一、评分办法

变更后标段二评分办法：

序号	评审因素	评审标准
1	**磋商报价（20 分）**	在所有的有效投标报价中，以最低投标报价为基准价，其价格分为满分。其他投标人的报价分统一按下列公式计算：投标报价得分=(评标基准价 / 投标报价)×价格权值（20%）×100（四舍五入后保留小数点后两位）。 注：根据《政府采购促进中小企业发展暂行办法》、《关于促进残疾人就业政府采购政策的通知》的相关规定，对残疾人福利性单位、小型和微型企业制造（生产）产品的价格给予 10%的扣除，用扣除后的价格参与评标。 残疾人福利性单位属于小型、微型企业的，不重复享受政策。
2	**技术部分得分(60 分)**	**技术服务方案（24 分）**：针对本项目需求，提供详细、完善的技术服务方案；包含服务保障方案、应急保障方案、故障恢复及处理方案、系统安全保障方案，能够结合项目特点制定技术服务方案，内容健全、详细的得 24-17 分；结合项目特点制定技术服务方案，内容较健全、内容较详细的得 16-8 分；制定了技术服务方案，内容一般的得 7-1 分；没有的不得分。 **项目管理实施方案 （16 分）**：设置了项目管理机构，并且有科学、具体的项目管理措施。包含：①实施计划②实施团队③实施进度④质量控制措施。以上因素每实质性响应一项得 4 分，满分 16 分，未实质性响应或未提供不得分。 **技术能力证明 （20 分）**： 1.为了保证项目高效、高质量的施工，实施人员精通安全相关知识外，还需精通网络相关知识，需具备 CISP 证书，提供身份证、毕业证、相关证书、用工合同及近半年社保缴纳证明，（需提供证书复印件），提供 3 人（含 3 人）以上的，得 5 分，2 人（含 2 人）以上的，得 3 分，提供 1 人的，得 1.5 分，不提供不得分。 2.为了顺利通过等级保护测评及相关整改，投标人须对等保有一

		定的了解，参与等保 2.0 标准起草大于等于 4 个的，得 6 分；参与等保标准起草大于等于 2 个的，得 3 分；参与等保标准起草大于等于 1 个的，得 1 分，未参与的不得分。 3.为保证投标人具备较强的应急响应处置能力，投标人具备连续三届国家级应急支撑单位的得 6 分，具备连续二届国家级应急支撑单位的得 4 分，具备一届国家级应急支撑单位的得 2 分，不具备不得分。 4.为了本项目顺利、高效施工和建设，投标人同时具备《信息系统建设和服务能力评估 CS4》、安全工程类和安全开发类证书得 3 分，不提供不得分。
3	**履约能力（10 分）**	**类似业绩情况（10 分）：**提供 2019 年以来的类似业绩证明材料，包含合同首页、标的及金额所在页、供货合同签字盖章页或中标（成交）通知书，加盖磋商供应商公章）。每提供 1 项得 **2** 分,满分 **10** 分；不提供不得分。
4	**售后服务（10 分）**	**售后服务（10 分）** 1、根据投标人提供的针对本项目的售后服务方案（含服务机构和人员、服务内容和流程、质量保证、响应时间、售后等内容）进行综合评审：售后服务方案详细严密，内容齐全、有针对性，合理的，得 8 分；售后服务方案较为详细严密，内容基本齐全、较为合理可行的，得 5 分；售后服务方案内容简单的，得 2 分，售后服务方案一般的，得 1 分，未提供或其他情况不得分。 2、提供售后服务相关承诺的，得 2 分；未提供不得分。
评标过程中，不得去掉报价中的最高报价和最低报价。		

二、类似业绩

变更后磋商供应商的类似业绩证明材料：

格式 17、磋商供应商的类似业绩证明材料

提供自 2019 年以来的类业绩证明材料。类似业绩是指与采购项目在产品类型、使用功能、合同规模、服务内容等方面相同的项目。须提供包含合同首页、标的及金额所在页、签字盖章页的合同或中标通知书复印件。

三、技术参数

变更后标段一技术参数：

序号	设备名称	配置参数	单位	数量
（一）	技术体系设计			
1	播出出口防火墙	1、标准机架式设备，双电源；要求配置≥6 个 10/100/1000M 自适应千兆电接口及≥2 个 SPF+万兆接口（不含光模块）及≥2 个接口扩展槽。 2、整机吞吐率≥8G，最大并发连接数 300 万，每秒新建连接数 6 万。本次项目要求提供至少 3 年质保服务和售后服务，至少三年入侵防御特征库升级服务，至少三年病毒库升级服务。 3、支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略，支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。提供相关界面截图。 4、支持详细的访问控制策略日志，每条匹配策略的会话均可记录其建立会话和拆除会话的日志；访问控制策略日志可本地记录或发送至 Syslog 服务器。提供策略配置界面截图及防火墙本地记录的策略建立会话及拆除会话的日志截图。 5、支持 IPv6 环境下的应用行为管理和控制。支持并开通 WEB 控制功能模块，包括 URL 访问分类管理、网页关键字过滤、http 文件下载类型管理等功能，提供截图。 6、支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。提供相关界面截图。 7、支持基于接口/安全域、地址、用户、服务、应用和时间的入侵防御策略设定，每个入侵防御策略均可配置检测事件及响应方式。提供相关界面截图。 8、可对 exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip 等常见的格式进行动态沙箱分析；可对 rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）做 PE 内嵌检测，并且能指出文件偏移位置； 提供相关界面截图。 9、支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。提供防火墙配置界面及威胁情报云端界面截图。 10、支持多链路智能选路，根据业务对抖动、时延和带宽的要求，在多条不同链路上智能动态选路，通过自动重传技术，实现链路切换时无丢包，业务不掉线。对 SD-WAN 隧道的时延、抖动、带宽占用率、丢包率等提供可视化展示；提供相关界面截图。	台	2

