货物采购需求及技术规格

一、总则

1、本技术规格所提出的要求是对本次采购货物及伴随服务的基本技术要求，并未涉及所有技术细节，也未充分引述有关标准、规范的全部条款。投标人应保证其提供的货物及伴随服务除了满足本技术规格的要求外，还应符合中国国家、行业、地方、国际或设备制造商所在国的有关标准、规范（尤其是必须符合中国国家标准的有关强制性规定)。当上述标准、规范的有关规定之间存在差异时，应以要求高的为准；当上述标准、规范的有关规定与本技术规格的规定之间存在差异时，应以本技术规格为准。

2、本技术规格中提及的工艺、材料、设备的标准及参考品牌或型号（如有）仅起说明作用，并没有强制性。投标人在投标文件中可以用替代工艺、材料、设备的标准及品牌或型号，但这种替代须实质上满足、等同或优于本技术规格的要求，同时须提供证明材料进行详尽的描述并经评标委员会认可，否则视为负偏离。

二、技术参数

标识重要性	标识符号	代表意思
核心指标项	▲	不满足的，投标无效
关键性指标项	★	评审项，每有一个不满足扣 3 分
无标识项		评审项，每有一个不满足扣 2 分
注：如某项标识中包含多条技术参数或要求，则该项标识所含内容均需满足或优于招标文件要求，否则不予认可。		

技术规格书：

序号	货物名称	技术参数及要求	数量
1	**核心交换机**	**一、▲硬件配置：** 1、投标产品 CPU（如有）使用国产自主 CPU,交换芯片使用国产自主交换芯片。**（需提供 CPU（如有）、交换芯片厂商和规格型号）** 2、配置双主控，冗余电源模块、冗余风扇模块，业务槽位≥6 个。 3、板卡接口数量：100G 光端口≥12 个（需要平均分配在两块板卡上）、25G 光端口≥8 个（需要平均分配在两块板卡上）、万兆光口≥52 个、千兆光口≥20 个、千兆电口≥24 个、业务槽数量≥6 个;配置 16 个万兆多模模块,4 个 25G 多模模块。 **二、▲性能指标：** 1、交换容量≥76Tbps，包转发率≥57600Mpps，以官网所	2 台

		列最低参数为准。**（提供官网截图或相关证明文件）** **三、功能特性：** 1、支持 IPv6 协议栈，具有 IPv4/v6 静态路由、OSPFv2，OSPFv3、BGP4、BGP4+、MPLS、MPLS VPN 等 IPv4/v6 动态路由功能。 2、支持 VLAN 功能，支持 Guest VLAN、Voice VLAN、QINQ、灵活 QINQ。 3、★支持 256 位全端口 MACSEC 加密。**（提供官网截图或相关证明文件）** 4、支持虚拟化技术，支持横向虚拟化，具备四虚一，支持一虚多技术。 5、★配置 m-lag 或 DRNI 或 VPC 跨设备链路聚合功能授权，在跨设备链路聚合组网环境中，支持多台设备配置实时同步。**（提供功能截图或相关证明文件）** 6、设备软件采用当前最高版本，配置所有功能的软件授权 license，后续所有功能启用均不需额外付费。 7、设备应具有良好的兼容性，能兼容招标人现有交换设备。 **四、▲原厂服务：** 提供原厂 5 年产品支持服务，服务级别为 7x24x4（7 表示每星期周一至周日，24 表示全天 24 小时，4 表示我司提出现场服务需求时能够在 4 小时之内到达现场）。	
2	**核心防火墙**	**一、▲硬件配置：** 所投产品采用国产自主芯片和国产自主操作系统。**（需提供芯片、操作系统厂商和规格型号）** 外形：1U 标准机架式硬件 千兆电口：≥4 个（2 对 bypass） 千兆光口：≥4 个 万兆光口：≥4 个（含 4 个万兆多模模块） 管理接口：1 个 电　　源：2 个交流冗余电源 拓展插槽：≥2 个（可扩展 QSFP+接口） **二、▲性能指标：** 网络层吞吐量：≥10Gbps 存储空间：≥1TB 并发连接数：≥1000 万 四层新建连接数：≥15 万 **三、功能特性：** 1、出站接入交换机:提供多出口 IPV4 和 IPV6 DNS 透明代理功能，支持根据源目的地址及域名等过滤条件，对	2 台

