报价唯一性

开标一览表

项目编号/包号：___常采公[2023]0004 号 ____

项目名称：__数据中心整合升级项目

序号	投标项目名称	投标报价	
		大写	小写
1	数据中心整合升级项目	贰佰肆拾万元整	2400000.00

注：1.此表中，每包的投标报价应和《投标分项报价表》中的总价相一致。
2.本表必须按包分别填写。

投标人名称（加盖公章）：__常州市盛景网络技术有限公司

日期：_2023_年_02__月_10__日

投标分项报价表

项目编号：常采公[2023]0004 号

序号	设备名称	品牌	规格型号	技术参数	数量	单位	投标价格（元）	
							单价	合价
1	路由器	H3C	SR6602-IE	指标项 技术要求（除特别说明外，以下为单台/套设备的配置要求） 体系架构 ★≥2 个业务扩展槽位，冗余交流电源（提供官网截图证明）； ▲一体化冗余风扇框，前后通风设计，提供设备冗余风扇框截图 ▲固定接口数≥20*10GE+12GE（提供官网截图证明） 性能要求 ★交换容量≥696Gbps，包转发率≥360Mpps，需提供官网截图证明 基本功能 支持 PPP、MP、HDLC、ETHERNET 等链路层协议 支持链路聚合（Link aggregation），支持动态聚合、手工聚合、跨板聚合 支持 IPv4 静态路由、RIPv1/v2、OSPFv2、BGP、IS-IS、路由策略 支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+ 广域网优化 ▲支持 WAN 优化手段（提供国家确定的认证机构出具的，处于有效期的测试报告证明） ▲支持并实配 Web cache 技术，是将用户通过 HTTP 协议访问过的指定地址服务器的 Web 页面内容，缓存在本地，在缓存文件的老化时间内用户访问相同内容时，直接从本地响应的一种缓存功能，从而减少设备到服务器的访问流量、降低传输成本、缓解目的端服务器压力，同时提高了用户访问网站的速度及降低响应时间，增强了用户体验。（提供国家确定的认证机构出具的，处于有效期的测试报告证明） ADVPN 功能 支持通过动态 VPN 技术，实现动态获取对端分支节点当前的公网地址，从而实现两个节点之间动态建立跨越 IP 核心网络的 ADVPN 隧道简化 VPN 网络部署复杂度和提高管理效率	2	台	187000.00	374000.00

				嵌入式自动化 ▲支持对系统软硬件的内部事件、状态进行监控，出现问题时收集实时信息并自动修复将实时信息发送到指定服务器（提供国家确定的认证机构出具的，处于有效期的测试报告证明） VPN 支持 MPLS L3VPN，MPLS L2VPN，SR,SRv6、SRv6-Policy、VXLAN 网管特性 支持 Netconf、SNMP、RMON、Netstream、NQA 可靠性 支持 VRRP、MPLS TE FRR、IP FRR（IS-IS/OSPF/LDP 等） 支持热补丁功能，可在线进行补丁升级 为提高设备硬件稳定性及可靠性，板卡、子卡支持热插拔功能 配置要求 ★配置双交流电源，提供不少于 32 个万兆光接口+16 个千兆光接口+12 个千兆电接口（提供承诺函加盖投标人公章） 资质 ▲提供工信部入网许可证复印件				
2	防火墙	H3C	M9000-AI-E4	指标项 技术要求（除特别说明外，以下为单台/套设备的配置要求） 架构 ▲采用非 X86 多核架构，设备采用控制、数据、业务相互解耦分离的全分布式架构，主控引擎、业务引擎、接口单元均采用硬件槽位分离的独立硬件模块，业务和接口扩容槽位≥4； ▲主控引擎需采用独立且可热插拔的硬件模块形态，占用专用的硬件槽位，数量≥2，支持 1:1 冗余备份，保障热插拔无丢包； ▲由于机房空间有限，投标设备高度需要严格控制，高度≤2U（提供官网截图证明）； ▲设备具备可插拔冗余电源模块，电源模块≥4，可插拔冗余风扇模块，风扇模块≥2，极端情况下支持单电源、单风扇模块运行，保障极端情况下设备的供电和散热稳定性 性能 ▲网络层吞吐量≥150Gbps，应用层吞吐量≥60Gbps； ▲并发连接数≥4000 万，每秒新建连接数（HTTP）≥100 万； ▲虚拟防火墙数量≥64，VRF 虚拟转发实例≥1024； 接口 ▲本次实配 40GE 光接口≥48 个（提供承诺函加盖投标人公章）； 存储扩展 ▲本次实配 480G SATA SSD≥2 块（提供承诺函加盖投标人公章）。 升级服务 ★提供 IPS 入侵防御+AV 防病毒功能模块以及对应 3 年特征库升级授权服务（提	2	台	412000.00	824000.00

