需求公示

1、招标方式：公开招标

2、采购预算：900.78 万元

3、最高限价：809.334 万元

4、供应商资格条件：

（1）一般资格要求：

①符合《中华人民共和国政府采购法》第 22 条的条件；

②具有独立法人（或负责人）资格，有统一社会信用代码的营业执照或民办非企业单位登记证书，且经营范围须包含本次采购项目内容。

③具有履行合同所必须的专业技术能力。

④根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》(财库[2016]125 号)的规定，对列入失信被执行人和重大税收违法案件当事人名单（查询网址“信用中国”网（www.creditchina.gov.cn）、政府采购严重违法失信行为记录名单（查询网址“中国政府采购”网（www.ccgp.gov.cn）的供应商，拒绝其参与本招

标项目，注：此项须提供采购公告发布之日起至投标截止时间相应网站查询截图（不提供以现场查询为准）。

⑤本项目不接受联合体

（6）特殊资格要求：无

4、技术参数

铜仁市电子政务外网三期工程政府采购项目采购内容及参数要求

一、国内设备表

序号	名称	规格程式	单位	数量	备注
Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ	
（一）网络建设					
1	市级政务外网核心路由器	1. 设备支持双主控且满配，支持电源冗余，要求所有业务板卡及电源、风扇均可热插拔； 2.整机业务载板插槽≥8 个； 3.★设备支持单槽位 200G 线速转发不丢包； 4.★交换容量≥4/110Tbps，包转发率≥450/14000Mpps(提供截图证明)； 5.整机高度≤3U ； 6.设备支持 100GE、50GE、25GE、10GE、GE、FE、E1、CPOS 等接口类型； 7.支持 100G/50GE 自适应端口、支持 100G/40G 自适应端口，支持 10G/GE 自适应端口； 8.★支持 RIP、OSPF、IS-IS、BGP 等路由协议，支持 VXLAN、GRE 等隧道技术(提供截图证明)； 9.支持基于硬件的 BFD 故障探测技术，支持最小发包间隔 5ms、支持单臂 BFD； 10.支持 LDP,VRRP,OSPF,ISIS,BGP,VRRP6,OSPFv3,ISIS6,BGP4+,MPLS L3VPN, MPLS TE, PIM SM 的 NSR（不中断路由技术），主备倒换不丢包，支； 11.★持 VRRP 等可靠性技术；(提供测试报告)； 12.实配：≥20 端口 100/1000Base-X-SFP 物理接口，≥4 个千兆单模光模块，三年质保、软件免费升级服务； 13.提供所投产品的工信部入网证。	台	2	

2	市级政务外网核心交换机	1. ★交换容量≥500Tbps；包转发率≥28000 Mpps； 2.主控引擎与交换网板物理分离；主控引擎≥2；独立交换网板槽位≥4（实配 2 个交换网板）；整机业务板槽位数≥8； 3.主控槽位与业务线卡槽位宽度相同，为全宽槽位,支持每槽位转发能力≥2.4Tbps； 4.★支持纵向虚拟化技术，支持把交换机和 AP 虚拟为一台设备； 5.支持业务板集成 AC 功能，业务单板+AC 只占用 1 个业务槽位，实现对 AP 的接入控制、AP 域管理、有线无线用户的统一认证管理； 6.实配：万兆光口≥24 个，千兆光口≥72 个，千兆电口≥48 个，万兆单模光模块≥2 个，三年质保、软件升级服务； 7.★提供所投产品的工信部入网证,投标产品是国内外主流厂商产品，所投厂商的交换机产品在中国区市场占有率排名前三。	台	2	
4	区县政务外网汇聚交换机	1.交换容量≥250Tbps，转发性能≥28000Mpps； 2.主控引擎≥2，业务槽位≥6 个，整机槽位≥8 个； 3.支持每槽位带宽≥320Gbps，提供第三方测试报告； 4.考虑到散热效果和设备可靠性，设备采用冗余风扇框设计，独立风扇框数≥2，为适应机柜并排部署，设备机箱采用后出风风道设计，提供设备散热气流流向截图 5.支持 GE/10GE 端口 200ms 大缓存，提供第三方测试报告。 7.实配：万兆光口≥16 个，千兆光口≥16 个，千兆电口≥48 个，万兆单模光模块≥2 个 8.★提供所投产品的工信部入网证,投标产品是国内外主流厂商产品，所投厂商的交换机产品在中国区市场占有率排名前三。 9.三年质保、软件免费升级服务	台	10	
5	政府大楼楼层接入交换机	1.交换容量≥336Gbps/3.36Tbps，包转发率≥51Mpps/126Mpps，24 个千兆电口，4 个千兆 SFP；(提供截图证明) 2.★支持静态路由、RIP、RIPng、OSPF；提供第三方测试报告, 3.★支持智能堆叠，堆叠后逻辑上虚拟为一台设备，具有统一的表项和管理，堆叠系统通过多台成员设备之间冗余备份，支持以太网电口堆叠，用网线连接实现堆叠功能,提供第三方测试报告. 4.支持 Openflow 1.3 标准，提供第三方测试报告 5.单台配置 2 块千兆多模光模块； 6.★提供工信部入网证，投标产品须是国内外主流厂商产品，所投厂商的交换机产品在中国区市场占有率排名前三。 7.三年质保、软件免费升级服务	台	25	
（二）安全建设					
6	态势感知综合分析功能模块	1.2U 机架式设备，intel 至强 10 核 CPU*2，内存：≥128G；存储：≥20TB；接口：2×1GE 管理口（电），2×1GE 监听口（电），2×10GE 监听口（光口，支持千兆光模块）；支持冗余电源；提供 2 个服务器节点插槽； 2.并发会话：≥400W；新建会话：≥6W；流量吞吐≥1Gbps；最大日志处理速度≥2.5weps； 3.流量还原：支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs 等；支持对流量中	套	1	

