**项目需求一览表**

**说明：**

1、本招标文件所称中小企业必须符合《政府采购促进中小企业发展暂行办法》第二条规定。

2、小型、微型企业提供中型企业制造的货物的，视同为中型企业。

3、小型、微型企业提供大型企业制造的货物的，视同为大型企业。

4、按照《财政部、司法部关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68号）的规定，监狱企业视同小型、微型企业。

5、按照《关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141号）的规定，残疾人福利性单位视同小型、微型企业。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

6、小型和微型企业产品的价格给予6%-10%的扣除，用扣除后的价格参与评审，具体扣除比例请以第三章《评标方法》的规定为准。

7、**根据财库〔2019〕9号及财库〔2019〕19号文件规定，台式计算机，便携式计算机、平板式微型计算机，激光打印机，针式打印机，液晶显示器，制冷压缩机（冷水机组、水源热泵机组、溴化锂吸收式冷水机组），空调机组[多联式空调（热泵）机组（制冷量＞14000W），单元式空气调节机（制冷量＞14000W）]，专用制冷、空调设备（机房空调），镇流器（管型荧光灯镇流器），空调机[房间空气调节器、多联式空调（热泵）机组（制冷量≤14000W）、单元式空气调节机（制冷量≤14000W）]，电热水器，普通照明用双端荧光灯，电视设备[普通电视设备（电视机）]，视频设备（视频监控设备、监视器），便器（坐便器、蹲便器、小便器），水嘴均为节能产品(政府采购品目清单内标注“★”的品目)，属于政府强制采购节能产品。若采购货物属于以上品目清单的产品时，供应商的投标货物必须使用政府强制采购的节能产品，供应商必须在投标文件中提供由国家确定的认证机构出具的处于有效期之内的节能产品认证证书复印件（加盖投标单位公章），否则相应投标无效。**

8、本采购需求中的品牌、型号仅起参考作用，投标人可选用其他品牌替代，但这些替代的产品品牌、品质必须要实质上相当于或优于参考品牌型号及其技术参数性能（配置）要求。

9、本采购需求中参考品牌、型号及技术参数性能（配置）不明确或有误的，或投标人选用其他品牌型号替代的，请说明品牌型号和详细的技术参数性能（配置）同时填写投标明细表和技术响应表。

