用户需求书

一、项目概况

1、项目名称：保亭黎族苗族自治县党政机关互联网统一出口建设项目

2、项目预算：¥2538700.00（人民币贰佰伍拾叁万捌仟柒佰元整）包干价。

3、资金来源：财政资金

4、交货地点：用户指定地点

5、付款方式：付款方式由双方协商。

6、验收要求：按招标文件的技术要求和国家行业标准进行验收

二、用户需求

（一）业务需求

各党政机关互联网业务需求为:1.网页浏览;2.业务办理;3.在线学习;4.VPN访问电子政务网络；5.其他应用。

本期需实现各单位以专线方式完成网络的统一出口，接入电子政务外网和互联网，同时将统一出口平台的信息安全技术网络安全保护等级提升为二级。

本项目其他业务需求分述如下。

1.宽带性能需求

为满足今后接入单位对带宽的需求，根据对 32 家党政机关接入互联网带宽情况统计及电信运营商对部分党政机关近期上网情况的分析，按照每秒并发量比例为0.35，政务信息系统访问每人平均宽度为2M/bps模型计算，带宽为816M/bps。建议主用链路带宽设计为 500M，备用链路带宽设计为 100M。各委办局的出口带宽测算为下表，建议带宽汇总为 12 条 30M，14 条 50M，6 条 100M。

序号	职能局名称	带宽
		M/bps
1	县纪委县监委	50
2	县委办公室	50
3	县委组织部	50
4	县委宣传部	50

序号	职能局名称	带宽
		M/bps
5	县委统战部	30
6	县委政法委	30
7	县委机构编制委员会办公室	30
8	县政协办公室	30
9	县人大办公室	30
10	县政府办公室	100
11	县发展和改革委员会	50
12	县自然资源和规划局	30
13	县旅游和文化广电体育局	100
14	县生态环境局	30
15	县农业农村局	50
16	县教育局	100
17	县科技和工业信息产业局	30
18	县财政局	50
19	县人力资源和社会保障局	30
20	县卫生和健康委员会	100
21	县公安局	30
22	县司法局	50
23	县民政局	50
24	县住房和城乡建设局	50
25	县交通局	50
26	县审计局	50
27	县退役军人事务局	30
28	县应急管理局	100
29	县市场监督管理局	100
30	县法院	50
31	县检察院	30

序号	职能局名称	带宽
		M/bps
32	县扶贫工作办公室	50
汇总		/

2.安全保障建设需求

保亭县网络安全系统将按照二级安全等级保护技术要求进行设计，完善网络体系结构、解决边界隔离、终端恶意代码感染、非法上网行为等网络安全问题。建成后将具备有效监管、审计功能，加强网络安全事件回溯等能力。

3.租赁运营商机柜需求

保亭县网络统一出口平台拟租赁运营商机柜。具体需求如下：

本项目需要将本期新增设备部署到运营商机房，因此本期项目计划租赁运营商机房 1 个机柜。

租赁的机房应满足等保二级对机房环境的要求：

（1）物料位置选择

机房场地应选择在具有防震、防风和防雨等能力的建筑内；

机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

（2）物理访问控制

机房出人口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进人的人员。

（3）防盗窃和防破坏

应将设备或主要部件进行固定，并设置明显的不易除去的标识；

应将通信线缆铺设在隐藏安全处。

（4）防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

（5）防火

机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

（6）防水和防潮

应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；

应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

（7）防静电

应采用防静电地板或地面并采用必要的接地防静电措施。

（8）温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

（9）电力供应

应在机房供电线路上配置稳压器和过电压防护设备；

应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求。

（10）电磁防护

电源线和通信线缆应隔离铺设，避免互相干扰。

4.系统可扩展性需求

随着网络建设的不断发展，信息应用系统管理与服务也将不断产生新的需求，平台逐步建设。故本项目的建设成果将做为信息应用系统建设持续发展的重要基础，因此在系统设计和建设上要充分考虑今后一段时期内可扩展性的需要。

