采购需求

一、采购需求一览表

序号	产品名称	数量	单位	规格参数	备注
1	防火墙（互联网出口）	1	台	1、硬件规格：硬件参数：1U；单交流电源；≥10*GE 电口，≥2*combo 口，≥500G 硬盘；网络吞吐量≥4Gbps；最大并发连接数≥150 万，每秒新建 HTTP 连接数≥4 万。 2、部署模式：支持路由模式、透明（网桥）模式、混模式，支持将多个物理网口加入一个网桥中；部署模式切换无需重启设备；支持镜像和被镜像。 3、支持源地址转换、目的地址转换、双向地址转换、NAT44。 4、支持 4G 扩展网卡。支持在 4G 接口上运行 IPSec VPN，提供 web 配置界面截图 访问控制：支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL 过滤、应用过滤、会话老化时间、终端过滤等高级访问控制功能。 5、支持与主流 VPN 厂商的 IPSec VPN 接入，支持的算法有 DES、3DES、AES128、SM2、SM3、SM4 等，支持预共享密钥、数字证书、国密证书方式建立隧道（提供功能截图证明并加盖生产厂家公章或投标专用章）。 6、防私接路由：支持识别和封堵私接主机，包括 360 随身 wifi、猎豹 wifi、无线路由器等软硬件网络共享方式；可制定策略分别设置私接终端类型个数为阀值进行封堵，同时支持基于 IP 配置白名单，支持自定义阻断时间，支持限速时长内添加到惩罚通道（提供功能截图证明并加盖生产厂家公章或投标专用章）。 7、支持 portal 服务器联动，支持 radius 服务器联动，支持实现 NAS-Identifier(32)在无线场景携带 AC 名字。 ▲8、支持非法外联学习和防护特性，可有效保障服务器安全，可	

				定义外联白名单地址和端口，也可通过流量自学习获得服务器合法的外联行为，学习时长可选择 1 小时、12 小时、一天、一周等。（提供功能截图证明并加盖生产厂家公章或投标专用章） 9、支持微信认证，可以选择获取 IP 地址、OpenID 或手机号等实名信息，支持与微信公众平台进行认证联动，认证方式包括公众号按钮跳转、公众号回复关键词等方式。认证过程中要求用户必须关注公众号，帮忙企业实现品牌营销（提供功能截图证明并加盖生产厂家公章或投标专用章）。 10、拥有自有数据来源，每日可获得不低于 6 亿次的互联网访问样本（提供功能截图证明并加盖生产厂家公章或投标专用章）。 11、支持实时获取威胁情报，并应用威胁情报对本地资产进行威胁检测，并可对检测到的威胁情报支持单点登陆威胁情报云平台查看该情报详情。 ▲12、支持 IP 准入、MAC 准入、IP+MAC 准入、本地 WEB 认证、Portal 认证、短信认证、免认证、微信认证、混合认证、AD 域单点登录和访客二维码认证（提供功能截图证明并加盖生产厂家公章或投标专用章） 13、支持缓存安卓和 iOS 文件，文件形式不限于视频、APP、文本文件等，并支持自学习性缓存，设备可自动缓存特定服务器的所有终端应用（提供功能截图证明并加盖生产厂家公章或投标专用章）。 ★14、获得公安部计算机信息系统安全专用产品销售许可证（提供证书复印件加盖生产厂家公章或投标专用章）。	
2	防火墙（服务器区）	1	台	1、硬件规格：1U；双交流电源；≥12*GE 电口，≥12*SFP 光口，≥500G 硬盘，网络吞吐量≥8Gbps，应用层吞吐量≥1000M；最大并发连接数≥300 万，每秒新建 HTTP 连接数≥10 万。 2、部署模式：支持路由模式、透明（网桥）模式、混模式，支持将多个物理网口加入一个网桥中；部署模式切换无需重启设备；支持镜像和被镜像。 3、支持源地址转换、目的地址转换、双向地址转换、NAT44。	

