务**	**租赁和商务服务业**	**1 项**	**1.租赁周期：自合同生效之日起三年。 2.租赁设备清单详见以下《安全管理中心区（运维中心）配套设施租赁服务租赁设备清单及设备技术要求一览表》。**

安全管理中心区（运维中心）配套设施租赁服务租赁设备清单及设备技术要求一览表

序号	设备名称	数量及单位	技术要求
1	IPSec/SSL 安全网关	1 台	1.性能要求：吞吐量≥5Gbps，最大并发连接数≥400 万，每秒新建连接数≥8 万，本次配置 SSLVPN 并发接入用户数 1000； 2.硬件要求：标准 1U 专用千兆硬件平台，可插拔双电源，硬盘≥960GB。标配千兆 Combo 接口≥8，千兆电口≥2，万兆光口≥2，1 个 Console 口，2 个 USB 接口； ●3.产品采用自主研发的关键芯片(CPU)； 4.为更便捷的操作，设备的 WEB 管理页面中可以直接打开 CLI 控制命令。 5.支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议。
2	堡垒机（国密版）	1 台	▲1.整机性能：支持最大字符并发数≥700 个，最大图像并发数≥200 个，支持最大可管理资产总数≥700，本次授权可管理资产总数≥200； ▲2.实配：提供 8 核/2.1GHzCPU≥1 颗，内存≥16GB，千兆电口≥4 个，万兆光口≥2 个，2*4000GB-SATA 硬盘+2*600GB-SAS 硬盘，电源冗余设计且满配； 3.标准 2U 专用千兆硬件平台； 4.设备采用旁路部署（支持集群部署），不影响业务环境；支持高可用部署，HA 秒级切换；

			5.支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理； 6.支持按部门组织架构（至少 5 个层级的部门）管理用户数据、资产数据、授权数据、审计数据； 7.每个部门可以管理本部门及下级部门的用户角色：部门管理员、运维管理员、审计管理员、运维员； 8.支持域认证与双因子认证结合使用，如同时使用 AD/LDAP 用户名+AD/LDAP 密码+动态令牌登录堡垒机、同时使用 AD/LDAP 用户名+AD/LDAP 密码+短信口令登录堡垒机； 9.支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库 Oracle、MSSQL、MySQL、VMwarevSphereClient、浏览器等客户端工具； ●10.通过 socks5/http/ssh 等代理协议连接管理异地云资源区中私有网络的云主机； 11.运维人员可以向管理员申请需要访问的设备，申请时可以选择：设备 IP、设备账户、运维有效期、备注事由等；并且运维工单以邮件方式通知管理员 12.管理员对运维工单进行审核之后以邮件方式通知给运维人员；如果允许，则运维人员才可访问，否则就无法访问； 13.H5 运维方式：支持 ssh、telnet、rlogin、rdp、vnc 协议的 H5 运维，无需本地运维客户端工具； ●14.支持通过堡垒机页面直接调用本地 Windows 系统里的 plsql、sqlplus、toad、sqlwb、ssms、mysql.exe 等数据库客户端工具； 15.支持在 mac 电脑里使用 navicat 工具通过堡垒机登录 mysql、oracle 等数据库服务器； 16.支持批量登录字符设备功能：能自动生成 SecurCRT/Xshell 工具的批量登录文件，实现在工具中批量自动登录多台设备；