5.系统可靠性需求

不同的应用功能需求对于系统可靠性要求有所不同，对于信息服务而言，系统需要 7x24 小时连续运行；对于安全管理而言，系统需要 7x24 小时连续运行，系统可靠性应达到 99.9%。

（二）网络安全建设需求

1.网络安全基础设施建设需求

结合等级保护 2.0 相关标准和要求以及国内外最新的安全防护体系模型，从保障用户业务安全高效运行为根本出发点，依据等级保护政策、标准、指南等文件要求以及用户业务安全需求，对保护对象进行区域划分和定级，对不同的保护对象从物理环境防护、通信网络防护、区域边界防护、计算环境防护等各方面进行不同级别的安全防护设计。同时统一的安全管理中心保障了防护的有效协同及一体化管理，保障了安全技术措施有效运行和落地。以等级保护安全框架为依据和参考，在满足国家法律法规和标准体系的前提下通过“一个中心、三重防护”

的安全设计，形成网络安全综合技术防护体系。突出技术思维和立体防范，注重全方位主动防御、动态防御、整体防控和精准防护。

（1）安全通信网络需求

安全通信网络重点关注的安全问题主要涉及网络架构安全、通信传输安全和通信设备安全等方面，具体包括对网络区域的合理划分、对重要网络区域的可靠隔离、对网络设备性能和网络带宽的有效保障、对通信链路冗余、对数据传输的完整性和保密性保护、对通信设备及通信应用程序的可信验证等。

（2）安全区域边界需求

区域边界重点关注的安全问题主要是对流入、流出边界的数据流进行有效的控制和监督。这里所说的边界包内部网络与外部网络之间的边界、内部网络不同安全域之间的边界等。具体措施包括访问控制、入侵防范、恶意代码和安全审计、安全审计等。

（3）安全管理中心需求

依据《网络安全等级保护安全设计技术要求》，同时参照《网络安全等级保护基本要求》、《网络安全等级保护安全管理中心技术要求》，对等级保护对象涉及到的安全管理中心进行设计，设计内容包括系统管理、安全管理、审计管理和网络监控等方面。

2.网络安全等保需求

依据《中华人民共和国网络安全法》，国家实行网络安全等级保护制度。网络运营者按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改；关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。

（1）业务信息安全保护等级的确定

保亭黎族苗族自治县党政机关互联网统一出口建设项目其安全受到破坏时，所侵害的客体属于社会秩序、公共利益。

保亭黎族苗族自治县党政机关互联网统一出口建设项目安全受到破坏时，其侵害程度为一般损害。根据或者业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据业务信息安全保护等级矩阵表，即可得到或者业务信息安全保护等级为第二级。

3.机房及配套需求

本项目计划租赁运营商机房机柜空间，以减少机房等基础配套投资费用。

本期租赁机架空间需求如下表所示：

序号	安全域	设备	数量	设备功耗（W）		备注
			（台）	单台设备	小计	
1	互联出口区	互联网防火墙	1	250	250	新增
2		上网行为管理系统	1	350	350	新增
3	政务外网出口区	政务外网防火墙	1	250	250	新增
4	安全管理区	安全管理汇聚交换机	1	100	100	新增
5		安管一体机	1	400	400	新增
6		准入及主机管理服务器	1	300	300	新增
8	核心交换区	核心交换机	2	250	500	新增
9	外联汇聚区	外联边界防火墙	1	250	250	新增
10		外联汇聚交换机	1	250	250	新增
合计			10		2650	

4.服务器需求

新增 1 台服务器（准入及主机管理服务器）用于准入系统的承载。

准入系统提供了强大监控能力，从网络到设备直至应用系统的监控。在对事件的监控信息的集中及关联分析的基础上，有效的实现了全网的安全预警、入侵行为的实时发现、入侵事件动态响应，通过于其它安全设备的联动来真正实现动态防御。