		出现文件传输行为进行发现和还原，并记录文件 MD5 发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk 等）、压缩格式文件（RAR、ZIP、GZ、7Z 等）、文档类型文件（word、excel、pdf、rtf、ppt 等）；支持常见数据库协议的识别或还原：DB2、Oracle、SQL Server、Sybase、MySQL、MongoDB、PostgreSQL 等协议；支持 TCP/UDP 会话记录、异常流量会话记录、web 访问记录、域名解析、SQL 访问记录、邮件行为、登录情况、文件传输、FTP 控制通道、SSL 加密协商、telnet 行为、IM 通信等行为描述。 4.★威胁发现（提供截图证明）：威胁检测告警能够直接体现攻击结果即企图、成功、失陷；支持威胁情报实时匹配检测和自定义威胁情报；原始告警数据包留存：告警相关的原始数据包能够本地留存，用于威胁事件的取证、分析；网络攻击支持的协议类型达到 100 种以上；网络攻击引擎支持多种 DDoS 检测：SYN FLOOD、NTP 放大、DNS 放大、CC 拒绝服务攻击、Udpflood、http flood、Pingflood、Dnsreqflood、Dnsreplyflood、ACK_FLOOD、PSH_ACK_FLOOD、ACK_FIN_FLOOD 等；基于 WEB 攻击检测技术，检测类型包含 SQL 注入、跨站脚本攻击、文件写入、文件下载、文件上传、文件读取、文件包含、弱口令、权限许可和访问控制、配置不当/错误、目录遍历、默认配置不当、命令执行、敏感信息/重要文件泄露、逻辑/设计错误、跨站请求伪造、后门程序、非法授权访问/权限绕过、代码执行、URL 跳转、系统/服务配置不当等等，告警事件能标记主机攻陷状态是否失陷；基于 PHP 动态沙箱（webshell）的检测机制：可检测传统 IDS 等产品无法发现的 web 后门上传行为； 5.★威胁分析（提供截图证明）：支持能够存储所有采集还原后的关键流量数据，最高可扩展至 PB 级别；能够定期接收云端提供的威胁情报，可支持在线和离线升级两种方式；支持基于威胁情报的威胁检测，检测类型包含 APT 事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件，并可自定义威胁情报；支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索，查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等；支持对告警从多维度进行分析展示，维度包含：威胁情报、WEB 攻击、邮件攻击、恶意软件、终端、沙箱、攻击链（侦察、入侵、命令控制、横向渗透、数据外泄、痕迹清理）；能够对告警进行深层次分析，分析内容包含：基本信息、主机详情、威胁情报详情、投递的恶意样本、在主机上运行的恶意样本、外联 C&C 服务器域名、C&C 服务器会话记录、C&C 服务器传送文件、受到的攻击等；支持对基于攻击成功与否的判定功能，能够精准识别攻击结果是企图、成功还是失陷； 6.★场景化分析 1：支持可基于机器学习和行为模型进行未知威胁和异常行为的检测分析，可检测异常行为包含：业务资产主动外连、HTTP 代理、SOCKS 代理、异常 DNS 服务器、DNS Tunnel、reGeorg Tunnel、DGA 域名、异地账号登录、暴力破解、明文密码泄露、弱口令监测、敏感关键词邮件、敏感后缀邮件。业务资产主动外连，检测行为特征包含：外连 IP、外连 IP 归属、服务商、外连流量大小；DGA 域名发现，通过结合机器学习技术发现动态恶意域名，检测行为特征包含包含请求域名以及检测的准确率； 7.场景化分析 2：支持 HTTP 代理发现分析，检测行为特征包含：代理 IP、			