				供承诺函加盖投标人公章）。 VPN 实现高性能 IPSec、L2TP、GRE VPN、SSL VPN 等功能。 ▲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。（提供功能截图） 攻击防护 实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC 和 IP 绑定功能，基于 MAC 的访问控制列表，802.1q VLAN 透传等功能。 NAT 功能 实现一对一、多对一、多对多等多种形式的 NAT，实现 DNS、FTP、H.323 等多种 NAT ALG 功能。 NAT 地址池支持动态探测和可用地址分配 URL 过滤 设备提供海量预分类的 URL 地址库，支持根据 URL 类别实现 URL 过滤； 设备支持管理者自定义新的 URL 地址和 URL 分类； ▲支持联动云端 URL 地址库进行全面实施核查（提供功能截图） 入侵防御 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（提供截图） 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。 支持超过 17000 种特征的攻击检测和防御 防病毒 可基于病毒特征进行检测，实现病毒库手动和自动升级，报文流处理模式，实现病毒日志和报表； 支持基于文件协议、邮件协议（SMTP/POP3/imap)、共享协议（NFS/SMB）的病毒功能（提供功能截图） 数据安全 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配。 流量控制 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。要求支持带宽通道独占以及共享管理模式,支持父子带宽策略。				

				安全接入 支持基于 MAC 和 IP 的接入认证，且最大用户数至少支持四千万。 加密流量检测 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。 IPv6 实现 IPV6 动态路由协议、IPV6 对象及策略、IPV6 状态防火墙、IPV6 攻击防范、IPV6 GRE/IPSEC VPN、IPV6 日志审计、IPV6 会话热备等功能。 支持 IPV6 下的访问控制、IPSec VPN、DDoS 防护等安全功能。 DDoS 防护 能够防范 DOS/DDOS 攻击： Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、SYN Flood、ICMP Flood、UDP Flood、HTTP Flood（cc）攻击、ARP 欺骗、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描的防范、端口扫描的防范、DNS Flood、ACK Flood、FIN Flood、分片 Flood、Tiny-Fragment。 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。 国密算法 支持国密 SM2/3/4 算法。 虚拟化能力 ▲所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、删除功能；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；提供国家确定的认证机构出具的，处于有效期的测试报告证明； HA 能力 支持 2 台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署。 ▲HA Track 方式支持 BFD/NQA/接口/路由多种类型，支持 Track 检测链路状态，来及时触发链路切换，保障业务连续性（提供功能截图） 设备管理 支持 SNMPv1、SNMPv2、SNMPv3、RMON 等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。 产品资质 ▲所投产品须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，提供证书复印件； ▲所投产品须具备中国信息安全认证中心颁发的国家信息安全产品认证证书（ISCCC），提供证书复印件；				