5.网络需求

结合当前网络现状，本期项目需新增 2 台核心交换机、1 台外联汇聚交换机、1 台安全管理汇聚交换机。

1. 核心层配置 2 台高性能模块化核心交换机，为党政机关统一互联网出口提供网络基础保障。核心交换机与互联网出口区上网行为管理设备相连，通过互联网出口区防火墙访问互联网。核心交换机通过政务外网防火墙租用裸光纤与政务外网接入路由器相连，通过县核心路由器访问电子政务外网。

2. 安全管理区新增 1 台安全管理汇聚交换机，汇聚安全设备后与核心交换机

相连。

3.32 个单位各自新增委办局接入交换机(每个局点部署 1 台委办局交换机，由各委办局自主负责采购，可以利旧原有交换机），并通过租用运营商 32 条专线接入新增的 1 台外联汇聚交换机；外联汇聚交换机通过外联防火墙上联核心交换机，以满足各单位对业务网络访问要求。

本期负责互联网出口区、安全管理区、核心交换区、外联汇聚区的建设；外联单位接入区的接入交换机与综合布线由各委办局负责建设。

本期工程负责 1 年的运营商 32 条专线建设，后续由各委办局负责购买。

6. 安全保障建设需求

保亭县网络安全系统将按照二级安全等级保护技术要求进行设计，完善网络体系结构、解决边界隔离、终端恶意代码感染、非法上网行为等网络安全问题。建成后将具备有效监管、审计功能，加强网络安全事件回溯等能力。

本期需新增上网行为管理、安管一体机、互联网防火墙、政务外网防火墙、外联边界防火墙、准入系统各 1 台。

（三）运行维护需求

委托企业进行系统平台软硬件的运维工作，主要负责区域内所有设备及系统的正常运行维护工作。

（四）运维服务内容

主要包括网络日志采集支撑、日常维护工作等运维方式，全方位保障本项目平台平稳、高效和有序的运行。

需配合建设单位采集整理网络平台安全日志，并按建设单位要求上报给上级部门。包括：

1. 健康检查运维服务

为了确保用户安全系统长期、稳定的工作，最大限度和降低系统的运行故障及延长系统设备的使用寿命，应定期对网络及安全设备进行健康检查服务，在保证系统安全的前提下采集系统配置、流量信息、系统状态等安全信息，依照标准化流程，定期对用户的系统进行检查，了解系统的整体工作状态。由被动服务变主动服务，通过健康检查服务排除故障隐患，降低故障率。

2. 安全事件审计运维服务

定期对各类系统产生的安全日志实现全面、有效的集中收集、管理、审计服务。

3.网络行为审计运维服务

网络行为审计服务深入了解网络用户、网络设备和网络应用的历史和实时行为，基于用户使用网络的实际行为来优化和调整网络，实现了真正以用户为中心行为分析，能够对典型的网络行为和用户行为进行实时的的网络服务和网络管理。网络行为审计服务通过收集并分析用户网络行为数据，从而发现违反安全策略的行为。即当发生安全事故或者发生违反安全策略的行为之后，通过检查、分析、比较用户网络行为数据，从中发现违反安全策略行为的记录。以利于事后追踪，为调查取证提供第一手的资料。

