技术要求

序号	名称	数量	参数配置
1	防火墙	1 台	标准 1U 机架式设备，国产化处理器，采用国产化操作系统，内存≥16GB，固态硬盘≥480G，接口：≥6 个千兆电口，≥4 个千兆 SFP 光口，冗余电源，防火墙网络层吞吐≥20G，TCP 并发连接≥800 万。SD-WAN 智能软件（含虚拟控制器软件）；入侵防御特征库 3 年升级服务许可；病毒过滤 3 年升级服务许可；威胁情报 3 年升级服务许可；Web 应用防护特征库 3 年升级服务许可；具有 SSL 功能模块并包含 50 个 SSLVPN 客户端许可；提供三年原厂维保，包括：系统、补丁免费升级服务。
			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；
			支持域名控制，支持对多级域名进行控制，域名对象支持通配符；
			支持配置文件、系统服务、路由、链路聚合、安全策略、NAT 策略、带宽管理、认证策略、IPV6 功能、URL 过滤、病毒过滤、内容过滤、审计、报表、防代理等安全功能虚拟化；
			支持防暴力破解、密码复杂度、密码有效性设置，如认证失败次数及锁定时间、密码格式、密码长度、密码找回、首次登陆修改密码、密码定期修改、密码有效时间等设置；
			支持链路和通道嵌套的流量控制功能，可基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级和针对 IP、设置白名单；
			支持在 WEB 界面进行网络抓包，支持设置接口、IP、协议、端口、包数等过滤条件，抓包文件支持导出；
2	堡垒机	2 台	标准 2U 机架式设备，国产化处理器，采用国产化操作系统，内存≥16GB，硬盘≥4T，接口：≥8 个千兆电口+4 个千兆光口+2 个万兆光口，≥2 个接口扩展，冗余电源;最大字符并发≥ 500 ；最大图形并发≥300，默认含 200 授权许可，最大扩展到 1200 授权，提供三年原厂维保，包括：系统、补丁免费升级服务。
			可根据扫描地址（段）、扫描端口、归口部门等信息进行配置扫描，也可实时终止扫描任务，扫描后资产设备可进行一键提交归档，方便用户统一管理；
			资源管理：支持非应用发布模式管理 Redis/MySQL/SQLServer 数据库，并记录运维过程中的 SQL 语句，支持 2 种使用方式： （1）通过浏览器直接启动本地数据库客户端工具访问数据库； （2）通过访问串模式使用本地数据库客户端工具访问数据库；
			支持资产扫描功能，可根据扫描地址（段）、扫描端口、归口部门等信息进行配置扫描，也可实时终止扫描任务，扫描后资产设备可进行一键提交归档，方便用户统一管理；
			支持任意浏览器无插件安装下播放审计到的字符运维、图形运维审计记录；