		代理端口、代理次数；SOCKS 代理发现，检测行为特征包含：代理 IP、代理端口、代理次数；异常 DNS 服务器发现，检测行为特征包含：异常 DNS 服务器地址、异常解析地址、上级 DNS 服务器地址；DNS Tunnel 发现，检测行为特征包含：请求地址、隧道服务器、请求次数；reGeorg Tunnel 发现，检测行为特征包含：tunnel 地址、关联图、操作命令、目标 IP；异地账号登录，检测行为特征包含：登录 IP 归属、账号、登录资产 IP、使用协议、登录次数、登录成功率；（提供截图证明） 8.★场景化分析 3：支持暴力破解分析，检测行为特征包含：登录 IP 归属、使用协议、爆破次数、爆破成功与否；明文密码泄露，检测行为特征包含：登录账号 IP、账号、密码、使用协议；弱口令监测，检测行为特征包含：弱口令、弱口令对应账号；敏感关键词邮件，不仅支持自定义关键词发现恶意邮件还支持邮件白名单，检测行为特征包含：发件人、收件人、关键词、邮件主题、抄送、附件文件名、邮件正文；敏感后缀邮件，内置异常软件的后缀库同时支持邮件白名单，检测行为特征包含：发件人、收件人、关键词、邮件主题、抄送、附件文件名、邮件正文；（提供截图证明） 9.★调查分析：支持威胁事件的追踪溯源分析能力，可基于事件告警进行调查分析，对攻击过程进行可视化展现，可展示命中威胁情报的内部主机之间的连接行为，能输出完整的基于时间序列和攻击链的事件报告，事件报告支持 word 格式导出（提供截图证明）。 10.支持通过 SPL 搜索语句进行详细检索并能够采用多字段组合来进行日志检索生成视图（提供截图证明） 11.支持自定义关键词发现恶意邮件还支持邮件白名单，检测内容包含：发件人、收件人、关键词、邮件主题、抄送、附件文件名、邮件正文（提供截图证明） 12.★以攻击者的维度进行分析，对攻击者进行画像，画像内容包括地理位置信息、国家信息、所属组织、使用的攻击手段、攻击的所有资产（提供截图证明） 13.支持以受害资产维度进行分析，分析内容包括失陷状态、受到的攻击类型、威胁级别、处于的攻击阶段、所属的资产分组（提供截图证明） 14. 支持分析平台横向扩展至多台设备集群（提供截图证明） 15.支持大屏展示整体资产风险态势，包含资产树结构、资产分类、开放服务统计、网段管理、资产风险趋势、资产风险状态（提供截图证明） 16. 支持与态势感知同品牌防火墙进行联动，发现威胁事件后支持对攻击 IP、★恶意域名和受害资产的流量进行阻断（将策略下发给防火墙，由防火墙执行阻断）（提供截图证明） 17.★提供告警展示场景，支持展示场景的切换。每个告警展示场景中支持自定义页面数据展示的范围，方便管理人员的日常运维工作（提供截图证明）			
7	日志采集探针	1. 2U 机架式设备；单台性能要求：10 核 CPU；存储 4TB；接口：2×1GE 管理口（电），2×1GE 监听口（电），2×10GE 监听口（光口，支持千兆光模块）；支持冗余电源；并发会话：≥300W；新建会话：≥5W；流量吞吐≥5G（HTTP 100KB）/2G（HTTP 21KB）/0.35G（HTTP 1.7KB）；协议解析能力≥3.1G（HTTP 100KB）/1.6G（HTTP 21KB）。	台	2	

		2.★支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库 3000+（提供截图证明）。 3.★漏洞特征库支持自动及手动升级，漏洞库数量大于 4000（提供截图证明）。 4.支持通过流量镜像的方式旁路部署在数据链路中，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断 TCP 威胁会话连接。 5.支持基于源地址、目的地址、应用、流量采样比、时间进行选择数据采集对象，可以针对采集对象进行网络流量数据采集和威胁检测数据采集，网络流量数据采集支持自定义流量载荷字节数。 6.支持基于 SSL 协议的 HTTPS 流量进行解密，可添加基于源地址、目的地址的解密策略；支持明文流量镜像；支持添加 SSL 入站检查配置文件。SSL 入站检查配置文件中指定 SSL 解密证书（提供截图证明）。 7.支持解析、生成及外发 TCP 流量日志。包括：传感器序列号、TCP 数据流的结束方式、TCP 数据流开始的时间、源 IP、源端口、目的 IP、目的端口、源 mac、目的 mac、协议、上行字节数、下行字节数、客户端系统信息、服务端系统信息、TCP 流的统计信息等字段。 8.支持解析、生成及外发 UDP 流量日志。包含：传感器序列号、UDP 数据流开始的时间、UDP 数据流结束的时间、源 ip、源端口、目的 ip、目的端口、源 mac、目的 mac、协议、上行字节数、下行字节数、上行包数、下行包数字段。 9.支持解析、生成及外发 Web 访问日志。包括：传感器序列号、日志生成时间、源 ip、源端口、目的 ip、目的端口、HTTP 请求方法、HTTP 包头的 URI 字段、uri_md5 值、host 字段、host_md5 值、origin 字段、cookie 字段、ser-Agent 字段、referer 字段、链接来源、原始数据、http 状态码、Content 类型等字段（提供截图证明）。 10.支持解析、生成及外发域名解析日志。包括：时间、源 ip、源端口、目的 ip、目的端口、DNS 访问类型、Host、Host 字段_MD5 值、地址资源、MX 记录、响应结果状态、域名规范名称等字段。 11.支持 FTP/SMB/TFTP 三种协议的解析、生成及外发文件传输日志。包括：传感器序列号、协议、日志生成时间、客户端 IP、客户端应用端口、服务端 IP、服务端应用口、传输模式、文件名字、文件 md5、文件类型等字段。 12.支持解析、生成及外发 LDAP 行为日志。包括：传感器序列号、协议、日志生成时间、源 ip、源端口、目的 ip、目的端口、用户名、LDAP 版本、ldap 操作类别、op 的具体操作描述等字段。 13.支持解析、生成及外发 ftp、smb、oracle、mysql、mssql、postgresql、ssh、pop3、smtp 协议的登陆动作日志。包括：日志生成时间、源 ip、源端口、目的 ip、目的端口、协议、登陆密码、登陆结果、用户名等字段。 14.支持解析、生成及外发 pop3、smtp、imap、webmail 协议的邮件行为日志。包括：传感器序列号、协议、message-id 信息、生成时间、源 ip、源端口、目的 ip、目的端口、邮件发送/接收时间、邮件抄送人、主题、被当前邮件回复的邮件 ID、密送人、附件名字、回访路径、邮件实际接收者、附件 md5、mime_type、邮件正文等字段（提供截图证明）。			

