一、资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求：

2.1、所采购产品需符合国家节能环保要求。结合本项目具体情况，根据财政部的相关规定符合政府采购促进中小企业发展政策的供应商为小、微型企业，产品有环境标志认证证书或节能标志认证证书的依据规定给予评审优惠 。

2.2、监狱企业及残疾人福利性单位视同小型、微型企业，享受预留份额、评审中价格扣除等政府采购促进中小企业发展的政府采购政策。

3、有效的工商营业执照副本扫描件、税务登记证副本扫描件、组织机构代码证副本或“三证合一”的营业执照副本扫描件。

4、法定代表人参与报价须提供法定代表人身份证扫描件，委托代理人须提供法定代表人授权委托书及委托代理人身份证扫描件。被授权人须为公司法人或正式员工，需提供该公司为其缴纳的近三个月社保证明扫描件。

5、单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。除单一来源采购项目外，为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

6、供应商不得为“信用中国”网站（www.creditchina.gov.cn ）中列入重大税收违法案件当事人名单的供应商，不得为“中国执行信息公开网”（http://zxgk.court.gov.cn/）中列入失信被执行人，不得为中国政府采购网（www.ccgp.gov.cn ）政府采购严重违法失信行为记录名单中被财政部门禁止参加政府采购活动的供应商（处罚决定规定的时间和地域范围内）。信用信息截止时点为有效期内。

7、报价中所有安全产品及软件产品需提供原厂商售后服务承诺函及厂商授权书加盖厂商公章一并上传。

8、该项目涉及到我院二甲复审和4级电子病历评级任务，要求工期在2022年5月15日前完工验收并取得第三方测评机构出具的信息安全等级保护三级测评报告，成交确认后，乙方应向甲方支付成交总价5%的保证金，作为乙方认真履行询价公告条款和售后的保证。缴纳账号：869010012010101890619，开户行：麦盖提县农村信用合作联社营业部，名称：麦盖提县人民医院，行号：402894800017。缴款备注“保证金”和询价单编号，例如：保证金32020103093700050。乙方没有履行本次询价约定的责任和义务所需承担的违约金、赔偿金及其他费用，甲方有权直接扣除保证金并终止合同并投诉采监部门。

关于保证金退还（如有）自合同约定的质保期届满后10个工作日内由甲方无息返还给乙方。

9、本次询价因涉及到等级保护机房改造建设及部分房屋改造，参与报价的供应商可来现场了解我院此次项目的现场环境（以防报价成交后无法供应和提供服务）。报价前可安排技术人员来现场勘察实际情况（现场勘察时间：询价发布之日起至本次询价结束前的1小时）全天24小时采购单位工作人员无条件配合勘探人员勘探并开具勘探证明，现场勘探地址：新疆喀什地区麦盖提县麦盖提镇文化路32号麦盖提县人民医院，联系方式：本次询价公告中的联系电话与联系人。报价时请一并上传踏勘证明，未参与现场踏勘成交后无法供货或提供服务，延误我院等级医院评审和病历评级，我院将投诉至采监部门。

10、本次采购含我院数据库调优集成服务。

二、产品清单

序号	产品名称	数量
1	整体装修	1
2	入侵防御系统	2
3	桌面安全管理系统	1
4	上网行为管理系统	1
5	核心交换设备	1
6	数据库防火墙	2
7	态势感知及溯源分析系统	1
8	负载均衡	1
9	堡垒机	1
10	数据可视化分析统计系统	1
11	漏洞扫描	1
12	智能工单与资产管理系统	1
13	信息安全等级保护测评（三级）	1
14	机房整体搬迁与数据迁移	1

三、详细招标参数

1、机房部分

整体装修		
技术指标	指标要求	数量
机房装修	数据中心机房一间 100 平米，需用机房专用高密度静电瓷面地板，墙面需采用专用机房墙板。区域按照信息安全等级保护三级要求用钢化玻璃进行隔断。提供机房操作间控制台工位及相关设备。提供不少于 80 寸液晶显示器 2 个用于动环及可视化展示。需提供区域舒适型 3P 空调 2 台,5P 的 1 台。提供不少于 27 个专业机柜（1200*60*2000mm，每机柜配置不少于 2 个 32A PDU）。提供机房防雷装置。提供不少于 64 口网络 KVM。整体机房必须按照等级保护 2.0 三级标准物理安全所有项建设。	1 批
机房外区域装修	6 个工作间及楼宇墙面采用高密度复合材料墙板。对整体机房楼宇区域进行二次封闭并提供双向刷卡（指纹、密码）门禁系统。（其中包含建设所需的主材、门、辅材、运输、安装、人工等费用）	1 批
链路铺设	完成数据中心机房到各楼宇间光纤链路及电力线路建设；完成数据中心机房整体静电网格及单独静电室外接地（其中包含建设所需的主材、辅材、运输、安装、人工等费用）	1 批
精密空调		
规格要求	制冷量：35kw，显冷量：37.6KW，循环风量 10000m3/h，加热能力：21KW，加湿能力：8KW，尺寸：900*995*1975，下沉式送风；高效、底噪的柔性斡旋式压缩机；高精度电子膨胀阀精确制冷、高效节能；7 英寸超大触摸显示屏；温湿度曲线直观显示；图像化直观显示各部件运行状态；多级密码保护，分级授权管理；显示器可调阅多条历史告警；可群控 32 台机组，轻松组网；标配 RS485 接口，支持 ModBus 协议。采取下走风。	2 套
UPS 系统		
技术要求	模块化 UPS 系统是由：功率模块（2U）、旁路模块（3U）、系统监控模块（1U）、机柜以及电池组构成；先进的双核 DSP 数字化控制技术，整流和逆变采用双 DSP 控制；风扇转速随温度智能变化，可降低噪音，延长风扇的使用寿命；完善的软硬件保护功能，超强的自诊断功能，丰富的历史记录；支持 30-46 节电池，可灵活配置电池节数，节省客户的投入；7 寸触摸彩屏显示，友好的人机界面；模块化设计，所有模块均支持热插拔功能；输入电压可变范围：	1 套

	305~485Vac（不降额）；138~305Vac（ 40%~100%负载之间线性降额）；输入频率变化范围：40~70Hz；输入功率因数：≥0.99；输出功率因数：输出额定电压：380Vac/400Vac/415Vac；输出频率精度：市电模式：同步状态下跟踪旁路输入；电池模式：50Hz/60Hz ±0.1%；逆变过载能力：105%＜负载≤110%，60 分钟后转旁路；110%＜负载≤125%，10 分钟后转旁路；125%＜负载≤150%，1 分钟后转旁路；负载＞150%，0.2 秒后转旁路；保护功能：输出短路保护、输出过载保护、过温保护、电池低压保护、输出过欠压保护、风扇故障保护等；通信接口：标配：RS232、USB、RS485、CAN、NET、并机、LBS、输入输出干接点、SNMP 卡功能、EPO 和电池温度补偿接口；	
功率模块	25KVA/25KW,	
蓄电池	12V200AH 不少于 64 节	
电池架	放置 32 节 12V200AH 蓄电池	
电池开关盒	电池组开关	
UPS 输入输出配电箱	250A3P 一个，200A3P 三个，国产开关	
电池组至主机	UPS 主机和电池架在同一房间	
设备底座	1 个 UPS 主机底座、1 个配电箱底座	
精密列头柜	按照现场所需配备响应的开关	1 套
环境动力监测		
技术要求	配备管理主机、含有系统管理平台，包含声光、短信报警，含有温湿度、烟感、漏水、电力、空调、消防、视频监控等模块	1 套
消防系统		
技术要求	按照机房实际需求提供七氟丙烷自动消防系统	2 套

2、安全产品

入侵防御系统		
技术指标	指标要求	数量
系统架构	系统架构	2 台

	产品应采用 2U 专用机架式硬件设备，1+1 冗余电源，系统硬件为全内置封闭式结构	
硬件架构	基本网络接口 千兆电口*6,2 对千兆电口 Bypass ,万兆光口*2	
性能要求	吞吐能力：吞吐量≥10000Mbps， 防护能力≥12000M， 并发 TCP 会话数≥1000 万。	
部署能力	部署模式 透明部署（基于透明网桥），需即插即用，无需做任何配置即可防护。支持旁路部署。 策略路由（支持流量牵引）	
	检测引擎：高性能攻击特征检测引擎	
	防护规则 系统提供完善的内置规则 提供高度灵活的自定义规则向导，适用于高级用户	
安全特性	规则数量≥24000 条（提供界面截图） 基本攻击拦截能力：支持拦截对操作系统、数据库、邮件服务、FTP 的攻击 病毒过滤：支持过滤病毒、木马、恶意软件通讯行为,病毒库≥8000 条。（提供界面截图）； DDOS 防护：TCP/UDP Flood 防护，基于最大上限阀值设置，而非 DDOS 特征库（提供界面截图）； 上网行为管理：识别应用库不少于 500 种，并能够对其进行访问控制（提供界面截图）； 支持恶意域名防护策略,能够对色情/赌博/钓鱼/黑客/欺诈/违规类别进行域名区分，并提供访问控制（提供界面截图）； 基本访问控制：基于规则、来源/目的 IP 的、来源/目的端口、时间 ACL NAT：支持源 NAT、目的 NAT、静态地址 NAT； 规则冲突检测：支持对已有的访问控制规则进行冲突检测，发现重复的访问控制策略，帮助用户优化访问控制策略，去除冗余条目。	
网络自适应能力	802.1Q 支持：支持 VLAN 解码，在 Trunk 线路上部署并提供防护 端口汇聚（Trunk）：支持端口汇聚（Trunk），显著提高设备间的吞吐能力（提供界面截图）； 路由配置：支持静态路由的配置；	

报表功能	报表类型：安全报表（入侵统计、按入侵类别统计、被攻击主机、攻击来源 IP 和地理位置、网络接口流量趋势）； 报表查询：按事件类型、统计目标或周期类型条件进行统计； 输出格式：支持将生成的报表以 HTML、Word 等通用格式输出；	
日志系统	日志类型：系统日志、审计日志和安全防护日志（入侵记录、攻击源 IP 所处地理位置、网络流量） 日志查询：可基于时间、IP、端口、协议、动作、规则、规则类别、危害等级、等条件进行日志查询。 日志管理：日志导出、清空、自动磁盘日志清理；	
系统监控	监控类型：安全事件监控、访问情况监控、设备负载监控 系统信息：显示网络接口状态，引擎状态、系统 CPU、内存及磁盘使用率	
系统诊断和调试功能	维护工具：抓包工具，可抓取的网络原始报文，用于分析网络状况 配置备份与导入：支持系统配置的备份与导入功能	
高可用性	HA 双机：支持主从部署模式；支持链路是否正常的监控。支持双机配置自动同步；硬件 BYPASS 内置 bypass 模块，设备故障直接切换到 bypass 模式。	
资质要求（提供相关资质复印件，生产厂商盖章）	涉密资质 获得国家保密局涉密信息系统安全保密测评中心颁发的符合国家保密标准 BMB13－2004《涉及国家秘密的计算机信息系统入侵检测产品技术要求》的《涉密信息系统产品检测证书》，并出具加盖厂商公章的复印件。	
	强制认证 获得中国信息安全认证中心颁发的符合 ISCCC-VP-123 要求的《IT 产品信息安全认证证书》，并出具加盖厂商公章的复印件	
	CNNVD 兼容性资质证书 获得中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》，并出具加盖厂商公章的复印件	
	应急支撑证书 设备生产厂商具备 CNCERT 颁发《网络安全应急服务支撑单位证书》，并出具加盖厂商公章的复印件 设备生产厂商至少为省级互联网应急中心网络安全信息通报成员单位，并出具加盖厂商公章的复印件	
	厂商实力	

