1. 被推荐供应商名单和推荐理由

A 包：

被推荐中标人名单：中国联合网络通信有限公司烟台市分公司

被推荐中标人理由：按照磋商文件规定的各项因素进行综合评审，评审总得分最高

B 包：

被推荐中标人名单：中国移动通信集团山东有限公司烟台分公司

被推荐中标人理由：按照磋商规定的各项因素进文件行综合评审，评审总得分最高

2.服务要求

一、项目说明

本项目为莱阳市人民政府办公室的莱阳市互联网出口建设整合，共划分为2个包；其中，A包为莱阳市互联网统一出口整合及主用带宽租用；B包：莱阳市互联网备用带宽租用。供应商需完成莱阳市互联网出口建设整合相关工作，供应商须对所报内容进行全部响应，若有遗漏，视为对采购人免费提供。

二、采购标的具体情况

（一）项目概况

山东省电子政务外网是我省电子政务领域重要的信息化基础设施，是满足各级政务部门经济调节、市场监管、社会管理和公共服务等方面需要的政务公用网络。政务外网纵向覆盖省、市、县（区）、镇街，横向连接市直各部门。烟台市电子政务外网是山东省电子政务外网在烟台的延伸和拓展，全市各级政府及部门的政务专用网络平台、资源共享的公用网络平台和互联网接入平台。莱阳市电子政务外网是烟台市电子政务外网的延伸，本项目在原有莱阳市电子政务外网基础上，对各政府单位互联网出口进行统一整合建设，由供应商使用独立、专用的线路、设备，新建、优化、完善市电子政务外网统一互联网出口平台以及相关的服务，按照《山东省电子政务外网技术规范（试行）》要求对互联网出口的安全防范进行部署，并负责后续的运行维护，满足莱阳市电子政务外网公共服务域所覆盖政府单位的互联网访问需求。

（二）采购内容及具体情况

1.项目建设依据

根据鲁政办发〔2017〕75号《山东省人民政府办公厅关于印发山东省政务信息系统整合共享实施方案的通知》和鲁政办字【2018】50号《山东省人民政府办公厅关于印发2018年政务信息系统整合共享工作要点的通知》的要求，到2018年年底，通过“统筹一片云(电子政务云)，规范两张网(电子政务内网、电子政务外网)，建成三大体系(数据资源体系、政务服务体系、业务协同体系)，强化四个支撑(政策支撑、产业支撑、标准支撑、安全支撑)，落实五项保障(体制保障、财力保障、智力保障、监督保障、审计保障)”，形成设施集约统一、资源有效共享、业务有机协同、工作有力推进的“12345”发展格局，完成全省政务信息系统整合。按照“统一机构、统一规划、统一网络、统一软件”的要求，依托省电子政务外网公共服务域，整合部门互联网出口，建设省市县三级互联网统一接入平台。本项目遵循的主要标准或要求如下：

中共中央办公厅、国务院办公厅关于转发《国家信息化领导小组关于我国子政务建设

指导意见》的通知（中办发[2002]17 号）；

中共中央办公厅、国务院办公厅关于转发《国家信息化领导小组关于推进国家电子政务网络建设的意见》的通知（中办发[2006]18 号）；

《国家电子政务外网安全等级保护基本要求（试行）》；

《国家电子政务外网 IPSec VPN 安全接入技术要求与实施指南》；

《国家发展改革委、财政部关于推进国家电子政务外网建设工作的通知》（发改高技[2009]988 号）；

《国家电子政务外网安全等级保护基本要求》（GW0103-2011）；

《国家电子政务外网安全接入平台技术规范》（GW0202-2014）；

《国家电子政务外网 IPv4 地址规划》（GW0206-2015）；

《国家电子政务外网 IPv4 地址地方分配部署指南》（GW0207-2015）；

《山东省人民政府办公厅关于印发山东省政务信息系统整合共享实施方案的通知》(鲁政办发〔2017〕75 号)；

《山东省人民政府办公厅关于印发 2018 年政务信息系统整合共享工作要点的通知》（鲁政办字[2018]50 号）；

《山东省电子政务外网技术规范（试行）》；

《山东省电子政务外网 IPv4 地址规划（试行）》。

（三）项目服务期限

自项目建设完成并投入使用之日起 1 年，合同期满后供应商服务质量良好且经双方协商无异议后可续签合同，续签合同一年一签，连续续签合同累计不超过 5 次。

2.项目建设原则

（1）安全性原则

互联网接入区是莱阳市各部门统一访问的互联网区域，其联网范围大，连接节点多，所以其安全性至关重要。为此，在规划设计的全过程中要充分体现系统建设和信息安全相结合的原则，从物理、技术、管理等方面制定严密的安全方案，形成多层次、全方位的安全防线。

（2）实用性原则

互联网统一出口的建设，要充分体现统一出口的实用性。要根据对各政务部门的业务需求进行调研，根据其调研的汇总需求，适当考虑其设备、技术的前瞻性，采用成熟的各种技术手段，实现各种功能，满足其政务部门的业务要求；再者，要充分考虑业务流量特