10、本项目需求一览表中标注▲号的内容为实质性要求和条件，必须满足或优于，否则投标无效。

11、本项目需求一览表中内容如与第六章“合同条款及格式”相关条款不一致的，以本表为准。

**A分标：**

|  |  |  |  |
| --- | --- | --- | --- |
| 项号 | 货物名称 | 数量 | 技术参数要求 |
| 一、中心机房设备 | | | |
| 1 | 下一代防火墙 | 2台 | ▲一、性能参数：  1、性能指标：网络层吞吐量≥18Gbps，应用层吞吐量≥2.5G； 并发连接数≥220W，新建连接数≥12W；  2、硬件指标：1U规格；存储≥SSD 64G；单电源；标配≥6个千兆电口，≥4个千万兆光口；  3、提供三年软件升级、IPS特征库、防病毒特征库升级及硬件质保服务；  二、功能参数：  1、支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；支持静态路由，ECMP等价路由；支持多播/组播路由协议；  ▲2、支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略路由选路功能；（投标文件中提供产品界面截图并加盖投标单位公章）  3、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NAT64、NAT46 地址转换；  4、访问控制规则支持模拟策略匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；  5、能够识别管控的应用类型超过1200种，应用识别规则总数超过3000条；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，支持基于时间、认证用户和VLAN进行流量控制；  ▲6、设备具备独立的入侵防护漏洞规则特征库，特征总数在7000条以上；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；（投标文件中提供产品界面截图并加盖投标单位公章）  7、支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护，支持SYN Flood、IPv4和IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测；  8、支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP、POP3、 RDP、Rlogin、SMB、Telnet）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；  9、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;  10、设备具备独立的热门威胁库，支持木马、勒索软件、蠕虫、挖矿病毒等种类，特征总数在50万条以上；支持恶意域名重定向功能，用于DNS代理服务器场景下定位内网感染僵尸网络病毒的真实主机IP地址；支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；（投标文件中提供产品界面截图并加盖投标单位公章）  11、支持业务安全和用户安全的风险展示；支持全网实时热点事件展示；支持在同一个界面对全网所有服务器和主机的安全状况进行风险评估，支持对当前所有业务的安全防护状态进行动态保护；  12、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；支持对检测到的攻击行为按照IP地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息；（投标文件中提供产品界面截图并加盖投标单位公章）  13、支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证；  14、支持抵御SQL注入、XSS攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、WEB整站系统漏洞等攻击；（投标文件中提供产品界面截图并加盖投标单位公章）  15、支持企业安全能力图谱，可展示设备对资产防护的有效性，对当前的风险预测、风险防御、风险检测能力进行展示，并对当前资产安全状态进行评级；同时展示当前设备的安全能力等级，展示每日安全能力的更新情况；  16、可扩展支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计；  17、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；  18、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，给出基于AI技术的病毒检测报告；（投标文件中提供产品界面截图并加盖投标单位公章）  19、支持对企业所有的网站提供保护情况的总览，包括哪些网站当前保护措施不足，哪些网站在有效保护中，当前的漏洞、恶意扫描、web攻击及篡改事件发生的总体情况，同时风险要可定位到某个网站，并可以对网站面临的威胁给出处理方式；（投标文件中提供产品界面截图并加盖投标单位公章） |