				4、支持 4G 扩展网卡。支持在 4G 接口上运行 IPSec VPN，提供 web 配置界面截图 访问控制：支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL 过滤、应用过滤、会话老化时间、终端过滤等高级访问控制功能。 5、支持与主流 VPN 厂商的 IPSec VPN 接入，支持的算法有 DES、3DES、AES128、SM2、SM3、SM4 等，支持预共享密钥、数字证书、国密证书方式建立隧道（提供功能截图证明并加盖生产厂家公章或投标专用章）。 6、防私接路由：支持识别和封堵私接主机，包括 360 随身 wifi、猎豹 wifi、无线路由器等软硬件网络共享方式；可制定策略分别设置私接终端类型个数为阀值进行封堵，同时支持基于 IP 配置白名单，支持自定义阻断时间，支持限速时长内添加到惩罚通道（提供功能截图证明并加盖生产厂家公章或投标专用章）。 7、支持 portal 服务器联动，支持 radius 服务器联动，支持实现 NAS-Identifier(32)在无线场景携带 AC 名字。 ▲8、支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口，也可通过流量自学习获得服务器合法的外联行为，学习时长可选择 1 小时、12 小时、一天、一周等。（提供功能截图证明并加盖生产厂家公章或投标专用章） 9、支持微信认证，可以选择获取 IP 地址、OpenID 或手机号等实名信息，支持与微信公众平台进行认证联动，认证方式包括公众号按钮跳转、公众号回复关键词等方式。认证过程中要求用户必须关注公众号，帮忙企业实现品牌营销（提供功能截图证明并加盖生产厂家公章或投标专用章）。 10、拥有自有数据来源，每日可获得不低于 6 亿次的互联网访问样本（提供功能截图证明并加盖生产厂家公章或投标专用章）。 11、支持实时获取威胁情报，并应用威胁情报对本地资产进行威胁检测，并可对检测到的威胁情报支持单点登陆威胁情报云平台查看	

				该情报详情。 ▲12、支持 IP 准入、MAC 准入、IP+MAC 准入、本地 WEB 认证、Portal 认证、短信认证、免认证、微信认证、混合认证、AD 域单点登录和访客二维码认证（提供功能截图证明并加盖生产厂家公章或投标专用章） 13、支持缓存安卓和 iOS 文件，文件形式不限于视频、APP、文本文件等，并支持自学习性缓存，设备可自动缓存特定服务器的所有终端应用（提供功能截图证明并加盖生产厂家公章或投标专用章）。 ★14、获得公安部计算机信息系统安全专用产品销售许可证（提供证书复印件加盖生产厂家公章或投标专用章）。	
3	WEB 应用防护系统	1	台	1、标准 1U 硬件， 2*GE 电管理口，≥4*GE 电业务口（含 2 组硬件 BYPASS 模块），≥4*GE 光业务口,硬盘≥1T，1*RJ45 串口，单电源。吞吐量≥1Gbps,HTTP 最大并发数≥5 万,HTTP 新建连接(CPS) ≥5000，物理保护链路 4 路，保护站点无限制。 2、端口镜像部署：镜像服务器流量即可实现安全审计和告警。 3、能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括 SQL 注入、命令注入 、Cookie 注入、代码注入、LDAP 注入、SSI 注入文件注入等）、跨站请求伪造等应用攻击行为。 4、内置主流 Webshell 特征库，对上传内容进行检查，防止恶意 Weshell 上传。 5、WAF 能自动识别扫描器的扫描行为，并智能阻断如 Nikto、Paros proxy、WebScarab、WebInspect、Whisker、libwhisker、Burpsuite、Wikto、Pangolin、Watchfire AppScan 、N-Stealth、Acunetix Web Vulnerability Scanner 等多种扫描器的扫描行为。 ▲6、支持按地理区域对攻击次数等进行统计，通过地图展示，并在地图上可以指定某一地理区域进行访问控制，阻断此区域 IP 的访问。（提供功能截图，以及提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章）	

				▲7、支持细粒度检测条件，可基于 URL、请求头部字段、目标 IP、请求方法等多种组合条件进行检测，检测指标可通过 URL 访问速率和 URL 访问集中度、请求离散度三重检测减少误判率；检测的客户端对象可支持 IP、IP+URL、IP+User_Agent 多种算法，客户端 IP 支持应用层字段解析，并支持自定义检测字段功能；支持基于地理位置的识别，可设置不同地理区域的检测，杜绝海外肉机攻击（提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章）。 8、支持云端威胁情报联动，可主动发现包括僵尸 IP、代理 IP、扫描 IP、黑产 IP、C&C 等恶意 IP 发起的访问行为，针对访问行为进行日志记录通知客户，实时统计威胁情报的攻击攻击类型占比和攻击的频率（提供界面截图并加盖生产厂家公章或投标专用章）。 9、云端高防联动：WAF 与云端高防中心联动，通过 WAF 一键开启防护，实现 3-7 的 DDOS 安全防护服务 10、系统提供防篡改功能，能够防止被篡改内容被浏览者访问到，一旦检测到被篡改，实时发送告警信息给管理员。 ▲11、可实现访问流程的校验，向网站提交表单前必须先访问指定的网页，并等待可配置的时间长度后才能正常提交表单（提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章）。 12、内置 SSL 硬件加速卡，实现对 HTTPS 的加解密，提供设备对 HTTPS 的处理性能（提供界面截图并加盖生产厂家公章或投标专用章）。 13、支持与同品牌的 APT 设备进行联动，对未知威胁流量进行检测和拦截（提供界面截图并加盖生产厂家公章或投标专用章）。 14、具有国家信息安全测评中心颁发的《信息技术产品安全测评证书》级别 EAL3+，提供证书复印件。	
4	数据库审计系	1	台	1、1U 机架设备，单电源；内存：≥8GB；硬盘容量≥1TB；网络端口：6 个千兆电口。	