		15.支持解析、生成及外发 Oracle、MySQL、MSSQL、PostgreSQL、MongoDB、DB2、Redis 等协议的数据库操作日志。包括：传感器序列号、日志生成时间、源 ip、源端口、目的 ip、目的端口、协议、协议版本、用户、数据库类型、数据库操作返回的状态信息、操作信息等字段。 支持解析、生成及外发 FTP 控制通道日志。包括：传感器序列号、日志生成时间、源 ip、源端口、目的 ip、目的端口、用户名、标记操作顺序、操作命令、操作结果等字段。 16.★支持解析、生成及外发 SSL 加密协商日志。包括：传感器序列号、日志生成时间、源 IP、源端口、目的 IP、目的端口、版本号、会话 id、服务器名字、证书中的颁发者的名字、证书的有效期的起始时间、证书的公钥、Sever 端证书的持有者等字段（提供截图证明）。			
8	互联网边界下一代防火墙	1.多核 AMP+架构，网络层吞吐量 8G，并发连接≥230 万，每秒新建连接数 15 万， 标准 2U 机箱，冗余电源，标准配置 6 个 10/100/1000M 自适应电口，另有 2 个接口板卡扩展插槽，可最大支持 22 个接口，1 个 Console 口，支持液晶屏；含三年硬件维保服务。 2.配置 3 年全功能模块升级订阅服务包（含应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务）。 3.支持 VTEP（VxLan Tunnel EndPoint）模式接入 VxLAN 网络，并可作为 VXLAN 二层、三层网关实现 VxLan 网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定 VLAN、VNI（VXLAN Network Identifier）、远程 VTEP，手动管理 VxLan 网络；支持 MAC、VNI、VTEP 静态绑定； 4.★支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能（提供截图证明）； 5.支持支持通过 802.3ad 协议、轮询、热备等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余，并可根据：源目的 MAC 组合、MAC 和 IP 组合或 TCP/UDP 端口组合等方式实现负载和备份； 6.支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持 RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持 PIM-SM（稀疏模式） 7.支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于 12 种路由负载均衡方式，支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP 等方式的链路探测，同时 TCP 与 HTTP 可使用自定义目标端口进行测试；（提供截图证明） 8.支持 ISP 路由负载均衡，最大可支持 8 条链路负载，支持自定义负载权重，支持基于优先级的 ISP 路由链路备份；支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP 等方式的链路探测，同时 TCP 与 HTTP 可使用自定义目标端口进行测试； 9.支持全面的 NAT 转换配置，包括一对一，一对多，多对一的源、目的地址转换，并至少支持 FULL_CONE 模式和 SYMMETRIC 模式； 10.支持在会话的源、目的地址同为 IPv4 地址时，可将目的地址转换至指	台	1	

		定服务器地址，同时可探测服务器是否存活； 11.接口支持配置 IPv6 地址，并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定，支持 IPv6 下静态路由及策略路由、动态路由，动态路由应包括 RIPng、OSPFv3、BGP4+（提供截图证明）； 12. 支持针对 IPv6 流量通过 HTTP、HTTPS 实现 Web 认证，用户身份信息可存储在本地或 Active Directory\Radius\TACACS+\POP3 等第三方服务器；通过 HTTPS 实现 Web 认证必须支持使用本地 CA 颁发的证书同时使用证书验证客户端身份（提供截图证明）； 13.支持作为轻量级“探针”与本方案中配置的网络威胁感知系统联动，上报网络活动产生的数据至网络威胁感知系统；并支持接收来自网络威胁感知系统推送的处置策略，及时拦截绕过防御措施产生的高级威胁（提供截图证明）； 14.★所投产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（万兆 EAL3+）； 15.★所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（万兆三级）； 16.★具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》（万兆）；			
9	政务外网核心下一代防火墙	1.多核 AMP+架构，网络层吞吐量 14G，并发连接≥300 万，每秒新建连接数 22 万， 标准 2U 机箱，冗余电源，标准配置 6 个 10/100/1000M 自适应电口，4 个 SFP 插槽，另有 2 个接口板卡扩展插槽，最大支持 22 个接口，1 个 Console 口，支持液晶屏，含三年硬件维保服务。 2.配置三年全功能模块升级订阅服务包（含应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务）。 3.支持基于 IP、用户、应用、时间的带宽管理规则，为精细化、细颗粒带宽管理提供至少 5 级带宽管理规则嵌套；支持设置每 IP 最大、最小带宽及带宽配额管理，可通过优先级实现多应用的差分服务，并支持对剩余带宽进行基于优先级的动态分配。 4.★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；所投产品应具备本地、云端双擎查杀能力，必须能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀，以及对至少 6 级压缩文件进行解压查杀；（提供截图证明） 5.支持针对 FTP、HTTP、IMAP、OTHER_APP、POP3、SMB、SMTP 等应用协议的漏洞攻击防护功能，至少可防御缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL 注入、WEB 攻击等类型的攻击； 6.★应支持内置高质量漏洞攻击特征，应能够防御“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”等高危流行漏洞；漏洞特征应具备丰富的描述信息，至少包括对应的攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息（提供截图证明）； 7.默认配置 128 个虚系统，支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计；（提	台	2	