		DNS 报文进行代理、放行及阻断功能，解决链路切换带来的跨运营商解析问题；链路状态结合 ICMPV6、HTTP、DNS、接口流量、报文延迟监测进行流量负载均衡；提供延迟、丢包率、抖动、带宽利用率的链路状态可视化监控。 3、提供针对策略路由的 DNS 重定向功能，提供独立的策略路由（PBR）日志记录界面，记录时间、PBR 名称、五元组、虚拟路由器、会话原因等信息，PBR 日志支持设置缓存大小和分布式外发。 4、★NAT 的端口扩展技术，突破单个 IP 地址转换端口的数量限制；提供 NAT 地址池中地址有效性探测、NAT444 功能；支持 4500+的应用识别及控制。**（提供功能截图或相关证明文件）** 5、智能分析诊断：支持数据包路径检测工具，可通过在线检测、模拟检测、已有检测源等检测手段，图形化展现数据包经过的每个防火墙功能模块的处理过程，图形化检测项包括：报文合法性检查、攻击防护、会话匹配、MAC 检查等，以便快速定位异常功能模块。 6、具备扩展僵尸网络防御专业功能模块，通过监控 C&C 连接发现内网肉鸡，阻断僵尸网络/勒索软件等高级威胁进一步破坏支持实时的僵尸 IP 与域名，提供僵尸网络检测软件著作权，支持僵尸网络防御规则库在线实时升级。 7、★提供移动运维 APP：通过移动 APP 对设备监控 CPU、内存及版本；整机流量、会话、接口流量趋势图；应用及用户排名可视化展示;实时告警消息推送;多维度威胁（级别、类型、攻击者、受害者）展示、威胁详情展示。支持扩展云巡检功能，一键启动巡检任务并生成巡检报告，并针对潜在的问题和风险给出优化和处置建议。 8、防火墙支持 DNS-rewrite 功能，生成映射关系，并修改 DNS 响应报文中的域名对应的 IP 地址，以隐藏和保护域名对应的服务器真实 IP 地址。 9、★零信任访问：通过 SPA 配置将零信任端口隐藏，只有正确敲门报文才能开放端口；支持零信任终端标签策略与数据安全，支持终端标签配置与规则，支持对零信任访问进行监控，提供不少于 8 个零信任接入授权。 10、★提供云安全运维平台一套，完全兼容与纳管现网防火墙设备，可对设备运维，实时查看威胁事件（含威胁名称、类型与级别、攻击者、受害者、威胁事件进行排名展示）。 11、支持与现网两组 HA 设备组成孪生模式，两对主备的防火墙支持配置同步、会话同步，优化流量转发功能，解	

		决非对称流量，保障多数据中心的业务的持续性、高效性。 12、提供加密流量检测（非 SSL 代理），通过对加密流量行为及特征进行检测，及时发现异常加密流量， 系统将记录威胁日志，提供加密特征库的在线升级。 **四、▲原厂服务：** 提供五年应用识别、ISP 信息库、共享接入特征库、加密流量检测库、防病毒功能授权及升级服务；提供原厂 5 年产品支持服务，服务级别为 7x24x4（7 表示 每星期周一至周日，24 表示全天 24 小时，4 表示我司提出现场服务需求时能够在 4 小时之内到达现场）。	
3	**负载均衡**	**一、▲硬件配置：** 所投产品采用国产自主芯片等和国产自主操作系统。**（需提供芯片、操作系统厂商和规格型号）** 外形：2U 标准机架式硬件 千兆电口：≥6 个 万兆光口：≥2 个（含 2 个万兆多模模块） 管理接口：1 个 电　　源：2 个交流冗余电源 **二、▲性能指标：** 网络层吞吐量：≥20Gbps 并发连接数：≥2000 万 四层新建连接数：≥30 万 七层新建连接数：≥50 万 **三、功能特性：** 1、▲支持和配置链路负载、全局负载、服务器负载、SSL 卸载、防火墙 ACL 授权。 2、★支持基于应用协议的智能选路，内置网上银行、Web 流媒体、游戏、音频视频规则库，并且规则库不少于 5000 条。**（提供功能截图或相关证明文件）** 3、支持链路负载投屏展示，能够分别基于链路监测、应用选路和 ISP 流量进行投屏展示分析。链路监测展示链路的健康状态、上下行带宽、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；ISP 展示基于运营商分类选择链路的示意图。 4、★支持在 Web 页面配置实现基于管理员自定义的时间计划来进行出站访问的流量调度。**（提供具有 CMA 标识第三方机构出具检测报告扫描件）** 5、支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应时间、加权最小流量、按主机加权最小流量、源 IP 源端口哈希、	2 台