（五）运维服务提供方式

按照<<海南省信息化管理条例>>规定,要求本项目承建方免费提供两年的运维服务；两年后由建设单位根据具体情况研究决定是采用外包或自运维模式。

附件 1：保亭黎族苗族自治县党政机关互联网统一出口建设项目软硬件设备、材料及链路租用采购需求表

序号	名　称	技术参数	单位	数量	备注
一	硬件				
1	互联网防火墙	1、多核 AMP+架构，网络层吞吐量 4G，全威胁应用吞吐性能不少于 1Gbps，并发连接≥180 万，每秒新建连接数 6 万，配置不少于 6 个 10/100/1000M 自适应电口，不少于 4 个千兆光口，1 个 Console 口； 2、含三年硬件维保服务，防病毒安全/IPS 特征库三年。 3、▲所投产品必须支持基于不同安全区域防御 DNS Flood、HTTP Flood 攻击，并支持警告、阻断、首包丢弃、TC 反弹技术、NS 重定向、自动重定向、手工确认等多种防护措施（投标文件需要提供能够体现上述功能及配置选项的截图，加盖生产厂商公章或投标专用章）； 4、所投产品必须支持 MTU≥9000byte 的巨型帧 Jumbo Frame； 5、▲所投产品必须能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀；本地病毒库规模大于 3000 万，支	台	1	

序号	名　称	技术参数	单位	数量	备注
		持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞防护（投标文件需要提供能够体现漏洞防护特征库分类信息、支持的执行动作以及支持的应用协议的截图，并加盖生产厂商公章或投标专用章）； 6、▲所投产品必须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；并对威胁情报发现的恶意主机执行自动阻断（投标文件需提供能够体现被入侵、攻破的主机状态的截图，加盖生产厂商公章或投标专用章）； 7、公安部《计算机信息系统安全专用产品销售许可证（增强级）》（要求提供证明材料，并加盖生产厂商公章或投标专用章）； 8、▲要求投标产品制造商具有强大的持续安全数据漏洞挖掘能力，能够对安全漏洞进行持续的挖掘与跟踪。2019 年向 CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前五名（要求提供证明材料，加盖生产厂商公章或投标专用章）； 9、▲为保证本项目交付后的安全效果，要求设备厂商具备专业的信息技术服务标准能力，应具有“信息化建设及服务能力评价资质一级”证书并取得权威机构的认证（要求提供证明材料，并加盖生产厂商公章或投标专用章）			
2	上网行为管理	1、 机架式硬件网关产品，使用多核架构设计，能够应对多种业务应用，带机量≥2000 人/终端；网络层应用吞吐性能≥8Gbps，应用层吞吐性能≥3.5Gbps； 2、 支持路由模式、透明（网桥）模式、混合模式，部署模式切换无需重启设备； 3、 提供≥12 个 GE 电口、≥12 个 GE 光口、≥1T 内置硬盘、	台	1	

序号	名　称	技术参数	单位	数量	备注
		冗余 1+1 电源设计； 4、 支持 DDNS，支持黑名单用户显示、SSL VPN 在线用户显示、实时用户/应用流速统计 5、 支持同步账号给认证服务器展示用户认证、账号信息，实现基于账号溯源； 6、 应用识别特征库数量≥5000+，可针对特定无应用指纹的应用：迅雷、P2P 下载支持行为模式的智能识别。支持智能和快速识别模式配置； 7、 支持首页展示网络状态、包括在线用户、审计日志类别及数量、流量分析、违规用户信息等，支持显示系统信息、实时流量、系统资源、接口状态、用户 TOP 流量、应用 TOP 流量统计、系统日志信息、审计日志信息等，提供 web 配置界面，加盖生产厂商公章或投标专用章； 8、 ▲支持小时/天/周为单位的用户流量、应用流量、设备流量趋势图、列表 TOP 统计展示；支持用户虚拟身份画像，以时间轴的形式展示用户上网行为轨迹；支持对单用户进行网站访问质量检测，提供 web 配置界面，加盖生产厂商公章或投标专用章； 9、 ▲支持基于防护策略的精准访问控制匹配次数、防盗链、SCRF、CC 攻击防护统计等，提供 web 配置界面，加盖生产厂商公章或投标专用章； 10、 用户行为审计：http、邮件、即时通讯、基础协议、娱乐股票、网络应用六个大类维度的用户应用审计： http 类审计支持网页访问、网络社区（微博、论坛）、网页搜索、http 外发文件、http 文件下载、web 网盘上传文件、web 网盘下载文件等细粒度的审计； 邮件类审计支持 smtp 的发邮件，imap&pop3 收邮件、外发的 web mail 邮件内容、外发的 web mail 邮件附件、接受的 webmail 邮件内容、接受的 webmail 邮件附件等细粒度的审计； 即时通讯类审计支持 IM 聊天行为审计、网页版微信审计、其他即时通讯类软件审计等细粒度的审计； 基础协议类审计支持 FTP 的账号和文件名相关审计；			