	统			2、处理能力：总网络吞吐量≥500Mbps；双向审计最大数据库流量≥100Mbps；峰值事务处理能力 TPS≥6000 条/秒；数据库实例授权许可数量≥4。 ▲3、针对缺少物理端口的数据库服务器环境，例如云环境、虚拟化环境等内部流量无法提供镜像流量的场景,支持在目标数据库安装 agent 代理解决数据库的审计（提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章)。 4、支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、MariaDB、PostgreSQL、GuassDB、HANA、Teradata、Cache、人大金仓、达梦、南大通用数据库、Redis 等数据库审计； 5、支持 MongoDB、Hbase、Hive、impala、Elastic Search、HDFS、Canssandra、greenplum、LibrA、graphbase、cache 等数据库审计；(提供功能截图并加盖生产厂家公章或投标专用章)。 6、支持主流业务协议 HTTP、HTTPS、Telnet、FTP 的审计； 7、可以通过导入证书的方式实现审计和防护，支持对 Mysql5.7 及以上版本、SQL server（2005 及以上版本）数据库采用了加密协议通讯的审计(提供功能截图并加盖生产厂家公章或投标专用章)。 8、支持数据库的双向审计（请求和返回），包括请求语句、返回结果集、返回行数、运行时长、运行结果、客户端信息、服务器端信息等内容，支持通过返回行数和内容大小控制返回结果集大小；(提供功能截图，并提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章)。 9、支持用户界面告警、钉钉、SNMP、邮件、短信五种方式告警（提供功能截图并盖原厂章)。 10、支持系统安全配置（登录超时、用户登录失败锁定策略、密码强弱策略、密码有效时间） 11、支持规律过滤规则，过滤规则包含 IP 过滤、SQL 模板过滤和	

				自定义过滤，自定义过滤条件不少于 28 个条件。 ▲12、支持对数据库自动建模及智能对异常行为告警功能（提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章）。 13、具有国家信息安全测评中心颁发的《信息技术产品安全测评证书》级别 EAL3+，提供证书复印件；	
5	日志审计	1	台	1、标准 1U 硬件；≥1*console 口；网络接口:1000M 电口≥6；硬盘≥1T；内存≥8G；单电源；日志处理能力≥2000EPS（峰值≥4000EPS）；标配资产授权≥30 个； 2、产品采用 CF 卡启动（提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章）。 3、支持手动或按周期自动备份系统配置，可随时对系统资产等配置进行还原操作，且自动备份周期与备份包个数可配；支持系统配置备份自动备份至远程服务器(提供截图并加盖生产厂家公章或投标专用章)。 支持 Syslog、SNMP Trap、OPSec、FTP 协议日志收集。 4、支持常见的虚拟机环境日志收集，包括 Xen、VMWare、Hyper-V 等（提供截图并加盖生产厂家公章或投标专用章）。 日志分析：可以基于日志等级进行过滤； 5、应该可以通过自定义配置将用户不关心的日志过滤掉； ▲6、支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件，（提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章）； 7、支持可由用户定义和修改的日志的聚合归并逻辑规则。 8 内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等 5 大类 50 子类的安全分析场景（提供截图并加盖生产厂家公章或投标专用章）。	

				9、具备安全评估模型，评估模型基于设备故障、认证登陆、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。（提供截图并加盖生产厂家公章或投标专用章） 10、内置 SOX、ISO27001、WEB 安全等解决方案包（提供截图并加盖生产厂家公章或投标专用章）。 11、内置完善的等级保护合规报表（内置综合性自动化审计报告；支持用户自定义报表；自定义的报表支持多个统计维度的数据集合；支持报表导出为 PDF 和 Word 格式文件。 用户支持双因子认证登录，双因子认证令牌支持绑定至具体用户。 ▲12、通过在目标主机上安装 agent 程序，支持监控目标主机的 CPU 利用率、内存使用率、磁盘使用情况、流量等信息，并支持设置报警阈值(提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章)。 13、资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定。拓扑可以显示资产采集的事件数量被采集资产的状态等信息。（提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章）	
6	APT 攻击预警平台	1	台	1、软硬一体化 2U 标准机架式设备；1+1 冗余电源；内存≥16G；硬盘容量≥1T*1；接口数量： Consle*1,USB*2,千兆电口≥6；网络层≥1Gbps，应用层≥500Mbps；WEB 检测：HTTP 最大并发数≥7 万/秒。 2、旁路镜像模式部署，不影响服务器处理性能和网络架构； 3、全流量检测：支持全流量检测，可根据需求打开或关闭全流量检测功能。 4、支持解析 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、Mysql、	