				▲所投产品须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，提供证书复印件；				
3	管理服务器	H3C	R4900 G5	指标项 技术要求（除特别说明外，以下为单台/套设备的配置要求） 外形 ▲≥2U 机架式服务器，含安装导轨，智能安全面板；(提供产品截图加盖投标人公章) 处理器 ★配置≥2 颗 Intel 至强 6342(2.8GHz/24 核/36MB/230W)或以上处理器（提供承诺函加盖投标人公章）； 内存 ★配置≥16*32GB 3200MHz DDR4 内存，最大支持 32 根 DDR4 内存，最高速率 3200MT/s（提供承诺函加盖投标人公章）。 硬盘 ★≥3 块 600GB 12G SAS 10K 2.5in HDD（提供承诺函加盖投标人公章）； 硬盘扩展 配置≥8 个 2.5 寸热插拔硬盘槽位，可扩展至≥37 个 2.5 寸热插拔硬盘槽位，同时可扩展 4 个 3.5 寸硬盘，且全部硬盘可在不打开主机箱盖的情况下热插拔维护。 IO 扩展 ▲最多提供≥15 个 PCIE4.0 速率插槽（其中包含 14 个 PCIe4.0 标准插槽和 1 个 OCP3.0 插槽）（提供官网截图证明）； 阵列卡 ★配置≥1 个 LSI 9460-8i 12Gb 2 端口 SAS RAID 卡(带 2GB 缓存,支持 8 个 SAS 口)，配置缓存数据保护（提供承诺函加盖投标人公章）； 网络 ★实配≥1 个 4 端口 1Gb Ethernet 电接口 OCP3.0 形态网卡，≥2 个双端口 10Gb Ethernet 光接口网卡(带多模模块) （提供承诺函加盖投标人公章）。 HBA ★实配≥2 个单端口 16Gb 光纤通道 HBA 卡(带 SFP+模块) （提供承诺函加盖投标人公章） GPU 扩展 ▲最大支持≥4 块双宽或 14 块单宽 GPU 卡（提供官网截图证明）； 电源 ★配置冗余热插拔白金电源，单个电源功率≥800W（提供承诺函加盖投标人公章）； 散热 配置≥6 个热插拔冗余风扇； 接口 可支持前部：1 个 Type-C; 2 个 USB3.0;1 个 VGA；后部：2xUSB3.0; 1x 串口；1xVGA；内置：2xUSB3.0 管理功能 配置独立管理端口，提供基于 Web 的远程管理控制、配备硬件监控、远程管理功能；支持 IPMI2.0 标准；提供 KVM 功能，实现远程开关机、重启、网络安装操作系统等操	2	台	98000.00	196000.00

				作； 支持外接 USB WIFI 模块，提供无线热点，支持使用手机或便携机直接登录服务器管理端口进行管理； 支持三维海洋传感温度监控功能，在主板等关键部件配置温度采集传感器，显示各组件温度传感器的温度读数，并可直接通过三维的温度图展示各部件温度传感器的分布图及数值； 告警功能 ▲支持多种方式对设备进行状态监控，支持 SNMP、SMTP、短信、微信、语音告警（提供官方技术白皮书证明）； 安全性 支持用户密码和国密算法动态令牌双因素认证方式登录服务器； 稳定性 ▲产品经过 9 级烈度地震抗震测试（提供国家确定的认证机构出具的测试报告证明）；				
4	48 口全光接入交换机	H3C	S6520X-54QC-EI	指标项 技术要求（除特别说明外，以下为单台/套设备的配置要求） 硬件架构 ▲万兆光接口数≥48，40G 光接口数≥2，扩展插槽数≥2（投标时提供官网截图） ▲模块化双电源，模块化双风扇，前/后通风，风道可调； 性能指标 ▲交换容量≥2.5Tbps，包转发率≥1080Mpps（提供官网截图证明）；； MAC 地址表≥128K，ARP 表 64K 路由协议 支持 IPv4 静态路由、RIP V1/V2、OSPF、BGP、ISIS；支持 IPv6 静态路由、RIPng、OSPFv3、BGP4+；支持 IPv4 和 IPv6 环境下的策略路由 VLAN 特性 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN； 堆叠 最大堆叠台数≥9 台，最大堆叠带宽≥320G； 支持通过标准以太端口进行堆叠（万兆或 40G 均支持） 组播协议 支持 IGMP v1/v2/v3，MLD v1/v2，支持 IGMP Snooping v1/v2/v3，MLD Snooping v1/v2，支持 PIM Snooping 可靠性 支持 VRRPv2/v3（虚拟路由冗余协议）；支持 RRPP（快速环网保护协议） VxLAN 支持 VxLAN 二、三层网关，支持 EVPN SDN/OPENFLOW 支持 OPENFLOW 1.3 标准，支持普通模式和 Openflow 模式切换 智能网管 ▲支持内置智能管理平台，可作为上端管理设备实现整网拓扑可视，实现在网络	2	台	32800.00	65600.00