| 2 | 负载均衡设备 | 1台 | ▲1、要求配置千兆电口≥6个，配置千兆光口≥2四层吞吐量≥6Gbps；并发连接数≥8000000；提供三年软件升级及硬件质保服务；  2、部署方式支持串接部署、旁路部署；支持三角传输模式；  3、设备形态必须独立专业负载设备，非插卡式扩展的负载均衡设备；  ▲4、单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权；  5、提供针对多站点业务发布的全局负载均衡功能，通过智能DNS等机制实现公网用户对多个数据中心或单个数据中心多条线路的最佳访问；  6、支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应、最小流量、加权最小流量、按主机加权最小流量、带宽比例、哈希、主备、首个可用、优先级等算法；  ▲7、通过某种编程语言（如lua）实现自定义的流量编排，对IP、TCP、UDP、SSL、HTTP和HTTPS等类型的流量进行分发、修改和统计等操作；  ▲8、支持图片优化技术，通过对图片格式的转换，减少传输流量，提升web页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的WebP或JPEG格式，优化加速效果；（投标文件中提供设备操作界面截图并加盖投标单位公章）  ▲9、支持静态IP和PPPOE两种线路接入方式；（投标文件中提供设备操作界面截图并加盖投标单位公章）  10、支持跨设备健康状态监视（透明监视），同时支持IPv4和IPv6；  ▲11、支持基于管理员自定义的时间计划来进行出站访问的流量调度分发；（投标文件中提供设备操作界面截图并加盖投标单位公章）  12、支持跨数据中心集群和跨数据中心会话保持；  ▲13、支持cookie加密，提升cookie安全性；（投标文件中提供设备操作界面截图并加盖投标单位公章）  ▲14、支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规HTTP应用可配置基于反映URL失效的HTTP响应状态码的观测判断机制，对于复杂应用可配置基于RST关闭连接和零窗口等异常TCP传输行为的观测判断机制；（投标文件中提供设备操作界面截图并加盖投标单位公章）  15、支持网站页面IP形式和域名形式外部链接的正常访问；支持静态和动态网站页面静态和动态引用站外内容的正常显示；支持静态和动态网站页面静态和动态外部链接的无限级正常跳转；  ▲16、IPv6改造方案能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配置的方式解决天窗问题；  ▲17、支持链路负载投屏展示，能够分别基于链路监测、应用选路和ISP流量进行投屏展示分析。链路监测展示链路的健康状态、上下行带宽、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；ISP展示基于运营商分类选择链路的示意图；  ▲18、支持基于URL的链路调度功能，内置不少于1000条的国外URL网址库，无需手动导入并支持自动更新，管理员可查看并进行编辑。可根据URL将访问国外网站的请求调度到指定线路；  ▲19、服务器负载状态支持投屏展示，能够显示设备的电源状态、风扇转速、磁盘温度、CPU温度、CPU和内存占用率、新建连接数、并发连接数、吞吐情况、SSL新建和SSL吞吐数据、压缩优化和缓存优化数据；业务的健康状态、新建连接数、并发连接数、上下行流量、每秒请求数；节点池的调度算法、健康状态、新建连接数、并发连接数、上下行流量。 |
| 3 | 运维安全管理系统 | 1台 | ▲一、基本要求  1、标准1U机架式设备，含交流电源，2\*USB接口，1\*RJ45串口，1\*GE管理口，配置不少于4个GE电口，不底于2T SATA硬盘。配置不少于100台设备管理授权，最大支持设备管理数不少于500台。字符并发会话数不少于300个，图形并发会话数不少于100个；  2、提供三年软件升级及硬件质保服务；  二、功能指标要求  3、采用物理旁路模式部署，不影响网络结构, 支持IP和端口DNAT网络环境部署，通过映射后的IP和端口信息能够访问运维安全管理系统；支持域名方式web访问到运维安全管理系统，并支持托管设备运维操作；  ▲4、支持与同品牌防火墙组成联动方案，可单点登录运维安全管理系统后直接运维托管设备，解决用户内外网运维问题；  5、系统默认自带三权分立用户，系统管理员、运维管理员和审计管理员权限相互制约。系统管理员负责对系统进行参数设置和维护，不可见托管设备和审计日志等信息；运维管理员负责运维人员和托管设备管理，可对运维行为进行分析，不能管理系统设置和维护；审计管理员负责所有用户行为分析和审计，不可运维托管设备和修改运维人员权限，不可修改系统配置；  6、运维安全管理系统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；  ▲7、支持设备访问授权和命令执行授权：除用户身份认证外，对特定目标设备访问与特定命令的执行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；  8、支持对不同用户设置不同的认证方式，即可配置用户1使用本地认证，用户2使用LDAP认证，其他所有用户使用RADIUS认证；  9、支持原厂自研的APP动态密码用户验证，使得动态密码随机种子得到有效的安全保护；  ▲10、用户登录运维安全管理系统支持多种认证方式，包括本地静态密码认证、LDAP认证、RADIUS认证、证书认证、USBKEY认证、短信认证、手机APP动态密码认证等身份认证方式；支持可知因素和不可知因素的双因素认证；  11、支持管理员以用户为基准，直接查询、新建或编辑与该用户相关的策略，支持查询该用户有权限运维的所有设备，且支持以设备访问中的设备为基准，直接查询该设备的所有审计信息、直接查询并编辑与该设备相关的策略、有权限运维该设备的所有普通用户；  ▲12、支持对托管设备所有设备账号密码手动批量备份；  ▲13、支持批量导入/导出设备信息；支持自动扫描发现托管设备中的所有设备系统账号、自动发现运维人员离职后遗留不用的僵尸账号、托管设备中长时间不被运维的僵尸设备，并以列表方式向管理员展示信息；  ▲14、支持本地字符客户端程序，如putty,xshell,securecrt等客户端直接访问运维安全管理系统选取托管设备进行运维，支持本地字符客户端程序一键快速访问目标托管设备进行运维；  