		源 IP 哈希、URI 哈希和 HOST 哈希等。 6、★支持常见的主流国产数据库的负载均衡功能，至少包含 OceanBase、TDSQL、达梦、南大通用和人大金仓。**（提供如上所有数据库厂商产品认证证书）** 7、支持常见的主动式健康检查功能，提供基于 SNMP、ICMP、SIP、ICMPv6、TCP/UDP、FTP、HTTP、DNS、RADIUS，HTTPS、LDAP、ORACLE/MSSQL/MYSQL 数据库等多种类型的探测判断机制。 8、★与招标人现有的致远互联软件实现兼容，产品间协同稳定运行。**（提供厂商互认兼容性认证相关证明材料）** 9、★支持在同一个虚拟服务下同时配置多个 IPv4 和 IPv6 地址以及多个不连续应用端口或者端口范围。**（提供功能截图或相关证明文件）** 10、指定 ssl 加密套件和客户端认证证书的 https/ssl 健康检查，自定义服务器端 SSL 协议策略(比如 SNI)加密流量。 11、支持对设备的管理日志进行新旧配置对比，及时发现设备管理上的变化。 **四、▲原厂服务：** 提供原厂 5 年产品支持服务，服务级别为 7x24x4（7 表示 每星期周一至周日，24 表示全天 24 小时，4 表示我司提出现场服务需求时能够在 4 小时之内到达现场）。	
4	**入侵防御设备**	**一、▲硬件配置：** 所投产品采用国产自主芯片和国产自主操作系统。 **（需提供芯片、操作系统厂商和规格型号）** 外形：1U 标准机架式硬件 千兆电口：≥8 个（3 对 bypass） 千兆光口：≥4 个 万兆光口：≥4 个（含 4 个万兆多模模块） 管理接口：1 个 电　　源：2 个交流冗余电源 拓展插槽：≥2 个 **二、▲性能指标：** 网络层吞吐量：≥15Gbps 应用层吞吐量：≥3Gbps 存储空间：≥4TB 并发连接数：≥400 万 四层新建连接数：≥25 万 **三、功能特性：** 1、配置入侵防护、抗拒绝服务、数据防泄漏、应用管理	1 台

