

公开招标山东石油化工学院 2024 年数据中心设备及教学设备升级采购项目(第二次) 货物类

分项报价明细表

序号	仪器设备名称	品牌型号	主要技术标准与参数	单位	数量	单价 (元)	合计（元）	备注
1	出口防火墙	品牌：奇安信 型号：网神 SecGate 3600第二代 防火墙 NSG (万兆) /V3.6.6.0	▲1、产品完全适配国产化应用场景，采用国产飞腾 CPU，国产网神多核多平台并行安全操作系统；标准 2U 机架式设备，冗余电源，硬盘4T，千兆电口4 个，万兆 SFP+光口（支持硬件 bypass）8 个，万兆多模光模块8 个，空余扩展板卡插槽1 个，网络层吞吐量40G，并发连接1200 万，新建连接数25 万/秒，硬件维保服务6年，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6 年。 2、产品支持路由、透明、交换、旁路以及混合模式接入，能够适应复杂的应用环境； 3、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，动态路由支持 RIP v1/v2/ng， OSPFv2/v3， BGP4/4+协议；	台	1	282000	282000	符合具备招标文件要求的质量标准和检测报告等。

		<p>4、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；</p> <p>5、支持配置 IPv6 地址，使用 IPv6 地址管理设备；</p> <p>6、支持 NAT64、NAT66、NAT-PT 等多种 IPv4/IPv6 过渡技术；</p> <p>▲7、支持虚拟防火墙，支持虚拟防火墙逻辑接口，在不占用物理网口的情况下实现虚拟系统之间的相互连接、访问；（提供产品功能截图）</p> <p>8、支持基于源安全域、目的安全域、目的地址、目的地区、服务、应用等多种方式进行访问控制；</p> <p>9、支持应用识别，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类；</p> <p>▲10、支持漏洞防护、间谍软件防护功能，支持自定义 TCP、UDP、HTTP 协议的漏洞特征和间谍软件特征，漏洞特征间、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，支持自定义漏洞、间谍软件的源、目的端口</p>					
--	--	---	--	--	--	--	--

			<p>范围；同时可标识自定义漏洞的 CVE 编号或CNNVD 编号；（提供产品功能截图）</p> <p>11、支持病毒查杀；本地病毒库规模可达3000 万，支持对压缩文件进行解压查杀；</p> <p>12、支持入侵防御特征库、威胁情报库、应用识别库等数据库的实时更新或手动更新；</p> <p>▲13、支持对常用协议的文件传输行为进行上传、下载、双向的文件类型过滤；（提供产品功能截图）</p> <p>▲14、支持作与本项目中的网络威胁感知分析系统联动，上报网络活动产生的数据至网络威胁感知分析系统；并接收来自网络威胁感知分析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；（提供产品功能截图）</p> <p>▲15、支持一体化安全策略，在单条策略中配置病毒防护、入侵防御、文件过滤、文件内容过滤、网址过滤、终端过滤等；支持在虚拟防火墙内独立配置并对产生的日志进行独立审计。（提供产品功能截图）</p>					
2	网络威	品牌：奇安	▲1、标准 2U 机架式设备，冗余电源，千兆电口4 个，CPU 数	台	1	320000	320000	符合具

	威胁感知分析系统	信 型号：奇安信网神威胁监测与分析系统 TSS10000/V4.0	量2 颗，单颗 CPU 核心数12 个，内存256G，SSD 硬盘960G，SATA 硬盘48T，日志分析能力17000 eps，产品维保服务6年，威胁情报更新服务6年，支持横向扩展至多台设备集群； 2、支持自动从流量中识别资产信息，包括但不限于：IP、端口、服务、操作系统、MAC 等，支持对资产打标签，并根据标签过滤资产列表； 3、支持对全部数据来源的分享展示与汇总展示，支持告警页面自定义配置自动刷新时间； 4、支持展示资产及资产分组之间互访信息，信息包括但不限于：互访协议、目的端口、互访次数； ▲5、支持从威胁情报、应用安全、系统安全和设备安全的业务场景维度对告警进行攻击分析；（提供产品功能截图） 6、支持基于威胁情报的威胁检测，检测类型包括但不限于：APT 事件、僵尸网络、勒索软件、黑市工具、远控木马、窃密木马、网络蠕虫、流氓推广、恶意下载、感染型病毒、挖矿病毒等； 7、支持可疑 DNS 解析：能够检测发现 DGA 域名与 DNS 隧道					备招标文件要求的质量标准和检测报告等。
--	----------	---	---	--	--	--	--	---------------------

