报价唯一性

投标分项报价表

项目编号/包号：常采公[2022]0235 号

项目名称：检察工作网安全体系建设及等保测评项目　　报价单位：人民币元

序号	分项名称	品牌商标	规格型号	技术参数	数量	单位	投标价格	
							单价	合价
1	边界路由器	华为	AR6280	详见技术参数附表	2	台	31000	62000
2	下一代防火墙	绿盟	NFNX3-HFC	详见技术参数附表	2	台	81000	162000
3	核心交换机	H3C	LS-7506X-S	详见技术参数附表	1	台	151000	151000
4	堡垒机	绿盟	OSMSNX3-HFC	详见技术参数附表	1	台	99900	99900
5	日志审计	绿盟	LASNX3-HFA	详见技术参数附表	1	台	82600	82600
6	防病毒系统	亚信	ESM V8.0	详见技术参数附表	1	套	40400	40400
		亚信	网络版V16.0	详见技术参数附表	1	套	6500	6500
7	网络可视化运维综合管理系统	网强	Emaster6.0	详见技术参数附表	1	套	122000	122000
附	网络机柜	图腾	42U	详见技术参数附表	1	台	3600	3600
	专业技术服务							
8	等保测评费用			详见技术参数附表	1	项	80000	80000
9	漏洞扫描服务			详见技术参数附表	1	项	50000	50000
10	应急响应服务			详见技术参数附表	1	项	30000	30000
11	全流量分析服务			详见技术参数附表	1	项	40000	40000
12	系统集成服务			详见技术参数附表	1	项	60000	60000
合　　计								990000

注：1.本表应按包分别填写。

2.如果不提供分项报价将视为没有实质性响应招标文件。

3.本表行数可以按照项目分项情况增加。

4.上述各项的服务内容如表格中填写不下的，可以逐项另页描述。

投标人名称（加盖公章）：中电鸿信信息科技有限公司

日期：2022年11月22日

技术参数附表

序号	设备名称	技术参数	
1	边界路由器	硬件规格	交换容量≥320Gbps，转发性能≥60Mpps，以官网最小值为准；
			★WAN：14*10GE 光（可切换为 GE 光）+10*GE 电 （所有 WAN 口可切换为 LAN）支持 8 个业务槽位，（提供原厂截图并加盖供应商公章）；
			▲所有业务板卡支持直接热插拔，（提供国家确定的认证机构出具的有效期内的检测报告并加盖供应商公章）；
		体系架构	采用无阻塞交换架构，（提供原厂截图并加盖供应商公章）；
		三层功能	支持静态路由，路由策略，RIP，OSPF，IS-IS，BGP；
		管理维护	支持升级管理，设备管理，web 网管；
		安全	支持国密算法，SAC 应用阻断，URL 过滤，防火墙功能
		配置	▲冗余交流电源，万兆光口≥14，千兆电口≥10，每台配置万兆单模模块*4 个+千兆单模光模块*2 个。
		其他	提供产品生产原厂出具的 3 年质保授权书复印件并加盖供应商公章。
2	下一代防火墙	硬件规格	▲标准式机架硬件设备，全内置封闭式结构，具有国产化的操作系统、硬件平台；CPU 配置为 4 核，主频为 2.6GHz；内存为 16GB，硬盘为 4T；接口配置：配置 6 个千兆电口，12 个千兆光口，2 个万兆光口；性能要求：网络层吞吐为 17G，最大并发 TCP 会话数为 6000 万，每秒新增 TCP 会话数为 200 万。
		防火墙	投标产品支持虚拟线、二层透明、路由、混合，适应各种网络环境需求。
			投标产品支持 IPMAC 绑定，支持手动和自动探测绑定
			投标产品能够在一条策略里配置源/目的 IP 地址/MAC 地址/IP 池/域名、安全区、应用/应用组、协议/端口、时间、用户、安全模板/模板组，详见证明材料；
			▲投标产品在策略匹配时有较高的匹配效率，详见证明材料“网络数据流安全处理方法”专利
			投标产品支持基于策略的双向 NAT、动态/静态 NAT。
			投标产品支持基于源/目的地址、接口的、基于服务、应用类型、用户的策略路由；
			投标产品支持链路探测，能够在每接口上以 ICMP/TCP/UDP 协议探测目标主机可达性，探测链路是否有效
			投标产品支持基于源、目地 IP、应用类型、时间段实行带宽限制、带宽保证等策略；
			▲投标产品支持 IPv6，拥有 IPv6 Enabled Security Logo 认证。详见证明材料
			投标产品支持泛洪类攻击防护:UDP/DNS/SYN/PING 泛洪;支持 ARP 欺骗类攻击；
		识别能力	投标产品支持对 2600+种应用的识别和控制
			支持达梦，人大金仓，神州通用等数据库识别