				MSSQL、DB2、Oracle、HTTPS、SMTPS、POP3S、IMAPS 等协议报文（HTTPS、SMTPS、POP3S、IMAPS 加密协议解析需要导入服务器私钥证书），并提供审计协议类型的端口号配置，可根据需要变更端口号；（提供截图证明并加盖生产厂家公章或投标专用章） 5、支持对 Telnet、FTP、POP3、SMTP、IMAP 等协议进行弱口令检测。 6、支持 WEB 特征攻击风险白名单配置，白名单颗粒度可达到 WEB 特征类别、WEB 特征规则和 HTTP 方法（提供截图证明并加盖生产厂家公章或投标专用章）。 7、支持与防火墙进行联动，支持自定义防火墙阻断时长，并展示最新联动状态、状态更新时间，支持查看阻断信息，阻断信息包括阻断 IP、阻断开始时间、阻断结束时间、阻断状态等（提供截图证明并加盖生产厂家公章或投标专用章）。 ▲8、支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现（提供截图证明并加盖生产厂家公章或投标专用章）。 9、采用多并发沙箱检测技术，集成主流的操作系统 winXP、win7 等多种检测环境，可结合平台内置的反病毒引擎和静态分析技术、动态模拟技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析。（提供截图证明并加盖生产厂家公章或投标专用章） 10、支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、同步验证、信息收集等功能。（提供截图证明并加盖生产厂家公章或投标专用章） ▲11、支持对私网地址 IP 地理位置信息添加，在产生告警时，定义 IP 可正常显示所属地理位置信息（提供截图证明并加盖生产厂家公章或投标专用章）。 12、支持 kafka、短信、邮件、syslog、ftp、钉钉等告警方式。支持对 kafka、syslog 发送的风险信息进行 AES 加密传输（提供截图证明并加盖生产厂家公章或投标专用章）。 ★13、获得公安部计算机信息系统安全专用产品销售许可证（提供	

				证书复印件加盖生产厂家公章或投标专用章)。	
7	主机安全及管理系统	1	台	1、基本配置：包含终端管理中心软件一套，实现对 10 台服务器及 500 台终端的统一管理和策略下发。支持对服务器进行防护。防护内容包括：病毒查杀、漏洞管理、网络防护、勒索防护等。支持 Windows server 2008、Windows server 2012、Windows server 2016、Centos 5.0 +、Redhat 5.0 + 、 Suse11 +、 Ubuntu 14 +等操作系统； 2、支持对 CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对 CPU、内存达到一定阈值时客户端进行熔断。(提供证明截图并加盖生产厂家公章或投标专用章) 3、高级威胁防护模块：对失陷后主机远控持久化行为进行检测(反弹 shell、远程控制)，可阻断远控（提供界面截图并加盖生产厂家公章或投标专用章)。 4、对内网的恶意攻击行为进行识别（漏洞利用、横向移动)，可阻断恶意探测行为（提供界面截图并加盖生产厂家公章或投标专用章)。 5、可对渗透的收尾阶段的数据清除行为进行识别和阻断（提供界面截图并加盖生产厂家公章或投标专用章)。 系统安全性模块：支持防端口扫描，锁定恶意的端口扫描，并记录告警。(提供界面截图并加盖生产厂家公章或投标专用章) 6、支持对系统登录行为进行一定的限制，可设置单个 IP 请求时间、登录失败次数、IP 临时锁定时间。 ▲7、识别渗透过程中的隧道代理（端口映射、端口转发、内网代理)，可阻断隧道代理搭建行为（提供界面截图并加盖生产厂家公章或投标专用章) 8、支持智能检测防御 CC 攻击，并可进行高、中、低三档设置。(提供界面截图并加盖生产厂家公章或投标专用章) 9、内核级防火墙（业务间流量东西向隔离）功能，包括 IP、端口、协议、流向等细粒度权限控制。	7