15、支持实时监控通过SSH、SFTP、RDP、VNC 、Telnet、FTP、X11等协议的操作行为，对监控到的非法操作可实时手工切断；  16、支持SSH(V1、V2)、TELNET， Rlogin等字符型、RDP、VNC、X11等图形化远程操作协议，支持FTP、SFTP、SCP、Samba等文件传输协议，支持RDP、VNC的客户端直接访问运维安全管理系统，FTP客户端Wincp直接访问运维安全管理系统；支持Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySql、PostgreSQL等数据库；支持HTTP、HTTPS操作审计，HTTP/HTTPS协议可以直接代理；  17、支持Telnet、SSH审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、协议类型、事件等级及操作内容回放；  18、支持RDP、VNC协议审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、协议/应用类型、事件等级、操作内容等；支持操作内容录像回放；  19、支持SQL语句级别审计，审计内容包括时间、用户、类型、用户IP、设备IP、数据库账号、数据库客户端名称和SQL关键字等信息，并可通过SQL语句审计结果定位数据库运维操作录像回放；  20、文件操作审计内容：包括访问起始和终止时间、用户名、用户IP地址、目标设备IP、设备名称、协议类型、事件等级、操作内容（如对文件的上传、下载、删除、修改等操作等）；  21、提供周期生成报表，用于审计或者上报，提供给用户按照自定义规则自动周期生成报表的功能。 |
| 4 | 入侵防护系统 | 1台 | ▲一、性能指标要求  1、产品应采用2U标准19"机架式硬件设备，提供冗余交流电源，2个USB接口，1个RJ45串口，1个GE管理口，配置不少于4个千电口（支持Bypass），4个千兆SFP插槽，2个接口扩展槽位，含防病毒功能模块；  2、网络层吞吐不底于11Gps，应用层吞吐量不底于2Gbps，最大并发会话数不底于200万，每秒新建会话数不底于6万；  3、提供三年软件升级、IPS特征库、防病毒特征库升级及硬件质保服务；  二、功能指标要求  4、系统应具备融合模式匹配、协议分析、异常检测、会话关联分析，以及抗IDS/IPS逃逸等多种技术，准确识别各种黑客入侵，为用户提供2~7层深度入侵防御；  5、系统应能识别超过1000多种的各类网络应用，至少应包括：商业系统类应用、协作类应用、互联网应用、媒体类应用等；  6、系统应提供覆盖广泛的攻击特征库，能够针对8000种以上的攻击行为、异常事件，以及网络资源滥用流量，进行检测和防御；  7、产品提供强大、灵活的流量管理功能，可以根据协议、端口、源/目的IP地址、网段、时间及带宽等因素，实现基于内容、面向对象的流量保护策略；  8、系统应具备防僵尸网络功能，从而提高整体安全防护能力；  9、系统应提供先进的DoS/DDoS攻击防护能力，支持双向阻断TCP/UDP/ICMP/ACK Flooding，以及UDP/ICMP Smurfing等常见的DoS/DdoS的攻击；  10、支持基于SCADA等工控协议的相关漏洞攻击检测与防护(投标文件中提供功能截图并加盖投标单位公章)；  11、系统应提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为；（投标文件中提供功能截图并加盖投标单位公章）  12、系统应提供敏感数据保护功能，能够识别、阻断通过自身的敏感数据信息（身份证号、银行卡、手机号等）；（投标文件中提供功能截图并加盖投标单位公章）  ▲13、系统应提供关键文件保护功能，能够识别、阻断通过自身的关键文件，以防止非法外传行为。能识别的关键文件类型应包含至少以下几类：文档类如Excel、PDF、PowerPoint、Word等，压缩文件类如CAB、GZIP、RAR、ZIP、JAR等，图像类如BMP、GIF、JPEG等，脚本类如BAT、CMD、WSF等；  ▲14、系统应具备攻击快照功能，详细记录触发告警的数据特征，以便做进一步的事件分析；  15、支持基于阈值和自学习检测，支持僵尸网络防护（C&C），支持文件信誉功能，支持内置Web信誉库(投标文件中提供功能截图并加盖投标单位公章)；  16、系统应具备用户身份识别能力，支持基于用户身份进行策略配置、日志记录与查询；支持自动与手动获取用户信息列表并生成组织结构图；  ▲17、系统支持IPv6/IPv4双协议栈功能，能同时辨识IPv4和IPv6通讯流量。支持多种隧道模式，确保IPv6过渡时代的网络通畅。支持IPv6环境下攻击检测技术和基于IPv6地址格式的安全控制策略，为IPv6环境提供入侵防护；  18、系统应提供定时自动发送报表功能，支持在指定的时间内将生成的报表以html、word、pdf等通用格式通过FTP或邮件发送给指定的管理员，以减少日常维护工作量；  19、可以支持透明（Layer2）、监听（Monitor）、直通（Direct）等安全区模式，支持通过“串联”或“并联”两种方式灵活接入网络；支持IPS和IDS的混合运行模式。 |