			●17.支持一键健康检查并且支持导出健康报告，可一键日志打包供排错分析； 18.系统管理口地址支持配置为 IPv4 和 IPv6；对运维人员登录目标设备上进行的操作进行全程记录，目标设备支持 IPv4 和 IPv6 地址。
3	服务器密码机	1 台	1.具有密钥管理、数据加/解密，签名/验证等密码运算服务功能； 2.采用国产 CPU，如飞腾、龙芯、兆芯、海光等；搭载国产主板、内存和硬盘，以及国产密码模块，确保硬件层面的自主可控； 3.可适配银河麒麟、中标麒麟、UOS（统一操作系统）、Deepin 等国产操作系统； 4.支持国家商用密码算法标准，包括 SM1、SM2、SM3、SM4 等，用于数据加密、解密、签名和验证，确保信息传输和存储的安全性； 5.提供高速的加密解密运算能力，支持多任务并行处理，满足数据加密的需求； 6.提供网络接口（如千兆、万兆以太网口）和加密接口（如 PCIe、USB），支持 SSL/TLS、IPSec、HTTPS 等标准协议，以及国密 SSL 协议； 7.内置安全的密钥管理系统，支持密钥的生成、存储、备份、恢复、更新和销毁等全生命周期管理，保障密钥的安全性 8.支持基于国密算法的身份认证机制，包括服务器认证、用户认证和设备认证，确保只有授权用户和设备可以接入； 9.具备审计日志功能，记录所有操作和异常事件，便于安全审计和问题追踪； 10.提供图形化的管理界面或者命令行接口，便于配置、监控和维护； 11.产品支持 IPV6/IPV4； 12.具备《商用密码产品认证证书》。
4	签名验签服务设备	1 台	1.用于服务端为用户实体提供基于 PKI 体系和数字证书的数字签名、验证签名等运算功能的服务器，保证关键业务信息的真实性、

			完整性和不可否认性； 2.国产自主芯片，支持 SM2、SM3、SM4 算法，具有身份认证、数据签名与签名验证等功能； 3.性能要求：SM2 签名速率≥20000 次/秒，验签速率≥8000 次/秒； 4.硬件要求:2U 机架设备，可插拔双电源； 5.支持应用实体密钥的产生，证书申请，并通过管理界面导入应用实体的签名证书、加密证书和加密密钥对； 6.可适配银河麒麟、中标麒麟、UOS（统一操作系统）、Deepin 等国产操作系统； 7.支持国密算法标准，包括但不限于 SM2 椭圆曲线公钥密码算法、SM3 密码哈希算法、SM4 分组密码算法，用于实现数字签名、验证签名、数据加密等功能； 8.通过 HTTP/TCP 等协议对外提供签名验签服务，支持在线签名、批量签名、数字信封、时间戳服务等； 9.内置密钥管理系统，支持密钥的生命周期管理，如生成、存储、更新、备份、恢复和销毁，并且支持硬件安全模块（HSM）或密码卡来增强密钥安全性； 10.支持集群部署、负载均衡、故障转移等功能，确保服务的连续性和稳定性，同时也便于根据业务需求进行横向或纵向扩展 11.产品支持 IPV6/IPV4； 12.具备《商用密码产品认证证书》。
5	国密门禁	1 台	1.支持卡务管理、多级权限管理、通行权限管理； 2.支持实时监控、远程开门、多种报警联动、消防联动、各种定时任务、反潜回、防尾随、多门互锁、多卡开门等功能； 3.使用国密算法对门禁设备之间的通讯进行加密； 4.具备系统初始化和密码卡备份功能； 5.具备《商用密码产品认证证书》。
6	国密密钥系统	1 台	密钥管理系统主要是进行密钥的生成、发行和更新，采购人通过