		入侵防护	投标产品支持扩展入侵防护功能模块，支持≥4000 种入侵规则过滤，详见证明材料
			投标产品支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL 注入、跨站脚本等等检测和防护
			投标产品支持对入侵规则库的分类组织和管理，包括：攻击手段/技术/流行度/危险度/服务类型
			投标产品支持自定义规则/规则组
		URL 过滤	投标产品支持内置 WEB 信誉库，提供 64 种精细分类（如艺术、商务、新闻论坛、论坛聊天、科技、体育等等）
		HA	投标产品支持主备、主主两种模式
			▲投标产品支持会话同步、状态同步，配置同步，支持链路状态的监测，详见“一种配置文件同步方法及装置”的专利证明材料
		系统管理	投标产品支持配置向导功能，可针对常见组网配置提供指导以帮助管理员快速部署上线设备
			投标产品能够根据威胁级别，实时显示安全攻击事件态势统计
			投标产品支持实时显示 Top10 应用、Top10 用户、各接口流量走势
			投标产品支持防火墙、入侵防护、URL 过滤、防病毒、内容过滤的日志记录
			投标产品能够呈现历史应用流量、应用会话走势图，并可按时、日、周显示
			投标产品支持事件关联分析，能够对防火墙的日志进行关联分析。详见证明材料
			投标产品事件关联分析支持多种排序，最少包含：基于流量、会话、风险等级。
		其他	提供产品生产原厂出具的 3 年质保授权书复印件并加盖供应商公章，详见证明材料
3	核心交换机	性能指标	主控槽位数≥2，业务槽位数≥6
			交换容量≥76.8Tbps，包转发率≥8640Mpps（官网最小值为准）
		板卡能力	支持 GE(光/电)、10GE（光/电）、40GE(光)、100GE(光)；
			▲支持 EPON OLT 接口，（提供原厂截图并加盖供应商公章）；
			为保证产品的后续带宽升级能力，要求投标产品单业务槽位万兆端口密度≥48，40G 端口密度≥24，100G 端口密度≥4；
			▲支持扩展独立防火墙、IPS、流量分析、应用控制等业务板卡，硬件模块非软件授权，（提供原厂截图并加盖供应商公章）；
		▲虚拟化	支持多虚一技术(N:1)，支持 4 框虚拟化技术，（提供原厂截图并加盖供应商公章）；
			支持一虚多技术（1:N），支持多虚一技术与一虚多技术的配合使用，（提供原厂截图并加盖供应商公章）。；
		IPv6	支持 RIPng、OSPFv3、BGP4+、IS-ISv6 协议；支持 IPv6 策略路由；支持 DHCPv6 功能、IPv6 portal 功能、IPv6 管理功能；支持基于 IPv6 的 VXLAN 二三层互通；；
		多业务融合	交换机支持集成 SDN 控制器，实现网络及 SDN 方案一体化部署，简化组网，简化运维，（提供原厂截图并加盖供应商公章）。

		有线无线一体化	支持交换机内置 AC 功能，（提供原厂截图并加盖供应商公章）。
		链路聚合	聚合组数≥1000 组，每组成员≥32 个；
			支持 DRNI 跨设备链路聚合
		安全	支持并配置 IEEE 802.1ae 介质访问控制安全技术，（提供原厂截图并加盖供应商公章）；
		兼容性	为保证系统平稳运行和统一运维管理，所投网络设备均为同一品牌；
		★配置要求	双电源、双主控，提供配 20 口千兆光+24 口千兆电+4 口万兆光，另配 4 个万兆单模光模块；
		其他	提供产品生产原厂出具的 3 年质保授权书复印件并加盖供应商公章。
4	堡垒机	规格性能	★投标产品为标准 1U 机架式硬件设备，采用国产 CPU：主频为 2.6GHz，4 核；国产操作系统，内存为 32GB，硬盘为 2TB+256GB，交流冗余电源，2 个 USB 接口，1 个串口，6 个千兆电口、4 个千兆光口，2 个万兆光口，1 个扩展插槽位，默认授权可管理设备数 300 台，最大支持管理 7000 台设备数。采用系统盘和数据盘的“双存储架构”进行数据存储物理隔离，数据存储空间为 2T。
		部署方式	投标产品支持域名方式 web 访问到堡垒机，并支持托管设备运维操作。
			投标产品支持 IP 和端口 DNAT 网络环境部署，通过映射后的 IP 和端口信息能够访问堡垒机，详见证明材料；
			投标产品支持对 IPv6 和 IPv4 双栈网络下托管设备运维管理和用户访问。
		身份认证	用户登录堡垒机支持多种认证方式，包括本地静态密码认证、LDAP 认证、RADIUS 认证、USBKEY 认证、OTP、短信认证等身份认证方式。
			▲投标产品支持对不同用户设置不同的认证方式，即可配置用户 1 使用本地认证，用户 2 使用 LDAP 认证，其他所有用户使用 RADIUS 认证，详见证明材料；
			▲投标产品支持公众号以及手机 APP（FreeOTP 和 Google Authenticator）方式进行 OTP 认证，详见证明材料；
		▲用户权限管控	投标产品支持管理员以用户为基准，支持直接查询、新建或编辑与该用户相关的策略，详见证明材料；
			投标产品支持管理员以设备访问中的设备为基准，支持直接查询并编辑与该设备相关的策略，详见证明材料；
		设备维护	支持智能扫描方式自动发现网络中的设备，通过 IP 地址扫描，快速发现指定 IP 地址范围内的主机、服务器和网络设备，并自动识别启用服务和端口，方便管理员快速添加设备。
		设备运维	密钥登录方式：在登录目标服务器时，使用的是秘钥登录，而非密码。在既可以使用密码，又可以使用秘钥的环境，可以自由选择登录认证方式。详见证明材料；
			支持本地字符客户端程序一键快速访问目标托管设备进行运维。