点，以及用户对使用习惯、功能等要求，合理使用网络安全技术，满足未来用户可能提出的要求，实现业务上网、网上工作、综合服务等政务业务的一站式工作平台的建设目标。

（3）先进性原则

互联网统一出口的建设需要保证当前及今后一段时间内的各类应用顺利运行。由于网络设备及技术更新换代频繁，盲目的追求系统的先进性也会带来更大投资风险，因此在规划、设计外网时，要充分考虑到先进性，在网络设备上，具有一定的扩展性和兼容性，在技术上，保证 3 至 5 年基本不过时，因此要满足全网使用 IPv4/IPv6 双协议栈。

（4）可靠性原则

互联网统一出口要求高度的稳定性、可靠性。因此在互联网统一出口设计和建设中，要从各个方面充分考虑网络线路的质量和设备的冗余，考虑政务业务系统可能对互联网统一出口的更多需求，在稳定性没有保证的情况下，要考虑其可能的备份措施。

（5）经济性原则

在互联网统一出口的设计和建设中，应尽可能地充分利用和保留原有各种网络资源及计算机系统资源等，保护已有投资，避免投资浪费，节约政府资金。网络结构和带宽可以满足当前及今后一段时期内各种应用的需求，新增设备选用上，要充分考虑其兼容性、可扩展性及性能价格比。

（6）可扩展性原则

在互联网统一出口设计和建设中，要求在不影响外网上各种应用的前提下，根据业务的需要，网络、系统可以进行顺利扩展或者平滑升级。网络可扩展的关键在于能否实现合理的模块化设计，采取模块化的设计可以根据网络需求的变化，在不影响现有网络运行的状况下，迅速扩展。因此，整个互联网统一出口工程建设过程中，在设计上要尽可能选用模块化的产品。

3.项目建设模式

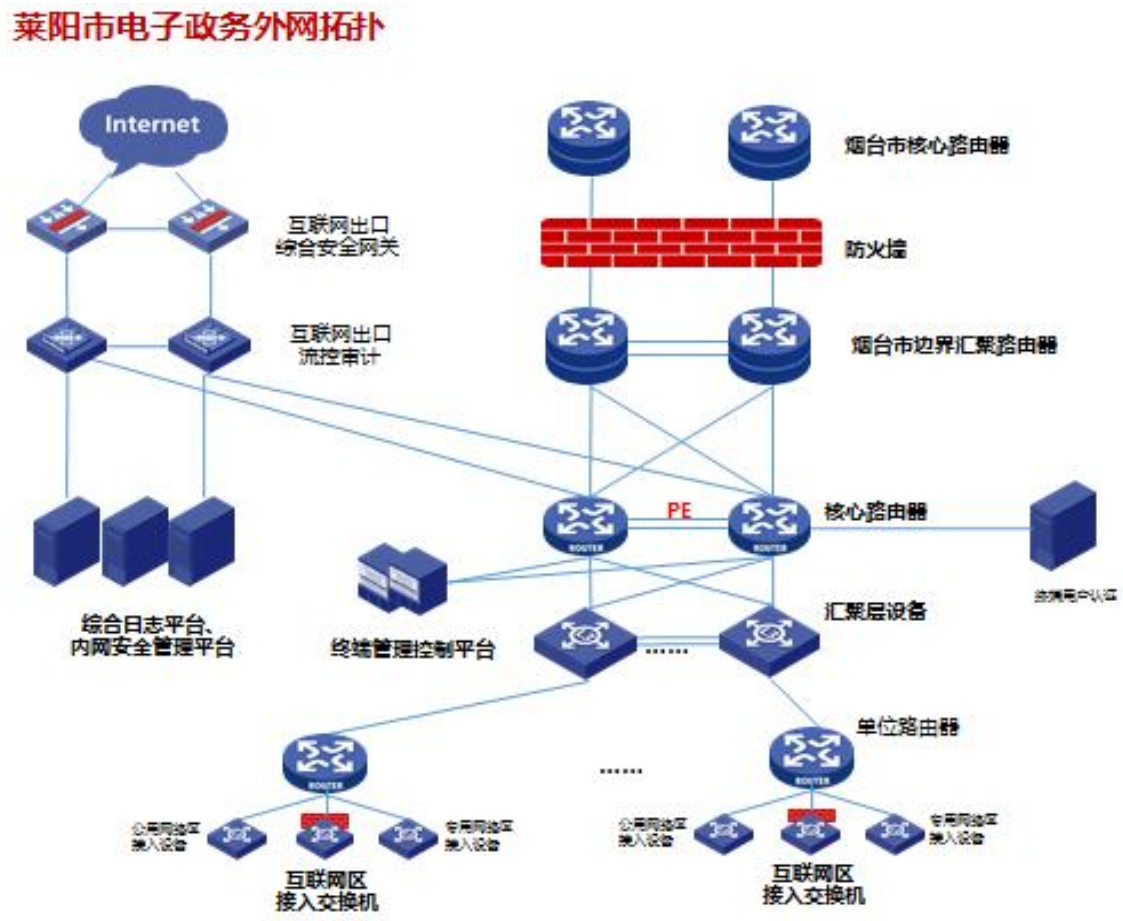
本项目委托供应商在原电子政务外网的基础上对莱阳市电子政务外网互联网统一出口建设整合，要求供应商须使用独立、专用的设备对莱阳市电子政务外网互联网统一出口进行建设及整合，不允许供应商的其它业务共享使用本项目内的相关路由、交换、安全等设备。