3	日志审计	2 台	标准 1U 机架式设备，国产化处理器， 采用国产化操作系统，内存≥16GB，硬盘≥4TB，接口：≥8 个千兆电口+2 个万兆光口+2 个扩展槽位，冗余电源，配置日志源≥100 个，支持扩展到 300 个以上，日志处理性能≥7000EPS，提供三年原厂维保，包括：系统、补丁免费升级服务。
			支持对镜像流量的审计，审计内容包括 mysql、pgsql、mongodb、redis、人大金仓、http 等数据库和流量审计；
			告警方式包括短信、邮件、钉钉等；
			支持系统基本配置，包括修改主机名称、网络接口 IP、路由等，内置抓包、PING、端口测试等工具；
			内置网站攻击、主机异常、账号异常、暴力破解、漏洞利用、权限异常等至少 10 种安全分析场景，内置关联规则至少 400 条；
4	网络管理准入系统	2 台	标准 1U 机架式设备，国产化处理器， 采用国产化操作系统，最大并发数 300，最大吞吐量 300Mbps，网络接口 6 个千兆电口 2 个千兆光口，扩展接口数量 2 扩，硬盘存储 1T 监控级硬盘，支持 Bypass，单电源，提供≥500 点授权。提供三年原厂维保，包括：系统、补丁免费升级服务。
			标准 2U 架式设备，国产化处理器， 采用国产化操作系统，最大并发数 1000，最大吞吐量 1Gbps，网络接口 8 个千兆电口，扩展接口数量 2 扩，硬盘存储 128G SSD 硬盘 1T 监控级硬盘，支持 Bypass，冗余双电源。提供≥1500 点授权。提供三年原厂维保，包括：系统、补丁免费升级服务。
			准入模式：支持策略路由、旁路镜像、透明网桥、端口控制、VLAN 控制、火线控制、ARP 准入、DHCP 准入、802.1x 等多种准入模式，并且单台设备支持同时启用四路准入模式；支持准入模式动态切换，并且模式切换无需重启准入网关设备；支持利用企业现有 DHCP 服务器进行 DHCP 准入，在 DHCP 服务器为用户终端分配 IP 的过程中，不需要考虑 DHCP 服务器是否和用户终端是否在同一网段，简化系统的处理逻辑，降低系统部署的成本，使后期系统维护更简单，请提供第三方证明材料；支持 VLAN 隔离准入模式下交换机上不配置隔离 VLAN 地址的方式实现阻断和引导，支持 DHCP 环境下控制；支持通过非 802.1X 准入给交换机下发 ACL 方式实现终端的准入控制，通过旁路部署方式不需额外部署客户端；同时支持有客户端和无客户端准入模式。
			端口准入：支持端口控制方式，支持设置不同时间段的开启/关闭端口，支持自定义模式触发关端口，自定义添加不少于十种；支持端口控制方式下控制的终端信息展示，支持 HUB 下违规终端阻断或告警；支持 VLAN 控制方式，支持通过 SNMP 进行 VLAN 切换控制。
			IPv6 环境准入：支持纯 IPv6 或 IPv4 和 IPv6 混合环境下的准入；支持引导页面内容定制化，包括：LOGO，文字，背景图片，标题等；支持手机、平板电脑、WIN 终端联网自动弹出重定向页面进行准入入网引导；支持访问任意域名（包括不存在的）进行准入引导。
			终端准入：支持 XP，Win7，Win8，Win10，WinServer 等微软操作系统的终端和服务器准入，并提供支持 802.1X 的客户端；支持 CentOS，Ubuntu，SUSE 等主流 Linux 操作系统的终端和服务器准入，并提供支持 802.1X 的客户端；支持兆心、飞腾、龙芯、申威、鲲鹏等信创终端和服务

			器准入，以及中标麒麟、银河麒麟、统信、深度等国产操作系统准入，并提供支持 802.1X 的客户端，支持麒麟 V10 和统信操作系统互认证；支持自定义终端注册信息，包括注册人，单位，部门，工号，电话，邮箱等用户信息，并具备注册日志备查。
			认证功能：支持本地认证、UKey 认证、Radius 认证、Email 认证、AD 域服务器、LDAP 服务器联动认证，支持动态密码认证，支持第三方认证通知以及通过第三方方式修改密码；支持认证账号有效期和多点登录，支持允许/禁止登录区域控制，支持允许/禁止登录时段控制；支持认证账号通过 Web 页面申请注册管理员审批并指定账号有效期，申请信息包括账号、密码、姓名、电话、邮箱、部门等，部门由管理员预设置后选择。
			具备与网内现有准入设备联动对接能力，支持基于上级准入系统作为认证源，承载下级准入系统范围内的入网终端认证，同步组织结构及用户信息，不需额外安装客户端实现安检、802.1X 等相关功能，提供与现有终端安全管理软件兼容性证明。
			提供制造商授权及服务承诺函。

1、提供网络管理准入系统制造商授权及服务承诺函

2、2022 年 1 月 1 日至投标截止日（以合同签署时间为准），投标人应具有至少 1 个以上的网络设备供货业绩。