	设备生产厂商应具有符合 GB/T 19001-2016/ISO 9001:2015 标准的《质量管理体系认证证书》，并出具加盖厂商公章的复印件 设备生产厂商应具有漏洞发现能力，具备《中国国家信息安全漏洞库（CNNVD）技术支撑单位资质》，至少曾经获得中国信息安全测评中心颁发《中国国家漏洞库-信息安全漏洞提交证明》，并出具加盖厂商公章的复印件 .设备生产厂商具备中国信息安全测评中心颁发的《国家信息安全测评 信息安全服务资质证书》（安全工程类一级）资质，能力范围包括：安全风险评估、安全需求分析、安全方案设计、安全集成、安全监控和维护等，并出具加盖厂商公章的复印件	
售后服务支持	技术支持服务上述硬件平台、所有软件功能模块提供三年原厂保修和升级服务。为应对网络安全事件，报价方应成立 WEB 安全应急处置小组进行紧急响应，响应时间：7×24 小时响应。	
桌面安全管理系统		
技术指标	指标要求	数量
基础要求	具有独立的自主知识产权的一体式机架结构硬件产品，不接受 PC SERVER 系统架构。必须为专用操作系统，非通用 Linux 系统或 Windows 系统。支持多级级联架构，满足分级管理要求。	1 台
硬件指标	1U 机架结构；单电源；标准配置 6 个 1000MBASE-T 接口；每秒事务数（TPS）：≥1000（次/秒），最大吞吐量：≥500Mbps，最大并发连接数：1000（条）；不得少于 500 授权。	
高可用性	必须具备 HA 模式，支持与原有设备 HA，需支持主备机心跳 IP 检测及虚地址管理模式。支持多级级联架构，满足分级管理要求。 支持负载均衡集群方式部署，支持超过 10 万点以上的终端点数。	
强制技术	支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面。 可支持端口镜像准入技术，通过对交换机镜像数据的实时分析，能够及时发现并阻断非授权终端的接入。 单台准入设备可支持至少 2 个核心交换机进行策略路由准入控制。	
定向引导	支持终端入网 IE 重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持 http 代理及多重重定向引导。 可根据用户的实际环境自定义非 80 端口的 Web 服务端口号及用户重定向引导。 能通过浏览器完成身份认证、客户端安装、设备注册、安全检查、检查结果展现等全流程引导管理。	

资产采集	自动采集各计算机的 IP 地址、计算机名、MAC 地址、网卡型号和生产厂商、计算机所在域、操作系统、主要硬件、软件信息。 能够提供计算机信息综合查询报表。	
硬件资产	能够对终端硬件初始记录、最新记录和变动记录形成报表，支持对硬件变动进行报警，并且能够查询变动的历史。	
软件资产	支持对软件资产进行实时统计，能够灵活指定必须使用的软件资产和禁止安装的软件资产，支持对软件变动进行报警，并且能够查询变动的历史。支持对终端违规安装的软件进行卸载;	
IP 地址资产	可通过矩阵图的方式自动进行网内 IP 地址的展示。 可通过颜色不同 标识出该 IP 的状态：未分配、开机、关机。IP 使用历史记录：设备名称、设备 IP、上线时间、离线时间、运行时长。 （报价时提供功能截图）	
软件使用管理	支持以软件为单位，审计使用的时间和次数。 支持以软件为单位，限制软件的打开和使用。	
Windows 安全登录	可以与用户已有认证系统（UKey、LDAP 等）相结合实现 Windows 系统安全登录与身份认证（替代 Windows 本地用户/密码认证模式）。	
杀毒软件	支持至少 18 种杀毒软件的检查。 能够区分版本不合规、病毒库不合规，提供自动下载程序修复和网址引导修复。	
系统配置安全	能够建立终端设备的安全性评估任务，支持对帐户密码安全性、屏保设置、共享安全、系统服务、进程及服务等项目进行检查、评定，对存在安全风险的终端支持实时自动修复。 支持终端安全状况图形化展示，能够显示每台终端的详细风险信息并提供评估得分的统计报表。	
重要进程管理	能够统计网内运行的所有进程，支持设置黑白名单指定禁止或允许的进程，支持进程 MD5 值识别方式，防止更改或伪造进程。	
进程运行分析	能够对指定进程的运行情况进行跟踪并以表格方式展现分析结果	
异常进程监控	能够对指定进程运行情况进行保护，防止进程被非法结束。	
私设网站检查	可设置终端主动进行网段内私设 WEB 站点的扫描。 可扫描浏览器是否有上网的历史记录。	
私设代理	管理员可设置策略禁止终端设置代理。	

控制	管理员可为被管控终端在管理系统后台设置指定代理、端口号，终端用户无感知。	
流量控制检查	可对上传、下载流量、总流量、发包频率、TCP 连接数、UDP 监听端口数进行控制。	
软件黑白名单	支持对终端应用进行控制管理，支持建立软件黑名单和白名单，强制终端只能在管理策略允许的范围内安装应用。	
软件分发	能够支持可执行程序、MSI 安装包或者文档数据文件自动下发与安装。能够支持指定组范围、指定时间进行安装并提供程序打包工具。能够自动统计分发成功率及软件安装成功率，支持进程、注册表、安装路径等多种参数判断方式。 支持根据操作系统不同分发不同升级包，提高软件分发功能对操作系统系统的适应性；	
远程协助方式	管理员计算机与被管理计算机采用专用 tcp 端口进行直接连接，远程协助时不占用服务器端口资源。 远程协助支持双向穿透 NAT 或 VPN 的远程屏幕控制。	
远程协助功能	支持实时查看远端计算机的操作进程、服务、系统日志等信息。 支持对远端计算机进行关机、重启、断网等管理。 对远端计算机远程查看和远程控制，可根据管理需要灵活配置是否强制管理还是授权管理。 支持对远端计算机进行文件级远程管理，可在用户无感知的情况下远程创建、重命名、拷贝、删除文件。 远程查看、远程控制可以根据管理需要和网络状况，选择、配置适合管理员的窗口分辨率、显示比例、色彩、鼠标按键、光标等。 权限管理员支持限制操作管理员远程控制的权限，是否允许强制查看、控制和文件传输，允许指定必须申请管理的终端列表。 支持终端向管理员主动发起远程请求。	
远程开机	支持远程开启计算机，支持定时、批量开启计算机。	
网络适应性	支持各种网络环境的终端管理，包括同一网段、单方处于 NAT 子网中、双方各自处于不同的 NAT 子网中、处于 VPN 环境中。 支持自动穿透管理计算机的防火墙设置。	
多方管理	支持一台计算机接受多台计算机同时维护管理。 支持一台计算机同时管理控制多台计算机。	
外联行为控制	能够检测出通过代理等方式产生的外联行为并进行报警阻断，在内网设备带出外网的情况下同样能够检测出上述外联行为并进行违规行为上报或者阻断。	

	支持仅断开与网络连通的网卡 支持配置终端可访问的外网 IP 和域名 支持禁止 DNS 域名解析服务，并支持配置白名单。	
违规访问控制	能够控制终端只能访问外网或只能访问内网，能够以策略方式按照区域、部门、组、ip 段或单台设备设定内网访问范围。 能够对违规网络访问行为进行报警和阻断。 支持内网设备带出后在访问外网时自动进行阻断和违规行为上报。	
网络代理使用管控	能够从网络协议层面检测网络代理的行为，支持基于网卡数据包的代理数据阻断功能，并支持报警、断网、锁屏等强制控制措施。 支持检测 Windows 的代理配置选项，检测不符合要求的代理配置情况，并支持自动清除、报警、断网、锁屏等强制控制措施。 代理行为的管制支持例外合法的代理地址。	
网络配置绑定	能够实时监测终端 IP 地址、MAC 地址、DNS 配置等相关网络信息，支持对应信息的实时绑定，当 IP 或 MAC 发生改变时能够强制恢复至修改前。管理员可以授权部分用户修改 IP 地址；	
外设管理	能够禁用终端设备的 USB 接口、光驱、软驱、打印机、调制解调器、串并口、1394、 红外、蓝牙及 PCMCIA 卡等外设接口。 能够单独禁用 USB 移动存储设备而不影响其他 USB 设备。 支持对手机的管控；通过外设使用控制策略，可以保证手机插入电脑后，不能把文件拷贝到手机	
反 ARP 欺骗	支持网关、关键服务器等 IP、MAC 的静态绑定，从而免受 ARP 的欺骗攻击。能够实时检测 ARP 欺骗的病毒源，能够对有 ARP 攻击的终端设备进行隔离。	
主机防火墙	能够提供基于协议、基于 IP 和端口、Ping 共 3 种拦截方式。 能够设定允许或禁止主机访问的 IP 段、端口和协议。 能够设定允许或禁止某个 IP 段访问本地主机的端口和协议。	
上网访问控制	能够基于 URL 关键字设定允许或禁止终端设备访问的网站，能够对违规访问设备进行报警或阻断。	
可信主机访问	能够设置为例外可信设备，与其他安装客户端的设备通信。	
移动介质授信管理	能够禁止未注册 USB 移动存储设备的随意接入。 必须支持新 USB 移动存储设备用户在线申请、注册，管理员在线审核，无需上交信息中心注册。 能够对指定的 USB 移动存储设备进行注册，设定所属部门和使用人，并进行加密、只读和可写的控制。	