包括构建莱阳市县市区级城域网使用到的各类网络设备、安全设备、专用硬件、服务器以及各组成部分之间所必须的各类长途线路、数字/数据专线、设备互联线路等各类线路、耗材费用，计入本项目。

本项目以本地线路租赁费的形式，支付县市区级城域网的相关设备建设、运维、线路费用。

4.项目总体要求

（1）层次结构



拓扑示意图

为提升莱阳市网络安全防护手段，对莱阳市互联网统一出口建设及整合。互联网接入区是实现政务外网连接互联网的网络区域。互联网接入区通过部署统一互联网出口提供政务部门工作人员访问互联网资源的网络通道。对于莱阳市级互联网统一出口，由于办公人员众多，终端设备多，且流量大、高并发、大吞吐的特点，本次方案在出口部署两套防火墙和两台流控审计设备，实现冗余组网，并与核心路由器相连。通过互联网统一出口保障接入政务外网的政务部门终端可以在防火墙、入侵防御、防病毒、行为审计、带宽控制、以及抗 DDoS 攻击、态势感知等系统的保护下安全快速的访问互联网。本次建设不仅需要满足统一互联网出口的安全防范，还需要确保终端用户层面的接入安全管控，本次方案在各政务部门内互联网接入区部署接入交换机，实现终端接入的同时，具有一旦内网发生病毒传播、内网攻击、网络环路等事件，可快速发现并及时自动阻断；对设备自身环路、下

联 HUB 环路等现象能够及时发现，实时上报环路网络设备名称、环路接口、发生时间等信息，并实现自动阻断的功能，减少因网络规划不清和使用不当造成的网络震荡。同时，依据网络安全法的相关要求，需要实现溯源到精确的终端使用用户，确保用户行为可精确追溯。

（2）网络安全要求

莱阳市电子政务外网公共服务域的安全建设应参考国家电子政务外网的相关标准《国家电子政务外网安全等级保护基本要求》（GW0103-2011）、《国家电子政务外网安全监测体系技术规范与实施指南》（GW0203-2014）和《信息系统等级保护安全设计技术要求》（GB/T25070-2010）三级相关标准。

第三级安全保护能力：应能够在统一安全策略下防护网络免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击，能够抵抗较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够及时发现安全漏洞和安全事件。在网络遭到损害后，能够较快恢复绝大部分功能。

互联网接入区通过安全设备和软件实现安全管理。实现防火墙、负载均衡、入侵防御、防病毒、流量控制、VPN 网关等功能；实现账号集中管理、统一登录平台（SSO）、身份集中管理、密码管理、认证授权、行为识别、行为控制、审计管理等功能；实现数据采集、数据分析、数据查询、报表展示、联动协同、系统监控与管理等功能。

实现互联网接入区各平台、基础支撑系统的安全事件监测、状态信息监测、运维监测、脆弱性监测、互联网行为监测、流量监测。综合利用动力环境管理、网络管理、终端管理、日志管理、风险管理、审计等安全管理功能，采取多种手段和安全管理规范，对运行环境、网络设备、安全设备、基础支持系统等 IT 资源实现实时安全监测与趋势分析，通过各级政务外网公共服务域安全监测系统的上下互联，以及与网络管理系统、审计系统等互联，实现体系化部署与监测管理。

三、莱阳市互联网统一出口建设整合要求

（一）第一包：莱阳市互联网统一出口整合及主用带宽租用

1.互联网出口主用带宽 4G，提供 2 个 C 段（255 个）公网 IPV4 地址，并支持 IPV6 技术，根据网络需求免费提供 IPV6 地址和更多的 IPV4 地址，确保满足后续业务需求。

2.委托供应商对电子政务外网互联网统一出口平台进行建设和后续的运行维护。

3.包括莱阳市互联网统一出口整合、线路租用所使用到的各类网络设备、安全设备、专用硬件、服务器以及各组成部分之间所必须的各类线路、耗材费用及建成后机房电力、

人员维护费用均计入本项目，以互联网带宽租赁服务费的形式支付，所有设备由成交供应商负责负责维护及更新，设备的管理权和使用权归采购人所有。

4.各类设备需按照采购人要求，放到采购人指定的位置，并实现与莱阳市城域网核心节点之间的网络连接，承担因此产生的各种费用。莱阳市互联网出口平台与莱阳市城域网核心节点间使用裸光纤冗余线路连接，网内终端通过 MPLS VPN 访问互联网，实现莱阳市各部门互联网统一出口。