			此软件自行生成和管理各类应用密钥，自行完成卡片的初始化工作。
7	国密卡	5 张	1.国密卡采用 SM1 算法来实现通信和数据交换的信息安全； 2.符合 ISO/IEC14443TypeA/B 国际标准，支持非接触式通信； 3.支持国密 CPU 卡标准，如 PBOC3.0、GM/T0009 等国家商用密码规范； 4.支持国密算法，包括但不限于：SM1、SM2、SM3、SM4； 5.存储选项多样，如 8K、16K、32K 等 EEPROM 或 Flash 存储空间，用于存放用户数据、应用程序和密钥； 6.在确保读卡器功率正常及正常环境条件下，读卡距离在 0~10 厘米之间； 7.工作温度范围在-25° C 至+85° C； 8.支持利用真随机数产生 256 位 SM2 密钥对,2048 位 RSA 密钥对，会话密钥、密钥加密密钥 KEK 等； 9.具有融合的系统架构，能实现国际加密算法，国密算法的同步支持，以便与各种不同密码体系的应用进行无缝对接； 10.数据区满足 50 次擦写； 11.存储器具备加密加扰校验功能. 12.具备《商用密码产品认证证书》。
8	门禁配件	2 套	1.包括人脸一体机（人脸+国密）、发卡器、双门控制器、国密读头、磁力锁、磁力锁支架、紧急按钮、电源箱； 2.人脸一体机：（1）支持壁挂，具备人脸、IC 卡、二维码三类识别方式（2）操作系统支持 Android8.0；（3）支持双目人脸识别，宽动态摄像头，支持强光抑制识别； 3.发卡器：（1）支持国密 CPU 卡（2）支持 SM1、SM2、SM3、SM4 国密算法；（3）读写时间：<0.3 秒；（4）工作电压：DC5V（5）工作温度：-10～50℃； 4.双门控制器： （1）输入支持 2 组标准门磁状态输入，2 组出门请示按钮输入，

			2 组标准防撬状态输入；（2）输出支持 2 组门锁继电器输出（有源、无源可选择），常开/常闭/常闭自动；2 组常开报警继电器输出；（3）工作温度-10℃—50℃，工作湿度 5%—90%；（4）100M/1000M 自适应以太网通讯； 5.国密读头：（1）支持密码开门（2）支持卡类：国密 CPU 卡（3）读写时间：<0.3 秒；（4）工作电压：DC5V（5）工作温度：-10～50℃； 6.磁力锁、磁力锁支架：（1）最大拉力单门≥280kg，双门≥280*2kg；（2）适用于木门或铁门；（3）支架的材质为高强度的金属材料，如不锈钢或经过特殊处理的铝合金； 7.紧急按钮：（1）额定电为 DC12V./AC12V；（2）常闭 / 常开触点；（3）拥有 1 块玻璃片； 8.电源箱：（1）为门禁控制系统提供稳定电源；（2）内置短路、过载、过压保护机制，防止电源异常对门禁系统造成损害，提升整个系统的安全性和可靠性：（3）采用耐用材料制成，具备良好的散热性能；（4）能够与不同品牌和型号的门禁系统兼容，满足不同门禁配置的电力需求。
9	半球高清网络摄像机	4 个	1.支持视频认证和加密； 2.内置国密芯片，全面符合国密标准，国密算法加密和认证，保证数据的安全性和真实性，采用高性能图像传感器 3.CMOS 或 CCD 传感器，能提供清晰的视频画面； 4.支持的帧率通常为 1-25 帧/秒，可根据网络带宽和存储需求调整； 5.配备红外 LED 灯，实现日夜转换，即便在低光照或无光环境下也能捕捉清晰图像； 6.支持高效的视频编码技术，降低存储和传输成本； 7.半球型设计，适合室内安装，具有防水、防尘等级（如 IP66），可在多种环境下稳定工作。 8.具备《商用密码产品认证证书》。