	能够控制指定USB移动存储设备在外网无法使用。 能够针对区域、部门、组、IP段或单台设备控制指定USB移动存储设备的读写权限，能够对终端和USB移动存储设备进行一对一绑定。	
移动介质安全管理	能够对USB移动存储设备中指定名称的文件进行允许或禁止访问的控制。 能够禁止访问USB移动存储设备中的可执行文件。 能够禁止USB移动存储设备的自动运行。	
移动介质审计	能够对USB移动存储介质的插入和拔出行为进行审计。 能够指定审计的设备范围，能够指定审计的USB设备，能够指定审计的文件名称和操作类型，能够对通过USB设备进行的文件拷入、拷出行为进行审计，支持按照使用设备、文件路径、操作名称、操作时间进行报表的查询。	
组策略管理	支持基于组策略的操作系统组件功能，如：禁用控制面板、禁止添加打印机、禁用任务管理器、阻止更改桌面背景、禁用注册表编辑器、阻止访问命令提示符等。 支持基于自定义工具定制组策略模板配置，可自动录制计算机的组策略配置信息，并可批量下发和批量执行。组策略模板执行的内容，在策略取消或停止后能自动回滚到执行前的配置状态。 支持定制windows组策略模板，支持批量下发，支持撤销。	
文档审计	能够记录终端用户日常的文档的操作行为，可以详细审计用户新建、拷贝、修改、移动、删除等操作行为。 支持软件过滤，只审计常用软件产生的文件变动行为。	
邮件审计	能够对用户日常邮件的收发做有效审计，审计内容包括邮件地址、邮件标题、邮件内容以及附件等，方便事后追查。	
网站审计	实时记录终端计算机访问过那些网站，并以柱状图、表单等图表方式形象的展现统计结果、访问量排行。 支持浏览器过滤，只审计常用浏览器产生的审计记录。	
刻录审计	可以通过黑白名单方式进行审计或不审计指定光盘刻录机，同时可以对指定审计某种文件格式以及所在路径的文件。	
软件商店	建立企业软件商店，里面是企业提供的来源安全的软件，并且可以限制员工下载、安装涉及版权的软件，比如设定只有设计部门的员工才能安装CAD软件，确保正版软件的授权点不被其他人占用，规范正版软件的使用 管理员可对采购的软件进行订单和授权管理，支持将采购订单导出	

	为软件正版化台账； 终端安装后，采集软件的下载、安装、使用情况，为采购计划提供参考。	
正版化管理	收集全网电脑安装的商业软件，根据其序列号判断正版软件和盗版软件 支持读取 offic、操作系统等软件的激活状态	
资质要求	公安部《信息安全产品检测报告》 公安部《计算机信息系统安全专用产品销售许可证》	
上网行为管理系统		
技术指标	指标要求	
硬件要求	1U 机箱，6 个千兆电口支持 1 对 Bypass，4 个 SFP 插槽（不含接口模块）；日志存储空间 1TB；建议适配带宽：800M，推荐用户数 800；包含 3 年系统版本升级、网站知识库及应用知识库升级许可；"必须支持 HA 模式，支持设备 HA。	1 台
支持 IPV6	满足国家 IPv6 发展“动员令”，支持部署在 IPv6 环境中，其所有功能（认证、应用控制、内容审计、报表等）都支持 IPv6（提供产品界面截图）	
告警管理	支持攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web 关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等；。	
Web 访问质量检测	针对内网用户的 web 访问质量进行检测，对整体网络提供清晰的整体网络质量评级;支持以列表形式展示访问质量差的用户名单;支持对单用户进行定向 web 访问质量检测	
共享接入管理（防共享）	设备能够发现私接路由（或者共享软件等）共享网络的行为：支持自定义配置终端数量和冻结时间，和添加信任列表；支持显示以 IP 或用户名的维度统计一段时间内的趋势图；支持例外排除功能（提供产品界面截图）。	
用户认证	支持触发式 WEB 认证，静态用户名密码认证等；支持 LDAP、Radius、POP3、Proxy 等第三方认证； 支持 ISA\Lotus LDAP\Oracle、SQL Server、DB2、MySQL 等数据库等第三方认证；支持绑定 IP 认证、绑定 MAC 认证，及 IP/MAC 绑定认证等；支持短信认证、微信认证；	
二维码认证	支持二维码认证，管理员扫描访客的二维码后对其网络访问授权	
用户密码	可设置用户密码不能等于用户名；新密码不能与旧密码相同；可设	

强度要求	置密码最小长度；可设置密码必须包括数字或字母或特殊字符；	
应用标签功能分类管	支持根据标签选择应用；支持给每个应用自定义标签；支持根据标签选择一类应用做控制；支持对每一种应用的定义和解释，帮助客户快速定位应用的分类	
应用识别规则库	设备内置应用识别规则库，支持超过 6000 条应用规则数，支持超过 2800 种以上的应用，1000 种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率； 支持根据应用的特征智能识别新更新的应用；支持根据 IP、端口、协议等自定义应用规则；支持根据不同的应用类型或具体的某种应用设置允许或拒绝。	
SSL 加密内容过滤及审计要求	针对 SSL 加密的网站、论坛发帖、web 邮箱以及客户端邮箱（如闪电邮）进行关键字过滤及内容审计。	
应用审计	支持记录 QQ、MSN 等 IM 聊天行为和传文件的内容；支持移动 APP（IOS 和 android）审计（如论坛类、微博类、新闻评论类等）； 支持金融类应用内容审计如：阿里旺旺、万德（Wind）、路透等应用的聊天内容。	
流控	支持流控通道实时可视化，能够实时看到各级流控通道的状态：包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽、优先级，启用状态等。（提供产品界面截图）；支持流控动态在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率（提供产品界面截图）；支持 P2P 智能流控，通过抑制 P2P 的上行流量，来减缓 P2P 的下行流量，从而解决网络出口在做流控后仍然压力较大的问题 持流控黑名单，基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中（提供产品界面截图）；支持流控单位，灵活配置流控单位是 IP 还是用户名（适用于公共账号：多个 IP 公用一个账号时，可以对每个 IP 进行限速，更加灵活准确）（提供产品界面截图）； 支持时间控制，基于时间段的带宽划分与分配策略；支持按日期设置流控策略，比如针对节假日设置不同流控策略；支持目标 IP 流控，基于访问行为的目标 IP/IP 组实现带宽划分与分配；支持流控策略适用多种对象，如用户、位置、适用终端、文件类型、URL 类	

	型等（提供产品界面截图）；	
报表	支持基于时间段/用户/用户组/终端类型/位置等多种维度的流速趋势报表、流控通道趋势报表、应用行为趋势报表、网站分类行为趋势报表等；支持从流量分析、时长分析、用户行为分析、网站分类分析、终端接入分析、终端接入安全等多维度下选择具体的基于用户/用户组/终端/网站/域名/应用/通道/搜索关键字等细粒度的排行、趋势等报表，整合成一个自定义报表进行订阅； 支持各细粒度报表直接拖拽进行整合成新报表，支持新建章节和预览功能。针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）（提供产品界面截图）。	
售后要求	提供原厂免费三年售后服务及 7*24 小服务，提供制造商授权书及售后服务承诺函	
交换机		
技术指标	指标要求	数量
设备参数	交换能力≥87.2Tbps，转发率≥26800Mpps，6 个业务槽位；支持主控模块冗余，主控冗余时模块间支持状态化故障切换；支持虚拟化背板堆叠，即多台设备可以统一界面管理、支持跨设备链路聚合、分布式路由等核心技术；支持 L3 MPLS VPN、支持 L2 VPN: VLL、支持分层 VPLS、支持 LDP 协议；支持 OPENFLOW 1.3 标准；支持 VxLAN；实配支持静态路由、动态路由：OSPF、BGP、IS-IS，路由条目数≥128000；实配支持 IP ACL、IP Precedence、DSCP、802.1Q/p、COS 数据流量分类和基于每个用户的服务质量策略；支持 IPv4 uRPF、DHCP Snooping、ARP 防攻击、IP Source Guard、CoPP、端口隔离、报文过滤功能，黑洞路由、黑洞 MAC；支持 802.1x/mac/Portal/Radius/Tacacs+认证；支持防火墙业务板卡、无线控制业务板卡扩展；主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔；本次配置：双主控、双电源、 48 端口千兆以太网电接口，24 端口千兆以太网光接口(SFP,LC)+4 端口万兆以太网光接口模块。光模块-SFP-GE-单模模块-(1310nm,10km,LC)。SFP+ 万兆模块(850nm,300m,LC)。	1 台
数据库防火墙		
硬件配置要求	提供软硬件一体化和标准机架式的设备：2U，配置至少 6 个千兆电口，至少 8 内存、冗余电源、硬件 Bypass 2 组	2 台
硬件性能	SQL 峰值处理能力至少 15000 条/秒	

要求	支持并发数至少 15000 条	
	可防护数据库实例数至少 16 个	
	日志存储量至少 40 亿条	
数据库兼容性	支持 Oracle、mySQL、SQL Server、DB2、Sybase、informix 等主流数据库协议的解析	
	支持 postgreSQL、Cache、Teradata、HANA 等专业数据库协议的解析	
	支持 GaussDB、达梦、人大金仓、南大通用、神舟通用等国产数据库协议的解析	
	支持主流大数据平台数据库的解析，包括 Redis、MongoDB、Hive、Kafka、ES 等	
布署模式要求	支持桥接模式、代理网关和旁路路由部署模式，并均支持数据风险操作阻断。（提供功能截图证明并加盖公章）	
	以上三种部署模式支持虚拟化部署。	
	支持 IPv4 / IPv6 网络布署。	
防护策略要求	支持内置针对 Oracle、mySQL、SQL Server、DB2、达梦等各数据库特征的默认防护策略（提供功能截图证明并加盖公章）	
	支持内置默认的刷库、拖库、撞库的防护策略（提供功能截图证明并加盖公章）	
	支持基于各类型数据库的 SQL 超级白名单功能，支持 PLSQL Developer、SQL Developer、DBArtisan、SQLPlus、Navicat、SQL Server Management Studio、Console 等客户端，超级白名单规则不少于 100 条。	
	支持加密 Oracle/MySQL 协议的解析和防护。	
	支持自定义规则策略配置及管理，可对预设条件进行阻断。预设条件至少包括访问的时间、执行时长、访问次数、访问客户端 IP、客户端操作系统主机名、MAC 地址、客户端操作系统用户名、数据库用户名、数据库实例、表、列、存储过程等、操作类型：DML、DDL、DCL、SQL 语句、SQL 字符串、SQL 语句、返回行数、敏感数据状态、关联表个数、响应状态等（提供功能截图证明并加盖公章）	
	支持 SQL 注入特征识别，支持基于 CVE 的 SQL 注入漏洞检测，支持根据内部 SQL 注入特征库进行识别并有效阻断，支持 sqlmap 注入检测。（提供功能截图证明并加盖公章）	
	支持虚拟补丁防护，内置多种数据库漏洞补丁，支持特征方式的缓冲区溢出检测规则以及其它漏洞检测规则，对外来攻击进行识别并	