		功能授权； 2、★威胁分布展示：支持安全日志级别、类别分布、TOP 源 IP 地理分布、入侵事件-攻击类别、趋势分布、高风险入侵事件趋势分布，TOP 入侵事件等多种威胁状态告警信息趋势图，清楚的了解不同威胁类别的威胁攻击分布情况。**（提供具有 CMA 标识第三方机构出具检测报告扫描件）** 3、系统特征库规则数量多达 10000+，且支持按规则名称、规则 ID、影响应用、影响系统、服务类型、威胁分类、攻击手段、危险程度、可信度等信息查询规则。 4、★支持敏感数据防护功能，防止内部敏感数据（身份证、电话号码、银行卡号）的泄露；支持文件识别，监控特定格式的文件的外发（可识别文件类型如文档、压缩文件、图像、音频、视频、脚本、程序等），支持自定义敏感数据。**（提供功能截图或相关证明文件）** 5、系统应提供先进的 DoS/DDoS 攻击防护能力，支持双向阻断 TCP/UDP/ICMP/ACKFlooding,以及 UDP/ICMPSmurfing 等常见的 DoS/DDoS 的攻击,在透明模式下防止 SYNFlood 攻击。 6、系统应能够有效抵御 SQL 注入、XSS 注入、webshell 等多种常见的应用层安全威胁,并可配置 SQL 注入白名单。 7、系统需提供至少八种以上内置规则模板，帮助用户快速上线。如 DMZ 区服务器、内网客户端、Web 服务器、Windows 服务器、Linux 服务器、攻防演练高频高危等规则模板，并可根据内置规则模板直接派生模板。 8、系统应支持不少于 10 种协议的暴力猜测防护，包含且不限于 Telnet、SSH、SMB、FTP、RDP、POP3、SMTP、IMAP、HTTP、数据库协议等，并能对暴力猜测阈值进行设置。 9、系统应支持弱口令检测配置，并提供至少 7 种非弱口令判别依据，支持导入自定义弱口令字典。须支持强密码复杂度，如同时包含大写、小写、特殊字符或数字等组合方式。 10、★支持对挖矿行为进行防护，并可将产生的挖矿行为生成日志，可通过源地址和目的地地址和信誉等级进行查询，可展示挖矿日志的威胁类型、挖矿值及协议等。**（提供具有 CMA 标识第三方机构出具检测报告扫描件）** 11、★支持对 Syslog 内容、格式自由定制，包括外发的日志模板自定义，编码方式至少支持 UTF-8、GB2312 和 UNICODE，且根据需求可对审计日志、入侵事件日志、恶意文件日志、文件传输控制日志、敏感数据日志、高级恶意样本日志、回连监控日志、C&C 通信日志、DNS 黑名单	

		日志、IP 黑名单日志、WEB 安全日志、服务器异常日志、URL 分类日志、DOS 防护日志、应用管理日志和设备日志等可选和可编辑。**（提供具有 CMA 标识第三方机构出具检测报告扫描件）** 12、支持不少于 1000 条访问控制策略，可基于 IP 地址、端口（单个、多个和范围）、协议、动作（阻断、允许）进行访问策略配置，并可支持是否生成访问控制策略的会话日志生成。系统需提供漏洞公告咨询和情报咨询；在漏洞公告中能关联显示已发布的规则，帮助用户更快设置防护策略。 14、★支持设备云端托管服务，将设备上确认威胁告警事件风险上报到云端平台，通过 APP 即时查看告警，实现 APP 运维管理。**（提供功能截图或相关证明文件）** 15、产品资质：产品应具有国家信息安全漏洞库(CNNVD)兼容性资质证书、国家信息安全测评信息技术产品安全测评证书（EAL4+级别）和 IPv6 Ready Logo 证书。**（提供证书扫描件）** **四、▲原厂服务：** 提供五年攻击规则库授权及升级服务；提供原厂 5 年产品支持服务，服务级别为 7x24x4（7 表示 每星期周一至周日，24 表示全天 24 小时，4 表示我司提出现场服务需求时能够在 4 小时之内到达现场）。	
5	**网页应用防火墙**	**一、▲硬件配置：** 所投产品采用国产自主芯片和国产自主操作系统。 外形：1U 标准机架式硬件 千兆电口：≥6 个（3 对 bypass） 千兆光口：≥4 个 管理接口：1 个 电　　源：2 个交流冗余电源 拓展插槽：≥2 个，支持扩展万兆光口 **二、▲性能指标：** 网络层吞吐量：≥20Gbps 应用层吞吐量：≥3Gbps 存储空间：≥256GB SSD +4TB HHD 并发连接数：≥70 万 七层新建连接数：≥6 万 **三、功能特性：** 1、▲支持串联、反向代理、旁路部署和集群部署模式。 2、XML 攻击防护:对以 XML 格式传输和存储的数据进行解码检测识别，支持导入 Schema 文件和 WSDL 文件对上传	2 台