		11、产品具备《计算机信息系统安全专用产品销售许可证》，且认证等级为增强级、具备《信息技术产品安全测评证书-EAL4+》证书，提供证明材料；为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。		
2	出口防火墙（无线发射）	1、2U 盒式设备，采用 X86 64 位多核高性能处理器和高速存储器，主控模块内存≥4G; 2、主机固化千兆电口≥16.千兆光口≥2,配置硬盘≥500GB，可扩展 4PFC 接口卡、4SFP 插卡、4SFP+插卡等，支持硬盘扩展插槽≥1，可扩展 500G 和 1T 的 HDD 硬盘，480G SSD 硬盘; 3、配置单电源，支持双电源扩展，可扩展类型支持交流电源、直流电源: 4、支持流量控制和 QOS 服务带宽保障，支持 HA 双击热备和负载均衡，支持动态路由及 ISP 智能选路，支持 IPSec VPN，IPsec vpn 隧道数≥4000; 5、含防病毒模块,可升级，IPS 吞吐量>1200Mbps。 6、整机吞吐率≥10G，最大并发连接数≥600 万，每秒新建连接数≥14 万。本次项目要求提供 3 年质保服务和售后服务，三年入侵防御特征库升级服务，三年病毒库升级服务。 7、支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略，支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。提供相关界面截图。 8、支持详细的访问控制策略日志，每条匹配策略的会话均可记录其建立会话和拆除会话的日志;访问控制策略日志可本地记录或发送至 Syslog 服务器。提供策略配置界面截图及防火墙本地记录的策略建立会话及拆除会话的日志截图。 9、支持 IPv6 环境下的应用行为管理和控制。支持并开通 WEB 控制功能模块，包括 URL 访问分类管理、网页关键字过滤、http 文件下载类型管理等功能，提供截图。 10、支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。提供相关界面截图。 11、支持基于接口/安全域、地址、用户、服务、应用和时间的入侵防御策略设定,每个入侵防御策略均可配置检测事件及响应方式。提供相关界面截图。 12、可对 exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip 等常见的格式进行动态沙箱分析；可对 rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）做 PE 内嵌检测，并且能指出文件偏移位置； 提供相关界面截图。	台	1

		13、支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。提供防火墙配置界面及威胁情报云端界面截图。 14、支持多链路智能选路，根据业务对抖动、时延和带宽的要求，在多条不同链路上智能动态选路，通过自动重传技术，实现链路切换时无丢包，业务不掉线。对 SD-WAN 隧道的时延、抖动、带宽占用率、丢包率等提供可视化展示；提供相关界面截图。 15、产品具备《计算机信息系统安全专用产品销售许可证》，且认证等级为增强级、具备《信息技术产品安全测评证书-EAL4+》证书，提供相证明材料；为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。		
3	新大楼出口防火墙	1、标准机架式设备，双电源；要求配置≥6 个 10/100/1000M 自适应千兆电接口及≥2 个 SPF+万兆接口（不含光模块）及≥2 个接口扩展槽。 2、整机吞吐率≥8G，最大并发连接数 300 万，每秒新建连接数 6 万。本次项目要求提供至少 3 年质保服务和售后服务，至少三年入侵防御特征库升级服务，至少三年病毒库升级服务。 3、支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略，支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。提供相关界面截图。 4、支持详细的访问控制策略日志，每条匹配策略的会话均可记录其建立会话和拆除会话的日志；访问控制策略日志可本地记录或发送至 Syslog 服务器。提供策略配置界面截图及防火墙本地记录的策略建立会话及拆除会话的日志截图。 5、支持 IPv6 环境下的应用行为管理和控制。支持并开通 WEB 控制功能模块，包括 URL 访问分类管理、网页关键字过滤、http 文件下载类型管理等功能，提供截图。 6、支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。提供相关界面截图。 7、支持基于接口/安全域、地址、用户、服务、应用和时间的入侵防御策略设定，每个入侵防御策略均可配置检测事件及响应方式。提供相关界面截图。 8、可对 exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip 等常见的格式进行动态沙箱分析；可对 rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）做 PE 内嵌检测，并且能指出文件偏移位置； 提供相关界面截图。	台	1