		供截图证明） 8.★支持威胁情报联动，可基于主机或威胁情报维度统计网络中确认被入侵的主机数量，同时可记录主机被入侵、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；并可在产品本地显示威胁情报详情。 9.支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能（提供截图证明）； 10. 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（提供截图证明）； 11. 支持 SSL VPN，支持使用 SSL VPN 客户端与防火墙建立 SSL VPN 加密隧道，支持对远程用户进行口令认证或证书认证，或证书认证+口令认证双因素；口令认证支持本地认证以及 LDAP/Radius/证书/Active Directory/TACACS+/POP3 等第三方用户认证系统；支持 USB-key 证书；支持本地 CA 并可为 SSL VPN 客户端颁发用于身份认证的证书（提供截图证明）； 12. 支持针对 IPv6 流量通过 HTTP、HTTPS 实现 Web 认证，用户身份信息可存储在本地或 Active Directory\Radius\TACACS+\POP3 等第三方服务器；通过 HTTPS 实现 Web 认证必须支持使用本地 CA 颁发的证书同时使用证书验证客户端身份（提供截图证明）； 13.支持作为轻量级“探针”与本方案中配置的网络威胁感知系统联动，上报网络活动产生的数据至网络威胁感知系统；并支持接收来自网络威胁感知系统推送的处置策略，及时拦截绕过防御措施产生的高级威胁（提供截图证明）； 14.★所投产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（万兆 EAL3+）； 15.★所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（万兆三级）； 16.★具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》（万兆）；			
10	市级横向接入单位下一代防火墙	1.硬件架构：设备形态 1U；采用多核架构； 2.配置要求：千兆 Combo 接口≥8；万兆光口≥2；SSL VPN 并发数实配 100 可扩展 500，IPSec VPN 隧道≥4000，虚拟防火墙数量≥50；配置 1 个电源，可扩展双电源；（提供产品截图） 3.性能要求：吞吐量≥2Gbps，最大并发连接数≥300 万，每秒新建连接数≥7 万，IPSec 吞吐量≥2Gbps，IPS 吞吐量≥1.5Gbps，SSL_VPN 吞吐量≥300Mbps ,SSL 代理吞吐量≥300Mbps 4.★策略管控：能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP 地址、端口、域名组、URL 分类、接入类型、终端类型、设备组、内容安全统一界面进行安全策略配置（提供功能截图） 5.★加密流量安全防护：支持对 HTTPS，POP3S，SMTPS,IMAPS 加密流量代	台	75	

		理解密后，并进行内容过滤，审计，安全防护。（提供功能截图） 6.集中管理及易用性：支持防火墙向云管理平台自动注册，云管理平台对防火墙进行统一的管理及运维。（提供功能截图） 7.支持 1*USB2.0+1*USB3.0 8.提供三年硬件维保、三年威胁防护服务（威胁防护服务包含 IPS，AV，URL，云沙箱） 9.★提供原厂商针对本项目的售后服务承诺函原件并加盖原厂鲜章。			
11	互联网上网行为管理	1.建议 400M 带宽网络环境使用；最大并发连接数为 100 万;最大新建连接数为 28000 个/秒； 1U 硬件;标配 6 个千兆电接口（其中含 1 个管理接口和 1 个 HA 接口）;提供 2 个扩展插槽;1T 硬盘;含专用操作系统与上网行为管理标准软件,含三年硬件维保服务,配置三年 URL 分类特征库订阅服务。 2.★应用协议库包含的应用数量不低于 6000 种，应用规则总数不低于 10000 种（提供截图证明）。 3.可以对下载工具、视频播放、网络游戏、金融理财、即时消息、移动应用有独立的分类进行识别控制。 4.为覆盖工作无关应用，移动应用不少于 1000 种，即时消息应不低于 150 种，网络游戏不低于 270 种，在线购物不低于 50 种，虚拟货币交易平台不低于 40 种； 5.为规避外发类风险，论坛发帖应不低于 3000 种，网络存储不低于 100 种，代理隧道不低于 100 种。 6.≥4000 万条 URL 数据，在官网上有公开的 URL 库更新情况详细说明； 7.当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈； 8.支持在安装终端管理软件时，不再需要安装客户端即可审计 IM 聊天内容。 9.可审计、控制 Oracle, MySql, SqlServer, PostgreSQL 等数据库的访问与操作，包括添加、删除、修改、查询等。 10.能够支持 IPv6 环境下的网址访问审计、生成分析报表等功能；能够在 IPv6 环境下，正确审计显示用户的 IPv6 地址。 11.★支持通过恶意软件特征检测方式识别失陷主机并记录日志（提供截图证明）； 12.支持对 802.1X、华为 controller、Kerberos、AD、POP3、Radius、数据库识别、PPPOE、华三 iMC、城市热点、深澜计费等系统的单点登录（提供截图证明）； 13. 支持配置禁用 PC 热点开启功能。禁用时 PC 仍可以使用网络，但是无法通过随身 wifi 或笔记本自带功能创建热点（提供截图证明）； 14.当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈（提供截图证明）； 15.★支持策略管理、日志审计、权限分配相互独立的三权制衡管理机制，避免超级管理员权限过大的弊端。系统管理员和审计员的账号创建，权限变更需要审核员审批才能生效。管理员和审计员的操作会形成日志受审核	台	1	