		的 XML 文件进行格式校验，防止攻击者恶意提交 XML 文件，支持外部实体、垃圾字符填充等注入攻击防护。 3、扫描防护:支持通过识别扫描工具的数据特征值，阻断扫描工具的探测。支持基于请求量统计和应答分布统计等算法对扫描行为进行分析并防护。 4、★支持 Nginx 插件部署以 Nginx 扩展模块的形式与 WAF 进行交互,保障业务的高稳定性。插件式部署是指由 Nginx 插件在将流量转发至源站前，通过子请求将流量复制一份发送给 WAF,由 WAF 做检测，并将检测结果返回给 Nginx，由 Nginx 完成阻断动作。**（提供具有 CMA 标识第三方机构出具检测报告扫描件）** 5、★自识别国密算法:支持一个站点同时配置通用协议证书和国密协议证书，支持 SM2、SM3、SM4 等国密算法，支持 HTTPS 站点通用协议和国密协议算法自识别。**（提供具有 CMA 标识第三方机构出具检测报告扫描件）** 6、★人机识别:可通过 JS 脚本识别自动化工具，并能够对自动化工具访问请求配置放过、阻断、接受、伪装等处置动作。可以根据客户端环境检测，识别攻击工具，主要包括:市面上主流扫描器，如 burpsuite、nessus 等，市面上主流自动化工具 selenium、phantomjs 等的脚本攻击识别。**（提供具有 CMA 标识第三方机构出具检测报告扫描件）** 7、会话追踪:会话追踪通过追踪用户向 Web 应用服务器发起的访问请求以及用户所有的 Web 操作，并记录详细的访问日志，为攻击事件事后分析、攻击场景还原以及关联用户所有的 Web 操作提供关联分析数据基础，同时还能进行用户行为研究，了解用户操作背后是否隐藏了潜在的攻击动机。 8、★页面动态混淆防护:在保证业务和页面展示效果的情况下，对响应页面中的 Form 表单、a 标签、Javascript 文件等关键信息进行混淆，支持对例外 URL 不进行混淆操作。**（提供具有 CMA 标识第三方机构出具检测报告扫描件）** 9、★紧急模式：支持配置并发连接数阈值，当并发连接数超过设置阀值时,WAF 自动进入紧急模式,已经代理的连接正常代理，对新增的请求直接转发，当连接数恢复正常时，自动退出紧急模式。**（提供具有 CMA 标识第三方机构出具检测报告扫描件）** 10、支持客户端证书+账号密码的双因子认证方式，提高 WAF 自身管理的安全性。支持一键例外策略，降低误报。支持独立的基于机器学习和词法分析的智能检测能力。支	

		持 IPv6/IPv4 双协议栈防御。支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测。 11、支持 Cookie 安全机制，包括 Cookie 加密和 Cookie 签名的防护算法。支持过期兼容时间配置。 **四、▲原厂服务：** 提供五年应用规则库授权及升级服务；提供原厂 5 年产品支持服务，服务级别为 7x24x4（7 表示 每星期周一至周日，24 表示全天 24 小时，4 表示我司提出现场服务需求时能够在 4 小时之内到达现场）。	
6	**接入交换机**	一、▲硬件配置： 1、投标产品 CPU（如有）使用国产自主 CPU,交换芯片使用国产自主交换芯片。**（需提供 CPU（如有）、交换芯片厂商和规格型号）** **2、1**U 标准机架式硬件，配置≥28 个千兆电端口、≥4 个千兆 Combo 端口、≥8 个万兆光端口、2 个模块化风扇（**风扇面板侧出风**）和 2 个可插拔电源（**电源面板侧出风**），1 个业务扩展槽位(支持扩展 40GE QSFP+、100GE QSFP28 接口板卡)。 二、▲性能指标： 1、交换容量≥2.4Tbps，包转发率≥660Mpps。以官网所列最低参数为准。**（提供功能截图或相关证明文件）** 三、功能特性： 1、支持 IPv6 协议栈，具有 IPv4/v6 静态路由、OSPFv2，OSPFv3、BGP4、BGP4+、MPLS、MPLS VPN 等 IPv4/v6 动态路 由功能。 2、支持 VLAN 功能，支持 Guest VLAN、Voice VLAN、QINQ、灵活 QINQ。 3、支持集群或堆叠多虚一技术，实现单一界面管理多台设备 4、★配置 m-lag 或 DRNI 或 VPC 跨设备链路聚合功能授权，在跨设备链路聚合组网环境中，支持多台设备配置实时同步。**（提供功能截图或相关证明文件）** 5、★支持 Telemetry GRPC 可视化**（提供功能截图或相关证明文件）**。 6、★支持 256 位全端口 MACSEC 加密**（提供功能截图或相关证明文件）。** 7、设备软件采用当前最高版本，配置所有功能的软件授权 license，后续所有功能启用均不需额外付费。 8、设备应具有良好的兼容性，能兼容招标人现有交换设备。	4 台