序号	名　称	技术参数	单位	数量	备注
		娱乐股票类审计，支持娱乐类的账号和评论审计，支持股票类的账号审计； 其他应用行为审计，支持管理员选择相关审计的应用大类。 11、 支持≥6000+条入侵攻击特征，包括 Web 服务器防护，包括网页防爬虫、网页防篡改、HTTPS 防护、DDoS 攻击防护、Web 攻击过滤、漏洞防护等 12、 支持服务器非法外联管控，并支持服务器外联白名单地址自学习 13、 ▲为保障产品选型符合安全审计标准，投标产品具备网络通讯安全审计产品（国标-增强级）销售许可证，提供有效证书复印件，并加盖生产厂商公章或投标专用章； 14、 为保证投标产品厂商在安全漏洞方面的整体研究水平和及时预防能力。具备网络安全漏洞统一收集验证、预警发布及应急处置体系，进而提高产品的安全性。产品生产厂商须进入国家信息安全漏洞共享平台（CNVD）技术组成员，要求提供有效证书复印件，并加盖生产厂商公章或投标专用章；			
3	政务外网防火墙	1、多核 AMP+架构，网络层吞吐量 4G，全威胁应用吞吐性能不少于 1Gbps，并发连接≥180 万，每秒新建连接数 6 万，配置不少于 6 个 10/100/1000M 自适应电口，不少于 4 个千兆光口，1 个 Console 口； 2、含三年硬件维保服务，防病毒安全/IPS 特征库三年。 3、▲所投产品必须支持基于不同安全区域防御 DNS Flood、HTTP Flood 攻击，并支持警告、阻断、首包丢弃、TC 反弹技术、NS 重定向、自动重定向、手工确认等多种防护措施（投标文件需要提供能够体现上述功能及配置选项的截图，加盖生产厂商公章或投标专用章）； 4、所投产品必须支持 MTU≥9000byte 的巨型帧 Jumbo Frame； 5、▲所投产品必须能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀；本地病毒库规模大于 3000 万，支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、	台	1	

序号	名　称	技术参数	单位	数量	备注
		WEB 攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞防护（投标文件需要提供能够体现漏洞防护特征库分类信息、支持的执行动作以及支持的应用协议的截图，并加盖生产厂商公章或投标专用章）； 6、▲所投产品必须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；并对威胁情报发现的恶意主机执行自动阻断（投标文件需提供能够体现被入侵、攻破的主机状态的截图，加盖生产厂商公章或投标专用章）； 7、公安部《计算机信息系统安全专用产品销售许可证（增强级）》（要求提供证明材料，并加盖生产厂商公章或投标专用章）； 8、▲要求投标产品制造商具有强大的持续安全数据漏洞挖掘能力，能够对安全漏洞进行持续的挖掘与跟踪。2019 年向 CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前五名（要求提供证明材料，加盖生产厂商公章或投标专用章）； 9、▲为保证本项目交付后的安全效果，要求设备厂商具备专业的信息技术服务标准能力，应具有“信息化建设及服务能力评价资质一级”证书并取得权威机构的认证（要求提供证明材料，并加盖生产厂商公章或投标专用章）			
4	核心交换机	1、 机框式可扩展交换机，独立业务槽位≥3 个，配置独立单主控； 2、 转发性能≥7000Mpps，交换容量≥38Tbps； 3、 配置≥24 个 GE 电口，≥24 个 GE 光口，≥8 个万兆光口；含 4 个万兆多模模块及 4 个千兆多模模块，1 条万兆堆叠线缆； 4、 ▲MAC 地址表容量≥1000K，学习速率≥128K/S，提供工信部权威第三方测试报告，加盖生产厂商公章或投标专	台	2	