	有效阻断支持，Oracle 数据库漏洞数量不低于 500 个。（提供功能截图证明并加盖公章）	
	支持数据库的动态脱敏功能。（提供功能截图证明并加盖公章）	
智能学习要求	支持基于机器学习技术对用户行为进行学习并生成基线规则，支持基线规则策略与其它防护策略同时生效。支持特征值大小控制。支持特征模型持续更新、手动修改、例外加入等操作。	
	支持对基线学习内容的特征展示和修改，特征内容至少包括数据库用户、源 IP、目标数据库 、源应用程序、主机名、系统用户名、表与操作、查询组、特权操作等。（提供功能截图证明并加盖公章）	
	支持偏离基线的行为检测，包括未授权的源 IP 特征、偏离基线的主机特征、操作系统用户特征、源应用程序特征、数据库用户特征、数据库 Schema 特征、表/操作访问特征、查询特征等。支持对于上述基线偏离行为进行风险级别和应对动作设置，应对动作支持操作 t 行为阻断并实时告警。（提供功能截图证明并加盖公章）	
日志查询要求	支持日志内容能够详尽的显示访问行为发生的具体特征，包括数据库名称、操作类型、数据库用户、操作对象、数据库 IP、客户端 IP、数据库 MAC 地址、客户端 MAC 地址、主机名、系统用户名、源应用程序、客户端端口、捕获时间、执行时长、响应状态、动作、记录方式、风险等级、匹配策略、SQL 内容、SQL 结果、SQL 模式、日志 ID、数据敏感度、返回行数等	
	支持根据日志具体特征、策略、风险等级、时间等进行条件检索，支持对实时防护数据和历史数据进行监控与查询，并支持结果导出，支持 PDF、EXCEL、WORD 等文件格式。	
	支持日志会话回放功能，还原用户的访问行为	
风险告警要求	支持以数据源和时间（年、月、日、时、分）的方式进行告警日志汇总显示和告警日志查询，支持以折线图的形式显示攻击趋势和访问来源趋势。	
	支持自定义告警的风险等级策略，包括低风险、中风险、高风险、致命四个等级	
	支持根据客户不同业务情况对告警信息进行自定义处理，包括加入基线、加入 SQL 注入例外、禁用 SQL 注入规则、阻断攻击、通过攻击	
风险扫描要求	支持根据内置策略以及数据库漏洞信息，对数据库进行风险配置及漏洞安全扫描。（提供功能截图证明并加盖公章）	

	支持对命中策略的风险生成报表	
统计报表要求	支持视图、服务器分析、来源分析、数据访问模式、特权操作、其他视图、基于时间的分析等报表类型的添加和删除操作。支持针对各类型报表进行详细内容的自定义配置。（提供功能截图证明并加盖公章）	
	支持报表自动生成和自动发送，并可生成定时和周期报表任务。	
可靠稳定要求	支持软件 byPass，设备运行时软件层面出现异常，自动透传数据库访问流量，防止单点故障。	
	支持硬件 byPass，设备断电或宕机时，自动透传数据库访问流量，防止单点故障。	
	支持主主、主备、双机、多机负载等高可用模式	
	支持旁路引流+智能路由模式保障防火墙故障业务无缝切换	
系统管理要求	支持三权分立，内置系统管理员、安全管理员、审计管理员，以满足合规要求。支持角色创建，支持针对某些功能页面进行授权。	
	支持对系统的 CPU、内存、磁盘、磁盘读写情况、网络流量、访问情况、事件统计、攻击记录、告警列表、引擎列表进行实时监控	
	支持系统配置+审计日志的全量备份 支持的备份方式：手工备份、定时自动备份、自动远程备份； 支持手工方式还原和备份文件手工、自动方式清理（提供功能截图证明并加盖公章）	
	支持系统时间手工、自动与 NTP 服务器同步，保证审计日志时间准确性。	
	支持用户登录安全设置，包括登录次数、超限锁定时间、用户会话超时等；支持导出文件密码设定。	
	支持告警配置及多种告警发送方式，至少包括 FTP、Email、syslog、SNMP。	
	支持页面方式进行系统升级和配置导入导出功能。	
	支持系统能够自动对审计进程、解析进程、存储进程、检索进程进行诊断分析，方便用户排除故障。	
	支持磁盘使用率监控，当磁盘使用率达到预定的阈值时，页面弹框提示管理员，同时系统停止记录日志或者覆盖以前的记录；支持磁盘使用率超限时，自动清理历史业务数据文件。	
	支持系统恢复出厂设置，支持页面关机和重启。	
资质要求	为了保证报价产品专业性，需提供报价产品由公安部颁发的《计算机信息系统安全专用产品销售许可证》及检测报告；	

	需提提供报价产品由中国信息安全认证中心（ISCCC）颁发的中国国家信息安全产品认证证书及检测报告；	
	需提供报价产品由国家信息安全漏洞库(CNNVD)兼容性服务认证证书；	
	为了保证报价产品安全性，报价产品厂家需具备阿里巴巴数据安全能力成熟度模型（DSMM）合作伙伴资格，并提供证书复印件作为证明；	
	为了保证报价产品专业性，报价产品厂家需具备 ZCAIA 网络安全与信息化产业联盟会员资格，并提供证书复印件作为证明；	
态势感知及溯源分析系统		
系统架构	产品应采用 1U 专用机架式硬件设备，系统硬件为全内置封闭式结构	1 套
主要功能	支持针对 IP 级别的访问控制策略，降低勒索病毒、内网渗透测试造成的内网风险	
基本网络接口	标配千兆电口≥6，每个千兆电口可以独立控制。扩展槽*2，每个扩展槽最高可扩展 8 个千兆电/光口。	
包转发率	≥ 32.7 Mpps	
交换容量	≥ 45 Gbps	
流量学习	支持对网络中的流量进行 AI 自学习，自动生成访问控制策略（提供界面截图，并加盖厂商公章）	
	自动生成基于源地址、目的地址、目的端口的访问控制策略	
	支持将学习完成的策略一键导入到访问控制策略	
	支持对学习完成的结果进行增删改操作	
	支持配置学习 IP 地址范围，IP 地址支持多个地址段的配置	
资产测绘	支持域名嗅探：支持将网络流量中的 http 域名信息（包括但不限于域名、ip 地址、端口号、网站标题、协议）挖掘并展示，同时支持以 ip 为维度进行分类。	
	支持 https 免证书加载即可探测域名信息（包括但不限于域名、ip 地址、端口号、网站标题、协议）。（提供界面截图，并加盖厂商公章）	
	支持域名嗅探结果内容以 html、docx、xls 格式导出。	
	支持自定义域名嗅探的 IP 地址范围。	
	资产详情：能够挖掘出相关资产的资产信息：包括但不限于资产的开启的端口、端口相关服务、应用版本号、网站标题、mac 地址、操作系统、主机名等。（提供界面截图，并加盖厂商公章）	

	支持以 IP 地址、服务为维度展示资产详情。	
	支持资产详情内容以 html、docx、xls 格式导出。	
	支持自定义资产梳理的 ip 范围、端口并发扫描数、应用识别并发数。	
微隔离	支持可视化方式显示隔离域内部连接关系，同时显示相关资产开启的活动端口与非活动端口（提供界面截图，并加盖厂商公章）	
	支持显示全局和隔离域视图	
	支持对隔离域内主机连接方式进行增加、删除、修改并立即呈现在可视化视图中。	
	支持隔离域视图内容（包括但不限于视图本体、资产开启的活动端口与相关服务、资产开启的非活动端口与相关服务）以 html、docx、xls 格式导出	
访问控制	支持基于源 IP 目的 IP、目的端口的访问控制	
	支持 IP 地址开放端口允许被单一或者多个地址连接	
	访问控制策略支持添加、停用、删除操作	
	访问控制支持拦截和放行策略	
	支持一键开启、关闭访问控制策略	
采集方式	多种数据采集引擎结合，支持对物理探针和虚拟化探针采集的 Web 攻击、主机入侵、诱捕流量及其它异常流量进行安全分析、关联与审计。	
	支持通过 Web 方式对平台内容进行综合展示。	
大屏展示	综合展示：展示内容包含但不限于国家地图攻击、世界地图攻击、攻击类型分布、攻击源 TOP5、危险级别分布、威胁趋势、紧急报警台等（提供界面截图，并加盖厂商公章）	
部署方式	大数据分析平台应采用 OVA 方式部署。	
	支持 KVM、VMware 等主流虚拟化平台。	
大数据分析平台的攻击行为分析与联动能力	外部攻击展示：支持对安全事件以外部攻击为维度进行 2D 及 3D 世界地图的动态攻击展示。（提供界面截图，并加盖厂商公章）	
	支持对安全事件以内部攻击为维度进行大屏展示。展示内容包含但不限于攻击源 TOP5、攻击目的 TOP5、年/月/周/日告警数、web 入侵/外部诱捕/本地诱捕/主机入侵数量、威胁情况分析、威胁数量等（提供界面截图，并加盖厂商公章）	
	支持配置本地物理位置、本地网络 IP 地址范围与掩码	
	网络行为安全分析：对各探针采集的实时数据流进行关联分析，含网络流量安全事件、日志安全事件等，采用关联性分析，深度挖掘	

	安全隐患。	
	大数据分析平台应采用 OVA 方式部署。	
	采用大数据技术基础架构，数据支撑规模大于 100 亿条以上。	
	支持采用虚拟化平台内进行部署。	
	事件分析：支持根据安全日志信息提供聚合分析数据，具备攻击时长、攻击种类数量、总攻击次数。	
	安全事链分析：对全系统的所有安全事件进行聚合分析，综合展示事件各维度的攻击行为状况，提供基于时间链的安全威胁回溯。（提供界面截图，并加盖厂商公章）	
	支持与探针联动拦截，对安全事件链中分析的来源 ip 进行拦截。当发出拦截指令后，探针将改来源 ip 地址加入其黑名单，阻止其访问接入的真实资产。（提供界面截图，并加盖厂商公章） 联动模式支持自动和手动两种模式，自动模式可自定义拦截阀值：时间周期、攻击事件种类、威胁情报、指定内/外网来源等。 支持指定拦截白名单，支持手动删除拦截 IP。	
	攻击行为分析：对攻击行为进行检测、深度挖掘分析及定位攻击手段。	
	日志检索：支持以全局日志、web 入侵、入侵检测、全息诱捕等维度进行多条件检索。	
	事件还原：支持对事件以时间轴的形式进行还原。	
	历史数据关联：支持将历史事件数据进行关联，综合评定整体风险情况。	
	历史事件：支持查看历史的事件情况，展示各种事件的历史纪录。	
报表功能	安全报表（风险类分布、风险数据发布、事件分析、全息诱捕）(需提供截图证明，并加盖原厂公章)	
	支持将生成的报表以 HTML5、Word 等通用格式输出	
全息诱捕	★支持通过网络虚拟出至少 128 台以上虚拟诱饵主机，并支持在至少 1 个 VLAN 生成和配置虚拟诱饵主机（提供界面截图，并加盖厂商公章）	
	支持在同一个 ip 地址上同时部署低交互蜜罐与高交互蜜罐。 低交互蜜罐为四层蜜罐，只创建 ip 地址与端口。 高交互蜜罐非虚机、非 Docker 形态	
	★支持多种高交互沙箱： Web 类：Vcenter、Webmail、phpMyadmin 服务类：ssh、telnet	