			支持 HTTP、HTTPS 操作审计，HTTP/HTTPS 协议可以直接代理。
			▲支持 SQL 语句级别审计，审计内容包括时间、用户、类型、用户 IP、设备 IP、数据库账号和 SQL 关键字等信息，并可通过 SQL 语句审计结果定位数据库运维操作录像回放，详见证明材料；
			可控制用户访问 web 服务器的 url 地址，防范运维人员违规访问 web 服务器，详见证明材料；
		业务指导	投标产品支持孤儿账号功能，能够提供对各从账号的运维使用率的分析功能，当发现使用率异常的从账号，对相关管理员采取告警、记录及通知等操作，详见证明材料；
			投标产品支持自动发现运维人员运维过程中创建的后门账号行为，并以列表方式向设备管理员展示托管设备中所有的后门账号信息。
		其他	提供产品生产原厂出具的 3 年质保授权书复印件并加盖供应商公章，详见证明材料
5	日志审计	硬件指标	★标准机架式国产化设备，采用国产 CPU：主频为 2.6GHz，4 核；内存为 32GB,硬盘为 4TB+128GB,具备冗余电源,提供的产品具有 1 个管理口、6 个千兆电口、4 个千兆光口、4TB SATA 硬盘。授权接入 40 个日志源。
		日志采集	系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等。
			系统支持的数据采集方式包括但不限于 SYSLOG、RSYSLOG、SNMP Trap、FTP、ODBC、JDBC、Net flow、WMI、二进制数据、专用 Agent 等方式采集日志。
			系统支持采集的设备厂家包括但不限于：NSFOCUS(绿盟科技)、Venustech(启明星辰)、Topsec(天融信)、DBAPPSecurit(安恒)、SANGFOR(深信服)、Hillstone(山石网科)、东软、瑞星、金山、网康、360 网神、Dptech(迪普)、艾科网信、Imperva、Juniper(瞻博网络)、F5、Symantec(赛门铁克)、Deep Security(趋势科技)、MaAfee(迈克菲)、Fortinet(飞塔)、Windows、Linux/Unix、Cisco(思科)、HUAWEI(华为)、H3C(华三)、中兴、Apache、nginx 、IIS、WebLogic、Vmware、Kvm、Xen、OpenStack、Hyper-V、华为 FusionSphere、Oracle、MySQL、PostgreSQL、SQL Server、Bind 等。
		日志管理	系统支持实现海量日志数据的采集并保存原始日志数据。
			系统支持界面配置即可完成未识别日志接入，无需编写 xml，详见证明材料；
			▲系统支持规则自适应日志接入，应支持将新接收的日志信息与系统内置规则、自定义规则进行匹配，将匹配度最高的规则与接收到的日志进行关联，完成自动接入，详见证明材料；
			系统支持 NAT 环境下的 Agent 部署模式。
			系统支持范式化日志多级提取。
			系统支持正则、KV、格式串等多种灵活的提取方式。
			系统能够实现范式化日志的枚举值管理，实现对范式化日志字段