				设备上对整网交换机的统一管理，无需再额外配置网管平台（提供官网截图证明）； 绿色节能 符合 IEEE 802.3az（EEE）节能标准，支持端口休眠，关闭没有应用的端口，节省能源，支持智能风扇调速 配置要求 ▲双电源、双风扇 产品资质 ▲具备工信部入网证，并提供证书复印件				
5	48 口万兆接入交换机	H3C	LS-5170-54S-EI	指标项 技术要求（除特别说明外，以下为单台/套设备的配置要求） 设备性能 ▲交换能力≥2.28Gbps，包转发速率≥174Mpps（提供官网截图证明）； 基本要求 ▲≥48 个千兆电口，≥6 个万兆光口（提供官网截图证明）；； 路由 支持 IPv4 静态路由、RIP V1/V2、OSPF，支持 IPv6 静态路由、RIPng，支持 IPv4 和 IPv6 环境下的策略路由； 可靠性 支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms； 虚拟化 支持多台交换机堆叠； VLAN 特性 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN； 链路聚合 支持最多 8 个端口聚合；支持最多 128 个聚合组（IRF2）；支持 LACP； SDN/OPENFLOW 支持 OPENFLOW 1.3 标准，支持普通模式和 Openflow 模式切换； 访问控制策略 支持基于第二层、第三层和第四层的 ACL；支持基于端口和 VLAN 的 ACL；支持出方向 ACL，以便于灵活实现数据包过滤； CPU 防护 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护交换机在各种环境下稳定工作； 智能管理 ▲支持智能管理平台，可配合上端管理设备实现整网拓扑可视（提供官网截图证明）； 防雷能力 支持 10KV 业务端口防雷能力； 绿色节能 符合 IEEE 802.3az（EEE）节能标准，支持端口休眠，关闭没有应用的端口，节省能源； 产品资质 ▲具备工信部入网证，并提供证书复印件；	12	台	7700.00	92400.00
6	云管理	华为	USG6500E	指标项 技术规格要求	1	台	141000.00	141000.00

	防火墙			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； 硬件架构 当风扇模块出现故障时，可以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； 严格前后风道； 策略管控 能够基于 IP、IPv6、MAC 地址、时间进行访问控制策略控制;支持自定义安全策略，安全策略组功能；支持策略冗余/命中分析； 路由功能 支持静态路由、策略路由、RIP、OSPF、BGP、ISIS 等路由协议 NAT 支持 NAT66，NAT64，6RD 隧道； 流量控制 支持每 IP， 每用户的最大连接数限制，防护服务器； 入侵防御及病毒防护 系统预定义 IPS 签名数量≥8000，支持用户自定义签名规则，支持正则表达式，病毒库数量≥500w； 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； 网安联动 ▲支持防火墙与 IDS 设备、网络安全智能分析系统联动，做态势感知，全网威胁展示，并能针对威胁生成阻断策略，提供功能截图； 智能威胁防御 支持防火墙与云沙箱，本地沙箱混合联动，敏感文件在本地沙箱检测，普通文件上传到云沙箱；提供功能截图 ▲支持流探针功能，对网络中的流量进行采集；提供国家确定的认证机构出具的测报报告证明 配置要求 ▲实配：千兆 Combo 接口≥8，万兆光口≥2，千兆 WAN 口≥2，含 SSL VPN 100 用户数，一块 64G M.2 SSD 存储卡，交流电源，配置三年威胁防护升级服务，三年云部署模式授权，三年边界防护服务；				
7	防病毒网关	亚信	AIS Edge EE (EE) V7.0 E3000	指标项 指标要求 硬件要求 ▲内存≥16G，设备自带千兆电口≥2 个，万兆光口≥4 个，四个扩展插槽，支持 750W 电源*2，1 个 iDRAC 接口，具备 iDRAC 远程访问管理能力； 性能要求 网络层吞吐量≥15 Gbps，防病毒吞吐率≥4Gbps	1	台	322000.00	322000.00