	数据库类：MySQL、Redis	
	支持对攻击事件的查看，包括攻击源，攻击资产，操作内容等。	
	支持对攻击者行为分析展示及攻击操作的视频录制和回放	
	支持分析黑客的身份信息包括 IP 地址、经纬度、地理位置等并在地图上显示。	
	高交互蜜罐支持按比例方式进行自动分配部署	
	支持显示真实主机和虚拟诱饵主机 IP 地址	
	支持捕获攻击主机后，自动拦截攻击主机的访问行为	
DDOS 攻击探测	支持 TCP/UDP Flood 检测，基于最大上限阀值设置，而非 DDOS 特征库	
Web 入侵探测与防护	支持但不限于以下 WEB 攻击攻击的探测：SQL 注入及 XSS 攻击、跨站请求伪造（CSRF）攻击、爬虫、恶意扫描、Cookie 安全、服务器信息伪装/过滤、缓冲区溢出、HTTP 请求类型过滤、Webshell 行为。规则库不低于 700 种。（提供界面截图，并加盖厂商公章）	
系统漏洞攻击探测与防护	支持探测针对操作系统、数据库、邮件服务、FTP 的攻击。规则库不低于 27000 条（提供界面截图，并加盖厂商公章）	
威胁情报库	支持内置威胁情报库，对匹配到威胁情报库中的目的地址的行为进行告警。CNC 服务器库组不少于 200 组。信誉不佳 IP 组不少于 100 组。SpamHaus 黑名单库不少于 34 组。（提供界面截图，并加盖厂商公章）	
产品资质	设备生产厂商应拥有对报价产品的自主知识产权，拥有该系统的计算机软件著作权。（出具加盖厂商公章的复印件）	
厂商资质	设备生产厂商应具有符合 GB/T 19001-2016/ISO 9001:2015 标准的《质量管理体系认证证书》，认证覆盖范围：计算机软件研发、网络信息安全技术服务（出具加盖厂商公章的复印件）	
	设备生产厂商至少具有一名由国家计算机网络应急处理协调中心省级分中心或国家中心聘请的公共互联网络安全专家（出具加盖厂商公章的复印件）	
技术支持服务	提供三年保修和升级服务。	
负载均衡系统		
设备形态	标准机架式设备，独立硬件平台，高性能系统架构，非任何插卡扩展形态的负载均衡设备。 支持软件版本，支持 VMware vSphere、华为云、浪潮和 KVM 等云平	1 台

	台。 1U,10 个千兆电口，6 个千兆光口,冗余电源,2 个扩展槽位,负载均衡吞吐 4G，并发连接 400 万，四层新建：12W，七层新建：16W；可扩展 8 个 10/100/1000BASE-T(100m，RJ45)或者 8 个 SFP 千兆光口。	
部署模式	支持串行、旁路、三角传输部署模式。	
高可用性	链路负载均衡和服务器负载部署支持 AS/AA 模式，同步配置实现无缝故障切换。	
双栈接入	支持主备之间会话同步，支持 IPV6/IPV4 双栈，支持 NAT66、NAT64、NAT46、DNS64 可对过渡型网络进行负载均衡。	
多功能合一	支持多功能合一同时支持链路负载均衡、服务器负载均衡和全局负载均衡的功能,无需额外购买相应授权。此外设备集成 TCP 协议优化、WEB 压缩缓存、页面加速、SSL 卸载、网络防火墙、Web 应用防火墙、DNS 防火墙、漏洞扫描、四七层 DDos 攻击防护等功能。	
链路负载均衡	入向链路负载均衡算法:轮询算法、比率算法、拓扑算法、备用地址算法、丢包算法、最小连接数算法、最小延时算法、最小新建连接算法、跳数算法、包速率算法、实时带宽算法、可用带宽算法。	
	出向链路负载均衡算法，轮询算法、加权轮询算法、带宽比率算法、首个有效算法、随机算法、加权随机算法、丢包算法、最小连接数算法、加权最小连接数算法、最小流量算法、加权最小流量算法、观察者算法、包速率算法、实时带宽算法、最小新建连接数算法、静态就近算法。	
	链路健康检查支持 ICMP、ARP 等类型，高级健康检查可自定义逻辑组合条件判断链路健康状态，当某一条链路故障时，将访问流量自动切换到其它链路，保障用户网络访问不中断。	
	提供链路信息统计，可统计链路健康状态、故障分类、流量走势、报文数走势、访问次数走势、带宽使用率走势、流量占比、报文数占比、访问次数占比等信息。支持在线用户信息统计，支持查看实时会话连接信息。	
过载保护	提供链路过载保护，可基于链路的实时上下行流量阈值保护链路，如果流量达到阈值，后续新增流量自动迁移到其它空闲链路。	
智能 DNS	提供智能 DNS 功能，单域名对应多个运营商地址，自动识别互联网用户访问请求返回用户对应的运营商链路，引导用户从最优路径的线路访问业务系统。	
DNS 代理	支持内网 DNS 请求透明、代理功能。	

	支持 DNS 记录缓存并查看。 支持 DNS 缓存记录包含 A 记录,AAAA 记录，CNAME 记录，MX 记录和 NS 记录，TXT 记录。	
DNS server	DNS server 支持 A 记录,AAAA 记录，CNAME 记录，MX 记录和 NS 记录，TXT 记录。支持主域名服务器、从域名服务器和转发域名服务器。支持视图（实现内外网项目域名不用记录）。 支持 DNS 视图访问控制	
地址库	地址库包含国内 ISP 地址库、全国地址库和全球地址库，支持地址库手动导入，支持地址库查询。 支持自定义地址库。	
域名库	域名地址库，内置国外域名地址库（超过 26W 条全球域名库），可将访问国外域名的请求分发至指定线路，实现对国外域名访问的优化，提升用户体验。支持域名库自定义。（支持域名库分类 30 种。）	
应用路由	根据源地址范围、源端口、协议、拓扑区域和具体应用进行出站链路选择，给用户最大选择力度，保证链路按需所用。 内置应用协议特征库，可识别主流 P2P 下载、P2P 视频、网络游戏、财经软件等应用，支持依据识别后的应用进行链路选择。 支持基于域名选路调度出站策略功能。 支持基于时间策略配置应用路由	
服务器负载均衡	提供 L4-L7 层内容交换服务器负载功能，单一设备上支持 128 个应用和服务器群组，可根据多种算法和要求调度用户的访问请求。	
	提供服务器负载均衡算法包括：轮询算法、比率算法、随机算法、源地址哈希算法、最小连接算法、加权最小连接算法、最快响应算法、观察者算法、首个有效算法等。	
	服务器健康检查采用主动健康检查和被动健康检查相结合的方式。主动健康检查类型包括 http、https、icmp、tcp、tcp_ecv、udp、smtp、pop3、imap、snmp、soap、dns、radius、arp、mysql、ldap、ftp、wap、fix、ssl 等。 支持服务器被动健康检查，通过监测服务器回包中的 reset 等异常字段判断服务器的当前健康状态。	
	连接限制，可以针对虚拟服务、源地址、目的地址条件或者组合条件进行限制。	
	通过监控数据库系统的服务器信息、软件版本、补丁信息、表空间情况、会话信息、回退信息、SGA、权限信息、告警等信息来判断	

	数据库系统运行是否正常，保证数据库系统的可用性和响应能力。	
	提供服务器信息统计。可以统计虚拟服务器的上下行流量、流量占比及排行，报文数量、报文占比及排行，访问次数、访问数占比及排行。可以统计真实服务器的上下行流量、流量占比及排行，报文数量、报文占比及排行，访问次数、访问数占比及排行，故障分类及故障分布。	
	客户端 IP 透传， 支持客户端 IP 透传，通过 HEADER、URL、COOKIE 方式透传用户客户端 IP。	
SSL 卸载	内置 SSL 卸载模块，SSL 工作减轻服务器负担。支持服务器 CA 证书导入，提供证书单向和双向认证，双向认证支持透传客户端证书给后台服务器。	
数据库读写分离	利用读写分离技术实现数据库负载且无需在服务器上安装任何插件或软件。通过对数据库操作请求做内容解析，将其中的写操作调度到指定服务器，减少服务器压力，提高数据库资源利用率，提升业务响应速度，(数据库支持 mysql/ oracle/ SQL Server/ DB2/ Sybase 的读写分离。)	
会话保持功能	提供服务器会话保持机制，支持源地址会话保持、源地址端口会话保持、会话 ID 会话保持、目的地址会话保持、cookie 哈希会话保持、cookie 插入会话保持、cookie 重写会话保持、cookie 被动会话保持、host 会话保持、URI 会话保持、URL 会话保持、Method 会话保持、User Agent 会话保持等多种会话保持机制。	
浪涌保护	提供服务器过载保护功能，可针对服务器负载状态如新建连接数、并发连接数进行智能保护，如果达到保护阈值新的访问请求会自动迁移至其他服务器，支持服务器温暖上线和软关机、平滑退出功能。 浪涌保护对于超过服务器的连接数上限或者请求数上限的新建连接缓存起来放入队列中，后续分批逐步发送给服务器，而不是直接丢弃数据包。	
可编程流量控制	通过某种编程语言（如 lua）实现自定义的流量编排，对 TCP、HTTP 和 HTTPS 等类型的流量进行分发、修改等操作。	
URL 限速功能	支持基于虚拟服务、服务器成员限速功能。 支持基于 URL 的流量控制、基于 URL 的连速率控制	
VMware 虚拟化平台联动	提供 VMware vSphere 联动功能，通过对接 vCenter 监测虚拟机的 CPU、内存、硬盘占用率及并发连接数阈值，动态增加或者减少虚拟机实例数量，实现虚拟服务器资源的合理利用；可以检测虚拟机	