			的灵活翻译，详见证明材料；
			系统应支持日志源监控能力，包括采集器维度及资产维度的监控，资产维度支持展示资产详细信息。
		日志转发	▲系统应提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源 IP 信息，详见证明材料；
		日志备份恢复	系统支持按类型、按日期(天)，手动、自动备份日志。
			系统支持设置日志存储备份策略，可设置备份周期、备份日志类型。
			系统支持日志备份远程服务器，如传送到 FTP 服务器。
			系统支持日志存储扩展，如 NFS 网络共享存储扩展，详见证明材料；
		日志查询分析	系统支持实时日志查询、历史日志查询。
			系统支持全文检索、模糊检索、正则检索等多种方式。
			系统支持日志检索结果存储为日志监控视图。
		事件告警	系统内置事件分类，并支持自定义事件分类，可定义事件分类的风险级别。
			▲系统支持多源事件关联分析能力，包括单源过滤模式、多源时序模式和多源关联模式，详见证明材料；
			系统支持基于事件分类的告警规则，支持短信、声音、邮件、界面提示等多种告警方式。
			系统支持告警抑制。
		资产管理	系统支持资产监控，支持根据设备类别对资产进行分类，根据 IP 可下钻至资产的整体数据、告警及关联事件。
			系统支持 6 种资产标签，根据标签可快速查询资产。
			系统支持资产以拓扑图形式展示，鼠标移动至资产图标可展示对应的资产信息。
		报表管理	系统能够按照多种维度统计日志信息。
			系统支持统计分析报表与多种文件格式导出。
			系统能支持自定义报表目录、LOGO 等，详见证明材料；
		其他	提供产品生产原厂出具的 3 年质保授权书复印件并加盖供应商公章。详见证明材料
6	防病毒系统（1 信创系统）	管理基础功能	产品采用 B/S 架构，支持通过 HTTPS 方式登录管理控制台，管理控制台访问需进行加密访问；
			管理端可以统计威胁类型分布、受影响客户端 TOP5、爆发病毒 Top5 等信息；
			管理端对于热点事件可以实现信息统计，包括感染途径分析等；
			可以通过管理控制台识别客户端的操作系统、体系架构、IP 地址、MAC 地址等信息，并进行管理；
			可以利用 IP 地址、设备 ID、操作系统的关联信息过滤客户端；
		服务器端支持系统	• UOS 1020 服务器版操作系统 arm64 • UOS 1020e 服务器版操作系统 arm64

			• 银河麒麟 V10 SP1 服务器版 arm64 • 银河麒麟 V10 SP1 服务器版 x86_64
		客户端支持操作系统	• UOS （版本 1020—1050、20SP1）桌面版操作系统 x86_64 • UOS （版本 1020—1030、20SP1、1020e）服务器版操作系统 x86_64 • UOS （版本 1020—1050、20SP1）桌面版操作系统 arm64 • UOS （版本 1020—1030、20SP1、1020e）服务器版操作系统 arm64 • UOS （20 Pro ）桌面操作系统 arm64 HUAWEI Kirin990 定制版 • UOS 1020e 服务器版操作系统 x86_64 • UOS 1020e 服务器版操作系统 arm64 • UOS （V20）桌面操作系统 Mips 定制版 • 银河麒麟（ Advanced Server V10 SP1)服务器版操作系统 arm64 • 银河麒麟（V10）桌面版操作系统 Mips 定制版 • 银河麒麟（ V10、 V10 SP1）桌面版操作系统 arm64 • 银河麒麟（ V10、 V10 SP1）服务器版操作系统 arm64 • 银河麒麟（ V10、 V10 SP1）桌面版操作系统 x86_64 • 银河麒麟（ V10、 V10 SP1）服务器版操作系统 x86_64 • 中标麒麟 （V7）服务器版操作系统 arm64
		安全防护病毒防护	提供自主知识产权的防病毒引擎；
			产品能够实时监控并清除来自各种途径的病毒、木马、蠕虫、恶意软件、勒索软件、黑客工具等恶意威胁；
			提供 U 盘扫描，可实时发现 U 盘里的病毒或恶意软件
			提供传统扫描、云扫描两种扫描方式，同时可以自由切换；
			▲支持对压缩文件扫描，并可设定最大的压缩层数为 16（提供原厂截图并加盖供应商公章）。
			提供压缩文件扫描功能，可以对超过固定大小文件不予扫描，以减少扫描时间；（提供原厂截图并加盖供应商公章）。
			▲对于恶意文件处理措施至少支持三种以上，包括厂家推荐措施、统一处理措施、以及针对不同类型病毒/恶意软件提供不同处理措施，同时不同病毒/恶意软件类型不少于 5 种分类（提供原厂截图并加盖供应商公章）。
			处置措施要提供至少两项措施，在首选措施失败的情况下，可以提供第二项措施进行处置；（提供原厂截图并加盖供应商公章）。
			为适应配置低的终端需求，不影响生产办公，终端在进行手动以及预设扫描时必须可以设置扫描时 CPU 占用比例，分高、中、低三个级别。低消耗下 CPU 高于 20%则暂停扫描以保证正常办公要求
			▲具备爆发阻止功能，管理端可配置爆发阻止策略，封堵共享目录（提供原厂截图并加盖供应商公章）。
			具备机器学习能力（提供原厂截图并加盖供应商公章）。
			▲支持终端防火墙功能，可依据以下标准设定规则：远程 IP，方