		<p>域名，支持根据时间范围、请求次数、DNS 域名总长度自定义 DNS 隧道检测规则；</p> <p>8、支持异常登录行为检测，检测内容包括但不限于：源 IP、账号、登录资产 IP、使用协议、登录结果等信息，且能进行异常时间配置，支持 ssh、telnet、ftp、smb 等常见协议特权账号登录行为分析，且能自定义特权账号；</p> <p>9、支持对 http、pop3、smtp、Telnet、ftp、imap 等各种协议进行弱口令检查，且能够自定义弱口令字典；</p> <p>▲10、支持 WEB 服务可疑爬虫或扫描分析，能自定义 web 访问频率，且能设置源 IP 白名单；（提供产品功能截图）</p> <p>▲11、支持外部访问分析，能展示源 IP、资产 IP、端口、协议、时间等详细信息，且能自定义源 IP 白名单；（提供产品功能截图）</p> <p>12、支持大屏展示威胁感知态势，包括但不限于：攻击态势、攻击概要、告警类型、告警变化趋势、攻击/受害 TOP 排行、告警等；</p> <p>13、可自定义选择报表生成的数据范围、报表格式、报表模版</p>					
--	--	---	--	--	--	--	--

			<p>；</p> <p>▲14、支持与本项目出口防火墙进行联动，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）；（提供产品功能截图）</p> <p>▲15、支持响应处置策略定义，可根据 workflow 进行处置动作定义，且能根据告警类型、攻击结果、威胁类别进行联动策略定义；（提供产品功能截图）</p> <p>16、支持邮件告警功能，可以定时向指定邮箱发送 APT 事件、攻击利用、恶意软件、拒绝服务等类型的告警信息。</p>					
3	全流量威胁检测系统	品牌：奇安信 型号：奇安信网神威胁监测与分析系统 TSS10000/V4.0	<p>▲1、标准 2U 机架式设备，冗余电源，千兆电口4 个，万兆光口2个，CPU 数量2 颗，单颗 CPU核心数12 个，内存64G，硬盘4T，网络吞吐量8Gbps，并发会话数700w，新建会话数8w，产品维保服务6年，规则库升级服务6年，威胁情报更新服务6年；</p> <p>2、通过流量镜像的方式旁路部署在网络中，可同时接入多个镜像口，每个镜像口相互独立，不影响原有网络架构和处理性能；</p>	台	2	147000	294000	符合具备招标文件要求的质量标准和检测报告等。

		<p>▲3、支持流量过滤策略，通过 IP、IP 段、端口、协议等进行流量过滤；（提供产品功能截图）</p> <p>4、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，包括但不限于：http、dns、dhcp、smtp、pop3、imap、webmail、db2、oracle、mysql、mssql-db、sybase、smb、ftp、snmp、telnet、nfs、icmp、ssl、ssh、redis、ldap、radius、kerberos、ntp、ipv6 等；</p> <p>▲5、支持对 HTTP、FTPD_ATA、SMB、SMTP、POP3、WEBMAIL、IMAP、TFTP、QQ、NFS 等类型协议的流量进行文件还原；（提供产品功能截图）</p> <p>6、支持 TCP/UDP 会话记录、异常流量会话记录、SSL 加密协商、登录行为、域名解析、文件传输、FTP 控制通道、LDAP 行为、web 访问、邮件行为、数据库操作、telnet 命令、旁路阻断、MQ流量、Radius 行为、Kerberos 行为、ICMP 流量、syn 流量等行为描述；</p> <p>7、支持多种攻击检测，能更全面的从流量中发现威胁，包括但不限于：SQL 注入、XSS、信息泄露、间谍软件、协议异常、</p>					
--	--	--	--	--	--	--	--

		<p>网络欺骗、黑市工具、代码执行、挖矿等；</p> <p>▲8、支持旁路 HTTPS 解密、威胁检测；（提供产品功能截图）</p> <p>9、支持威胁告警的相关 pcap 数据留存，支持本地下载及外发；</p> <p>10、系统默认内置检测规则，支持检测 WEB 攻击、Webshell 攻击、网络攻击、后门程序、僵木蠕检测、C2 外连、恶意通信、SMB 远程溢出攻击、文件上传、弱口令、暴力猜解、挖矿、黑客工具、明文密码传输、漏洞利用、ARP 欺骗、恶意扫描等风险；</p> <p>11、支持 HTTP、SMB、FTP、IMAP、POP3、SMTP、MSSql、MySql、Oracle、SIP、Redis、Ldap、Nntp、SSH、Telnet、Sybase、VNC、RADMIN、RDP 等协议暴力破解检测，能识别出尝试登录次数、账户信息、爆破成功与否的攻击状态；</p> <p>12、支持自定义漏洞规则支持根据攻击载荷自定义漏洞检测规则，可自定义载荷检测位置、检测字段、匹配方式（文本匹配/正则匹配）、匹配载荷内容；</p>					
--	--	--	--	--	--	--	--

			13、支持将威胁告警、网络日志等日志传输给本项目网络威胁感知分析系统； ▲14、支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升未知威胁检测能力；（提供产品功能截图） 15、支持一键对系统进行深度配置和排错，支持一键检测故障、资源占用、进程检测、设备连接状态、设备信息收集等功能。 。					
其他费用	0							
合计（元）	小写：896000							
	大写：捌拾玖万陆仟元整							

投标人（公章）：

法定代表人或授权人签字（或盖章）：