10	视频安全管理系统	1 套	1.支持视频认证和加密； 2.内置国密密码卡，全面符合国密标准，国密算法加密和认证，保证数据的安全性和真实性； 3.可支 SVAC2.0、H.264、H.265 编码； 4.支持多种网络协议（如 TCP/IP、HTTP、HTTPS、RTSP、ONVIF 等），保证设备间通讯的安全与兼容性； 5.支持本地存储、网络存储(NAS/SAN)、云存储等多种模式，具备智能存储策略，如按事件重要性存储、低帧率存储等，以及数据加密保护； 6.支持 SSL/TLS 加密通信，用户权限管理，防止非法访问和操作，确保数据安全； 7.易于与其他安防系统（如门禁、消防、报警系统）及业务管理系统集成，实现统一管理和联动响应。 8.具备《商用密码产品认证证书》。
11	边界防火墙	1 台	▲1.整机性能：防火墙吞吐量≥9Gbps，最大并发连接数≥400 万，每秒新建连接数≥8 万； ▲2.实配：千兆 Combo 接口≥8，千兆电口≥2，万兆光口≥2，1 个 Console 口，2 个 USB 接口，提供 IPS、AV 特征库升级授权≥36 个月，提供 URL 远程查询升级授权≥36 个月，可插拔双电源，内存≥8GB，硬盘≥64G； 3.IPS 吞吐量≥2.2Gbps，IPSecVPN 吞吐量≥3.7Gbps，SSLVPN 吞吐量≥500Mbps； 4.IPSecVPN 隧道数≥4000，SSLVPN 并发在线用户数≥1000，免费送 100 个； 5.防火墙转发时延≤18μs； 6.实配虚拟防火墙数量≥100； 7.标准机架式 1U 设备； ●8.投标产品采用自主研发的关键芯片(CPU)； 9.当风扇模块出现故障时，在防火墙不断电的情况下，对风扇模

			块进行更换；为了避免防火墙过热，要求更换风扇模块所用的时间控制在 1 分钟内； 10.严格前后风道； 11.支持设备的 WEB 管理页面中直接打开 CLI 控制命令； 12.支持基于源 IP/目的 IP，服务类型，应用类型，安全域，时间段等字段进行安全策略规则的配置； ●13.支持一条安全策略中同时配置 ipv4 和 ipv6 地址； 14.支持安全策略阻断时设备发送反馈报文快速断开连接，如针对 TCP 报文反馈 reset 报文，针对 UDP 和 ICMP 报文反馈 ICMP 不可达报文； 15.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议； ●16.支持 SRv6 协议； 17.策略路由支持的匹配条件：源 IP/目的 IP，服务类型，应用类型，用户(组)，入接口，DSCP 优先级； 18.支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议； 19.支持 IPv6overIPv4 隧道，6RD 隧道； 20.支持每 IP 最大连接数限制，防护服务器； 21.支持 NAT66，NAT64 功能；	
12	INC 硬件服务设备	3 台	1.国产品牌机架式服务器； 2.配置≥2 颗国产 CPU，核数≥16 核，主频≥2.9GHz； 3.配置≥2 条 32GBDDR4 内存条； 4.配置≥1 块 2T3.5 寸 HDDSAS 硬盘； 5.配置不少于 2 个千兆电口（支持 IPV6 路由协议）；配置 2 个交流电源模块，支持 1+1 冗余。	
七	**广域网对接(含二平面)配套设施租赁服务**	**租赁和商务服务业**	**1 项**	**1.租赁周期：自合同生效之日起三年。 2.租赁设备清单详见以下《广域网对接（含二平面）配套设施租赁服务租赁设备清单及设备技术要求一览表》。**

广域网对接（含二平面）配套设施租赁服务租赁设备清单及设备技术要求一览表			
序号	设备名称	数量及单位	技术要求
1	子网、企业边界防火墙	2 台	▲1.整机性能：防火墙吞吐量≥25Gbps，最大并发连接数≥1000万，每秒新建连接数≥25 万； ▲2.实配：千兆 Combo 接口≥8，千兆电口≥4，千兆光口≥4，万兆光口≥6，2 个交流电源，1 个固态硬盘-960GB-SATA； 3.配置 3 年 AV 防病毒升级服务、IPS 特征库升级服务和 URL 远程查询升级服务授权； 4.IPS 吞吐量≥10Gbps，IPSecVPN 吞吐量≥25Gbps，SSLVPN 吞吐量≥1.5Gbps； 5.IPSecVPN 隧道数≥15000，SSLVPN 并发在线用户数≥2000； 6.防火墙转发时延≤18μs； 7.虚拟防火墙数量≥1000； 8.支持 2 条万兆光 Bypass 链路； 9.支持扩展槽位≥2； 10.支持 USB3.0； 11.标准机架式 1U 设备； ●12.投标产品采用自主研发的关键芯片(CPU)； 13.当风扇模块出现故障时，在防火墙不断电的情况下，对风扇模块进行更换；为了避免防火墙过热，要求更换风扇模块所用的时间控制在 1 分钟内； 14.支持冗余电源，要求防火墙安装了两块电源模块时，其中的一块可以进行热插拔； 15.严格前后风道； 16.支持设备的 WEB 管理页面中直接打开 CLI 控制命令； 17.支持基于源 IP/目的 IP，服务类型，应用类型，安全域，时间段等字段进行安全策略规则的配置；