序号	名　称	技术参数	单位	数量	备注
		用章； 5、 支持安全业务插卡 FW、IPS、ACG、LB、SSL VPN，提供官网截图证明； 6、 支持以太网多环保护技术，能够快速阻断环路； 7、 支持堆叠技术； 8、 支持 IEEE 802.1ae 介质访问控制安全技术； 9、 ▲内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级，提供工信部权威第三方测试报告，加盖生产厂商公章或投标专用章； 10、为方便运维管理，与对外联汇聚交换机、安全汇聚交换机同一品牌，并进行配置下发和统一管理；			
5	安全管理汇聚交换机	1、 转发性能≥133Mpps，交换容量≥560Gbps； 2、 配置≥48 个 GE 光口、≥4 个 10GE 光口；2 个万兆多模光模块； 3、 MAC 地址表容量≥64K，路由表容量≥32K 4、 支持以太网多环保护技术，能够快速阻断环路； 5、 支持堆叠技术； 6、 为方便运维管理，与核心交换机同一品牌；	台	1	
6	准入系统	1、 配置≥100 点网络设备管理授权，≥2000 点终端安全管理授权，≥2000 点终端管理软件（具备终端识别功能）； 2、 ▲终端软件能够兼容保亭县政府办公 OA SSL VPN 及省政务外网 SSL VPN 环境，如不支持应提供对接开发服务；提供技术承诺函，加盖生产厂商公章或投标专用章； 3、 ▲使用同一个客户端接入保亭县政府办公 OA SSL VPN 及省政务外网 SSL VPN 环境，实现网络准入、用户认证、终端安全状态检查、桌面资产管理等所有功能，可避免多个客户端带来的管理不便。 4、 精准识别终端类型，支持账号与终端绑定、基于账号的溯源； 5、 支持与包括微软防病毒软件在内的主流防病毒软件联动，支持与微软 WSUS/SCCM 协同的自动补丁管理。与微软无缝集成，当用户安全认证时，自动检查、下载、安装补丁，实现操作系统补丁自动升级，提升系统易用性。可定	套	1	

序号	名　称	技术参数	单位	数量	备注
		期巡查操作系统补丁； 6、 支持 802.1x、Portal、L2TIP IPSec VPN、SSL VPN、无线等多种网络环境的身份认证，支持基于端口的 802.1x 和基于 MAC 地址的 802.1x，可管理 HUB 或非智能交换机下的多个用户。 7、 ▲VPN 接入及 NAT 穿越：支持 L2TP 接入方式，可以设置备用 LNS，支持虚拟网卡，指定 USB Key 认证等；支持 L2TP+IPSec，可以支持 LNS 服务器和 IPSec 服务器合一和分开，支持 NAT 穿越，支持 PPP 协商过程中获取安全认证服务器信息，发起安全认证。提供功能截图并加盖生产厂商公章或投标专用章； 8、 ▲统一身份认证：支持 PAP/CHAP/EAP-MD5/EAP-PEAP/EAP-TLS/WAPI 等认证协议，支持 USB Key、数字证书、LDAP 服务器、Windows 域管理器、WLAN 等方式的认证及多种方式的组合鉴别；提供功能截图并加盖生产厂商公章或投标专用章； 9、 支持 USB、软驱、光驱、串口、并口、红外、蓝牙、1394 和 Modem 等外设的管理，可区分 USB 存储设备和非存储设备，支持离线策略，拔掉网线依然生效；支持对检测终端 USB 接入状态进行记录和上报，如用户插拔 USB 时间、操作文件名、操作文件大小等详细信息。提供功能截图并加盖生产厂商公章或投标专用章； 10、 ▲支持防内网外联技术：防止内网的主机通过 3G/4G、拨号、多网卡等方式访问外网网络而造成的内部信息泄露。可以支持内网终端屏蔽所有网卡的外部网络访问流量，也可以支持在不连接内网时的外部网络访问。可以设置不检测不控制的特例网卡名单。对出现问题的终端支持审计。提供功能截图并加盖生产厂商公章或投标专用章； 11、 多种终端识别技术：支持通过客户端、DHCP、HTTP、MAC 地址等技术准确识别接入网络的终端厂商、终端类型和操作系统信息； 12、 ▲基于场景的终端网络接入授权：支持根据终端接入区域、接入时间段、终端 IP 地址、终端 MAC 地址、终端厂			