	的健康状态，保证用户分配到可用服务上。	
全局负载均衡	提供针对多站点业务发布的全局负载均衡功能，通过智能 DNS 实现公网用户对多个数据中心多条线路的最佳访问，可实现应用级别的健康检查功能，支持数据中心互备或者双活。 支持 HTTP 重定向。 全局负载均衡算法：轮询、比率、拓扑、全局可用、备选地址、丢包、节点最小流量、节点最小连接、节点最小 CPU 使用率、节点最小内存使用率、动态就近；拓扑算法支持基于数据中心、虚拟服务池的流量调度。 提供节点过载保护，可基于节点的 CPU、内存、会话、流量保护节点，如果达到阈值，后续新增流量自动迁移到其它空闲节点。	
协议优化	提供 TCP 连接复用功能，降低服务器频繁三次握手的资源消耗，减少服务器端的工作负荷，提升业务效率。 提供 HTTP 压缩功能，采用工业标准的 GZIP 和 Deflate 压缩算法，减少传输数据量并降低带宽消耗。 提供 WEB 缓存加速功能,可缓存动静态网页内容，智能控制客户端端浏览器行为。 提供对 http 头的改写和错误页重定向。	
单边加速	支持单边加速功能，非对称式部署的 TCP 协议优化技术，提升远端用户访问应用服务的速度。无需在用户终端或应用服务器上安装任何插件和软件，不受操作系统类型、浏览器版本等兼容性因素限制，并且用户首次访问应用服务即可产生加速效果。	
页面加速	提供 CSS 加速功能，支持内嵌 CSS,合并 CSS,最小化 CSS，将 CSS 移动到 head 中，将 CSS 移动到 JS 前。 提供 JavaScript 加速功能，支持内嵌 JS，合并 JS，最小化 JS。 提供 HTML 加速功能，支持去除空白，去除注释。 提供图片加速功能，支持内嵌图片，转换图片格式。	
安全防护	提供网络防火墙功能，支持基于五元组进行访问控制。	
	提供 Web 应用防火墙功能。支持跨站脚本攻击(XSS)、扫描器防护(Scanner)、SQL 注入攻击(SQLi)、系统命令注入攻击(OSI)、远程文件包含攻击(RFI)、路径遍历(Path Traversal)、信息泄露攻击(Info Leak)、LDAP 注入攻击(LDAP Injection)、XPath 注入攻击(XPath Injection)、SSI 注入攻击(SSI Injection)、Web 服务器漏洞攻击、Webshell 检测、HTTP 协议违规。	
	提供 DNS 防火墙功能。支持 DNS 安全认证，兼容 IETF 提供的国际	

	标准DNS 安全扩展 (DNS Security Extensions, DNSSEC)。支持DNS协议漏洞攻击、DNS反射放大攻击、DNS投毒攻击防护，保障智能DNS解析过程的安全性和可靠性。	
数据库安全	提供数据库安全功能，检查访问数据库的权限，杜绝非授权用户访问数据，保证数据库的安全，（支持MySQL、Oracle、SQL Server、DB2、Sybase）。	
四七层DDOS防护	支持提供四七层抗DDoS攻击功能。支持IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、NTP。其中IP： IP FLOOD 攻击、IP FRAG FLOOD 攻击、DOS 攻击、端口扫描、IP 地址扫描。ICMP：ICMP FLOOD 攻击。TCP： TCP FLOOD 攻击、SYN FLOOD 攻击、FIN FLOOD 攻击、RST FLOOD 攻击、新建SESSION FLOOD 攻击、SESSION FLOOD 攻击。UDP： UDP FLOOD 攻击。DNS： DNS QUERY FLOOD 攻击、DNS REPLY FLOOD 攻击、DNS 投毒攻击检测、DNS 协议漏洞攻击、DNS NX攻击。HTTP: HTTP FLOOD 攻击、HTTP 新建连接 FLOOD攻击、HTTP 并发连接 FLOOD攻击、HTTP URI CC攻击。HTTPS: HTTPS FLOOD 攻击、HTTPS 新建连接 FLOOD攻击、HTTPS 并发连接 FLOOD攻击。NTP: NTP REQUEST FLOOD 攻击、NTP REPLY FLOOD 攻击。防御手段：60多种防御手段。DDoS支持黑白名单。25个DDoS专家模板。	
漏扫功能	提供漏洞扫描功能。设备内置漏洞特征库，可针对应用服务器或者整个IP网段进行定向扫描分析，发现服务器操作系统漏洞并生成漏洞分析报告。	
应用性能分析	支持Oracle数据库、MySQL 数据库关键性能指标监控，并将相关数据在设备上通过图表多维度展现。支持配置监测周期，支持配置所监控得服务器的用户名，密码，数据库名。支持查询数据库的当前和历史数据，支持显示数据库的版本，运行时间，Session信息，查询缓存数据，内存使用，日志信息，存储信息等。	
可视化报表	设备内置数据中心，通过设备的管理界面上看到自带的各类统计信息及可视化报表，可以根据用户需求定制报表模板，然后基于定制化的报表模板导出数据报表，支持数据报表导出，支持日报表、周报表、月报表。	
大屏展示	支持投屏功能，可显示链路稳定性检测、链路调度与故障迁移监测。	
智能告警	内置智能告警系统，支持E-mail、声音、短信、NetBios、控制台、SNMP Trap五种告警方式，管理员可基于业务安全所关注方面	

	来选择告警触发事件与对应的告警方式，当业务网络环境中发生问题时（如服务器宕机、网络攻击、链路中断等故障场景），即会自动向管理员发送告警信息	
API/XML 接口	可编程接口 API、可编程接口 XML，可提供 Python 和 Java 的 SDK 工具，可实现与第三方应用平台的集成与二次开发	
云对接	支持 openstack 负载均衡组件对接，简化配置流程。通过 openstack 负载均衡页面，即可实现业务配置自动下发和南北向流量自动打通，无需用户操作负载均衡设备环节。支持多租户，层次化绑定（支持 VLAN 个数大于 4094）等特性。	
系统管理	支持 WEB 界面管理与 CLI 命令行下管理。	
	SNMP 支持 V1/V2/V3 版本，TRAP。	
	动态路由支持 OSPF、OSPF6、RIP、BGP、BGP4+	
	NTP 时间同步可自定义服务器或互联网 NTP 服务器。	
	多级可编辑管理员权限，超级管理员、虚系统、日志审计、安全策略、设备维护。	
	自定义配置日志类型，格式为 syslog、welf。	
VPN 功能	支持 SSL VPN 功能	
产品资质	中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》（提供证书扫描件） 所投产品具备国家工业和信息化部颁发的《电信设备进网许可证》《IPv6 Ready go 认证证书》 具有公安部颁发的《计算机信息系统安全专用产品销售许可证》 所投产品生产厂家通过 CMMI5 认证，以保证产品代码质量与稳定性 具有国家互联网应急响应 网络安全应急服务国家级支撑单位 CNCERT 证书（国家级）	
售后服务	厂商本地有售后服务机构和人员。提供快速本地化现场技术支持，7*24 小时的技术支持服务。	
运维审计系统		
系统架构	1U 标准机架式设备，独立硬件平台，高性能系统架构，不少于 2 个千兆电口，1 个 1000MIPMI 专用远程管理王口，模块化设计，松耦合、B/S 架构。	1 台
	采用 HTTPS 方式远程安全管理，无需安装客户端，支持 IE（IE11 以上）、Edge、Chrome、Firefox、Safari 等业界主流浏览器	
	支持移动智能设备访问	
	支持多 IP、多域名访问	

	支持 NAT 地址映射部署，通过映射后的 IP 地址访问堡垒机	
	旁路部署，逻辑串联模式	
	支持一键式部署	
	支持单机部署、主备部署方式、HA 双机热备	
	支持集群分布式部署，支持基于水平可扩展的集群化架构设计与部署，支持跨地域、跨数据中心，多层次部署	
组织架构管理	支持以 Excel 文件的方式批量导入用户信息，支持导入用户时关联角色和组织架构	
	支持从 AD 域导入用户，支持 AD 用户自动同步	
	新建用户时，支持手动指定密码或生成重置免密链接，通过邮件的方式发送给用户	
	支持新建用户时，设置用户首次登录时强制修改密码	
	支持用户绑定企业微信、个人微信、钉钉、飞书第三方应用，能够通过这些应用进行 扫码登录及接受各类消息推送	
	支持通过用户密码策略来限制用户密码长度、密码强度	
	支持通过用户密码策略来限制用户密码有效期	
	支持通过用户密码策略来限制用户密码是否能与前 N 次的密码重复	
	支持创建临时用户，到期后自动将临时用户禁用，可以手动禁用、激活用户	
	支持本地认证、CAS、OIDC、RADIUS、SSO Token、SAML2、AD 域/LDAP 等用户认证方式	
	支持异地登录提醒，在非经常登录的城市访问门户时，将通过邮件、微信或手机 短信向用户发送异地登录提醒	
	支持防暴力破解功能，连续多次失败登录将自动锁定账户或 IP，可配置解锁时长、到期自动解锁，也可以手动解锁	
	支持通过用户安全策略定义用户的 IP 地址黑、白名单，禁止非法地址访问	
	支持通过用户安全策略定义用户的允许登录时段，其它时段将禁止用户登录门户	
	支持手机短信验证码、MFA 多因子认证方式来登录门户及其它重要操作	
	管理员可单独或批量修改用户的认证方式	
	管理员可重置其他用户密码、可修改其他用户昵称	
	管理员可手动锁定/解锁用户，被锁定的用户禁止登录门户	

	支持以 Excel 文件的方式批量导出用户信息	
	支持组织管理员通过邀请的方式加入当前组织	
	支持用户按照组进行划分	
	支持资产授权按照组进行授权，自动继承组的权限	
	支持按照组名称进行筛选	
	支持一个用户同时加入多个组	
	可以根据项目或者公司组织架构进行多组织划分，各个组织之间相互隔离，各个组织可以设定组织管理员，由组织管理员进行组织内的独立审计、独立管理，包括对用户的资产授权、权限的划分等，为用户提供更加细颗粒的管理体验，逻辑上实现一套 JumpServer 多套使用的场景	
资源管理	支持以 Excel 文件的方式批量录入主机及账号密码	
	支持以 API 的方式批量导入公有云主机及私有云主机资源	
	支持主流公有云厂商，包括阿里云、华为云、腾讯云、AWS、Azure、谷歌云、青云、金山云、VMware 等云账号下资产的自动同步	
	支持按区域/网络对主机进行分组管理	
	支持资源按标签管理，支持批量为主机资源添加和删除标签、支持以标签视图展 示主机资源	
	支持常用的系统类型，包括 Linux/Unix、Windows、MacOS、存储设备、网络设备	
	支持以主机名称、IP 关键字的方式对主机资源进行全局检索、筛选	
	支持主机列表字段自定义筛选，可以从不同的维度进行主机字段查询	
	支持以 Excel、csv 文件的方式批量导出主机资产信息	
	支持按照资产树列表的方式对资产进行节点划分	
	支持资产数节点下资产的批量移动	
	支持告警消息方式包含系统消息、企业微信消息、邮件消息等多种方式	
	支持自动获取纳管资产的括 CPU、内存等资产信息	
运维管理	支持内网访问机制，针对公有云等位于互联网上的主机资源，避免将不必要的端口暴露到公网	
	支持以 Web 页面图形化形式展示主机列表	
	支持以跳板机字符形式展示主机列表，同时支持 Linux 和	