		9、支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。提供防火墙配置界面及威胁情报云端界面截图。 10、支持多链路智能选路，根据业务对抖动、时延和带宽的要求，在多条不同链路上智能动态选路，通过自动重传技术，实现链路切换时无丢包，业务不掉线。对 SD-WAN 隧道的时延、抖动、带宽占用率、丢包率等提供可视化展示；提供相关界面截图。 11、产品具备《计算机信息系统安全专用产品销售许可证》，且认证等级为增强级、具备《信息技术产品安全测评证书-EAL4+》证书，提供相证明材料；为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。		
4	旧大楼出口防火墙(利旧媒资+制作防火墙）	利旧现有媒资制作系统防火墙 1、2U 盒式设备，采用 X86 64 位多核高性能处理器和高速存储器，主控模块内存≥4G; 2、主机固化千兆电口≥16.千兆光口≥2,配置硬盘≥500GB,支持扩展槽位≥2，可扩展 4PFC 接口卡、4SFP 插卡、4SFP+插卡等，支持硬盘扩展插槽≥1，可扩展 500G 和 1T 的 HDD 硬盘，480G SSD 硬盘; 3、配置单电源，支持双电源扩展，可扩展类型支持交流电源、直流电源: 4、整机吞吐量≥10Gbps;每秒最大新建连接数≥14 万;最大并发连接数≥600 万; 5、支持流量控制和 QOS 服务带宽保障，支持 HA 双击热备和负载均衡，支持动态路由及 ISP 智能选路，支持 IPSec VPN，IPsec vpn 隧道数≥4000; 6、含防病毒模块,可升级，IPS 吞吐量>1200Mbps。	台	1
5	边界防火墙（应用服务一、应用服务二）	1、标准机架式设备，双电源；要求配置≥6 个 10/100/1000M 自适应千兆电接口及≥2 个 SPF+万兆接口（不含光模块）及≥2 个接口扩展槽。 2、整机吞吐率≥10Gbps，最大并发连接数≥300 万，每秒新建连接数 6 万。本次项目要求提供 3 年质保服务和售后服务，三年入侵防御特征库升级服务，三年病毒库升级服务。≥60G SSD 硬盘；默认支持下一代防火墙访问控制、入侵防御、网络防病毒、上网行为及 URL 分类管理、流控和 IPSec VPN 模块;多链路接入授权≥3 条，第三方 IPsec VPN 接入授权≥10。 3、支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略，支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。提供相关界面截图。 4、支持详细的访问控制策略日志，每条匹配策略的会话均	台	3

		可记录其建立会话和拆除会话的日志;访问控制策略日志可本地记录或发送至 Syslog 服务器。提供策略配置界面截图及防火墙本地记录的策略建立会话及拆除会话的日志截图。 5、支持 IPv6 环境下的应用行为管理和控制。支持并开通 WEB 控制功能模块，包括 URL 访问分类管理、网页关键字过滤、http 文件下载类型管理等功能，提供截图。 6、支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每 IP 总连接数控制、每 IP 新建连接数控制。提供相关界面截图。 7、支持基于接口/安全域、地址、用户、服务、应用和时间的入侵防御策略设定,每个入侵防御策略均可配置检测事件及响应方式。提供相关界面截图。 8、可对 exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip 等常见的格式进行动态沙箱分析；可对 rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）做 PE 内嵌检测，并且能指出文件偏移位置； 提供相关界面截图。 9、支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。提供防火墙配置界面及威胁情报云端界面截图。 10、支持多链路智能选路，根据业务对抖动、时延和带宽的要求,在多条不同链路上智能动态选路,通过自动重传技术，实现链路切换时无丢包，业务不掉线。对 SD-WAN 隧道的时延、抖动、带宽占用率、丢包率等提供可视化展示；提供相关界面截图。 11、产品具备《计算机信息系统安全专用产品销售许可证》，且认证等级为增强级、具备《信息技术产品安全测评证书-EAL4+》证书，提供相证明材料；为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。		
6	VPN	1、要求≥1 个 RJ-45 Console 口，≥6 个 10/100/1000M 自适应电口，≥2 个千兆 SFP 插槽，≥2 个万兆 SFP+ 插槽，≥2 个网络接口扩展槽位;SSL 加密吞吐≥400Mbps，推荐并发用户数≥2000，IPSec 加密吞吐 ≥400Mbps，整机吞吐≥5Gbps;≥100 个 PC 端并发用户授权，适用于 VPN、密码机和可信网关产品在 Windows、MAC OS、桌面式 Linux 等操作系统上的并发授权，支持国家商用密码算法。要求支持多系统引导，并可在 WEB 界面上直接配置启动顺序，至少三个操作系统，WEB 界面操作双系统和备份系统，用户可自由选择当前启动系统;要求支持 KMC 与 GDOI 模式组网，支持密钥管理中心统一管理下发密钥及策略，使用组播技术更新密钥，无需更改原路由策略;要求支持 IPSec、SSL 、	台	1