				防病毒能力 产品支持超过100种协议，如:HTTP/SMTP/POP3/FTP/SMB/TFTP/TCP/UDP/NFS/SNMP/ICMP/RTMP/DNS/IRC等 为了提升病毒文件的检测能力，产品可与APT增强侦测模块联动，获取APT增强侦测模块侦测到的C&C黑名单，并阻止C&C违规外联，有拦截弹框提示且提供事件详情 ▲能够支持win7、win10的SMB文件共享协议的病毒检测查杀（要求提供截图并加盖公章） 产品支持提交可疑文件、URL、IP及域对象至APT增强定制化沙箱模块做联动分析，并根据分析结果做进一步处理 产品支持双防病毒引擎，并可按需切换 支持对最多20层的压缩文件进行解压查杀 支持反向代理部署模式，支持该模式下对HTTP/HTTPS流量解析检测，并支持阻断或监控模式 （要求提供截图并加盖公章） ▲产品支持客户可自定义病毒文件扫描的大小，最大可支持2G（要求提供截图并加盖公章） 入侵检测及虚拟补丁 产品支持服务器及终端虚拟补丁和主动式主机入侵防御系统，可在漏洞攻击主机之前予以侦测和拦截 产品需支持用户自定义IPS规则，支持设置严重等级、规则种类、源/目的IP地址、源/目的端口、协议类型（至少包含HTTP、TCP、UDP协议）等 部署模式 产品部署方式支持桥接模式、路由模式、监控模式（旁路模式） 日志及报告 产品提供基于策略（源和用户/目标/通讯类型/时段）的流量日志记录/查询/打印/导出 产品可按照时间，协议，威胁类型等查询条件查询日志 产品支持Syslog协议，可以实时传输日志到Syslog 服务器 产品提供恶意软件/入侵防御/Web信誉服务违例事件安全报告，前N个用户违例报告，以及按应用程序/URL类别/带宽使用等前N个通信报告 升级方式 产品支持自动/手动在线升级，可配置自动升级周期				

				安全可靠性 产品提供硬件 BYPASS 功能，在断电时能自动实现直通功能 ，恢复通讯时间不能超过 10 秒 产品支持最新版本检测和提示功能，提升设备的可维护性 产品资质 ▲产品必须具备防病毒网关类的销售许可证，并且在计算信息系统安全专用产销售许可服务平台上的防病毒类中的网关防病毒类别内可查询 ▲产品具备高级威胁网络防护系统的 IPV6 Ready Logo 金牌认证（提供证明文件复印件）。				
8	僵木蠕毒网关防护平台	奇安信	QAXTIP	指标项 具体要求 硬件要求 ▲硬件规格：机架式，CPU 不低于 2.1GHZ；不低于 12 核/24 线程，内存不低于 32G 3200MHZ，3 块不低于 1.2T SAS 10k 2.5 热插拔硬盘作为数据盘；具备至少 2 个千兆电口，2 个万兆光口 解析能力 ▲要求具备运营商级解析能力，解析稳定性更高，延时更低，需提供针对全国的“互联网域名解析服务业务”《中华人民共和国增值电信业务经营许可证》提供证书并加盖公章 ▲解析稳定性高，累计域名解析量 120 亿+，拦截恶意域名 26W+。（提供产品截图，并加盖原厂公章） 威胁情报能力 ▲威胁情报库 ioc 数量 1.4 亿+。（要求提供截图并加盖公章） ▲安全 DNS 威胁情报服务器不低于 200W+活跃情报，每小时更新。（提供产品截图，并加盖原厂公章） 安全 DNS 威胁分析能力基于威胁情报中心商业威胁情报，能够对 APT 攻击、勒索软件、窃密木马、远控木马、僵尸网络等几十种网络威胁请求进行有效检测和拦截。 域名监控 ▲支持客户自定义域名监控任务，实时统计监控域名访问情况与告警情况，通过邮件策略配置，及时将告警信息传递给客户，方便客户快速定位问题并处理。 监测防护模块 ▲能够监测并阻断单位内部上网行为，如 1、黑市工具 2、僵尸网络 3、窃密木马 4、网络蠕虫 5、其他事件（黄赌毒等） 6、远控木马 7、KNOWN APT 8、挖矿病毒 9、恶意下载 10、感染性病毒 11、勒索病毒 12、流氓推广 展示分析模块 能够展示近 24 小时解析数据统计展示近 24 小时 DNS 解析总量、 威胁解	1	台	296000.00	296000.00

