

报价唯一性

投标分项报价表（分包号：JSZC-320481-JZCG-G2024-0055）

序号	1 分项服务名称	2 分项单位	3 数量	4 分项单价	5 分项总价	6
1	<p>下一代防火墙（学校端）</p> <p>1、▲网络层吞吐量≥2G，应用层吞吐量≥800M，最大并发连接数≥100万，每秒新建连接数≥3万，内存≥4G，硬盘≥64GB，设备至少配备6个千兆电口和2个千兆光口，提供3年原厂硬件质保，软件升级及3年入侵防御规则库升级服务和3年云端威胁情报同步服务，（需提供厂商售后服务承诺函且加盖投标人公章）</p> <p>2、支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式</p> <p>3、支持 IPv4/IPv6 双栈工作模式，以适应 IPv6 发展趋势</p> <p>4、▲支持 IPSec VPN 智能选路功能，根据线路质量和应用实现自动链路切换（需提供产品功能截图证明并提供权威机构（国家认证认可监督管理委员会批准设立并授权的国家认可机构）认证证书或检测报告复印件并加盖投标人公章）</p> <p>5、支持基于网络区域、网络对象、MAC 地址、服务、应用、域名等维度进行访问控制策略设置</p> <p>6、支持僵尸主机检测功能，产品预定义特征库超过 128 万种，可识别主机的异常外联行为</p> <p>7、支持预定义漏洞特征数量超过 15000 种，支持在产品漏洞特征库中以漏洞名称、漏洞 ID、漏洞 CVE 标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义 IPS 规则</p> <p>8、▲支持云威胁情报网关技术，通过全球超过 30 个 pop 节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。（需提供产品功能截图证明并提供 POP 节点在线查询链接和提供权威机构（国家认证认可监督管理委员会批准设立并授权的国家认可机构）认证证书或检测报告复印件并加盖投标人公章）</p> <p>9、▲支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报全网设备下发。（需提供产品功能截图证明并提供权威机构（国家认证认可监督管理委员会批准设立并授权的国家认可机构）认证证书或检测报告复印件并加盖投标人公章）</p> <p>10、支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之</p>		30	20000	600000	



		<p>间的访问关系、访问细节协议端口等信息</p> <p>11、▲支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理（需提供产品功能截图证明且加盖投标人公章）</p> <p>12、▲所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务(一级)资质，需提供相关证明材料且加盖投标人公章</p> <p>13、▲要求所投产品的生产厂家同时为国家信息安全漏洞共享平台(CNVD)技术组成员和用户组成员，需提供相关证明材料且加盖投标人公章</p>				
2	下一代防火墙（中心端）	<p>1、▲网络层吞吐量≥20G，应用层吞吐量≥9G，最大并发连接数≥200万，每秒新建连接数≥9万，内存≥8G，硬盘≥128GB，设备至少配备8个千兆电口和2个万兆光口，提供3年原厂硬件质保，软件升级及3年入侵防御规则库升级服务和3年云端威胁情报同步服务，（需提供厂商售后服务承诺函且加盖投标人公章）</p> <p>2、支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式</p> <p>3、▲当主机故障时，支持双机切换时不丢包，可实现双机部署下升级不断网（需提供产品功能截图证明并提供权威机构（国家认证认可监督管理委员会批准设立并授权的国家认可机构）认证证书或检测报告复印件并加盖投标人公章）</p> <p>4、支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于3种的调度算法，至少包括带宽比例、加权流量、线路优先等（需提供产品功能截图证明且加盖投标人公章）</p> <p>5、支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势（需提供产品功能截图证明且加盖投标人公章）</p> <p>6、▲支持IPSec VPN智能选路功能，根据线路质量和应用实现自动链路切换（需提供产品功能截图证明并提供权威机构（国家认证认可监督管理委员会批准设立并授权的国家认可机构）认证证书或检测报告复印件并加盖投标人公章）</p> <p>7、支持基于网络区域、网络对象、MAC地址、服务、应用、域名等维度进行访问控制策略设置</p> <p>8、支持僵尸主机检测功能，产品预定义特征库超过128万种，可识别主机的异常外联行为（需提供产品功能截图证明且加盖投标人公章）</p> <p>9、支持预定义漏洞特征数量超过15000种，支持在产品漏洞特征库中以漏洞名称、漏洞ID、漏洞CVE标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义IPS规则（需提供产品功能截图证</p>			68000	68000