		PPTP、L2TP VPN 的统一用户账号和认证体系，实现用户名密码的一次性配置即可适用于全部 VPN 类型的接入。 2、支持多系统引导，可在管理员界面直接配置启动顺序，至少支持两个操作系统，管理员可自由选择当前启动系统，每个系统拥有独立的配置文件，且分别支持加密导入导出（提供截图证明）。 3、支持管理员分权管理，支持三权分立，包括系统管理员，安全管理员，审计管理员；支持自定义权限模板，为管理员分配管理权限；（提供截图证明） 4、支持分级管理，将用户组、资源、角色按照组织架构进行分级管理，可以为各级别管理员分别创建管理员，并可逐级授权。（提供截图证明） 5、PC 客户端支持龙芯、兆芯、飞腾、鲲鹏等国产化平台，支持中标麒麟，银河麒麟，普华、深度（deepin）、优麒麟、UOS、中科方德等国产化操作系统；（提供至少二种国产化操作系统的厂商互认证明材料） 6、支持登录门户加密协议选择，TLS1.2/1.1/1.0 SSL3.0/2.0；支持加密算法套件选择 RSA_DES_CBC_SHA，RSA_RC4_MD5， RSA_RC4_SHA，RSA_WITH_AES_SHA；支持安全密钥更新周期设置；（提供截图证明） 7、支持单点登录功能（SSO）,支持移动用户登录 VPN 后再登录内部 B/S、C/S 应用系统时不需要二次重复认证。支持针对不同的访问资源设定不同的 SSO 用户名和密码,支持用户自行修改 SSO 账号。支持 CS 单点登录工具助手，支持自动识别登录窗口自动形成配置文件。（提供截图证明） 8、支持 DMVPN 动态组网功能，网络扩展时仅需配置新增节点,无需配置原中心节点和分支节点,即可扩展 VPN 网络(提供截图证明）。 9、VPN 产品需与同品牌堡垒机产品联动，支持在 VPN 界面直接输入堡垒机账号认证，并单点登录到堡垒机运维界面，无需任何定制开发直接部署。 10、为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。		
7	网闸	1、标准 2U 机箱，双冗余电源；内网：要求配置≥2 个 SFP 插槽，≥4 个 10/100/1000M Base-TX 网络接口，≥1 个 10/100/1000M Base-TX 管理接口，≥1 个 10/100/1000M Base-TX HA 接口（双机热备口）；外网：要求配置≥2 个 SFP 插槽，≥4 个 10/100/1000M Base-TX 网络接口，≥1 个 10/100/1000M Base-TX 管理接口，≥1 个 10/100/1000M Base-TX HA 接口(双机热备口);整机吞吐大于等于 400Mpps，并大连接数≥4 万，延时≤1ms，整机配液晶屏，设备健康监控声光报警装置；配置视频传输模块及全功能模块，要求提供至少 3 年质保服务和售后服务。	台	1

		2、内外网主机系统分别支持双系统引导，并可在 WEB 界面上直接配置启动顺序，在 A 系统发生故障时，可以随时切换到 B 系统；且支持系统(包括配置)备份；（提供产品功能界面截图证明）支持恢复出厂版本功能，一键恢复系统到出厂状态。 3、支持接口冗余模式设置包括：轮询、热备、链路聚合协议，可对用户的客户端版本和进程进行检查，进行准入控制（提供产品功能界面截图证明）。 4、支持灵活的数据库冲突处理策略，当关键 m 字数据发生冲突时可选择：覆盖/丢弃；支持数据库同步客户端的双机热备技术，为用户提供更高的冗余技术支持（提供产品功能界面截图证明）。 5、支持数据库 SQL 语句过滤功能。支持用户身份认证，支持 IPv4、IPv6 双协议栈接入(提供产品功能界面截图证明)。 6、支持用户认证，包括口令、证书等认证方式；并支持用户在线时段控制；内置近 30 种视频厂商协议模板，可简化配置、调试步骤；支持视频格式过滤，包括 G.711、G.729、H.264、H.263、MP4、PS 等（提供产品功能界面截图证明）。 7、支持 HTTPS 的 Web 方式管理，实现了远程管理信息加密传输；提供《公安部计算机信息系统安全产品质量监督检验中心检测报告》证明。 8、支持视频功能类型过滤，包括实时点播、历史回放、录像下载、云台控制、回放控制、录像检索、设备查询等（提供产品功能界面截图证明）。 9、为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。		
8	数据库审计	1、标准机架式设备，要求配置≥6 个电口（含 1 个管理口，1 个 HA 口），≥1 个接口扩展槽，≥1 个 RJ45 串口，硬盘≥2T。被审计数据库授权数不低于 13 个，提供至少 3 年质保服务和售后服务。 2、支持旁路部署方式，无须在被审计系统上安装软件，对原有网络不造成影响,审计产品的故障不影响被审计系统的正常运行，支持对部署在 vmware、KVM、Xen 等虚拟化环境中的数据库进行审计，审计系统可虚拟化部署。 3、支持国产数据库人大金仓、达梦、南大通用、神通、高斯等数据库的审计。支持 MongoDB、redis 数据库的审计。支持 Hbase、hive、ES 的审计。需提供截图证明。 4、支持对针对数据库的 XSS 攻击、SQL 注入、CVE 高危漏洞利用、口令攻击、缓冲区溢出等攻击行为进行审计。需提供截图证明。 5、支持双向审计，支持对 Select 操作返回行数和返回内容的审计。需提供截图证明。 6、系统支持数据库中存储过程自动学习，可学习存储过程	台	1