				析数量 、 健康资产 I P 数、受威胁资产 IP 数 。方便用户直观了解当前 DNS 解析 以及资产 I P 健康 情况。 运营分析模块 运营分析模块包含域名解析分析 日志 和告警事件分析 日志 两部分内容。域名解析分析页主要展示解析趋势以及 部分解析 事件概览 。告警 事件分析 主要展示威胁解析趋势以及威胁分类概览； 部署模块 机构管理、出口 I P 配置。机构管理功能，用户可以 根据实际场 景定义机构分类，进行资产 I P 归属设置 。 出口 I P 配置功能，支持用户配置出口 I P； 数据可视化 支持查看域名解析/拦截趋势，实时全局掌控解析态势。 支持以域名解析维度，查看自定义时间内域名解析日志。 支持以告警事件维度，查看自定义时间内的事件分析日志。 支持查看请求类型分布、威胁类型统计、资产 IP 解析域名信息。 资产管理-支持告警事件邮件通知，方便客户快速定位问题并处理。 支持自定义监控资产 IP 任务，实时监控资产 IP 解析域名情况并对威胁进行告警，方便及时了解内部资产威胁情况。 日志审计 支持记录用户后台操作行为，便于查看历史操作记录。 质保 ▲要求提供原厂实施服务，投标时必须提供原厂服务承诺函原件				
9	应用交付网关	深信服	AD-1000-B1300	指标项 技术规格 硬件参数 ▲4 层吞吐量≥3Gbps，四层并发连接数≥8000000，4 层新建连接数 CPS≥100000，7 层新建连接数 RPS≥150000，内存大小≥8G，硬盘容量≥128G minisata SSD，接口≥6 千兆电口+2 千兆光口 SFP。（提供多线路授权、售后服务承诺书、三年质保服务，并加盖原厂公章） 功能参数 ▲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。（提供设备操作界面截图证明材料，并加盖厂商公章） ▲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、加权最小流量、按主机加权最小流量、加权源 IP 哈希、带宽比例、哈希、	1	台	89000.00	89000.00

				首个可用、优先级等算法。（提供设备操作界面截图证明材料，并加盖厂商公章） 支持通过某种编程语言（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。（提供设备操作界面截图证明材料，并加盖厂商公章） ▲支持静态 IP 和 PPPOE 两种线路接入方式。（提供设备操作界面截图证明材料，并加盖厂商公章） ▲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。（提供设备操作界面截图证明材料，并加盖厂商公章） ▲支持 cookie 加密，提升 cookie 安全性。（提供设备操作界面截图证明材料，并加盖厂商公章） 支持常见的主动式健康检查功能，提供基于 SNMP、ICMP、TCP/UDP、FTP、HTTP、DNS、RADIUS、ORACLE/MSSQL/MYSQL 数据库等多种类型的探测判断机制，支持对 HTTPS 服务进行内容健康检查。 ▲链路健康检查与服务器健康检查联动，入站负载跟服务器负载结合的时候，如果后端服务器全挂，则入站负载时也认为该虚拟 IP（此时要求入站负载的虚拟 IP 与虚拟服务发布的 IP 组相同）也离线，从而达到联动效果。（提供设备操作界面截图证明材料，并加盖厂商公章） ▲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。（提供设备操作界面截图证明材料，并加盖厂商公章） ▲对于超过服务器的连接数上限或者请求数上限的新建连接缓存起来放入队列中，后续分批逐步发送给服务器，而不是直接丢弃数据包。（提供设备操作界面截图证明材料，并加盖厂商公章）				

				▲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。（提供设备操作界面截图证明材料，并加盖厂商公章） ▲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。（提供设备操作界面截图证明材料，并加盖厂商公章） IPv6 支持双栈模式，支持 NAT46、NAT64、NAT66、FTP ALG、DNS64 等协议转换。 ▲免费开通 HTTP 压缩、HTTP 缓存、TCP 连接复用、SSL 卸载等功能，无需额外购买相应授权。 支持双机热备部署方式，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换。 内置智能告警系统，支持 E-mail、SNMP Trap 两种告警方式，管理员可基于业务安全所关注方面来选择告警触发事件与对应的告警方式，当业务网络环境中发生问题时（如服务器宕机、网络攻击、链路中断等故障场景），即会自动向管理员发送告警信息。（提供设备操作界面截图证明材料，并加盖厂商公章） 产品资质 ▲所投产品具备国家工业和信息化部颁发的《电信设备进网许可证》，提供证明材料且加盖厂商公章。 ▲所投产品具备《IPv6 Ready Phase-2 金色认证证书》，提供证明材料且加盖厂商公章。				
合　　计								2400000.00

投标人名称（公章）：常州市盛景网络技术有限公司

法定代表人或代理人（签字或盖章）：