			●18.支持一条安全策略中同时配置 ipv4 和 ipv6 地址； 19.支持安全策略阻断时设备发送反馈报文快速断开连接，如针对 TCP 报文反馈 reset 报文，针对 UDP 和 ICMP 报文反馈 ICMP 不可达报文； 20.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议； ●21.支持 SRv6 协议； 22.策略路由支持的匹配条件：源 IP/目的 IP，服务类型，应用类型，用户(组)，入接口，DSCP 优先级； 23.支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议； 24.支持 IPv6overIPv4 隧道，6RD 隧道； 25.支持每 IP 的最大连接数限制，防护服务器； 26.支持 NAT66，NAT64 功能；	
八	**城域网区配套设施租赁服务**	租赁和商务服务业	1 项	**1.租赁周期：自合同生效之日起三年。 2.租赁设备清单详见以下《城域网区配套设施租赁服务租赁设备清单及设备技术要求一览表》。**
城域网区配套设施租赁服务租赁设备清单及设备技术要求一览表				
序号	**设备名称**	**数量及单位**	**技术要求**	
1	城域网横向边界防火墙	2 台	▲1.防火墙吞吐量≥50Gbps，最大并发连接数≥2000 万，每秒新建连接数≥50 万； ▲2.实配：千兆 Combo 接口≥8，千兆电口≥4，万兆光口≥10,2 个交流电源，1 个固态硬盘-960GB-SATA； 3.IPS 吞吐量≥18Gbps,IPSecVPN 吞吐量≥30Gbps,SSLVPN 吞吐量≥3Gbps； 4.IPSecVPN 隧道数≥20000，SSLVPN 并发在线用户数≥5000； 5.防火墙转发时延≤18μs；	

			6.配置 3 年 IPS、AV 特征库升级服务和 URL 远程查询升级服务授权； 7.支持 2 条万兆光 Bypass 链路； ●8.产品采用自主研发的关键芯片(CPU)； 9.严格前后风道； 10.支持设备的 WEB 管理页面中直接打开 CLI 控制命令； 11.支持基于源 IP/目的 IP，服务类型，应用类型，安全域，时间段等字段进行安全策略规则的配置； ●12.支持一条安全策略中同时配置 ipv4 和 ipv6 地址； 13.支持安全策略阻断时设备发送反馈报文快速断开连接，如针对 TCP 报文反馈 reset 报文，针对 UDP 和 ICMP 报文反馈 ICMP 不可达报文； 14.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议； ●15.支持 SRv6 协议； 16.策略路由支持的匹配条件：源 IP/目的 IP，服务类型，应用类型，用户(组)，入接口，DSCP 优先级； 17.支持 IPv6 协议栈、IPV6 穿越技术、IPV6 路由协议； 18.支持 IPv6overIPv4 隧道，6RD 隧道； 19.支持每 IP 的最大连接数限制，防护服务器；
2	汇聚路由器万兆板卡	5 个	1.扩容锐捷 RSR7708 的业务板卡，不少于 2 个万兆光口（不含光模块）； 2.提供三年标准保修服务。
3	万兆单模光模块	10 个	万兆单模光模块，波长 1310nm,传输距离 10KM，要求与“SDN 交换机”同一品牌。
▲一、商务要求			
服务期、交付时间、交付及服务地点			1.服务期：自合同生效之日起三年。 2.交付时间：设备自合同签订之日起 90 日内安装调试完毕并交付使用。 3.交付及服务地点：采购人指定地点。