		员监督（提供截图证明）； 16.★公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》； 17.★中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》，级别为 EAL3+ ； 18.★中华人民共和国工业和信息化部颁发的电信设备进网许可证；			
12	互联网安全接入平台	接入网关设备（含三年硬件维保）： 1、两台硬件设备：采用非 X86 64 位多核高性能处理器和高速存储器主控模块内存≥8G；≥8 个千兆光口+16 个千兆电口+2 个万兆光口，≥2 个扩展槽位，≥2 个硬盘槽位，可扩展 500G/1T 硬盘，配置双电源。 2、整机最大可扩展接口数量 8SPF+24GE+2*10GE，可扩展 4GE Bypass 功能接口 3、整机大包吞吐量≥8Gbps；最大并发连接数≥800 万；每秒新建连接数≥120K; 4、免费支持高性能 IPSec、L2TP、GRE VPN 功能,支持 IPsec VPN 隧道自动建立，无需流量触发； 支持 IPsec VPN 智能选路，根据应用和隧道质量调度流量。 可基于每个 SSL VPN 用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控。 5、支持流量自学习功能，可设置自学习时间，并自动生成 DDoS 防范策略。 6、支持静态路由、RIP v1/2、OSPF、ISIS、BGP、策略路由等 7、设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配 CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能， 8、设备支持高可靠性（包含主备/主主模式）部署。 9、支持高性能 SSL VPN 功能，最大支持并发用户数≥4000；实配 2400 用户数 SSL VPN 授权； 智能管理平台标准版： 1. 支持 B/S 架构； 2. 支持对全网交换机、路由器等设备实现统一网管； 3. 可以为不同的管理员设置不同的用户名、密码，并限制管理员的管理权限和管理范围，实现用户分权管理； 4. 支持用户名、密码与用户 IP、MAC、VLAN、设备 IP、设备端口、主机名、域用户、SSID、AD 域、硬盘序列号、IMEI、主板序列号等多种元素的绑定认证；支持第一次认证成功时的自学习绑定属性功能； 5. 可以在认证通过后下发用户的 ACL、VLAN、QoS 给接入设备，由设备动态控制用户的访问网络权限。 6.可基于用户角色、接入位置、接入终端类型等情境，向联动设备下发事先配置的接入控制策略，按用户不同的情境场景控制用户的网络使用行为；支持一用户多策略授权，从同一地点可获取不同的接入权限，实现内外网隔离场景； 7. 能够提供接入用户网络拓扑，在拓扑上实现在线用户查询、强制下线、下发消息等功能，便于用户的管理； 8. 支持获取在线终端的位置信息，并绘制终端的移动轨迹；	套	1	

		10.可通过管理平台主动向用户、用户组、应用推送消息，支持的消息类型有文本、图片、图文、文件等； 11.支持多种形式的APP：本地APP、轻应用、虚拟APP；支持APP的下载、推送、自动触发安装、升级、卸载； 12.支持SSL VPN隧道加密传输，包括IP层VPN、TCP端口转发VPN，以及基于应用的VPN控制； 13.支持文档自动添加水印，防止偷拍并能实现泄露追踪溯源,防止应用数据的截屏、拷贝、粘贴，防止应用破解。 14.★传统终端（PC、便携机）与移动终端（手机、PAD）的控制策略、生命周期管理等基于同一管理平台进行管理；			
13	日志审计系统	1.日志审计系统主机(冗余电源，包含日志审计系统软件)。性能：事件采集10000EPS，事件处理最高3000EPS。 2.硬件规格：标准1U机箱，6个千兆电口，2个扩展插槽（可选2万兆光、4千兆电、4千兆光），1个Console接口，4T硬盘，包含200授权节点，含三年硬件维保服务。 3.支持单一部署，也支持级联部署、上级支持查询下级节点数据（下级节点数据不用上传到上级），管理中心内嵌数据库，用户无需另外安装数据库管理系统 4.界面100%都是B/S模式，无需安装客户端，WEB浏览器访问管理中心，浏览器端无需安装Java运行环境。支持chrome浏览。 5.能够对企业和组织的IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计，最大支持 1000个日志源事件采集。 6.支持审计各种网络设备（路由器、交换机、等）配置日志、运行日志、告警日志等； 7.支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防DDOS攻击，Web应用防火墙、等）配置日志、运行日志、告警日志等； 8.支持审计各种主机操作系统（包括Windows,Solaris, Linux, AIX, HP-UX,UNIX,AS400）配置日志、运行日志、告警日志等； 9.支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等； 10.支持审计各种中间件（tomcat、apache、webshpere、 weblogic等）配置日志、运行日志、告警日志等； 11.支持各种应用各种应用系统（邮件，Web，FTP，Telnet、等）配置日志、运行日志、告警日志等；以及用户自己的业务系统的日志、事件、告警等安全信息进行全面的审计。 12. 系统应提供从总体上把握日志告警和日志统计分析的实时综合性监控界面；用户可以自定义监控主页。（提供截图证明） 13.★系统支持自定义资产属性；支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。（提供截图证明） 14.系统提供灵活简单的归一化方式,对系统新增的日志类型只需修改配置文件即可支持,不需修改系统程序（提供截图证明）。	台	1	