		中涉及的操作并与审计事件中的存储过程名进行关联，方便确认存储过程是否存在风险。需提供截图证明 7、支持审计 HTTP 和 HTTPS 协议的 URL、访问模式、cookie、页面内容、Post 内容。需提供截图证明。 8、支持中间件环境下的 SQL 语句关联到 HTTP 操作，HTTP 操作关联到 HTTP-ID，实现中间件环境下的审计追溯。需提供截图证明。 9、支持自动建立数据库操作行为基线。数据库操作行为基线包括数据库账号、操作类型（SQL 模板）等行为特征。需提供截图证明。 10、数据库审计支持用户环境中的数据库和资源账号、表名的自动发现，方便用户使用，数据库审计支持用户数据库中敏感信息的自动发现，可定位敏感数据存储的服务器、库名、表名、列名，并形成针对敏感信息的审计规则，需提供截图证明。 11、支持对敏感信息敏感级别进行定义，各级别可对应不同风险值，方便对敏感数据泄露进行风险进行评估，敏感数据发现可支持 Oracle、ms-sql、Mysql、DB2、PostgreSQL、ES 等常见关系型数据库与大数据库协议。需提供截图证明。 12、数据库审计策略支持频次统计，某一操作在周期时间内达到设定的次数阀值后可以进行单独记录和展示，周期事件和次数可按需配置，支持用户操作轨迹图展示，轨迹图维度可根据资源账号、源 ip、客户端程序名、命令、表名、错误码等按需定义，可根据昨天、最近七天、最近 30 天以及自定义时间进行轨迹显示，可显示下一节点数量，可在某一维度中进行筛选，提供截图证明。 13、支持与 Web 应用防火墙（WAF）的联动，可对 WAF 上报的应用系统攻击实现场景还原展示。需提供截图证明。 14、为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。		
9	堡垒机	1、标准上架设备，≥6 个千兆电口，≥1 个 Console 管理口，存储容量≥2TB，带液晶面板，≥2 个扩展槽。最大支持≥1000 路字符会话或≥300 路图形会话并发。要求提供至少 3 年维保服务，≥100 个点的被管资源数，≥3 个管理员双因素认证 USBKEY，至少 5 个运维人员双因素认证 USBKEY。 2、系统内置系统管理员、审计管理员、安全管理员三种角色，系统管理员可针对不同用户指定不同的管理权限，可设定用户（组）和资源（组）的管理范围，需提供产品界面截图。 3、支持用户密码策略，包括：最小密码长度（强制最小 8 位）、密码复杂度（小写字母，大写字母，数字，特殊字符）、不允许密码与用户一致设置，不允许密码与用户逆序，密码周期（过期前提醒）、历史密码对比。需提供产品界面截图。	台	1

		4、实现数据库命令级审计，支持的数据库类型包括：Oracle（支持 ORACLE RAC）、SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、Teradata，不需采用数据镜像方式实现，以免增加部署的复杂性和网络负担。需提供产品界面截图。 5、支持通过应用发布实现字符协议和文件传输协议的命令级审计和图形审计的双重审计效果，命令级审计便于重现真实的完整操作命令，图形审计便于直观的查看到真实的操作行为，并支持通过搜索操作语句或执行结果中关键字定位审计回放。需提供产品界面截图。 6、支持通过应用发布进行协议扩展，支持 http/https 协议、X11 协议、VMware vSphere Client、Radmin 等第三方客户端工具，并支持模拟帐号密码代填登录；应用发布调用只能推送应用工具窗口，不得推送 windows 桌面，以提升用户体验。需提供产品界面截图。 7、能够支持如下运维工具：Putty，SecureCRT、XSHELL、SSH Secure Shell Client、WinSCP、FFFTP、FlashFxp、FileZilla、SQLPlus、PLSQLDev、Toad for Oracle、Db2cmd（DB2）、Quest Central for DB2、Teradata SQL Assistant、SqlDbx Personal、SqlDbx Professional、pgAdmin3、Mysql Command、SSMS、Dbvisualizer、Navicat。需提供界面截图。 8、支持僵尸、幽灵、孤儿帐号稽核功能，并可以导出异常账号稽核情况报告，方便管理员统计异常账号情况。僵尸帐号：周期内登录次数低于 3 次的用户帐号和资源帐号；幽灵帐户：堡垒机中未托管但又真实存在的的资源帐号；孤儿帐户：没有建立授权关系的用户帐号和资源帐号。提供界面截图。 9、为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。		
10	网络准入	1、2U 机架式设备，≥1 个 RJ-45 Console 口，≥6 个 10/100/1000M 自适应电口，≥2 个千兆 SFP 接口，≥2 个万兆 SFP+接口，≥2 个网络接口扩展槽位，冗余电源；整机最大吞吐量≥12Gbps，最大支持管理 2000 个终端设备。提供≥50 个点全功能模块授权，要求提供至少三年维保服务。 2、支持对网络攻击行为，如 Smurf 入侵、LAND 攻击、WINNUK 攻击等，支持对攻击行为的发现和告警。（提供第三方检测报告，报告中必须有此能力体现） 3、支持多种准入控制技术（802.1X、EVG、DHCP、ARP、SNMP、端口镜像、策略路由、透明网桥），并且支持至少四种以上准入技术的复用，如 802.1x、DHCP、端口镜像、策略路由混合部署。（提供功能截图） 4、支持网络资产自动采集功能，并能够自动分类网络中的接入设备，如交换路由设备、PC 设备、服务器、IP 电话、	台	1