合同签订时间	自中标通知书发出之日起15日内。
付款条件（进度和方式）	分期付款： 第一期：2024年12月31日前，收到发票后10个工作日内支付合同金额的30%。 第二期：2025年12月31日前，收到发票后10个工作日支付合同金额的35%。 第三期：2026年12月31日前，收到发票后10个工作日支付合同金额的35%。 （注：每次支付前，中标人须向采购人提供付款申请和对应金额的合法发票，采购人在收到发票后10个工作日内支付至中标人账户。）
售后服务要求	1.中标人负责送货到采购人现场，在采购人要求的时间内完成本项目采购需求中所有货物及工程的安装调试；设备到位后的安装、调试、培训，均由生产厂商或中标人负责提供，并由专职工程师分工执行。 2.所有设备必须是全新、原装的，未使用过的产品，货物到货后，设备到货后，中标人和采购人应在现场进行清点核对，清点核对过程中如果发现因包装或运输不当引起的仪器外观或内部的损坏，中标人承担所有责任。 3.中标人交货时须提供产品说明书、保修卡、合格证产品目录、图纸、操作手册、试用说明、维护手册或服务指南等供货商品的配套资料。 4.服务期内，中标人须负责所投入的设备的故障维修、更换、保养等。 5.响应及故障修复时间：中标人接到通知后应在4小时内响应并到采购人指定现场，按国家及行业标准进行及时处理，若未能在24小时内完成问题处理的，由中标人负责必须提供备用机。 6.中标人的响应设备，在质保期如有质量监督部门要求对产品进行检测、检验时，必须派出厂方代表协助检查，无论产品有无质量问题，中标人均应承担全部费用及相应的责任。
二、与实现项目目标相关的其他要求	
（一）投标人的履约能力要求	
管理体系要求	详见《第四章　评标方法及评标标准》
业绩要求	详见《第四章　评标方法及评标标准》

（二）验收标准
1.质量要求：符合现行国家相关标准、行业标准、地方标准或者其他标准、规范。 2.验收过程中所产生的一切费用均由中标人承担。报价时应考虑相关费用。 3.中标人在服务、货物工程交付验收时，由采购单位对照招标文件的项目要求及技术需求，全面核对检验。如不符合招标文件的技术需求及要求以及提供虚假承诺的，按相关规定做违约处理，中标人承担所有责任和费用，采购人保留进一步追究责任的权利。 4.验收方式： 1）货物验收：货物交付完毕后接到中标人的验收申请后 5 个工作日内进行验收； 2）完成合同约定的全部事项，并满足使用要求； 3）验收材料齐全； 4）满足合同或合同附件规定的其他验收条件。 5.验收依据：招标文件、投标文件、国家有关的质量标准规定均为验收依据。 6.采购人有权委托相关具部门、单位、机构针对交付成果、进行检验。其检查结果将作为验收标准的组成部分之一。 7.验收时中标人必须派代表参加。
（三）其他要求
1.投入的项目团队：至少投入 1 名项目经理，1 名网络安全专家，1 名网络工程师，3 名专业安全服务人员。 2.为保证项目顺利实施，投标人可根据自身情况在投标文件中提供项目技术实施方案、质量和保密保证措施及承诺和售后服务方案等内容。 3.本项目所要求提供的设备均为配套本运维服务项目的设备，投标人须在服务期内无条件提供，并保持设备的顺利、畅通运行，服务期满后中标人可与采购人协商进行设备后续的处理工作。
（四）采购人的特殊要求及说明
本项目货物不接受进口产品（即通过中国海关报关验放进入中国境内且产自关境外的产品）参与投标，如有此类产品参与投标的做无效标处理。
（五）核心产品
本项目属性为服务类项目，无核心产品。