| 5 | 网络接入管理系统 | 1台 | ▲1、须为标准机架式硬件产品，1个consol口，2个usb口，6个千兆电口，具有独立自主知识产权，基于linux开发的专用系统；  2、所有功能的实现基于一套系统，不得多个管理页面(含通过跳转等多ip管理地址)，一个客户端（只有2个或2个以下进程）占用资源；  ▲3、1U机架结构；标准配置6个1000MBASE-T接口；每秒事务数（TPS)：≥1000（次/秒），最大吞吐量：≥500Mbps，最大并发连接数：1000（条）；终端管理用户数量≥500（许可）；  4、支持在IPv4和IPv6双栈环境下的终端准入控制、重定向、认证、安检、修复等；  ▲5、准入设备必须具备HA模式，HA须支持主备机心跳IP检测及虚地址管理模式。可提供第三方监控平台，在出现重大异常情况时能及时通知网络设备放开网络；  ▲6、设备自身支持堆叠功能；设备自身须支持热备及数据负载均衡；  7、准入设备应至少提供安全客户端（Agent）、安全控件、无客户端等多种可供自定义部署和管理的模式；  8、使用安全客户端模式部署时，非802.1x准入技术下Windows客户端程序需支持Windows XP/7/8/8.1/10,安装包不得大于3M（非IE控件），内存占用合计不大于20M；  9、X86终端下应支持自定义安装包，包括但不限于AD域专用安装包（加入AD的终端无安装权限）、自身携带浏览器安装包、主机防护安装包；飞腾架构专用客户端、龙芯架构专用客户端；  10、具有Mac OS、Linux、iOS、Android等系统专属客户端，支持认证引导和准入管理；  11、支持策略路由准入技术，同时可提供5个或以上的自身端口用于策略路由下一跳，从而对于多台汇聚交换机引流来的终端进行管理；  12、支持端口镜像准入技术，同时可提供5个或以上的自身端口用于镜像流量准入；  13、准入设备须支持802.1x协议准入方式，无需第三方RADIUS服务器支持；  ▲14、准入设备支持基于多厂商Virtual Gateway的VLAN隔离技术，实现无客户端下端口级准入控制，不得改变现有网络环境不得改变现有的网络环境（包括但不限于不得另行在网内开启DHCP服务、采用ARP干扰等）,隔离终端采用VLAN切换的方式，须一个正常vlan对应一个隔离vlan；(投标文件中提供功能截图并加盖投标单位公章)  15、采用隔离vlan技术时须支持对小路由、hub的管理，可对其下接入的终端实现颗粒度管控；  16、支持vlan隔离技术与端口镜像技术混合使用；  17、准入设备应具有软件分发和部署功能，管理员可以预定义软件分发的路径、运行参数、是否执行等任务策略，以提升软件部署效率。能够自动判断并统计软件分发、部署的成功率，支持进程、注册表、文件等多种参数的组合判断；  18、支持终端入网IE浏览器重定向引导（访问http,https）。可根据用户的实际环境自定义非80端口的Web服务端口号及用户重定向引导。支持自动发现全网拓扑；  ▲19、能够在拓扑图上选取设备查看其基本状态信息、设备型号、所处位置、子节点、路由表、ARP表等信息；(投标文件中提供功能截图并加盖投标单位公章)  ▲20、支持在界面上提供对该网络设备进行TELNET、SSH等管理；(投标文件中提供功能截图并加盖投标单位公章)  21、能够在网络拓扑图上由用户自定义显示的节点类型，方便用户通过不同方式查看拓扑连接；  22、支持可网管型交换机面板图形化展现各接口状态（up、down、trunk、单/多MAC等），以及各接口下联的终端详细信息（IP、地址、MAC地址等）；  23、能够支持自上而下逐级查找终端的具体位置、安全状态、认证用户、上下线时间等信息；  24、提供专属的模块对移动终端进行管理，自动识别移动终端并进行策略匹配（不得用widows混合进行策略下发），策略包括但不限于禁止移动终端入网、安装app方可入网、是否注册、审核、安全基线检查等；  25、能够全面结合用户已有的认证或业务系统，可以与钉钉、RADIUS、LDAP、邮件、AD、WEB系统做联动认证；  ▲26、移动终端可以支持通过将指纹和用户账户绑定的方法，实现移动终端用户按压指纹认证入网；  27、支持用户在认证页面自行进行账号的申请。用户可自行提交用户名、密码、姓名、电话、部门、E-Mail等信息。管理员审核通过后，用户即可使用该账号进行认证。有效解决用户账号和密码创建和分发的困难。能够提供来宾角色选择，能够设定来宾设备的访问权限和入网时长；  28、员工可以为来宾申请来宾码，来宾使用来宾码可以接入网络；能够设定那些角色的用户能够申请来宾码；  ▲29、已入网员工可以通过扫描来宾终端上二维码，放行来宾用户入网；  30、准入设备须提供系统安全配置、用户行为规范等类别检查项，至少提供50种以上安全检查项，安全检查项管理员均可设置自动修复（非web跳转链接），可针对不同检查项单独设置周期检查时间；  31、准入设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分发表等功能。准入设备能够对补丁进行分级，分为：严重、重要、中等的类别。能够在终端的浏览器页面显示入网终端的补丁检查情况；  ▲32、准入系统自身能够支持windows系列补丁库、补丁检查和补丁分发安装。支持windows10补丁检查及自动修复；  33、支持主流的20种以上的杀毒软件检查，包括微软MSE、可牛、Avast等，支持杀毒软件版本、病毒库和运行情况的检查，能够在页面显示出检查结果；  34、支持Guest来宾帐户、WSUS更新配置、密码策略设置、屏幕保护设置、弱口令帐户、网卡绑定、系统共享资源进行检查加固。支持对终端的磁盘使用率、垃圾文件、IE主页、网络监听端口等安全性配置进行检查和修复；  35、通过检测终端文件、指定文件版本、大小、MD5，注册表的项、注册表值，进程、服务状态进行检查。通过安装包运行、访问站点、开关服务、关闭进程、执行文件、删除文件、修改注册表进行修复。可以灵活的对终端进行安全检查和修复；  36、支持国产操作系统，提供中标麒麟、银河麒麟、龙芯等客户端；  37、支持Linux系统安全检查，包括ip/mac绑定、操作系统版本、磁盘使用、计算机名称、网络监听端口、系统时间、网络监听端口、密码策略、弱口令、必须及禁止安装的进程、软件白名单的检查；  ▲38、软件产品正版化检查，支持进行windows、office、WPS产品授权信息进行正版化检查；  39、提供IP地址分配矩阵图。可以通过组织架构为维度查看IP地址分配矩阵图。能够直接、快捷的查看全网终端历史上线、下线、在线时长等详细的IP使用情况；  40、提供未关机终端自动统计功能，并能够按照部门、时间段等条件生成统计报表。能够对设备类型、时间进行统计设置；  ▲41、支持移动终端专用平台管理页面，方便使用平板、智能手机进行准入设备基本操作。可实现设备快速定位、设备审核、实时报警监控、小助手确认码生成、准入控制器管理、平台基本信息、关机与重启；  42、支持通过Web管理界面进行ping、抓包、traceroute、nslookup等功能，并可以设置命令参数进行相关调试；  43、支持系统报警、网络报警、终端报警等报警类型，超过20种以上自定义报警类型。支持报警信息通过Syslog、邮件、短信进行输出。 |