		网络打印机等，同时能够及时发现网络中出现的新设备，对外来终端的接入行为进行告警。（提供功能截图） 5、支持展示和管理当前内网中受管理的网络设备和终端设备，当预置的设备类型选项卡无法满足显示需求时，可新建选项卡来单独列出所关注的设备。并在可通过设备详情查看设备基本信息、注册信息、认证安检信息、准入状态、硬件信息、软件资产信息。（提供功能截图） 6、支持全网监控统计功能，实时显示全网监控状态信息的资产动态、安全违规事件、设备信息、在线终端统计、终端类型统计、终端厂商分类统计、实时告警、终端安全分析统计等信息。（提供功能截图） **7、为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。**		
11	日志审计	1、2U 标准机架式，冗余电源，≥6 个千兆电口，≥1 个管理口，≥2 个 USB 接口，存储容量≥2TB。要求所提供的产品提供 3 年质保服务和售后服务，审计节点授权数≥80 个。 2、系统提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点;可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表；必须提供截图； 3、系统必须内置基本的仪表板。用户可以在工作台中自定义仪表板，按需设计仪表板显示的内容和布局，可以为用户建立不同维度的仪表板；必须提供截图； 4、范式化字段至少应包括事件接收时间、事件产生时间、事件持续时间、用户名称、源地址、源 MAC 地址、源端口、操作、目的地址、目的 MAC 地址、目的端口、事件名称、事件摘要、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等；针对不支持的事件类型做范式化不需改动编码，通过修改配置文件即可完成。必须提供截图； 5、可以对选中的日志提供在线/离线地图定位、源 IP 与目的 IP 分布走向的视网膜图展示、描述日志之间行为相关关系的事件拓扑图等多种分析工具；必须提供截图； 6、告警动作支持告警重定义、弹出提示框、发出警示音、发送邮件、发送 SNMP Trap、发送短信、执行命令脚本、设备联动、发送飞鸽传书、发送 Syslog、加入观察列表、从观察列表中删除；必须提供截图； 7、内置 Cisco PIX 和交换机的事件编码知识库；内置 Windows、Linux、Solaris、AIX 操作系统的事件 ID 知识库；内置 Oracle、SQL Server、MySQL、Informix、DB2 数据库的事件编码知识库;能够查看系统内置的事件库中事件类型名称及其描述信息。必须提供截图。 8、为了保障项目的顺利实施，设备原厂商需具备应急支撑	台	1

		单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。		
12	安全管理平台	1、系统采用 B/S 架构，管理员只需浏览器即可连接到系统进行各种操作。浏览器至少支持 IE、Chrome 与 Firefox 等。用户可以对界面颜色进行选择调整。 2、在态势总览中能够对全网安全信息进行综合展示，包括对全网的安全、运维概况的量化评估，对资产、运行、攻击、脆弱性的概况评估，能够显示不同时间段维度的事件告警趋势曲线，对不同类型告警事件进行周期性预测，对攻击链的各个阶段进行监控，能显示实时攻击情况、攻击源、受攻击的资产、业务系统情况、包括相关的 TOP、各类事件数量和次数，规则和情报命中情况，及威胁情况的信息，能显示漏洞类型的分布图、高危漏洞的详情及影响的资产，对告警处理情况跟踪、包括告警的数量、工单及处理率等。支持对需要进一步追溯的部分进行下钻。（要求提供截图证明） 3、利用攻击链分析模型、按事件类型和攻击行为信息将整个攻击过程进行拆分统计，对各阶段事件的源目地址、类型、数量及分布情况等维度信息进行分析，对全网业务资产被攻击情况进行全程监控、全景呈现，从不同时间段维度对攻击链个阶段趋势进行分析展示，同时引入扇子分析模型，可从时间维度对各攻击阶段的事件量进行展示，并可选定任意时间区间进行自动的重点分析计算，结果呈现。供用户了解攻击者的攻击规律，攻击手法，攻击意图。为后续的防御、诱捕、反制提供数据支撑。（要求提供截图证明） 4、系统可提供通过导入或者主动自动抓取的方式获取外部相关网络威胁情报信息，并能将这些威胁情报用于关联分析。（要求提供截图证明） 5、可结合等保模板及任务计划对可对当前资产的等保合规情况及任务趋势进行图表展现，包括等保计划、等保任务的统计；不合规设计的指标、系统、强度情况的 top 呈现，且支持分级筛选；系统达标率 top；任务数量趋势、负责人处理率的排行。内置最新的等保 2.0 四级标准模板，且支持自定义模板功能，用户可按需定制；可随意添加任务计划，选择所需的等保模板，支持对计划进行编辑、指派、归档和查看。支持对等保处理流程信息的记录和筛选。（要求提供截图证明） 6、潜伏威胁态势从网络态势感知“知己”的角度，已失陷主机为监测对象对越过了边界防护的攻击在内网中潜伏的情况进行呈现。具体包括潜伏威胁概况图呈现网络上的嗅探行为，入侵利用，C&C 控制，横向扩散，数据外传统计；用户网络失陷主机个数，失陷主机所属区域分布，失陷主机确定度指标，威胁度指标展示；潜伏威胁安全事件统计，安全事件源地址 TOP5，目的地址 TOP5；威胁事件影响的内网区域列表，设备列表。（要求提供截图证明）	套	1