开标一览表

序号	标的的名称	数量及单位①	单价②	投标报价 ③=①×②
一、机房优化改造集成服务				
1	机房空调系统优化改造服务	1 项	456016.00	456016.00
二、安全服务				
1	网络安全运维服务	1 项	600000.00	600000.00
2	网络运维服务	1 项	450000.00	450000.00
3	应急响应服务	1 项	330000.00	330000.00
4	应急演练服务	1 项	270000.00	270000.00
5	安全风险评估及整改服务	1 项	240000.00	240000.00
6	等保测评服务	1 项	270000.00	270000.00
7	商用密码应用安全性评估服务	1 项	200000.00	200000.00
8	安全监测系统服务	1 项	660000.00	660000.00
9	安全培训	1 项	140000.00	140000.00
三、集成服务				
1	网络集成服务	1 项	520000.00	520000.00
2	安全集成服务	1 项	230000.00	230000.00
3	设备系统集成服务	1 项	400000.00	400000.00
4	网络运维服务系统集成	1 项	3500000.00	3500000.00
四、线路租赁服务				
1	互联网出口线路 1	1 条	432000.00	432000.00
2	互联网出口线路 2	1 条	216000.00	216000.00
3	互联网出口线路 3	1 条	54000.00	54000.00
4	城域网横向电路 1	2 条	144000.00	288000.00
5	城域网横向电路 2	27 条	27000.00	729000.00
6	城域网横向电路 3	163 条	18720.00	3051360.00
7	城域网横向电路 4	73 条	15120.00	1103760.00
8	城域网横向电路 5	3 条	12600.00	37800.00
9	城域网横向电路 6	5 条	10800.00	54000.00
10	5G 网关备用线路服务	1 套	6064.00	6064.00
11	接入路由器	20 台	2810.00	56200.00

五	互联网服务接入区配套设施租赁服务			
互联网服务接入区配套设施租赁服务租赁设备清单及设备技术要求一览表				
1	分布式拒绝服务攻击防护系统	2 台	187100.00	374200.00
2	出口路由器	2 台	172750.00	345500.00
3	SDN 交换机	2 台	47850.00	95700.00
4	出口防火墙	2 台	224675.00	449350.00
5	入侵防御设备	2 台	75650.00	151300.00
六	安全管理中心区（运维中心）配套设施租赁服务			
安全管理中心区（运维中心）配套设施租赁服务租赁设备清单及设备技术要求一览表				
1	IPSec/SSL 安全网关	1 台	74200.00	74200.00
2	堡垒机（国密版）	1 台	224100.00	224100.00
3	服务器密码机	1 台	89400.00	89400.00
4	签名验签服务设备	1 台	74700.00	74700.00
5	国密门禁	1 台	55100.00	55100.00
6	国密密钥系统	1 台	21100.00	21100.00
7	国密卡	5 张	60.00	300.00
8	门禁配件	2 套	15800.00	31600.00
9	半球高清网络摄像机	4 个	2700.00	10800.00
10	视频安全管理系统	1 套	25300.00	25300.00
11	边界防火墙	1 台	85600.00	85600.00
12	INC 硬件服务设备	3 台	50500.00	151500.00
七	广域网对接（含二平面）配套设施租赁服务			
广域网对接（含二平面）配套设施租赁服务租赁设备清单及设备技术要求一览表				
1	子网、企业边界防火墙	2 台	137800.00	275600.00
八	城域网区配套设施租赁服务			
城域网区配套设施租赁服务租赁设备清单及设备技术要求一览表				
1	城域网横向边界防火墙	2 台	224675.00	449350.00
2	汇聚路由器万兆板卡	5 个	22800.00	114000.00
3	万兆单模光模块	10 个	510.00	5100.00
合计金额大写：人民币壹仟柒佰叁拾玖万捌仟元整（¥17398000.00）				