序号	名　称	技术参数	单位	数量	备注
		商、终端操作系统、终端类型、AP、手机号码、IMSI 号码等对网络接入终端授予不同的访问权限。提供功能截图并加盖生产厂商公章或投标专用章；			
7	准入及主机管理服务器	1、标准机架式 X86 服务器； 2、≥intel 两路 2.2GHz，12 核 CPU 模块，≥128G 内存，≥1.8T*3 10K SAS 硬盘 3、≥4 端口 GE 网卡，≥550W 冗余白金电源，导轨，冗余风扇	台	1	
8	安管一体机	安管平台： 1、 提供≥4 个 GE 电口、≥4 个 GE 光口，提供≥2 个管理口，内存≥96G，硬盘容量≥8T； 2、 配置具备综合日志审计功能≥200 日志源、运维审计功能≥60 个资产管理； 3、 可统一在管理平台对日志审计、运维审计各个组件的运维数据进行集中统计展示，提供 web 配置界面，加盖生产厂商公章或投标专用章； 4、 ▲可在管理平台进行各个组件的基础安全业务策略配置的免跳转下发，提供 web 配置界面，加盖生产厂商公章或投标专用章； 5、 设备采用旁路部署模式，系统与目标资源 IP 可达，协议互通即可，不需要改变网络拓扑结构 综合日志审计： 6、 具备日志收集实时监控，可基于设备类型、日志类型、日志等级进行监控查看 7、 支持按照日志等级（调试、通知、重要、警告、错误、严重、设备故障、设备不可用及其他信息）列表展示日志范式化分析结果、下钻支持日志详情 8、 支持用户自定义统计维度展示关联事件审计结果，最多同时展示 6 个维度审计结果 9、 ▲支持全文检索原始日志，检索字段变色高亮；支持任意信息、任意时间进行内容查询匹配，支持可选包含/不包含匹配方式，提供 web 配置界面，加盖生产厂商公章或投标专用章	台	1	

序号	名　称	技术参数	单位	数量	备注
		运维审计： 10、最大图形并发连接数≥150，最大字符并发连接数≥300，支持≥50 个资产管理 11、 系统支持账号分权管理，包括超级管理员、配置管理员、操作员、审计员及自动化人员等多种角色，并可根据功能自定义用户角色 12、 支持访问控制策略按部门分权，不同部门的配置管理员只能针对自己部门及自己直属子部门设备进行访问权限设置 13、 支持审计功能按部门分权，使得不同部门的审计管理员只能审计自己部门、自己直属子部门设备上的操作日志 14、 ▲支持动态权限管控，管理员可基于用户属性、设备属性、系统账号属性来创建弹性动态权限规则，只要满足相关属性的用户、设备、账号即会被自动赋予对应访问权限提供 web 配置界面，加盖生产厂商公章或投标专用章； 资质要求： 15、 投标产品具备公安部《计算机信息系统安全专用产品销售许可证》，提供有效证书复印件，并加盖生产厂商公章或投标专用章； 16、 ▲为保证投标产品厂商在安全漏洞方面的整体研究水平和及时预防能力。具备网络安全漏洞统一收集验证、预警发布及应急处置体系，进而提高产品的安全性。产品生产厂商须进入中国国家信息安全漏洞库（CNNVD）一级技术支撑单位。要求提供有效证书复印件并加盖生产厂商公章或投标专用章；			
9	外联边界防火墙	1、 机架式硬件设备，网络层吞吐性能≥20Gbps，全威胁应用吞吐性能≥13Gbps； 2、 配置≥500 点 SSL VPN 授权；防病毒安全/IPS 特征库 3 年； 3、 配置入侵防御、防病毒攻击和链路负载均衡功能授权或模块 4、 提供≥10 个 GE 电口、≥8 个 GE 光口、≥8 个 10GE 光口、内置≥480G SSD 或 HDD 硬盘、冗余 1+1 电源设计；	台	1	