| 6 | 核心交换机万兆接口卡 | 2块 | ▲1、板卡自带44个千兆光接口，4个万兆光接口；  ▲2、为保证系统兼容性，要求与在用的锐捷S8612E核心交换机兼容使用。 |
| 7 | 48口万兆汇聚交换机 | 2台 | ▲1、固化10/100/1000M以太网端口≥48，固化1G/10G SFP+万兆光接口≥4个，2个模块化电源插槽，本次配置1块交流电源，配置1根3m万兆SFP+光缆（包含一根线缆+两个接口模块）；  ▲2、支持RIP/RIPng、OSPF、策略路由等三层路由协议；  ▲3、交换容量≥4Tbps，转发率≥160Mpps；  4、支持基于端口的出方向和入方向限速，限端口速粒度≤64Kbps；  5、支持基于流的出方向和入方向限速，且流限速粒度≤8Kbps；  6、支持虚拟化功能，非堆叠模块实现，不占用扩展槽；  7、符合国家低碳环保等政策要求，支持IEEE 802.3az标准的EEE节能技术；  ▲8、支持专门基础网络保护机制的NFPP功能，支持多种类型的防护，如ARP防护，当ARP速率超过攻击水线，对有攻击行为的用户进行隔离，保证设备和整网的安全稳定运行；  9、支持软件定义网络SDN，符合OpenFlow 1.3协议标准，支持SDN和SDN Ready功能；  ▲10、交换机采用专业的内置防雷技术，要求支持业界领先的防雷能力，业务端口防雷不低于10kv；  ▲11、整机采用绿色环保设计，满负荷情况下电源功率≤50W；  ▲12、设备自带云管理功能，支持一键设备发现；  ▲13、为保证兼容性与统一管理，要求该项产品必须与安全管理平台兼容使用。 |
| 8 | 万兆多模模块 | 16个 | 万兆多模LC接口模块，适用于SFP+接口。 |
| 9 | 万兆光纤跳线 | 8条 | 10M 万兆多模双芯 LC-LC光纤跳线。 |
| 二、21个社区设备 | | | |
| 10 | 52口交换机 | 15台 | ▲1、提供10/100/1000MBase-T 端口端口数≥48，提供非复用的千兆SFP光插槽≥4，整机可用千兆端口数量≥52个；  ▲2、交换容量≥3Tbps，包转发率≥150Mpps；  3、设备MAC地址≥16K，ARP表项≥1000条；  ▲4、支持静态路由、RIP/RIPng、OSPFv2/OSPFv3等三层路由协议；  5、要求所投设备支持1对1、1对多、多对1和基于流的镜像；且支持RSPAN和ERSPAN；  6、支持RSTP/MSTP；  7、支持专门基础网络保护机制，增强设备防攻击能力，即使在受到攻击的情况下，也能保护系统各种服务的正常运行，保持较低的CPU负载，从而保障整个网络的稳定运行；  8、支持虚拟化功能，最多可将9台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤30ms；  9、支持SNTP、Syslog，CLI兼容业界主流标准；  ▲10、交换机采用专业的内置防雷技术，要求支持业界领先的防雷能力，业务端口防雷不低于9kv；  11、符合国家低碳环保等政策要求，支持IEEE 802.3az标准的EEE节能技术；  ▲12、要求所投产品支持openflow 1.3协议。  ▲13、为保证兼容性与统一管理，要求该项产品必须与安全管理平台兼容使用。 |
| 11 | 28口交换机 | 6台 | ▲1、提供10/100/1000MBase-T 端口端口数≥24，提供非复用的千兆SFP光插槽≥4，整机可用千兆端口数量≥28个；  ▲2、交换容量≥3Tbps，包转发率≥120Mpps；  3、设备MAC地址≥16K，ARP表项≥1000条；  ▲4、支持静态路由、RIP/RIPng、OSPFv2/OSPFv3等三层路由协议；  5、要求所投设备支持1对1、1对多、多对1和基于流的镜像；且支持RSPAN和ERSPAN；  6、支持RSTP/MSTP；  7、支持专门基础网络保护机制，增强设备防攻击能力，即使在受到攻击的情况下，也能保护系统各种服务的正常运行，保持较低的CPU负载，从而保障整个网络的稳定运行；  8、支持虚拟化功能，最多可将9台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤30ms；  9、支持SNTP、Syslog，CLI兼容业界主流标准；  ▲10、交换机采用专业的内置防雷技术，要求支持业界领先的防雷能力，业务端口防雷不低于9kv；  ▲11、符合国家低碳环保等政策要求，支持IEEE 802.3az标准的EEE节能技术；  ▲12、要求所投产品支持openflow 1.3协议。  ▲13、设备自带云管理功能，支持一键设备发现  ▲14、为保证兼容性与统一管理，要求该项产品必须与安全管理平台兼容使用。 |