5.供应商应使用独立、专用的设备构建莱阳市互联网统一出口平台。不允许供应商的其它业务共享使用本项目内的相关路由、交换、安全等设备。所有链路两端均采用光模块链接，不接受光电转换设备链接，模块由成交供应商提供，其规格见产品技术参数。

序号	设备名称	主要规格参数	单位	数量
1	自安全交换机	1.交换容量≥590Gbps，整机转发性能≥210Mpps，如有双重指标场景下，以最小指标为准； 2.整机可用端口数≥28，其中千兆电口≥24，千兆光口≥4； 3.支持静态路由、RIP、OSPF； 4.支持识别终端接入 IP、MAC、端口等信息，并关联用户身份；支持 IP 仿冒、MAC 仿冒溯源与阻断； 5.支持 6KV 端口防雷；支持对病毒的网络层传播行为进行溯源及阻断，防止内网病毒扩散；支持防 IP 扫描、防 UDP 端口扫描、防 TCP 端口扫描等异常行为； 6.通过运维平台可实现策略配置和安全策略的一键下发与集中管理，实现网络状况、安全事件的实时上报和统一显示。 7.支持识别 IPC 等哑终端设备类型，并支持开启终端安全功能，只允许特定类型的设备接入网络；	台	100
2	内网安全管理平台	1.支持全局拓扑及分区拓扑管理、支持对管理设备的统一升级； 2.支持自动及手动生成网络拓扑，可自定义设备名称、设备连线类型，并支持显示链路状态、互联接口、接口带宽等信息； 3.支持联动认证设备或其他网络安全设备实现网络接入终端的类型识别，可识别 IOS、Andriod、Windows 系统，并可手动自定义调整； 4.支持基于用户/用户组制定安全策略，包括账号有效期、最大在线终端数量、单用户安全策略、基于时间的安全策略，并可限定用户登陆设备和登陆 IP； 5.可实现用户网络准入的接入轨迹并形成历史记录； 6.为保证网络准入安全，防止黑客暴力破解，需支持按照登录失败次数等元素进行限制，并可自定义解封时长及失败周期； 7.支持防终端私接功能：通过图形化界面可针对 IP/Mac/接入端口进行统一操作，一键下发绑定策略，对违法终端可阻断入网并进行告警 8.支持对 IP 扫描、端口扫描、ARP 攻击等进行大数据收集分析，并给出告警及处理建议，并支持一键阻断策略下发。	套	1

		9.支持对 Ddos 类攻击的信息感知收集，包括 SYN FLOOD、ICMP FLOOD 等异常连接数攻击行为的收集分析，并给出告警及处理建议，并支持一键阻断策略下发。 10.支持对传播类病毒、蠕虫病毒的传播行为识别进行收集分析，提升网络对新型网络安全威胁的整体防御能力，并给出告警及处理建议，并支持一键阻断策略下发。 11.为防止私接设备对网络稳定产生影响，以及可能发生的漏洞利用造成的安全威胁，需对小路由器、摄像头的厂商信息进行识别，支持私接告警并支持一键下发阻断策略； 12.可对网络异常事件进行统一管理，根据大数据分析结果实时展示异常事件种类及个数、并可自定义周期展现威胁趋势图，且可根据安全威胁评估等方面统计出网络风险源 TOP 排行榜。 13.本次实际配置≥100 点网络设备管理功能授权		
3	终端管理控制平台	1.交换容量≥57.6Tbps，整机转发性能≥10065 Mpps，如有双重指标场景下，以最小指标为准； 2.采用 CLOS 多级交换架构，主控与交换网板物理分离；业务槽位数≥4 个，独立交换网板数量≥1 个，支持冗余主控，冗余电源； 3.本次实配主控数量≥2 个，交流电源≥2 个，满配独立交换网板；1G SFP 光口≥8 个，10/100/1000 M 以太网电口≥8 个，10G SFP+光口≥12 个 3 米堆叠线缆； 4.可扩展功能类型：准入控制、应用交付、应用防火墙、入侵防御、上网行为管理及流控、无线控制器、SSLVPN 等； 5.支持独创的流定义技术，可以定义不同模块间的业务流走向；支持 VXLAN 等主流 OVERLAY 标准技术和 openflow1.3 等 SDN 标准技术； 6.支持静态路由、策略路由、等价路由、RIP v1/v2、OSPF、IS-IS 和 BGP 等；支持 IPv4 和 IPv6 双协；支持 RIPng、OSPFv3、IS-IS v6、BGP4+等； 7.支持多虚一虚拟化、一虚多虚拟化部署； 8.可以根据业务需求，智能调度业务流量经过物理/逻辑业务模块； 9.支持主机和业务模块统一 IP 管理和统一的配置界面，支持统一网管功能，支持紧耦合部署; 10.支持 Portal、IP 认证、Mac 认证等准入方式；为提高用户使用体验，支持基于用户/用户组的 Portal 无感知漫游； 11.支持与第三方计费系统（如深澜、城市热点等）对接，支持设置用户流量阈值，实现用户上线自动计费、用户流量低于阈值时自动停止计费，需提供对接实施成功证明; 12.支持基于用户/用户组的访问控制策略，用户漫游，策略随行； 13.接入管理精确到用户，支持配置基于用户/用户组的网络策略，可限制用户接入端口、单用户最大终端数，提供用户登录日志；	套	2
4	防火墙	1.2U，≥4 个千兆电口、≥4 个千兆光口、≥2 个万兆光口，冗余电源，6 个扩展槽位，防火墙吞吐≥95G，并发连接≥2200 万，每秒新建连接≥52 万，全威胁吞吐量≥11G。含攻击规则特征库 5 年升级许可；专业病毒库 5 年升级服务许可； 2.支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、SIP、	台	2

		NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板； 3.支持对 HTTP/SMTP/POP3/FTP/IM 等协议进行病毒防御；； 4.访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址； 5.支持独立的入侵防护规则特征库，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库； 6.支持 DNS Doctoring 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡； 7.支持对 IPV4/IPV6 域名的访问控制，支持对多级域名进行控制，域名对象支持通配符； 8.支持对 IPv6 报文进行病毒防御、入侵防御、URL 过滤、抗 DDOS、WAF 防护、僵木蠕、流量控制、连接限制、文件过滤、数据过滤等； 9.支持对 SSL 加密协议进行解密检测，防止恶意流量通过 SSL 加密逃逸。 10.支持资产管理，可查看资产详情、安全防护策略，并对资产进行分组和防护优化；		
5	上网行为管理设备	1.2U，≥6 个千兆电口， ≥4 个千兆光口，≥2 个万兆光口，冗余电源，4 个扩展槽位,适配带宽：≥10G，最大并发连接数≥1200 万 推荐用户数：≥150000 人，含 5 年的系统版本，URL 库及应用特征库升级许可 2.支持路由模式，旁路模式、网桥模式、混合模式部署；切换部署模式无需重启，不影响设备正常使用。 3.支持将多个以太网物理端口捆绑成一条逻辑端口（即将多个端口捆绑成一个逻辑的端口以增加带宽，同时增加链路备份）支持基于轮循、主备、哈希、广播、802.3ad、发送自适应、双向自适应等多种负载方式。 4.支持即插即用功能。不管电脑的 IP 如何配置，开启即插即用功能后，只要插上网线即可上网。 5.能基于组织结构记录用户访问的具体 url、标题、网站类型、访问时间、动作等信息，通过详细信息可以查看用户访问的源和目的地址，以及访问的端口。 6.支持所有访问的会话日志记录，包括: 源 IP、目的 IP、协议类型、七层应用名称、源端口、目的端口、是否进行 NAT 转换(可显示转换后的 IP 和端口)、会话产生的时间和会话持续时间。 7.能基于组织结构记录用户搜索的关键字、搜索的类型时间、动作等信息，通过详细信息可以查看用户访问的源和目的地址，以及访问的端口。 8.支持基于源 ip、地址薄、用户及用户组的流控策略。支持基于每个人的限速以及整体限速。支持每个用户的源，服务等，进行最大上下行会话数控制，避免网络滥用。 9.支持对 TCP、UDP、ICMP、TCP SYN 超时时间，无回应 UDP 超时时间设置，并能支持按照新建会话与总会话比例设置老化开始或者结束。 10.支持 DNS 链路健康检查算法；支持 ICMP 链路健康检查算法；	台	2