		7、综合威胁,弱点，资产价值三方面安全要素，根据风险计算模型，进行全网、各区域、资产的风险量化评估和风险赋值，使用户从安全风险的高度集中把控全网，各安全域、特定资产的风险态势。通过风险地图对全网所受风险的区域分布进行宏观呈现，对影响风险的各类安全事件分布状况、脆弱威胁排名、源目攻击关系，资产和安全域风险 top 资产、安全域风险等级分布状况进行直观展示。（要求提供截图证明） 8、为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。		
13	入侵检测	1、≥1 个 RJ-个 Console 口，≥6 个 10/100/1000 Base-T 接口，≥2 个 USB 口，≥2 个千兆光接口插槽，≥2 个万兆光口插槽，≥2 个扩展插槽，冗余电源，≥2T 硬盘，提供至少三年的特征库升级、至少一年威胁情报升级模块授权，至少三年维保服务。 2、支持常见 HTTP、FTP、TFTP、SMTP、TLS、SSH、IMAP、SMB、Dcerpc、DNS、IKEV2、NFS、Krb5、DHCP、SNMP、SIP、RFB、RDP 等应用层协议；提供产品界面截图。 3、系统综合分析页面提供最近 24 小时/7 天/15 天内接入流量网络中发生的整体安全态势，包括对网络内风险资产进行统计分析、对攻击、受害攻击进行聚合分析输出 TOP10，同时可对网络内告警事件趋势与告警风险级别绘制柱状图与并状态，并可对告警攻击 TOP5 进行排序便于客户直观了解脆弱点；提供产品界面截图。 4、支持对常见的拒绝服务攻击（DDOS）的检测能力，针对 TCP FLOOD、UDP FLOOD、ICMP FLOOD 攻击行为进行检测，并支持通过控制界面配置攻击的检测时间和阈值条件;提供产品界面截图。 5、支持对检测的告警事件结合双向检测机制、原始数据包和研判模型进行深层次研判给出告警事件的攻击结果，至少包含的结果类型为：攻击尝试、攻击成功、正在利用。（需提供界面截图） 6、支持自定义规则，可结合用户业务进行深度检测，自定义内容包括源 IP、源端口、目的 IP、目的端口、协议、事件威胁等级、主机状态、事件类型、攻击阶段、攻击结果、攻击手段；支持关联规则分析，进行双向检测规则编写，完美兼容业界主流 snort 规则。（需提供界面截图） 7、系统具备攻击链分析模型，通过被攻击者视角展示主机遭受攻击状态迁移图和攻击阶段统计，分析内部资产被外部地址攻击详情，多维度分析攻击异常开始时间，使用手段。（需提供界面截图） 8、为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发	台	1