		四、▲原厂服务： 提供原厂 5 年产品支持服务，服务级别为 7x24x4（7 表示 每星期周一至周日，24 表示全天 24 小时，4 表示我司提出 现场服务需求时能够在 4 小时之内到达现场）。	
7	**零信任（软件）**	1、▲信息技术应用创新零信任综合网关一套，支持信息技术应用创新云平台环境部署，软件买断模式，并发用户接入数量≥200 个。 2、通过隧道模式，可以支持基于 TCP、UDP、ICMP 等协议代理访问业务资源，支持发布 IP、IP 范围、IP 段、具体域名及通配符域名等形式的服务器地址，满足常见办公业务的代理，收缩业务暴露面。为简化资源发布配置，隧道模式应支持同一个资源发布多个服务器地址；管理员还可基于业务的特殊性，自主选择优先使用长连接或短连接进行业务代理。 3、为提升终端用户使用的便利性，零信任系统需要支持跟单位现有的桌面云服务器进行单点登录对接，实现仅需在零信任进行认证即可直接进入云桌面进行业务办公，无需重复验证。 4、为提升业务应用的数据安全性，零信任系统应支持针对发布的 WEB 应用开启 WEB 水印，水印内容至少包括：用户名+当前年月日，起到威慑与溯源作用，有效预防数据泄露。 5、支持配置是否允许用户自助申请应用访问权限，启用后，管理员可以在控制台根据审批状态查看应用申请详情，包括但不限于：申请时间、用户名、所属组织架构、角色、应用名称、应用访问地址、申请理由、申请有效期等。应用管理员可对待审批的应用进行批准或驳回操作，支持批量操作。 6、★为强化系统认证安全性，可配置在触发异常环境的条件时，用户需完成增强认证才可登录。可配置的异常环境包括但不限于：帐号首次登录、帐号在该终端首次登录、闲置帐号登录、弱密码登录、异常时间登录、非常用地点登录等。**（提供功能截图或相关证明文件）** 7、可直接为已经集成零信任 SDK 并发布到安卓或 ios 应用市场的公有化生态应用配置策略，使其具有零信任接入能力及数据防泄漏能力，如泛微 OA、致远 OA 等。 8、为了最大程度缩小网络、业务暴露面，零信任平台需提供单包授权能力（SPA），支持 UDP+TCP 组合的单包授权技术，未授权用户无法连接零信任设备，无法扫描到服务端口，不会出现敲门放大漏洞。	1 套