| 12 | 安全管理平台 | 1套 | 1、平台整体技术要求：产品架构支持中文界面，纯B/S架构，所有操作均在B/S模式下完成；  2、系统可对网络设备、无线设备、服务器、数据库、中间件、应用等多厂商、多版本设备及资源的统一监控和管理；  ▲3、支持Windows、Linux两种平台上运行，此次配置资源节点（资源包括交换机、路由器、防火墙、无线AC、服务器、数据库）管理授权数≥50个；提供2年软件维护服务，包含补丁软件升级和故障处理服务；提供软件实施工程师现场软件安装调试，包括：实施环境调研、数据模型搭建、软件安装、软件调试、实施文档编写等；  ▲4、能够基于用户体验，从用户角度出发，在不需要借助认证系统的环境下就可获取到用户连接数、用户信号强弱、客户端类型、操作系统等信息；（投标文件中需提供系统功能截图并加盖投标单位公章）；  ▲5、具备SQL语句性能消耗TOP10分析，包含ElapsedTime、BufferGets、CPUTime、DiskReads等；（投标文件中需提供系统功能截图并加盖投标单位公章）  ▲6、系统具备业务运行概括视图功能，运行概况视图中至少应包含健康分析、关键业务系统实时扫描、业务状态视图等功能，可在一个页面上了解业务的健康走势、实时运行状况、健康度、繁忙度、告警数量、宕机时长、宕机次数等信息；（投标文件中需提供系统功能截图并加盖投标单位公章）  7、自动发现网络中的二、三层网络设备，可以自动构成网络拓扑图，支持自定义拓扑功能，提供图形化拖拽方式自动绘制网络拓扑图，支持自定义图标、图片的导入功能；  8、系统具备拓扑事件播放功能，可以实现设备跟踪式事件播放功能，方便、及时、准确定位拓扑内资源的告警情况；  9、系统具备事件告警管理平台，应区别事件、告警管理；  10、支持告警触发自动操作功能，系统可以根据告警的类型和告警级别自动触发脚本级自动化操作功能；  11、系统支持分级式部署模式，上下级系统独立运行，权限相对独立且各级系统均有本地的独立Portal和采集服务；  12、分级管理具有下级系统支持注册机制，下级系统连接上级系统进行注册请求，上级系统审批后方能进行数据互通；  13、上级系统可设定下级系统上传的资源数据、静态数据、动态数据范围和周期，要求静态资源数据、动态告警数据可设定不同的时间周期；  14、系统内置多纬度多视角报表模版包括资源类报表模版、资源分析类报表模版、TOPN报表模版、告警统计类报表模版；  15、系统支持基于windows平台的告警客户端，用户可不用登录监控系统通过该客户端即可方便接收到监控对象的各类告警信息，并通过弹出对话框、气泡消息等多种提醒方式对新告警进行提醒；  16、系统提供配置向导功能，帮助用户快速了解系统逐步配置过程；  ▲17、该项产品必须与在用的锐捷RIIL6.0运维管理平台兼容运行。 |
| 13 | 本地施工及辅材 | 21项 | 21个社区的熔纤、线路整理等本地施工及电源线、线槽、标签、扎带、电源排插等辅材 |
| ▲**商务条款** | | 一、售后服务及其他要求：  1、免费送货上门，免费安装调试，免费提供技术支持及培训，按国家实行“三包”；  2、质保期：交货验收合格之日起一年（项目需求一览表的“技术参数要求”里有特殊要求的按特殊要求执行）；  3、交货期：自签定合同之日起30日内；  4、交货地点：南宁市良庆区（采购人指定地点）；  5、一旦发生故障，要求6小时内响应，8小时内上门服务，12小时内解决故障，否则提供同档次替代品；  二、付款条件：货物交付验收完毕30日内，采购人支付合同金额的95%给中标人，合同金额5%于质保期满后30日内采购人一次性支付给中标人（无息）。  三、报价要求：投标报价为采购人指定地点的现场交货价，包括：  （1）货物的价格：包括全部设备货款、现场安装、调试费（不含尾气检测费用）；  （2）货物的标准附件、备品备件、专用工具的价格；  （3）运输、二次运输、装卸、培训、技术支持、售后服务费；  （4）保险费和各项税金等费用。  四、在签订合同后7日内，中标人需向采购人提供以下全新未开封正品行货设备各一套进行初步测试验收：下一代防火墙（项号1）、负载均衡设备（项号2）、运维安全管理系统（项号3）、入侵防护系统（项号4）、网络准入管理系统（项号5）、48口万兆汇聚交换机（项号7）、安全管理平台（项号12）；中标人所投产品必须满足招标文件技术参数及性能配置的要求。如产生检测费，检测费由中标人负责。如果测试后，中标人所投产品不能满足投标文件要求的，视为违约，验收不通过，由此引发的所有损失由中标人负责，同时按有国家相关法律法规规定进行处罚。  五、验收条件及标准：  1. 中标方代表必须参与及协助采购人现场拆封、安装、调试，验货时严格按照招标文件参数要求及投标人投标文件中承诺的参数进行验货，中标方所供货物必须与招标文件要求的技术参数相符，否则采购方有权拒收货物，直至终止合同，由此造成的一切损失由中标方负责。项目验收时提供必须的电子版操作说明、施工图等各种验收相关文档。  2.中标人交货前应对产品作出全面检查和对验收文件进行整理，并列出清单，作为招标人收货验收和使用的技术条件依据，检验的结果应随货物交甲方。中标人不能完整交付货物及本款规定的单证和工具的，必须负责补齐，否则视为未按合同约定交货。  3. 中标人需负责安装、调试，并培训招标人的使用操作人员，直到设备运行符合技术要求，招标人方可验收。  4.招标人组织验收，中标人必须到场配合，验收合格后双方签署验收合格凭证。  5.其他未尽事宜应严格按照《关于印发广西壮族自治区政府采购项目履约验收管理办法的通知》[桂财采〔2015〕22号]以及《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》[财库〔2016〕205号]规定执行。 | |
| **核心产品** | | 本分标核心产品为：**第12项“安全管理平台”。** | |
| **产品要求** | | 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。 | |
| **其它** | | 投标人可根据自身的情况编写技术与实施方案（内容可以包括但不限于对项目技术环境及情况基本的了解、建设思路及需求分析、各项施工技术措施、安装进度计划、安装调试方案和验收措施、各系统功能以及实现方式及设备架构设计图、安装维保人员配置等）。 | |