	Windows 跳板机	
	支持 SSH、RDP、VNC、Telnet、FTP/SFTP 等协议访问主机	
	支持 SQL Server、MariaDB、Oracle、PostgresSQL 等数据库访问协议	
	支持 RDP 协议的 RDP 粘贴复制功能	
	支持通过浏览器 Web 页面访问主机，包括 SSH、RDP、Telnet、VNC 和应用发布	
	支持以本地 C/S 客户端工具的方式访问主机，包括：Xshell、Putty、 SecureCRT、WinSCP、mstsc、FTP/SFTP、xftp 客户端	
	支持 SSH key 方式登录 SSH 资源	
	支持会话分享，保证多人协同操作，同时支持会话加密分享	
	支持 XRDP 的连接方式，可以使用 XRDP 的方式实现 Windows、Linux 资产的连接，特别是针对 Windows 资产可以实现文件或文件内容的 Ctrl+c、Ctrl+v，方便用户对文件或文件内容进行上传下载、粘贴复制，方便用户操作，并进行审计,支持通过 XRDP 连接远程应用时的复制粘贴、上传下载（磁盘挂载）权限控制	
	支持对文件上传、下载，文件内容粘贴、复制权限进行单独设定	
	支持将指定文件批量发送至多台主机，或将分散在大量主机上的某类文件收集到指定位置	
	支持通过 web 页面直接使用 rz、sz 的方式进行文件传输	
	支持远程桌面共享本地磁盘，通过映射的方式实现文件传输	
	支持针对不同服务器和用户制定不同的运维策略	
	能够设置是否允许用户在访问目标设备时，对主机进行文件上传、下载等传输操作	
	支持开启会话背景水印，对会话的截图和拍照将带有会话创建者的信息，方便事后对泄露的信息进行追踪	
	支持对重要资产登录时进行二次复核，需要经过管理员的审批才能进行正常登录，实现工单审批登录	
	支持禁止 RDP 会话使用系统剪切板功能，一旦禁止，运维人员将无法拷贝 Windows 服务器上的数据，可以避免重要文本数据被窃取	
	支持基于 IP 黑白名单的访问策略，限制运维人员只能从指定 IP 访问关键设备资源	
	支持基于黑、白名单的敏感指令审计规则，针对定义好的敏感指令可以进行阻断 响应或触发审核操作，审核不通过的敏感指令将会	

	被拦截，以实现安全监管的目 的，保障运维操作的合规、安全、可控	
	支持对数据库运维过程的执行的预设非法 SQL 进行拦截	
	指令审核支持以站内信、邮件等方式进行审批	
	支持对运维操作自动录屏录像功能，无论是手动或是自动自行，均提供审计记录	
	支持对团队成员所进行的运维操作次数、在线时长、登录次数进行 TOP 排名	
	支持改密计划，可以在 web 页面添加改密计划，自定义设置密码策略、密码长度，并且支持免密导出备份	
	支持批量命令操作，可以直接通过 web 页面对服务器批量执行命令	
	支持通过 WEB GUI 的方式对数据库（MySQL、Oracle、MariaDB、PostgreSQL、Sql Server 数据库）进行可视化的页面操作，用户通过创建系统用户、数据库应用，然后对其进行授权操作，就可以通过 WEB 页面的方式进行可视化的数据库界面操作，并且对用户的操作自动进行录屏录像的功能，也可以对其操作的命令进行记录，支持导入 SQL 文件和导出查询数据集(支持 CSV、XLSX 格式)(Web 数据库可视化页面)	
	支持对资产、应用账号进行定时备份	
	支持自动发现、收集资产上已经存在的用户，查看资产用户登录情况，排查未授权账号，排除安全隐患，有效规避相关风险	
	支持 K8s 集群纳管，查看 Kubernetes 的 Namespace 和 Pod，并且支持对 Pod 内的 Container 进行连接和审计(Web Terminal 连接方式)	
协同会诊	运维过程中可将远程会话分享给其他用户，所有参与者均可同步观看远程会话的操作过程	
	支持以 URL 的方式邀请其他用户加入分享的会话	
	一个会话的参与者人数不设上限	
	会话创建者可随时停止会话的分享	
应用发布	堡垒机支持 windows2012 及以上的 remoteAPP 方式的应用发布，支持对 Windows RemoteApp 应用权限动作的单独控制，包括文件上传、下载、复制、粘贴	
	支持对各类常规应用程序的密码代填	
	支持第三方应用的发布，实现权限的细粒度的划分，如 Navicat、谷歌、火狐等，通过 web 页面直接对应用进行访问	
工单与审	支持工单管理，用户可以根据自己的需求申请资产、权限、使用周	

批流程	期，管理员可以直接对工单进行审批操作	
	支持以 API 的形式直接调用工单，与第三方系统进行集成	
	支持通过企业微信、邮件接收待办工单消息并提供进一步的处理入口	
	支持工单流程的自定义设置，可以根据申请资产的类型不同设置不同的审批流程，支持工单流程设置权限	
安全审计	提供基于角色的访问控制来实现权限控制	
	支持细粒度的功能权限授权和资源权限授权	
	同一用户可同时拥有多个角色，并通过界面统一查看该用户所拥有的全部功能权限和资源权限集合	
	支持实时会话查看，管理员可随时进入任何活跃会话进行监管，一旦发现违规操作，可强制结束会话 提供敏感指令拦截功能	
	管理员可以随时终端会话	
	支持对 Windows、Linux/Unix、数据库的运维操作进行审计录像	
	审计录像可存储在云端或本地存储，避免被篡改	
	审计录像支持倍速播放、拖动、暂停	
	可将审计录像下载到本地进行离线播放和备份	
	支持 Windows 键盘操作记录、Linux/Unix 命令、数据库 SQL 语句进行指令记录	
系统管理	能够显示系统当前在线用户和数量	
	能够显示系统当前所有在线活跃会话	
	能够显示系统当前所有设备的状态和数量	
	支持中英文多语言版本	
	支持 HTTPS 协议证书替换	
	支持访问协议、访问端口、访问地址设置	
	支持对接腾讯、阿里短信平台服务，用户登录时进行短息认证	
	支持修改数据的存储方式和位置，支持将数据存放在云厂商对象存储	
	支持邮件服务器配置	
	支持门户安全策略配置，可定义防暴力破解规则	
	支持门户 IP 黑白名单管理	
	支持管理控制台 IP 白名单管理	
	支持查看门户及管理控制台的用户登录日志	
	支持将指定操作日志发送到第三方 syslog 服务器	

	支持根据用户名称、操作类型、客户端 IP、操作结果进行日志筛选	
	支持自定义产品图标、产品信息名称等	
	支持通过导入升级包的方式一键升级	
	能够显示系统当前各项配额的使用情况	
	支持 License 更换	
	核心功能均提供 API 接口，可通过 Open API 进行功能扩展，或与其它业务系统 进行深度集成	
服务支持	7×24 小时电话支持服务，1 个小时内响应客户工单；接到故障申报后，工程师通过电话支持、远程接 入等方式协助客户及时排除软件故障	
	合计 5 人天的原厂专业服务，可提供现场安装、现场培训、现场紧急救助、软件故障现场排查等专业支持服 务；并且可以根据企业 IT 规划提供相关顾问咨询服务	
	提供软件补丁、增强功能包等软件升级服务，无缝升级软件版本	
	提供客户支持门户，支持客户在线访问网站并下载相关资料，及时掌握最新的软件特性、维护经验、使用技巧等相关知识	
数据可视化分析统计系统		
仪表板管理	支持仪表板的新建、重命名、删除、复制、移动、搜索等	1 套
	支持仪表板分组的新建、重命名、删除、移动等	
	支持以树状形式展示仪表板分组	
视图制作	支持视图的创建及复用，支持通过简单的拖拉操作，制作视图。	
	支持多种图表类型，包括明细表/汇总表/透视表/指标卡/基础柱状图/堆叠柱状图/横向柱状图/横向堆叠柱状图/基础折线图/堆叠折线图/饼图/南丁格尔玫瑰图/漏斗图/雷达图/仪表盘/中国地图/气泡地图/散点图/气泡图/矩形树图/组合图/水波图/瀑布图/词云图等	
	支持对柱状图、折线图等有纵坐标的图表，设置纵坐标起始和结束值范围。	
	支持视图数据集的切换	
	支持视图数据集的编辑	
	支持选择视图的样式优先级	
	支持选择图表的排序方式，根据维度、指标升序、降序展示	
	支持视图的下钻上卷	
	支持指标的多种汇总计算方式，如求和、平均、最大值、最小值等	

	支持指标的高级计算，如同比、环比等	
	支持对图表类型的图形属性进行设置	
	支持对图表类型的组件样式进行设置	
	支持通过过滤条件筛选视图数据	
仪表板制作	支持在线编辑仪表板	
	支持仪表板中添加多种组件，如：视图/时间组件/文本组件/数字组件/样式组件/图片/tab 组件/链接等	
	支持动态设置日期组件的默认值等	
	支持通过一个过滤组件，过滤多个视图（视图数据来自多个数据集）	
	支持组件样式设置，如图形属性、组件背景、组件样式等	
	支持仪表板中视图的下钻	
	支持仪表板中视图间的联动	
	支持仪表板中各组件背景图片及边框的设置 New	
	支持仪表板跳转，如跳转至系统内其他仪表板、外部链接。	
	支持仪表板背景、组件间隙、刷新时间、展示数据量等设置	
	支持一键切换仪表板主题	
	支持仪表板导出为 pdf	
	支持撤销、重做、清空画布内容	
	支持仪表板的全屏预览	
	支持仪表板的收藏	
	支持默认仪表板的设置	
	支持仪表板模板的导出	
	支持仪表板模版保存	
仪表板共享	支持按组织/角色/用户分享，查阅分享记录等	
	支持创建公共链接，外部用户可通过密码访问仪表板	
数据集管理	支持添加多种类型的数据集，数据库数据集/SQL 数据集/Excel 数据集/自定义数据集/关联数据集/API 数据集	
	支持数据集的添加、移动、重命名、删除、预览等	
	数据库数据集和 SQL 数据集支持直连和定时同步两种连接方式	
	定时同步类型数据集，支持全量更新和增量更新两种方式	
	支持创建定时任务，以此控制数据集的更新	
	支持定时更新任务的查看	
	支持对数据集的字段类型/字段名/展示字段进行设置	