			向（出站\入站），协议（所有协议\ICMP\TCP\UDP\TCP+UDP）,端口（提供原厂截图并加盖供应商公章）。
			可设定清除动作前，备份文件
			支持管理员自定义 SHA1 黑名单，并可指定其动作包括（阻止，隔离，记录）
			同时支持支持扫描例外目录和扫描例外文件
		客户端基础功能	支持两种以上安装方式，包括安装包部署、浏览器部署；
			支持以“普通模式”和“调试模式”收集客户端的故障信息，可以将收集的故障信息方便地反馈至安全厂商的服务人员进行故障排查分析。（提供原厂截图并加盖供应商公章）。
			可支持客户端在线实时迁移至指定的另一台服务器（提供原厂截图并加盖供应商公章）。
			▲支持客户端基于 IP 地址端的自动分组，将满足条件的客户端自动分组（提供原厂截图并加盖供应商公章）。
			▲可设置离线天数后的客户端自动删除，即时回收授权（提供原厂截图并加盖供应商公章）。
			支持客户端的防卸载功能，避免用户自行卸载，管理员可设置卸载密码
			支持客户端的防退出功能，避免用户恶意退出，管理员可设置退出密码
			可提供命令行方式远程连接到目标终端，支持的命令包括但不限于查看进程，网络连接，查看目录和文件，删除文件，结束进程等
		更新基础功能	支持在线、离线两种更新方式；
			支持预设更新，可以设定更新频率为每小时、每日、每周、每月；
			支持客户端自定义代理服务器配置，满足灵活更新需求
			支持指定单个或多个客户端做为更新代理，并可指定某特定 IP 地址段的客户端从其他客户端获取更新（提供原厂截图并加盖供应商公章）。
			▲支持管理员选择客户端立即更新或回退至上一版本（提供原厂截图并加盖供应商公章）。
			支持服务器端病毒码及引擎的还原功能；
			支持 IOC，IOA 情报的单独更新和各自版本信息
		日志基础功能	具有病毒日志查询与统计功能，可以随时对网络中病毒发生的情况进行查询统计；
			支持按日志类型分别设定日志保留时长，支持的日志类型包括：病毒日志，防火墙日志，高级威胁日志，调查分析日志，系统日志，黑名单日志，外设管控日志，进程管控日志，违规外联日志，终端审计日志
			针对客户端防病毒感染情况进行监控，并进行邮件通知。
		其他	提供产品生产原厂出具的 3 年质保授权书复印件并加盖供应商公章。
	防病毒	支持系统	Windows XP/7/8/8.1/10/11、Windows Server

	系统（2WIN 系统）		2008/2012/2016/2019
		安全防护	产品支持基于程序行为评估其可信度，并阻止未授权更改；
			产品支持多种（不少于五种）扫描引擎，所有防毒引擎必须为自主知识产品非 OEM 产品；
			▲产品支持三种以上扫描方式，且每种扫描方式应支持灵活的处理配置策略（不少于七种病毒类型）定制处理措施；（提供原厂截图并加盖供应商公章）。
			产品支持多种处置措施，以保证对于文件多种处理的可选择性，处置措施包含但不限于：清除、隔离、删除、不予处理、拒绝访问；
			产品应支持客户端选择云安全扫描和传统病毒码扫描两种运行方式；
			▲产品需支持检测全局可疑站点（C&C）识别，并提供记录或者阻止的处理措施；（提供原厂截图并加盖供应商公章）。
		防火墙	▲产品需具备主机入侵检测防护能力；（提供原厂截图并加盖供应商公章）。
			产品需支持终端根据源 IP（支持 IPv6）、目的 IP（支持 IPv6）、源端口、目的端口、应用程序及注册表项，出站、入站等进行策略配置；
		移动设备防护	产品支持对插入移动设备内的所有文件进行安全检测；
		web 防护	产品具备 Web 信誉评估功能，包含 HTTPS 通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新；（提供原厂截图并加盖供应商公章）。
		客户端	产品支持多种客户端安装方式，包括但不限与：打包安装、MSI 安装、浏览器安装、远程安装、登录脚本安装、UNC 安装；
		爆发阻止	▲产品支持病毒爆发防御功能。当最新病毒爆发时，可在病毒代码未完成之前自动对企业网络中的病毒传播端口、共享等进行关闭，切断病毒传播途径，预防最新病毒的攻击；（提供原厂截图并加盖供应商公章）。
		漏洞弱点扫描	产品具备 CVE 漏洞弱点扫描功能，防护经由网页/电子邮件下载文档时被扫描利用；
		勒索软件防护	▲产品具备勒索软件防护功能，需阻止勒索软件关联的进程，需具备检测到勒索行为前自动备份和恢复文档的能力；（提供原厂截图并加盖供应商公章）。
		更新升级	产品支持更新代理功能，可将客户端设置为更新代理服务器，指定其他客户端从更新代理服务器更新组件、域策略；
			产品具备客户端并发更新数量的控制功能，可按不同时间段进行更新并发限制；
			产品具备病毒码及扫描引擎还原功能，可将服务端、客户端的病毒码及扫描引擎还原至上一版本；
		其他	提供产品生产原厂出具的 3 年质保授权书复印件并加盖供应商公章。