		支持 TCP 链路健康检查算法；支持自定义的链路健康检查算法；		
6	安全态势感知检测平台	（一）安全态势感知平台硬件要求： 1. 2U，≥6 个千兆电口，≥2 个万兆光口，冗余电源，存储≥240SSD+32TB，内存≥128G，软硬一体设备，提供态势分析、安全监测、安全处置、资产管理、知识情报等功能模块。 2.支持态势大屏展示，包括全网态势、资产态势、漏洞态势、攻击态势，支持大屏展示时间设置，支持态势大屏中相关信息下钻跳转到对应的详细页面。 3.支持通过资产视角进行漏洞的查询展示及处置，展示信息包括资产名称、资产 IP、业务系统、漏洞总数、不处置漏洞、责任人，支持按照 TXT、CSV、EXCEL 进行导出，支持对资产下所有漏洞进行批量及独立处置。 4.支持对安全处置情况进行概览分析，包括待处置告警数、待处置漏洞数、待处置风险资产数、待处置威胁源数、待处置漏洞 TOP5、风险资产 TOP5、威胁源 TOP5。 5.支持对全网安全分析，包括外联主机数、内网威胁源、外网威胁源、失陷主机数、外联主机 TOP5、内部威胁源 TOP5、外部威胁源 TOP5。 6.支持资产攻击信息分析，包括威胁数量、遭受威胁类型、威胁源 TOP5、攻击链分析、攻击链日志列表、攻击链日志关系图、攻击链日志时序图，支持 8 种攻击链阶段，包括侦查跟踪、载荷投递、漏洞利用、安装植入、命令控制、横向移动、目标达成、痕迹清理，支持以不同颜色标识攻击链命中阶段，支持按照攻击链阶段及日志级别进行分析。 7.支持内置分析模型，包括但不限于失陷状态、FTP 登录失败、敏感文件信息泄露、成功暴力破解、文件上传漏洞等，支持模型查看、启用、停用等操作，支持模型批量删除、批量启用、批量停用，支持导入内置模型，状态为启用的模型不允许操作，支持按照模型名称、模式、模型状态、模型分类、关注度进行过滤查询。 （二）威胁检测探针要求： 1. 2U，≥6 个千兆电口，≥4 个千兆光口，≥2 个万兆接口，冗余电源，4 个扩展槽位,综合威胁检测能力：≥10Gbps，含 5 年升级许可，包含攻击检测规则库、应用识别库、地理信息库、僵尸主机规则库、威胁情报库、URL 分类库。 2.支持对文件还原捕获，可自定义捕获文件大小，最大支持还原 100M 大小的文件，文件信息可详细审计，包括但不限于哈希、文件类型、威胁程度等； 3.支持机器学习检测，能够对目标文件实时检测并实时还原效果，在不依赖规则库的前提下实现对未知恶意程序检测； 4.产品具备静态病毒防护、动态病毒防护功能，其中可执行恶意软件样本库检测率≥90% 5.支持独立的攻击检测引擎和僵尸主机特征库； 6.支持独立的 DDoS 检测引擎,包括但不限于 IP FRAG FLOOD 攻击检测、DOS 攻击检测、ICMP FLOOD 攻击检测、TCP FLOOD 攻击检测、SYN FLOOD 攻击检测 HTTPS 并发连接 FLOOD 攻	套	1

		击检测、HTTPS 自定义端口等多种 FLOOD 攻击检测； 7.支持暴力破解检测，包括 SMTP、IMAP、POP3、FTP、SMB、TELENT、LDAP、ORACLE、MYSQL、MSSQL、MONGODB、POSTGRESQL、DB2 等协议的口令暴力破解行为，并可以对发生的暴力破解行为事件进行告警、追溯和联动阻断； 8.支持隐蔽通信检测，包括但不限于对 HTTP、FTP、SMTP、IMAP、POP3、TELENT 等服务的隐蔽通信检测，可设置相应的警告、联动阻断动作； 9.支持通过威胁情报检测已知 APT 事件，通过恶意程序检测未知 APT 事件，通过僵尸行为规则库检测已知的 APT 组织； 10.支持 SSL 卸载功能，实现对 HTTPS、IMAPS、SMTPS、FTP、SIP 等加密流量的分析检测。		

（1）市级互联网出口主用带宽链路要求

提供市级互联网出口主用带宽 4G。供应商提供的互联网链路到达 Internet 骨干核心路由器的跳数不超过 3 跳，并可根据采购人要求实现核心业务 QoS 保障。

供应商应保证与采购人互联的设备至供应商骨干层的时延和丢包率符合正常的标准，时延≤50ms，丢包率≤0.5%；实际带宽 可用率大于 95%，年可用性大于 99.99%。

部分市级单位、部门本次暂不进行互联网整合，供应商需提前规划认真准备，本次报价应含当前及后续互联网整合费用。待部门、单位互联网整合时，根据实际产生费用支付，不再进行单独采购。

（2）市级互联网出口平台建设要求

莱阳市电子政务外网互联网统一出口应满足终端数多、流量大、并发连接数高、吞吐量大等实际需求，实现防火墙、入侵防御、防病毒、行为审计、带宽控制、抗 DDoS 攻击、网络安全威胁态势感知等功能，支持完善的 IPv6 功能，确保满足后续业务需求。电子政务外网互联网出口建设应满足国家公安部 82 号令要求，对网络用户的上网行为进行审计。

各政务部门内互联网接入区部署接入交换机，整体采用纯二层部署，上联采用电口连接至各单位政务外网接入路由器。各政务部门内互联网接入区需要避免受到来自各委办单位内部产生的威胁攻击，还应具备网络环路检测与自愈，网络渗透防护、异常连接数攻击防护、病毒传播检测与抑制及用户位置精确溯源等能力，作为电子政务外网互联网区的第一道防线，与终端管理控制平台和内网安全管理平台联动，实现内网威胁可视、可管、可控、可溯源，以达到用户轻松接入，网络管理员轻松运维的效果。

供应商应部署终端管理控制平台，终端通过 WEB 认证实现用户的准入控制，打印机、摄像头等非智能终端通过 IP/MAC 认证实现设备的准入控制，做到实现用户的“一次认证、永久接入”，提升用户上网体验。平台可记录用户名、接入时间、接入终端、接入位置等