		9、支持用户使用单位现有零信任客户端接入到本次采购的零信任网关。 10、★应支持将具有异常登录行为的用户日志自动打标签为用户安全日志，以便于管理员快速审计定位。用户安全日志包括但不限于：帐号安全（应包含帐号首次登录、异常时间登录、非常用地点登录、弱密码登录、爆破登录、闲置帐号登录、帐号在新终端登录等）、中间人攻击、SPA安全（应包含SPA端口扫描、SPA爆破攻击、SPA敲门伪造、SPA重放攻击、SPA安全码泄漏等）、cookie劫持等。**（提供功能截图或相关证明文件）** 13、▲提供原厂5年产品支持服务，服务级别为 7x24x4（7 表示 每星期周一至周日，24 表示全天 24 小时，4 表示我司提出 现场服务需求时能够在 4 小时之内到达现场）。	
8	**运维审计与风险控制系统（软件）**	1、信息技术应用创新运维审计与风险控制系统1套，支持信息技术应用创新云平台环境部署，软件买断模式，可管理设备数量≥200个，运维用户无限制；单台设备字符类并发会话≥200个、图形类并发会话≥50个。 2、★具备自动化编排能力，通过编排动作流的方式，对目标资产进行定时或周期性的自动化运维。动作流可包括：上传文件、执行命令、下载文件等。**（提供功能截图或相关证明文件）** 3、支持按部门组织架构（至少10个层级的部门）管理用户数据、资产数据、授权数据、审计数据，且数据相互隔离；可按部门层级分别设定各部门不同权限的管理员，如部门内的运维管理员、审计管理员、系统管理员等。每个部门管理员仅可管理本部门及下级部门的相关配置。 4、★支持Windows/macOS操作系统下C/S架构的堡垒机专用客户端，可通过此专用客户端登录堡垒机，对堡垒机进行简单的管理及运维资产操作；支持UOS /麒麟等国产操作系统下C/S架构的堡垒机专用客户端登录堡垒机并进行管理及运维操作。**（提供功能截图或相关证明文件）** 5、★支持DB2、Oracle、MySql、SQL Server、PostgreSQL、KingbaseES、DM、GBase8a、GBASE8s的协议运维代理，可直接调用本地windows系统的数据库客户端工具。**（提供功能截图或相关证明文件）** 6、自动收集授权关系：支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权。 7、★支持同时对数据库会话记录图形审计及命令提取，	1套

		并且实现点击任意一条数据库命令，自动跳转到对应的录像片段。**（提供功能截图或相关证明文件）** 8、支持对数据库运维会话的上行和下行命令进行审计。 9、支持国密 TLS 双向认证通信，开启后需同时使用支持国密算法的浏览器、国密 USBkey 才能访问堡垒机，只使用国密浏览器无法访问堡垒机。 10、★审计日志要求：支持保存 SFTP/FTP 传输的原始文件;支持保存 SSH 的 rz 命令（zmodem）传输的原始文件;支持保存远程桌面之间传输的原始文件。**（提供具有 CMA 标识第三方机构出具检测报告扫描件）**	
9	**辅材**	提供系统集成所必须的网络跳线，光纤跳线等（跳线规格需和招标人数据中心现使用跳线规格一致）。	1 批
10	**安装部署培训服务**	操作系统、数据库安装配置、网络设备安装配置、网线标签整理、使用培训等。	1 项

三、**备品备件及专用工具**

1、备品备件：中标人提供能够满足质量保证期内的设备维修要求的备品备件，备品备件应是新品。

2、专用工具：中标人提供设备安装、调试、验收、维修、保养所必要的专用工具、仪器、仪表等工具。

四、包装运输

1、中标人负责设备包装、办理运输和保险，将设备安全运抵交货地点。

2、设备制造完成并通过试验后应及时包装，否则应得到切实的保护，确保其不受污损。

3、在包装箱外应标明招标人的订货号、发货号。

4、各种包装应能确保各零部件在运输过程中不致遭到损坏、丢失、变形、受潮和腐蚀。

5、包装箱上应有明显的包装储运图示标志。

6、整体产品或分别运输的部件都要适应运输和装载的要求。

7、随产品提供的技术资料应完整无缺。

五、质保及售后服务

在质保期内，非招标人过失和故意并且在正常使用的情况下发现商品有缺陷，中标人将免费修理或替换该设备；在质保期间内，非招标人过失和故意并且在正常使用的情况下设备发生故障，中标人应及时提供免费服务。

六、其他要求

项目验收前采购人保留测试权力,如发现中标人技术参数要求响应情况与投标产品不符等虚假响应的，将按违约处理，中标人承担一切责任。

投标人承诺：若我方中标，项目验收前采购人保留邀请第三方测试权力，测试费用由我方支付。如发现我方技术参数要求响应情况与投标产品不符等虚假响应的，将按违约处理，我方承担一切责任。