7	网络可视化运维综合管理系统	系统平台	1、 基于 Java 平台开发，部署在 Windows 国产化中标麒麟、UOS 等操作系统。B/S 模式。
		资产管理	1、整合的资源监控和管理模块,融监控、CMDB、报表、快照、知识库、体验化于一体。 2、▲CMDB 可以管理设备的保修和服务信息，及时提醒用户续保，展现设备的图片信息和物理信息。支持二维码扫码查看功能，扫码即可查看设备的详细情况，并且在巡检时扫二维码即可查看信息。（提供原厂截图并加盖供应商公章）。 3、提供快照功能，把网络异常瞬间的各个设备和资源的情况生成快照。
		IPV6 支持	支持在 IPv4 和 IPv6 双栈环境和过渡架构下实时监控，IPV6 单设备发现，实现统一平台监控和管理
		综合管理	1、跨厂商、跨平台，集网络设备、服务器、数据库、中间件、服务、防火墙、安全设备、光纤交换机等各种软硬件实现一体化监控，提供统一告警信息，智能的异常策略。 2、提供快照功能，用户可以把网络异常瞬间的各个设备和资源的情况生成快照，以便后续对指标和关联性逐项分析。 3、可以监控、CMDB、报表、快照、知识库、体验化于一体，无需各模块切换，支持设备的批量操作，导入、导入、删除、配置、地域、管理状态、关键状态、管理人等功能。
		网络管理	1、 对支持 SNMP 协议的交换机、路由器、防火墙、均衡负载等设备监控。 2、 监管内容包括端口状态、流量、端口错包率，端口丢包率等信息。 3、 网络设备接口监控，实时检测每个端口的上下行速率利用率 丢包率 包长等,自动识别端口所属 VLAN,及与上联设备的连接关系和容量。
		面板展现	直观展现设备真实背板情况及设备接口的连接信息，可以对设端口进行实时查看、打开和关闭等操作，能及时查看各个端口的基本信息,接口列表可监控指标当前值。当某个交换机出现异常速率或者异常流量时，能够提醒及时把相对应的端口宕掉。
		服务器管理	支持监控多种主流操作系统，包括 Windows、Linux AS、AIX、Solaris、HP-UX 等。操作系统的详细信息，包括多个 CPU 中每个 CPU 的实时负载情况。 ▲硬件管理监控，主板、CPU、内存、系统磁盘、风扇状态、电源状态、网卡状态等硬件监控。支持通过自定义 SNMP OID 脚本，采集特殊的服务器特殊指标项。支持通过自定义 SNMP OID 脚本，采集特殊的服务器特殊指标项。(提供原厂截图并加盖供应商公章)。
		数据库监控	1、支持的数据库类型 sqlserver2005,sqlserver2008,sqlserver2012,oracle、mysql 等。 2、对表空间进行容量规划，表空间的使用情况进行定期分析和预警；实时监控当前数据库连接、监听器的管理并能够在连接数据

			库出现问题时告警；对数据库的碎片情况进行监测；对 SQL 的执行效率进行分析； 4、数据库的监控包括配置的连接监控、语句的执行情况监控、数据库的性能及其阀值的监控。 5、数据库监视器实例对数据库连接失败、执行语句失败、性能阀值越界产生报警事件。
		中间件监控	1、支持的中间件类型 tomcat ,DB2,IIS,apache,tuxedo, jboss, weblogic, websphere 等。 2、通过模拟监视和性能指标两种方式进行：实时监控当前中间件的连接响应时间、监听器的管理模式，能够在连接中间件出现问题时告警检测。监控中间件的响应时间、请求数、传输速度、内存总数、连接数、收到字节数、发送字节数、总请求数、发生错误请求数等等诸多指标，并可直观了解所在服务器的性能和使用情况
		服务管理	监控网页、邮件、文件、DNS 等服务 ，监控响应时间、状态码、服务健康度、可用率、日志分析。服务应用运行情况监控以及服务管理等内容监控
		指标系统	1、提供指标系统，包括通断指标、性能指标、扩展指标、安全指标、自定义指标、复合指标、配置指标等等。 2、设置不同类型指标的轮询周期、阈值、异常策略、告警方法、异常过滤方法和告警过滤方法。 3、支持设置多阈值策略，可设置交集或并集阈值策略，以适应多种设置场景以避免遗漏特殊告警。 4、用户可以自定义 SNMP 采集器、SQL 采集器、Tcp 采集器来采集各种系统的各个实时指标，并在拓扑图、实时运行情况等等界面展现。 并能提供实时健康度和可用率等等服务水平相关指标。 ▲5、支持指标轮询周期、阈值和异常等级、告警方法、异常过滤和告警过滤。可自定义 ssh、telnet、SNMP、tcp、SQL、ping 取值，SSH 取值和 TELNET 取值在同一模块中，提供 SSH 和 telnet 取值模版和方式不低于 15 个模版，snmp、sql 模版不低于 5 个（提供原厂截图并加盖供应商公章）。
		▲模板管理	1、提供通过“模板”来设置指标轮询周期、阈值和异常等级、告警方法、异常过滤和告警过滤（提供原厂截图并加盖供应商公章）。 2、通过模板设置通断指标、性能指标、扩展指标、安全指标、自定义指标、复合指标和配置指标等等（提供原厂截图并加盖供应商公章）。 3、提供各种内建模板，包括 SNMP 网络设备模板、Windows2003 模板、Windows2008 模板、LinuxAS4 模板、LinuxAS5 模板、HP-UX 基本模板、HP-UX 告警模板、AIX 基本模板、AIX 高级模板、防火墙模板、Oracle 数据库模板、SQLserver 数据库模板、各中间件模板等等（提供原厂截图并加盖供应商公章）。
		智能基线	1、采用大数据分析和 AI 自动学习能力，根据历史运维数据自动生成标准基线，形成高负载与低负载的运行规律。