内容，并以日志的形式发送至内网安全管理平台，方便安全事件回溯，当发生病毒传播、网络内部攻击、网络环路等事件，可快速发现并及时自动阻断，对设备自身环路等现象能够及时发现，实时上报环路网络设备名称、环路接口、发生时间等信息，并实现自动阻断的功能。

供应商应部署内网安全管理平台，需实现全网设备的统一管理和策略的一键下发，对所有设备及用户进行管控，实现全网用户的实名接入和策略跟随，同时网络用户的异常行为可以通过实时日志报表的形式推送给网络管理员，做到全网可管、可控、可视化。

供应商应部署电子政务外网安全态势感知监测平台，将网络安全的思维模式从单纯强调防护，转变到注重预警、检测、响应的格局，安全能力从“防范”为主转向“持续检测和快速响应”，实时防御将以威胁为中心，提升我市电子政务外网安全。

（二）第二包：莱阳市互联网备用带宽租用

1.互联网出口备用带宽 1G，提供 1 个 C 段(255*1)公网 IPV4 地址，并支持 IPV6 技术，根据网络需求免费提供 IPV6 地址，确保满足后续业务需求。

2.成交供应商负责将互联网线路接入到互联网统一出口设备所在地。

四、服务要求

1.驻场服务要求

供应商需提供全年 7×24 小时驻场服务，常驻采购人技术工程师总人数不少于 1 人，必须保证 7×24 小时不少于 1 人在岗，负责互联网出口平台、安全接入平台的运维等（可为安全产品厂家技术人员）。

2.迁移服务要求

项目运行期，如政府政务云中心或机房等，需要将相关设备或平台等做迁移，供应商需要免费提供迁移服务，包括因迁移新架设的线路也需要免费提供。

3.技术文档

提供完整的建设方案及安装、调试、使用技术文档、应急方案。

五、其他要求

1.供应商承诺与采购人同意的其它服务商（含运营商）紧密配合，不对其它服务商（含运营商）采取歧视性措施。若采购人后期有广域网、城域网地址迁移或带宽升级需求，供应商应承诺在迁移或升级过程中与其他服务商全力配合。**（供应商须提供承诺函，格式自拟）**

2.供应商遵守省、市政务外网主管单位制定的运维服务指标体系和评估评价标准，承

诺配合采购人对互联网出口整合运行情况进行年度评价和绩效考核；年度综合考评结果为不合格的，即视为不具备相应的服务能力，采购人有权终止合同，报相关采购主管部门备案，并在后续采购中予以综合考虑。采购人可指定第三方对供应商服务情况进行监督和考核。

3.供应商承诺在该项目建设和后期的运行维护中，接受采购人的监督和管理，为采购人提供各类运行数据；根据采购人需要，提供线路使用情况和设备运行情况报告与分析。

4.供应商承诺具备应急通信的能力，并制定完善的紧急故障处理流程及应急预案。如遇不可抗力因素（如地震、洪水等）造成的线路阻断，应在短期内采用应急手段恢复通信；对于可预见的原因，影响采购人通信的，应提前 24 小时通知实际用户。

5.互联网主用带宽线路供应商承诺提供的线路与互联网备用带宽线路供应商的光缆由两条不同物理路由的管道进行承载。

6.供应商必须根据莱阳市电子政务外网主管单位要求，负责各接入部门的政务外网升级和互联网出口整合等工作。各类设备需按照采购人要求，放到采购人指定的位置。在合同期内采购人拥有设备的管理权和使用权。

7.供应商承诺在该项目建设和后期的运行维护中，若出现上级政策、技术规范、标准等方面变化，无条件进行适应性改造或升级，相关服务价格不变。

8.供应商需协助采购人制定详细的政务外网互联网出口管理办法、运维工作细则，在服务过程中须详细记录服务内容，每月初向采购人提供上月工作报告，包括日常巡检、故障处理等。

9.供应商承诺选用安全自主可控的国产软、硬件设备组网，设备须全新未拆封，支持 IPv4/IPv6 双协议栈。

10.供应商应在响应文件中明确在服务期内各类软件、安全库、特征库免费升级，并详细阐述质量保证措施及售后服务的内容和形式。

11.供应商应负责免费培训采购人指定的技术人员和管理人员，制定培训计划表，列出每种培训的地点和时间（每季度一次），培训内容应包括所提供设备的原理和技术性能、操作维护方法、安装调试、排除故障等各个方面，并提供培训教材（中文）和培训计划表。

12.为保证提供优良的设备售后服务，签订合同前，所有设备需提供原厂质保函和授权书；所有设备在服务期内需提供原厂质保服务。

13.电子政务外网公共服务域执行《山东省电子政务外网技术规范》、《山东省电子政务外网 IPv4 地址规划》、《国家电子政务外网安全等级保护基本要求》（GW0103-2011）、

《国家电子政务外网安全监测体系技术规范与实施指南》（GW0203-2014）和《信息系统等级保护安全设计技术要求》（GB/T25070-2010）三级相关标准，按网络安全等级保护第三级标准建设。