		<p>明且加盖投标人公章)</p> <p>10、▲支持云威胁情报网关技术，通过全球超过 30+pop 节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。（需提供产品功能截图证明并提供 POP 节点在线查询链接和提供权威机构（国家认证认可监督管理委员会批准设立并授权的国家认可机构）认证证书或检测报告复印件并加盖投标人公章）</p> <p>11、▲支持云端未知威胁主动探测技术，实现 5min 内未知威胁情报全网设备下发。（需提供产品功能截图证明并提供权威机构（国家认证认可监督管理委员会批准设立并授权的国家认可机构）认证证书或检测报告复印件并加盖投标人公章）</p> <p>12、支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息</p> <p>13、支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理（需提供产品功能截图证明且加盖投标人公章）</p> <p>14、所投产品具备计算机信息系统安全专用产品销售许可证或具备中国国家信息安全产品认证证书，提供相关证明材料且加盖投标人公章</p> <p>15、所投产品厂商参与制定《信息安全技术第二代防火墙安全技术要求》，需提供相关证明材料且加盖投标人公章</p> <p>16、▲所投产品连续 8 年入围 Gartner 企业级防火墙魔力象限，需提供相关证明材料且加盖投标人公章</p> <p>17、▲所投产品具备 Cyber Ratings AAA 认证，需提供相关证明材料且加盖投标人公章</p> <p>18、▲所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务(一级)资质，需提供相关证明材料且加盖投标人公章</p> <p>19、▲要求所投产品的生产厂家同时为国家信息安全漏洞共享平台(CNVD)技术组成员和用户组成员，需提供相关证明材料且加盖投标人公章</p>				
3	网信安一体化服务	<p>针对配置新一代防火墙的学校，开展配套安全服务，包括：</p> <p>1、设备安装调试；</p> <p>2、资产梳理（每年 2 次）：协助甲方完成资产梳理工作，服务完成后提交《资产梳理表》；</p> <p>3、制度建设（每年 1 次）：编写网络安全制度，包括制定安全策略、建立安全规范、实施安全技术措施、加</p>	年	2	60000	120000



强安全培训和监督检查等多个方面，编写完成后提交《安全管理制度》；

4、漏扫服务（每年4次）：对客户网络进行定期扫描、发现主机操作系统、网络设备、数据库、安全设备等存在的安全漏洞，弱口令，开放的端口等。并提出安全加固建议。

5、渗透测试（每年1次）：模拟黑客可能使用的攻击和漏洞发现技术，对目标信息系统进行渗透测试安全验证，发现逻辑性更强、更深层次的弱点，让管理者能够直观了解自己网络和系统安全状况。关注：挂马威胁检测，病毒威胁检测，后门威胁检测，通信威胁检测，注入跨站检测；

6、安全巡查（每年4次）：对本次安全设备进行定期巡检，巡检内容包括设备状态、资源占用率、日志、告警、安全策略等，完成后出具巡检报告，服务完成后提交《网络安全巡检报告》；

7、安全加固（每年4次）：协助制定安全防护建设方案：协助客户、优化防护方案；制定安全部署方案；安全设备运维策略添加与优化：添加防护策略，日常防护优化，保障业务系统安全；服务器安全配置整改加固：协助对系统漏洞、配置不安全项等脆弱点进行安全整改；

8、攻防演练（每年1次）：根据客户需求，进行网络攻防方案，包括但不限于网页篡改、病毒事件、口令暴力破解等场景，由有经验的高级安全服务专家配合客户进行现场防御的操作演练，目的在于检查应急处置的可行性，同时提升客户安全工作人员的事件应急处理能力。

投标总报价（人民币：元）

788000

备注：1. 投标报价采用总承包方式，“投标总报价”应包括采购人需求的服务（包含与服务相关的货物）价格、质量保证费用、培训费用等...项目在指定地点、环境交付、安装、调试、验收所需费用和所有相关税金费用及为完成整个项目所产生的其它所有费用，招标文件另有规定的除外。

2. “投标分项报价表”中“投标总报价”数额应当与“开标一览表”中“投标总报价”数额一致。