		15.★能够在世界地图上实时定位事件源/目的 IP 地址的地理位置；（截图证明） 16.报表可根据设置自动运行,调度生成日报、周报和月报；（截图证明） 17.★所投产品具备中国信息安全认证中心《中国国家安全产品认证证书》（3C），增强级； 18.★所投产品具备《计算机软件著作权登记证书》； 19.★所投产品具备公安部《计算机信息系统专用产品销售许可证》； 20.★所投产品具备国家信息安全测评中心《信息技术产品安全测试证书》EAL3+。			
14	堡垒机	1.采用专用硬件平台和安全操作系统，外观：标准 2U 机架式，支持 4 个千兆电口,另支持 3 个扩展槽位，总容量 4TB 硬盘，冗余电源，支持液晶屏，最大支持 800 路字符会话并发。300 设备授权，含三年硬件维保服务。 2.物理旁路，逻辑串联模式，不影响原有网络架构;HA 双机热备、支持跨地域、跨数据中心，多层次部署. 3.支持 SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin 等协议 4.支持 Linux/Unix、Windows、H3C、Huawei、Cisco 等系统 5.支持图形、字符，混合协议下的批量登录 6.支持 IPv6 网络环境下的运维、操作审计 7.通过应用发布实现对 MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client、Radmin、dbisql 等应用程序/客户端的扩展 8.支持按 IP 范围、端口进行资源设备自动发现，实现快速批量添加资源设备（提供截图证明） 9.支持资源按标签管理，实现添加主机时快速分类 10.支持云主机资源批量添加，包括阿里云、百度云、华为云、腾讯云、Ucloud、AWS、Azure 云平台的资源（提供截图证明） 11.不限操作客户端系统类型，无需安装任何客户端插件，使用 H5 即可直接运维 windows、Linux、网络设备等资源 12.支持第三方客户端运维字符类型资源;通过群发命令、预置命令，实现同时运维多台资源设备;运维过程中支持会话协同，可邀请其他用户参与、协助操作。（提供截图证明） 13.支持以云盘形式在堡垒机上存储常用文件，实现操作端、堡垒机、目标服务器三者之间文件共享。 14.不限操作客户端系统类型，无需安装任何客户端插件，使用 H5 即可直接运维 windows、Linux、网络设备等资源（提供截图证明）; 15.★所投产品具备 IT 信息安全产品认证证书; 16.★所投产品具备《计算机软件著作权登记证书》; 17.★所投产品具备公安部《计算机信息系统专用产品销售许可证》。	台	1	
15	区县政务外网下一代防火墙	1.多核 AMP+架构，网络层吞吐量 8G，并发连接≥210 万，每秒新建连接数 10 万， 标准 2U 机箱，冗余电源，标准配置 6 个 10/100/1000M 自适应电口，2 个 SFP 插槽，支持 1 个扩展槽，1 个 Console 口，支持液晶屏，含三年硬件维保服务。 2、★配置三年全功能模块升级订阅服务包（含应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务）。	台	10	

		3.支持接收针对突发重大安全事件的“应急响应消息”，针对该消息可以选择“自动”或“手动”处理。至少在界面显示安全事件的名称、类型、当前防护状态、处置状态以及相应的操作等信息；并自动检测、呈现针对该事件的处置结果，提示导致处置未生效的错误配置；（提供截图证明） 4.提供可明文或加密方式调用的 Restful API，并可指定 Restful API 使用的本地端口;为确保设备管理的安全性,支持限制特定主机调用 Restful API；支持定义第三方设备、平台通过调用 Restful API ，至少可配置所投设备的访问控制策略、源 NAT 策略、目的 NAT 策略、静态路由、高可用以及区域、地址、服务、时间、用户对象等功能；（提供截图证明） 5.支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能；（提供截图证明） 6.支持作为轻量级“探针”与本方案中配置的网络威胁感知系统联动，上报网络活动产生的数据至网络威胁感知系统；并支持接收来自网络威胁感知系统推送的处置策略，及时拦截绕过防御措施产生的高级威胁。（提供截图证明） 7.★支持基于 MD5 的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀（提供截图证明）； 8.★支持自定义基于 TCP、UDP、HTTP 协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围（提供截图证明）； 9.接口支持配置 IPv6 地址，并可使用 IPv6 地址管理设备；支持 IPv6 手动及自动的 IP/MAC 探测及绑定，支持 IPv6 下静态路由及策略路由、动态路由，动态路由应包括 RIPng、OSPFv3、BGP4+； 10. 支持统计网络内威胁事件的数量及对应的风险等级；支持一键跳转查看详情并自动显示关联日志；可基于网络连接、应用名称、威胁事件处置威胁事件（提供截图证明）； 11.★所投产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（万兆 EAL3+）； 12.★所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》（万兆三级）；			
（三）运维管理平台建设					
16	运维管理平台	1. 平台整体技术要求：产品架构支持中文界面，纯 B/S 架构，系统采用 J2EE 平台，所有操作均在 B/S 模式下完成，具有完全自主知识产权证明，内置合法数据库方便系统快速部署； 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.★提供业务分析与健康度评价，实现以健康曲线、雷达扫描等方式呈现整体信息化运行水平；（提供该功能的截图，提供工信部软件评测机构级别出具的第三方测试报告扫描件，提供该功能的用户使用报告复印件，加盖原厂鲜章。）； 4. 业务模型应预留北向 API 接口，可对接业务系统推送的业务指标，方便用户所综合评价业务质量。（提供该功能的截图，加盖原厂鲜章。）； 5.★拓扑图应以不同方式展示管理对象的状态信息，如颜色、粗细、流动	套	1	