注：

1.以上要求仅供参考，供应商提供的服务应相当于或优于以上要求，并填写偏离表，针对本项目供应商可提供除以上服务内容外的增值服务项目或内容。

2.成交供应商须保障采购人在使用成果资料的过程中不受到第三方关于侵犯专利权的指控。如果任何第三方提出侵权指控，成交供应商须与第三方交涉，并承担由此而产生的索赔、损失、损害、支出等一切费用（含律师费）。如采购人因此而遭致损失的，成交供应商应赔偿该损失。

服务期：自项目建设完成并投入使用之日起 1 年，合同期满后供应商服务质量良好且经双方协商无异议后可续签合同，续签合同一年一签，连续续签合同累计不超过 5 次。

3. 评审委员会劳动报酬支付表

山东省政府采购评审劳务报酬支付表

填表时间：2024 年 7 月 22 日

项目编号	SDGP370682000202402000056		项目名称	莱阳市互联网出口建设整合		分包数量	1 个
采购人	莱阳市人民政府办公室		采购代理机构	山东浚诚项目管理有限公司			
预算金额	¥788600.00/年	中标（成交）金额	包1：688500.00/年 包2：99300.00/年	评审地点	烟台市公共资源交易中心莱阳分中心		
评审时间	2024 年 7 月 22 日 14:30 — 16:10						

评审专家姓名及身份证号	开户银行及账号	评审劳务报酬（元）	误工补偿（元）	住宿费（元）	城市间交通费（元）	扣减（元）	支付金额	评审专家确认签字	备注
时永森 [redacted]	[redacted]	400	—	—	180	—	580	时永森	[redacted]
田世杜 [redacted]	[redacted]	400	—	—	180	—	580	田世杜	[redacted]
合计						总计		1160	

采购人代表：

采购代理机构项目负责人：

采购代理机构：

4.二轮报价

A包

二轮报价表

项目名称： 莱阳市互联网出口建设整合

项目编号： SDGP370682000202402000056_SDGP370682000202402000056-A

序号	名称	报价方式	单位	组成个数	上次报价	本次报价	小计
1	投标总价	总价	元	1	[illegible]	688500.00	688500.00

供应商承诺：

供应商盖章： 中国联合网络通信有限公司烟台市分公司

日期： 2024年07月22日

B包：

二轮报价表

项目名称： 莱阳市互联网出口建设整合

项目编号： SDGP370682000202402000056 SDGP370682000202402000056-B

序号	名称	报价方式	单位	组成个数	上次报价	本次报价	小计
1	投标总价	总价	元	1	[illegible]	99300.00	99300.00

供应商承诺：

项目服务期：自项目建设完成并投入使用之日起1年，合同期满后供应商服务质量良好且经双方协商无异议后可续签合同，续签合同一年一签，连续续签合同累计不超过5次。

供应商盖章： 中国移动通信集团山东有限公司烟台分公司

日期： 2024年07月22日

5. 成交供应商类似项目业绩清单

A 包：

类似项目业绩

1. 类似项目业绩原件清单

供应商名称：中国联合网络通信有限公司烟台市分公司

项目名称：莱阳市互联网出口建设整合

序号	项目名称	签订时间	备注
1	牟平区电子政务外网行政服务域链路租用与安全维护服务项目	2023 年 11 月 22 日	/
2	烟台经济技术开发区管理委员会办公室互联网出口整合项目	2024 年 6 月 18 日	/
	合计份数：2		

供应商授权代表签字或盖章：

供应商单位全称（盖章）：中国联合网络通信有限公司烟台市分公司

日期：2024 年 7 月 22 日

B 包：

类似项目业绩原件清单

供应商名称：中国移动通信集团山东有限公司烟台分公司

项目名称：莱阳市互联网出口建设整合

序号	项目名称	签订时间	备注
1	莱州市公安局前端感知网络线路租赁(五年)	2022.6.17	
2	龙口市电子政务外网公共服务域安全防护与保障服务项目合同	2022.9.1	
3	山东中医药高等专科学校互联网及平台运营服务项目	2023.6.30	
	合计份数	3	

供应商授权代表签字或盖章：

供应商单位全称(盖章)：中国移动通信集团山东有限公司烟台分公司

日期:2024 年 7 月 22 日

6. 未成交供应商未成交原因

A 包：

中国移动通信集团山东有限公司烟台分公司：综合评审得分较低

中国广电山东网络有限公司烟台市分公司：综合评审得分较低

B 包：

中国联合网络通信有限公司烟台市分公司：综合评审得分较低

中国电信股份有限公司烟台分公司：综合评审得分较低

中国广电山东网络有限公司烟台市分公司：综合评审得分较低

7、代理服务费收费标准及金额：

本项目的成交服务费参照《招标代理服务费收费管理暂行办法》（计价格【2002】1980号）及国发改办价格【2003】857号、发改价【2011】534号文规定收取。由各包成交供应商在领取中标通知书时支付给代理公司。

本项目成交服务费A包：20000元整，B包5000元整