			2、系统提供智能化模板告警策略，根据各自设备自动建立基线数据。 3、基线告警后，系统在详细页中展示过去的历史曲线，定位故障点第一时间数据。
		拓扑展示	1、自动生成物理拓扑图。支持自定义灵活部署物理、示意、业务、及机柜拓扑图等，以可视化动态展现资源的结构分布、链路关系、性能指标和运行状态等，并能通过颜色策略、动态流量、告警提示变化来表示每个资源的异常等级 2、布局至少包括（径向类、树状、坐标类、蜗牛状等）类型，图片布局至少包括（图片类、矢量图元、图片鱼眼、小圆点类、小圆点鱼眼等）类型，链路样式至少包括（默认、直线、流量光速、方向箭头、方向气球、正交、流模式、贝塞尔曲线、磁线）等类型。 ▲3、拓扑支持分层分级展现，支持收缩设置父子级的关系，可快速进入下线拓扑，方便运维人员进行操作及查看，同时支持在同一拓扑图中，支持建立分区，分组，收缩和展开，以及链路合并功能，且能够在收缩的情况下，看到下级的异常情况，并指示灯和数字提醒。拓扑图支持鹰眼功能，方便大环境平移直观查看。（提供原厂截图并加盖供应商公章）。 4、支持页面添加文字和区域框并自动拉伸，以及颜色调整，支持各行业和各省地图背景专业图库，适用于多种场景，并支持上传图元背景。
		个性化定制	1、在一个页面上提供系统总览、异常一览、报表一览、我的关注。把多个重要的监控类型设为我的关注，显示这些设备的实时运行情况和历史运行情况。 2、▲提供“我的”界面。在一个页面上配置多个组件，支持第三方界面直接嵌入。可以自行定义页面轮换间隔时间（如 15 秒、30 秒、40 秒、1 分钟、2 分钟、3 分钟、5 分钟）。（提供原厂截图并加盖供应商公章）。 3、系统可以自动在多个界面自动轮换，包括整体页面、我的页面、故障页面、分析页面。提供换肤功能，至少 4 种不同界面风格。
		告警方式	1、支持多种告警方式，消息框告警，声音，短信，邮件等方式并进行多种组合。 2、平安通知，系统自带自检测功能，可定时通知网管平台运行情况，做到平台稳定性自检测，确认网络故障信息及时通知用户
		异常处理	1、可自动判断偶然波动，避免误报事件 2、对不同的异常和告警生成过滤条件并进行过滤 3、系统在一段时间内对连续性的同一故障只报一次警，避免告警风暴 4、支持故障智能依赖树配置，找出故障真正的来源，系统能够通过异常依赖树智能分析各个异常间的逻辑关联关系，提供根本原因分析
		报表和订阅	1、报表系统支持自定义和内建报表模板，模板可以分为内建、公