		效果、自定义图标等；（提供该功能的截图，加盖原厂鲜章。）； 6. 提供良好的可视化效果，包括交互界面、拓扑效果和故障捕获效果。拓扑功能需支持自动扫描和事件播放功能；（提供该功能的截图，加盖原厂鲜章。）； 7. 支持数据下钻功能，查看每个设备和链路的详细信息，如设备的详细信息、告警详情、面板信息、网络接口、业务结构图、下联设备等； 8. 要求提供咨询、梳理、实施、培训以及 3 年维保； 9.本次要求提供不少于 1200 个监控节点授权； 10.平台应具有的流程、报表二次开发自定义功能； 11.支持对 IP 地址的记录、分配、统计、自动关联资产信息表等功能； 12.支持对 IT 资产情况的记录、分配、统计、自动关联资产信息表等功能； 13.支持资产清单设备的二维码生成，通过 APP 能扫描二维码能查看到设备相关信息； 14.支持对应用系统的记录、统计、自动关联资产信息表等功能； 15.自动预警提醒，定期提醒各运维人员完成对应用系统数据更新，支持超文链接跳转功能； 16.支持修改、删除功能，保留修改痕迹，并根据制度和流程生成任务工单，执行任务处理流程（预警响应、应急处置等）时可以传输文档（pdf、word、excel）； 17.支持任务分配管理，实现任务分配、处理、结果反馈、确认流程的过程管理。			
（四）其他					
17	等保测评	参照等保三级要求以及相关国家标准，对服务器、网络设备、安全设备、运维管理系统等，评估系统是否具备足够的信息安全防护能力,提供等级保护（市）三级（一次）、八县两区二级测评（一次）服务	次	1	
18	机柜租用费	电信枢纽机房 42U 服务器机柜，三年租赁费	架	7	
19	机房搬迁	市政府大楼五楼核心机房设备搬迁至电信枢纽机房	批	1	
20	系统集成及运维服务	本期项目所投设备、软件系统集成及运维服务： 1. 系统集成要求：基于现有数据中心建设情况，完成本期扩容所涉及产品及功能软件的实施，要求实施期间平稳过渡，不得出现因扩容/升级导致数据中心业务中断的情况发生。 2.运维服务要求：1）现场巡检：不少于 1 次/季度对机房设备和综合运行环境进行巡查，提供每季度巡检报告，并对每一次重大故障和问题的原因、解决方法、完成情况等形成专门报告，及时报送用户部门确认；2）系统监控：对维护主机、应用系统、数据库、网络设备等对象进行实时监测，提供图形化管理界面，并对故障进行短信告警；3）故障响应：提供 7×24 小时的技术响应和服务，提供专门的技术服务电话，必须在接到用户方电话后 30 分钟内响应，对于紧急软硬件故障，必须在 1 小时内到达现场并提出解决方案。对于非紧急软硬件故障，必须在 8 小时内提出解决方案。	批	1	

		3.提供壹年运维服务，要求投标人提供服务承诺函。			

二、主材需求表（市政府大楼综合布线改造）

序号	名称	规格程式	单位	数量
Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ
1	光纤跳线	楼层交换机连接备件，长 3 米。	条	25
2	六类非屏蔽跳线(1m)	服务器机柜配线架连接服务器	条	25
3	24 芯单模室内光缆	24 芯单模室内光缆，走光缆管道井敷设，连接行政中心各大楼楼层交换机，以及到核心网络机房线缆	米	9000
4	光纤尾纤	用于光缆熔接。	米	50
5	24 位机架式光端盒（含适配器）	用于光缆熔接。	个	5
6	其余辅材	金属线管、金属软管，各类控制线、数据线等等	批	1

5、评审办法

采用综合评分法进行评审

6、商务要求：

（1）交货时间或服务时间：以合同签订为准;

（2）交货地点或服务地点：采购人指定的地点;

7、无效标情形：

（1）递交的投标文件不完整或未按采购文件要求加盖公章及签字的；

（2）供应商不符合国家及招标文件规定的资格条件的；

（3）投标报价高于财政采购预算采购人无法支付的；

（4）投标文件对采购文件的实质性要求和条件未作出响应的；

（5）未交纳投标保证金的；

（6）投标有效期不满足采购文件要求的；

（7）违反政府采购法律法规,足以导致响应文件无效的情形。

特别说明：本公示内容仅为招标人对本项目的需求公示，具体内容以最终招标文件发售稿为准！