**B分标：**

|  |  |  |  |
| --- | --- | --- | --- |
| 项号 | 货物名称 | 数量 | 技术参数要求 |
| 1 | 南宁市良庆区经济贸易和信息化局数字电路租赁服务 | 1项 | 1、21条30M数字电路；  2、采用MSTP或IP RAN技术，实现本地网内点对多点专线电路的组网需求，要求专线电路与互联网隔离；  3、要求免费提供所有终端接入设备，接口类型：RJ45电口；  4、传输汇聚层至核心层均为自愈环保护，传输设备具有全程网管监控功能，能实行7\*24小时实时监控；  ▲5、网络参数要求：  （1）端到端电路的传输比特差错率(误码率)：≤1.0×10E－7；  （2）网络可用率≥99.9%；  （3）端到端电路平均网络延时≤50ms；  （4）端到端电路丢包率≤1%；  （5）端对端电路最大时延≤10ms、时延抖动率≤10ms。  ▲6、网络施工、测试以及割接升级期间，不对现有业务系统产生影响。 |
| **商务条款** | | 一、合同签订期：自中标通知书发出之日起10日内  ▲二、交付使用期：自签订合同之日起20日（自然日）内，线路经采购单位验收合格视为正式开通使用。租用期自验收合格之日起，期限1年。  三、提交服务成果地点：采购人指定地点  四、售后服务要求：  ▲1、质量保证期1年（自交货并验收合格之日起计）  2、处理问题响应时间：接到采购人处理问题通知后6小时内到达采购人指定现场  3、在租用期限内，中标人应严格遵守《中华人民共和国电信条例》，维护双方权益，应按信息产业部颁布的《电信服务标准》的电路质量要求，保证采购人租用线路畅通及安全使用；  4、提供7×24小时热线电话服务,并指定专人负责上门受理调试日常维护及平时协助采购单位维护检测等工作；  5、每个季度对网络进行一次巡检，检查网络设备和主干光缆的运行情况，提交巡检报告；  6、当用户网络需要扩展或升级时，负责免费提供相应解决方案；  7、因中标人施工、网络割接等原因影响宽带网络运行的，应当提前一天通知用户，并且尽快消除故障、恢复通信线路。  五、其他要求：  ▲1、报价必须含以下部分，包括：  （1）服务的价格；  （2）必要的保险费用和各项税金；  （3）其他（如运输、装卸、安装、调试、培训、技术支持、售后服务、更新升级等费用，根据项目具体情况填写）：  ▲2、付款方式：本项目无预付款，供应商所提交的服务经采购人书面验收合格后，一次性支付合同款。  六、验收条件及标准：  1. 中标人需负责安装、调试，并培训招标人的使用操作人员，直到设备运行符合技术要求，招标人方可验收。  2.招标人组织验收，中标人必须到场配合，验收合格后双方签署验收合格凭证。  3.其他未尽事宜应严格按照《关于印发广西壮族自治区政府采购项目履约验收管理办法的通知》[桂财采〔2015〕22号]以及《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》[财库〔2016〕205号]规定执行。 | |
| **核心产品** | | 本分标无核心产品。 | |
| **产品要求** | | 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。 | |
| **其它** | | 投标人可根据自身的情况编写技术与实施方案（内容可以包括但不限于互联网电路接入网技术、施工进度计划和工期保证措施、安全控制措施及安装质量控制保证方案、工程项目安全管理、实施质量保证措施及质量管理程序、赶工计划等）。 | |