			共、个人、共享模板； 2、报表支持订阅、退订； 3、报表种类有日周月年报表和快照报表和一日内不同时段报表； 4、运行周期有一次性报表和周期性报表。
		分析和统计	1、报表可以实时统计分析每次轮询数据、30 分钟统计、2 小时统计、日统计等多种实时统计和数据保存。 2、同时展现各指标的轮询统计数据，分成日周月年曲线进行图形趋势分析。 3、自定义时间段分析各个指标的历史情况。 4、支持多设备多指标分析，用户可以对多个设备的多个指标在指定的同一个时间段内进行对比分析，并导出到 Excel。
		智能巡检	1、支持按不同巡检内容和设备制定周期性的定点智能巡检,自定义添加检测点,构建巡检规则。 2、以模板规范标准值为依据,根据预设的要求进行数据采集,进行自主分析判断,进行定期巡检。 3、以报表的形式直观反映巡检结果,将巡检异常状态以告警灯形式展现,快速反映本次巡检的异常，越界次数、标准值和当前值的差异性,系统会定期生成并主动发送运维人员。 4、支持对系统监控巡查的整体进行评价和备注说明,导出多种格式向领导汇报。
		故障分析	1、系统可以方便用户实时查看系统中的不同异常类型，并能筛选出不同状态 2、在查看和筛选时，同一屏幕上，可以通过立体饼图和立体柱状图动态展现不同等级和不同种类异常的各项分类数据和总数。
		个性化定制	用户可以通过个性化设置，简单在界面上定制用户的单位名称、系统名称
		地域和权限管理	1、不同的操作员角色应可以灵活的分配展现内容，不同角色的操作员登录后只展现该角色权限允许的监控管理界面。
		日志管理	记录设备管理用户登录登录设备成功或失败信息，包括登录名、登录结果（失败原因），登陆时间，日志类型等，日志可以导出到 Excel 表格中。
		系统备份与恢复数据维护	1、支持检测和查看数据类型的范围和容量。支持数据备份结束以客户端和消息进行通知。支持下载数据到任何终端。通过核心数据存储设置，自定义保留用户最为关心的数据指标。 2、▲支持一键备份与定时备份功能。支持一键恢复和上传数据恢复。（提供原厂截图并加盖供应商公章）。 3、对系统性能数据、异常数据、报表数据、日志数据进行当前容量的检测，并可设置超过阈值告警方式，执行立即清理功能。
		大屏幕展示	1、可视化数据实时采集，数据处理、数据分析、数据异常等相关性，帮助用户解决业务问题。采用炫酷的动态图形展示，将概览统计，核心资源监控、趋势分析、雷达分析、TOPN、拓扑图、业务雷达图、系统运行情况（繁忙度和响应时间，下属状态），服务器运行状况、中间件数据库运行状况、网络运行状况、机房运

			行状况、安全告警状况等等，以动态方式在展示中心多个或单个可视化数据集中展现。 2、▲灵活部署和多屏展示，支持不同分辨率，可根据多屏或单屏自定义配置多个界面，灵活部署在各类拼接屏或单屏轮换，进行自定义轮播展示。内建数据展示 12 个以上模板智能匹配，根据不同的行业满足用户业务、IT 资源、网络结构等各场景的展示需求。（提供原厂截图并加盖供应商公章）。 3、支持不同分辨率及滚动式展示平台，采用炫酷的动态图形化，提供系统总览、业务数据 3D 展示组件和动效素材，轻松搭建专业水准的可视化应用展现。
		网元数量	可管理网络设备、服务器、数据库、中间件、服务资源、网页资源、安全设备管理 60 网元。
		测试要求	中标人在签订合同前需到实地考察网络情况，并根据招标要求提供最新软件对以上功能进行逐一测试，测试通过方可签订合同。如测试不通过，采购人可取消中标人中标资格并追究相关责任和赔偿。
		原厂商服务	提供产品生产原厂出具的 3 年质保授权书复印件并加盖供应商公章。 原厂商产品为具有自主知识产权的国产网管系统。 国产化认证证书不少于 15 个。 产品厂家要求具有 ITIL 认证工程师证书 3 名，并在投标时提供相关认证证书扫描件并加盖供应商公章，并由原厂工程师完成实施和后续服务。
附	网络机柜	42U，600*600，九折型材，配 8 位国标排插组件 1 套，固定板 3 块，风扇组件 1 套(配 2 只风扇)；重型脚轮 4 只，M12 支脚 4 只，M6 方螺母螺钉 20 套，内六角扳手 1 只，机柜前门为玻璃门,后门为钢板门。	
	专业技术服务		
8	等保测评费用		工作网等级保护三级的测评服务费
9	漏洞扫描服务		针对主机系统、WEB 应用、弱口令等开展漏扫服务，不低于 1 年 4 次漏扫服务
10	应急响应服务		针对突发的安全事件时，应急响应实施人员及时采取行动限制事件扩散和影响的范围，限制潜在的损失与破坏。并在此基础上，安全服务实施人员协助检查所有受影响的系统，排除系统安全风险并协助追查事件来源、提出解决方案、协助后续处置。
11	全流量分析服务		对全网进行全流量分析，并提供分析报告，便于技术科对单位网络的整体健康状况有个全面的了解。
12	系统集成服务		对整个项目所涉及到的产品提供安装调试以及 3 年质保，维保等服务