	支持数据集的维度、指标间的互相切换	
	支持自定义计算字段（内置常用计算函数支持）	
	支持创建数据集间的关联关系（左连接、右连接、内连接）	
数据源管理	支持多种数据源，如：多 sheet 页 Excel 文件，MySQL / Oracle / SQL Server/ PostgreSQL / Elasticsearch / ClickHouse / MongoDB /AWS RedShift/ MariaDB / Doris / Hive 数据库 / DB2 / API 数据源	
	支持数据源的新建、编辑、删除等	
	支持数据源的高级设置，如最大连接数、最小连接数、连接超时时间等	
	支持 Excel 数据集数据的替换、追加	
	支持数据源有效性校验	
	支持定时检测数据源的连接状态	
用户管理	支持用户的新建、编辑、删除、修改密码、启用/禁用、搜索等	
	支持给用户分配组织	
	支持给用户分配角色	
角色管理	支持角色的新建、编辑、删除、搜索等	
组织管理	支持组织的新建、编辑、删除、搜索、排序、移动等	
权限管理	支持从组织、角色、用户维度（组织架构维度）进行使用、管理、授权等形式的权限控制	
	支持从数据源、数据集、仪表板（资源维度）进行使用、管理、授权等形式的权限控制	
	支持菜单和操作层面的权限控制	
	支持数据集的行级权限控制	
	支持数据集的列级权限控制	
显示设置	支持头部系统 Logo、登录页 Logo、登录页图片、登录页标题、系统名称等显示设置	
主题设置	支持自定义主题的新建、编辑、删除等	
	支持对主题进行基础配色、字体配色、边框配色、背景配色等多属性的设置	
LDAP 设置	支持 LDAP 认证对接	
单点登录	支持单点登录系统对接	
集成与扩展	提供完善的 API 接口及文档	
模板管理	支持系统模板和用户模板	

	支持模板的分类、导入、重命名、删除、搜索等	
消息管理	支持系统常见消息的通知	
	支持消息的接收配置	
	支持消息状态标记	
	支持已读消息的删除	
任务管理	支持数据同步，可以对平台定时任务进行全生命周期管理	
	支持定时报告，可以定时以邮件形式发送仪表板报告	
数据对接	实现与医院信息系统数据进行无缝对接（包含接口服务费）。	
漏洞扫描系统		
硬件规格	20 个任务并发，可扩展至 25 个任务并发，限制扫描指定 1024 个 IP 地址,可扩展至无限 IP 授权，电口*6,内置 2 对电口 Bypass,支持 3 级 Bypass,DSI*1，DMI*1,USB*2,console*1,扩展槽*1,接口吞吐量 4000Mbps(可扩展至 8000Mbps)，1U	1 台
扫描方式	支持直接扫描	
	支持对多个扫描任务并发执行，支持多任务自动调度；单个任务允许扫描的最大扫描范围不小于一个 B 类网段。	
	支持设备内置 VPN 拨号扫描（提供截图并原厂盖章）	
	支持 HTTP 代理（提供 HTTP 代理服务器的功能。用来获取通过用户名和密码登录时的 cookie，从而进行登录扫描。）（提供截图并原厂盖章）	
	支持 SOCKS 代理扫描	
	支持主机/Web/弱口令 单项扫描	
	支持定时扫描/支持自定义紧急漏洞扫描	
流量控制	支持网卡限速，防止扫描消耗过多带宽	
访问控制	支持添加指定 IPv4,IPv6 地址访问设备	
主机漏洞数量	≥ 54000 个	
检测漏洞类型	支持 Windows/Linux/Unix 等操作系统漏洞检测	
	支持 IIS/Apache/Nginx 等 Web 服务器漏洞检测	
	支持 MSSQL/MySQL/Oracle/DB2/Redis/PostgreSQL 等数据库漏洞检测	
	支持 FTP/EMAIL/DNS/SNMP/P2P/Finger 等检测	
	支持虚拟化漏洞、常用应用软件漏洞检测	
	支持 F5/FortiOS/JunOS/CISCO/华为等网络设备检测	

操作系统指纹识别	自动判断被扫描主机的操作系统类型及版本	
CVE/CNNVD 编号显示	支持显示 CVE/CNNVD/CNVD 漏洞编号	
主机登陆扫描	支持 Windows、SSH、Kerbeors、明文协议的登陆扫描，登陆到相应的系统中进行	
Web 漏洞数量	≥ 7000 个	
协议支持	支持 WEB 2.0 扫描	
	支持 HTTP/HTTPS 协议	
验证性扫描	支持对 SQL 注入、XSS 攻击、文件包含类等漏洞在扫描结果中有验证性，给予管理员漏洞存在性、可利用性以及漏洞利用方式的提醒（提供截图并原厂盖章）	
域名反查	支持 IP 地址到域名的反查扫描	
URL 排除	支持用户自定义不扫描的目标 URL	
紧急漏洞扫描	支持紧急漏洞扫描，通过近期热门的高危漏洞库，对全网进行安全检查	
Web 漏洞检测能力	支持 SQL 注入/XSS 跨站/命令执行/目录遍历/上传漏洞等检测	
	支持表单弱密码检测、CMS 类型识别	
Web 登陆扫描	必须支持登录扫描功能，可自动通过内置的 WEB 代理来抓取用户登录信息，无需手工输入 Cookies、Session 等信息，即可实现登录扫描功能；	
联动扫描	支持与同品牌 Web 应用防火墙页面统计中获取的 URL 来补充漏洞扫描系统的爬虫库（提供截图并原厂盖章）	
协议类型	支持检查 3389（RDP 远程桌面）弱密码	
	支持检查 FTP/SSH/TELNET/MSSQL/MYSQL/ORACLE/SMB/VNC 弱密码/EMAIL 弱密码	
自定义字典	支持字典编辑与字典上传	
报表类型	支持领导报表和详细报表：领导报表查看任务的总体数据情况;详细报表查看漏洞类型统计与详细信息、解决方案输出	
	支持条件报表（可以通过选择报表条件来生成相应的报表）	
输出格式	支持将生成的报表以 HTML、Word、PDF、Excel、等通用格式输出	
资产管理	支持对管理员所管理的资产进行分部门集中管理，便于漏洞扫描、	

	漏洞修补以及资产对比。	
API 接口	可扩展模块功能提供二次开发接口模块，提供 HTTP RPC 接口支持，方便与第三方产品联动。能将任务的扫描结果（IP、主机漏洞、Web 漏洞、弱密码漏洞）同步出来，便于调用和查看。	
系统诊断功能	内置一个有 ping、ping6、route、arp、traceroute 和 nslookup 的网络工具。	
多用户	支持多用户配置，可以控制每个用户的扫描目的 IP，扫描迸发，并且管理员可以对所有用户的扫描任务进行管理（提供截图并原厂盖章）	
审计功能	提供审计功能，能够对登录日志、操作日志和异常报告进行记录和查询。	
备份机制	提供备份恢复机制，能够对扫描结果、日志、扫描模板、参数集等配置文件进行导出和导入操作；	
日志类型	系统日志、审计日志	
syslog 输出	扫描结果支持以 syslog 方式输出到外部服务器	
告警通知	磁盘使用率接近上限告警、扫描完成后需自动发送报表	
固件升级	支持固件在线升级方式，可按计划执行自动升级；产品同时应支持手动升级方式，可利用已经下载的升级包实现升级。	
规则升级	支持规则在线升级方式，可按计划执行自动升级；产品同时应支持手动升级方式，可利用已经下载的升级包实现升级。	
销售许可证	获得公安部颁发的《计算机信息系统安全专用产品销售许可证》，认证的产品类型/级别：网络脆弱性扫描（增强级），并出具加盖厂商公章的复印件	
强制认证	获得中国信息安全认证中心颁发的符合 GB/T 20278-2006 《信息安全技术 网络脆弱性扫描产品技术要求》增强级认证《中国国家信息安全产品认证证书》，并出具加盖厂商公章的复印件	
涉密认证	获得国家保密局涉密信息系统安全保密测评中心颁发的符合国家保密标准 BMB12－2004《涉及国家秘密的计算机信息系统漏洞扫描产品技术要求》的《涉密信息系统产品检测证书》，并出具加盖厂商公章的复印件	
CNNVD 兼容性资质证书	获得中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》	
厂商资质	设备生产厂商应具有符合 GB/T 19001-2016/ISO 9001:2015 标准的	

要求（提供相关资质复印件，生产厂商盖章）	《质量管理体系认证证书》	
	设备生产厂商应具有漏洞发现能力，具备《中国国家信息安全漏洞库（CNNVD）技术支撑单位资质》，至少曾经获得中国信息安全测评中心颁发《中国国家漏洞库-信息安全漏洞提交证明》	
	设备生产厂商具备中国信息安全测评中心颁发的《国家信息安全测评 信息安全服务资质证书》（安全工程类一级）资质，能力范围包括：安全风险评估、安全需求分析、安全方案设计、安全集成、安全监控和维护等	
	设备生产厂商具备 CNCERT 颁发《网络安全应急服务支撑单位证书》	
售后服务支持	上述硬件平台、所有非扩展软件功能模块提供三年原厂保修和升级服务。	
	需附送原厂 webshell 工具一套。	
	为应对网络安全事件，报价方应成立安全应急处置小组进行紧急响应，响应时间：7×24 小时响应。	
智能工单与资产管理系统		
架构	要求系统设计符合 J2EE 标准，基于最流行的开发架构（AJAX+Struts+Spring+Hibernate），系统支持分布式部署。支 Windows、Unix、Linu、及各类国产操作系统、支持 Oracle、SQL Server、MySQ、达梦、K-DB 等关系型数据库要求采用 B/S 结构开发，使用户对系统的维护和使用不受场所和地点的限制。提供二次开发接口，便于未来系统扩容。	1 套
用户管理	不限用户数量，支持多角色管理，支持组织机构管理。	
资产管理	支持资产目录编制，支持资产模板自定义，支持资产关联，可定义资产维护计划，维护内容，关联自动派单。可以创建资产二维码标签，资产快查询，资产快修。	
工单管理	支持 H5 移动端提交工单、支持维护计划工单，指定维护工单，故障工单，可以人工派单或运维组自主分配。	
绩效统计	故障跟踪，满意度评价，运维统计，任务统计，时效统计。	
消息管理	支持短信、微信等第三方消息接口。	
知识管理	常见问题汇总，主题管理，知识管理。	
大数据屏展示	提供自定义首页功能，用户可以根据管理需要自行定制各类管理面板，包括排名，数据曲线图，告警统计，自由组合指标显示；根据我院业务、应用等现有情况，提供从设计到前端集成展示的定制化服务，通过专有的定制页面输出我院运维信息。可对界面进行个性	

	化定制。	
现有接入	需要与现有资产系统对接。	
信息安全等级保护测评		
技术要求	出具医院信息系统第三方测评机构信息安全等级保护 2.0 标准的三级符合性测评报告。	1