		类）、微软 MAPP 成员单位，提供相关证明材料。		
14	漏洞扫描	1、标准上架设备，≥6 个 100/1000M 扫描电口、≥1 个 RJ45 Console 口，≥2 个 USB 接口，≥2 个接口扩展插槽，可扫描授权≥100 个 IP 地址，具体 IP 地址不限，并发扫描≥20IP。要求提供至少 3 年漏洞库升级授权，至少 3 年 Web 应用检测特征库升级服务，≥5 个域名扫描授权，提供≥20 种核查类型授权，核查资产数量不限制，授权在创建作业时能添加的资产数量总数≥256 个，授权作业合并后导出报告中包含的资产总数≥256 个，至少 3 年期维保服务。 2、漏洞扫描方法应不少于 120000 种，提供截图证明。 3、支持对主流操作系统的识别与扫描，包括：Windows、Redhat、Ubuntu、深度、红旗、中标麒麟等，提供截图证明。 4、提供自主发现的 CVE 安全漏洞列表，要求数量不少于 50 个；自主发现的 CNNVD 安全漏洞列表及证书，要求数量不少于 10 个。 5、支持对主流数据库的识别与扫描，包括：Oracle、Sybase、GBASE、GaussDB、达梦、人大金仓、优炫等，能够扫描的数据库漏洞扫描方法不小于 2600 种，提供截图证明。 6、支持对主流虚拟化软件平台进行扫描，包括：OpenStack 、KVM、Vmware、Xen、Docker、Huawei FusionSphere 等，能够扫描的虚拟化软件平台漏洞扫描方法不小于 600 种，提供截图证明。 7、支持多种协议口令猜测，包括 SMB、Snmp、Telnet、Pop3、SSH、Ftp、RDP、DB2、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、ActiveMQ、WebLogic、WebCAM 等，提供截图证明。 8、支持国产应用软件的识别与扫描，包括：Foxit、WPS、永中、数科、用友、景云、北信源等，提供截图证明。 9、支持 35 种以上默认扫描策略模板，如常规安全扫描，中高危漏洞扫描，高危漏洞扫描，web 服务组件扫描，网络设备扫描，云平台漏洞扫描，虚拟化扫描，主机信息收集，攻击性扫描，SQL SERVER 数据库扫描，Apple 类扫描，视频监控类扫描等等，同时针对市场应急响应的漏洞提供应急响应策略模板，提供截图证明。 10、产品具备网络脆弱性扫描类《计算机信息系统安全专用产品销售许可证》，要求为增强级、具备《信息技术产品安全测评证书》，级别 EAL3+，提供相关证明材料；为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。	台	1
15	终端安全管控系统	1、需支持主流 Windows 系统，包括：Windows XP－windows 10，winServer 2003+；需支持主流 Linux 操作系统，包括：CentOS 6+、RedHat 6+、Debian 7+、Ubuntu 14+、fedora 14+、	套	1

		SUSE 11+；本次配置≥30 个 Windows 客户端，≥5 个 Linux 客户端，提供至少三年病毒特征库升级服务，至少三年软件升级服务。 2、客户端安装需支持独立打包安装、下载器安装、命令行安装、Portal 引导安装，降低安装部署工作量。支持自定义管理员角色及管辖组织结构，实现分权分域管理。提供截图证明。 3、支持首页声音告警，有新事件及时提醒管理人员关注。支持通过 kafka 将日志发送至第三方平台。支持通过 syslog 将日志发送至第三方平台。为增加安全能力时效性，特征库需支持每一项独立升级，至少包含：系统版本、客户端病毒库、情报库、补丁库、弱密码库、webshell 规则库、web 应有组件规则库。以上功能提供截图证明。 4、支持 web 应用清点，包括：Apache、Tomcat、Nginx、Resin、IIS、Squid、Weblogic、Jboss、ActiveMQ、Zookeeper 的版本、安装路径、使用端口信息；支持详细记录终端进程每一次变动信息，包括：进程 ID、进程名、动作（启动、退出）、进程路径、父进程 ID、父进程名、进程命令行参数、启动或退出时间，以上功能提供截图证明。 5、支持详细记录终端服务变动信息，包括：服务名、服务描述、服务类型、服务启动类型、服务运行状态、服务上一次运行状态、服务操作类型、可执行文件路径、服务命令行参数。以上功能提供截图证明。 6.支持详细记录终端指令信息，包括：IP、命令类型、次数、具体参数内容。支持安全核查后进行百分制评分，评分模式开关和各项评分占比可单独配置。支持多引擎协同检测，增加病毒检出率；支持自定义选择病毒检测引擎。以上功能提供截图证明。 7.为了保障项目的顺利实施，设备原厂商需具备应急支撑单位资质、信息安全服务资质（安全工程类三级、安全开发类）、微软 MAPP 成员单位，提供相关证明材料。		

四、服务要求

变更后标段一第五部分　磋商及采购项目服务要求

一、磋商要求

1.磋商说明

1.1.磋商供应商可以按照磋商文件的规定磋商，但必须对所投包号中的所有内容作为一个整体进行磋商，不能拆分或少报。否则，磋商无效。

1.2.磋商报价应包括产品费、验收费、手续费、保险费、培训费、售前、售中、售后服务费、招标代理费、税金及不可预见费等全部费用。（说明：具体内容应根据项目特点实事求是的填写）。若磋商报价不能完全包括上述内容，该磋

商将被认为非实质性响应。

1.3.磋商供应商必须如实填写"技术规格响应表"，在"磋商产品技术参数、指标"栏中列出所投产品的具体规格和具体技术参数、指标；以招标人需求为最低指标要求，磋商供应商对超出或不满足最低指标要求的指标需列出"＋、-偏差。如果与磋商响应文件中提供的产品检测报告等证明材料中的实质性响应情况不一致或直接复制磋商文件"采购需求技术参数、指标"内容的，按无效磋商处理。

2.报价说明

本次磋商文件中规定的采购预算额度为磋商最高限价，磋商供应商的磋商报价不得超出此额度。否则，磋商无效。

3.重要指标

3.1.技术参数中除注明签订合同时提供的相关授权、服务承诺等资料以外，其余相关资料在磋商时必须附在磋商响应文件中。

4.商务要求

4.1.交货期：自合同签订合同之日起30天；

4.2.交货地点：采购人指定地点；

质保期及免费服务期：三年

4.3.付款方式：详见“第四部分青海省政府采购项目合同书范本”中“四、付款方式”的规定。