序号	名　称	技术参数	单位	数量	备注
		5、 能够实现高性能的 IPSec、L2TP、GRE VPN、SSL VPN 等隧道功能。 6、 支持 SM1/2/3/4 国密加密卡，提供功能截图； 7、 可实现包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的防护策略。 8、 ▲支持 sql 注入、跨站脚本、远程代码执行、字符编码等攻击的防护，支持对网络设备、网页服务器、数据库等设备的专属特征分类，支持 CC 攻击防护，可基于检测请求报文头的 X-forward-for 字段,以获取真正的源 IP 地址，提供功能截图并加盖生产厂商公章或投标专用章 9、 ▲支持基于对包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的防护策略。且缺省动作支持黑名单，提供功能截图并加盖生产厂商公章或投标专用章 10、 实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御，实现攻击特征库的分类。IPS 发现攻击后抓取报文，并支持通过 WEB 下载对应抓包文件，供客户进行分析 11、 支持超过≥7000 种特征的攻击检测和防御 12、支持 HTTPS 加密流量的安全检测，支持 TCP 代理和 SSL 代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项 13、 ▲支持报文示踪功能，支持真实流量、导入报文、构造报文等方式，用于分析和追踪设备中各个安全业务模块（如：攻击防范、uRPF、会话管理和连接数限制等）对报文的处理过程，通过查看报文示踪记录的详细信息，有利于管理员对网络故障的快速排查和定位。提供功能截图并			

序号	名　称	技术参数	单位	数量	备注
		加盖生产厂商公章或投标专用章 14、 投标产品具备公安部监制的计算机信息系统安全专用产品销售许可证，提供有效证书复印件并加盖生产厂商公章或投标专用章； 15、 ▲投标产品同时具备中国网络安全审查技术与认证中心颁发的 EAL4 增强级认证证书及信息产业信息安全测评中心出具的防火墙 EAL4+级型式试验报告，提供有效证书复印件并加盖生产厂商公章或投标专用章；			
10	外联汇聚交换机	1、 转发性能≥133Mpps，交换容量≥560Gbps； 2、 配置≥48 个 GE 光口、≥4 个 10GE 光口；2 个万兆多模光模块； 3、 MAC 地址表容量≥64K，路由表容量≥32K 4、 支持以太网多环保护技术，能够快速阻断环路； 5、 支持堆叠技术； 6、 为方便运维管理，与核心交换机同一品牌；	台	1	
11	光模块	千兆单模模块	个	20	
12	光模块	千兆多模模块	个	30	
13	耗材	尾纤网线电源线等	项	1	
二	**资源租赁服务**				
1	互联网统一主出口	500M 出口	月	12	1 年
2	互联网统一备出口	100M 出口	月	12	1 年
3	裸光纤	政务外网防火墙与电子政务外网互联	月	12	1 年
4	委办局汇聚链路	30M 专线,12 条	月	12	1 年，后续费用由各委办局负责购买
5	委办局汇聚链路	50M 专线，14 条	月	12	1 年，后续费用由各委办局负责购买

序号	名　称	技术参数	单位	数量	备注
6	委办局汇聚链路	100M 专线，6 条	月	12	1 年，后续费用由各委办局负责购买
7	主机托管服务费	1 个机柜空间租用，用电租用，设备管理	个	1	1 年
三	**系统集成服务**				
	集成费		项	1	