				10、支持流量画像，支持全网流量可视化 （提供界面截图并加盖生产厂家公章或投标专用章）。 11、支持登录防护，包括以系统账号为粒度的异常登录防护、支持五个任意维度(任意地理位置，任意 IP，任意域名，任意计算机名，任意时间)的系统登录访问策略设置。 12、提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密。支持白名单设置。（提供界面截图并加盖生产厂家公章或投标专用章） 文件推送：支持下发文件、安装应用程序、远程执行命令。 13、屏幕水印：支持对屏幕拍照泄密数据的行为进行溯源。（提供界面截图并加盖生产厂家公章或投标专用章） 14、集中管控：管理平台支持一键卸载客户端、一键设置客户端卸载密码、一键停止/恢复所有防护、一键解除绑定。 ▲15、支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露（提供界面截图并加盖生产厂家公章或投标专用章）。 16、能监测节点遭受网络攻击的趋势信息，可以直观的了解攻击目标、攻击源、攻击方式的变化趋势和详细资料。	
8	堡垒机	1	台	1、配置规格：标准 1U 硬件，≥2*GE 电管理口，≥4*GE 电业务口，≥4*GE 光业务口,硬盘≥1T；1*RJ45 串口，单电源。最大资产数≥200 个，最大字符连接≥200 个，最大图型连接≥50 个。 2、支持按部门组织架构（至少 5 个层级的部门）管理用户数据、资产数据、授权数据、审计数据。（提供功能截图证明并加盖生产厂家公章或投标专用章） 3、每个部门的部门管理员可以管理本部门及下级部门的主机、授权关系、策略。 4、身份认证要求：产品内置 VPN 模块，无需与其他 VPN 设备联动，实现运维入口安全接入。 5、支持与 get、post、soap 发送方式的 http 短信网关平台进行联	8

				动，实现短信动态口令双因素认证机制，如与阿里云短信服务、SendCloud 联动（提供功能截图证明并加盖生产厂家公章或投标专用章）。 6、支持手机 APP 动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定 APP 动态口令。 基于不同的用户设置不同的双因子认证模式，如 user1 用动态令牌、user2 用 USBkey、user3 手机 APP 动态口令认证（提供功能截图证明并盖生产厂家公章或投标专用章）。 7、支持域认证与双因子认证结合使用，如同时使用 AD/LDAP 用户名+AD/LDAP 密码+手机 APP 动态口令登录堡垒机、同时使用 AD/LDAP 用户名+AD/LDAP 密码+短信口令登录堡垒机。 ▲8、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，甚至可自动完成授权（提供功能截图，以及提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章）。 9、设备管理要求：支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库 Oracle、MSSQL、MySQL、DB2、VMware vSphere Client、AS400 等客户端工具。 10、支持 sqlserver 数据库协议代理运维，可直接调用本地 windows 系统的数据库客户端工具，支持自动登录、无需应用发布前置机。 11、支持 DB2、oracle、mysql、sqlserver 主流数据库协议代理运维，可直接调用本地 windows 系统的数据库客户端工具，支持自动登录、无需应用发布前置机（提供功能截图证明并盖生产厂家公章或投标专用章）。 12、可以通过 socks5/http/ssh 等代理协议连接管理异地云资源区中私有网络的云主机（提供功能截图证明并盖生产厂家公章或投标专用章）。 13、导出的设备信息文件加密存储，解密时须由 2 个管理员同时解	

				密才能查看到设备信息文件内容。 14、自动改密要求：支持完善的自动改密策略，包括改密前发送密码、发送失败不改密、改密后发送密码、密码文件加密、密码强度控制、自动密码恢复等。发送方式包括邮件、FTP、SFTP 等（提供功能截图证明并盖生产厂家公章或投标专用章）。 15、支持通过堡垒机页面直接调用本地 Windows 系统里的 plsql、sqlplus、toad、sqlwb、ssms、mysql.exe 等数据库客户端工具。 16、支持使用本地的 SecurCRT/Xshell/OpenSSH 工具通过 SSH 网关代理方式直接登录字符设备（提供功能截图证明并盖生产厂家公章或投标专用章）。 17、AD/LDAP 环境，支持直接使用登录堡垒机的 AD/LDAP 用户及密码可以直接自动登录到服务器里。 18、支持保存 SSH 的 sz/rz 命令（zmodem）传输的原始文件（提供功能截图，以及提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章）。 ▲19、支持保存 RDP 粘贴板（桌面之间复制-粘贴）传输及 RDP 磁盘映射传输的原始文件（提供功能截图，以及提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章）。 ▲20、安全策略要求：支持对重要命令进行审核：运维人员执行命令后，须等到管理员审批通过后才可执行成功（提供中国国家认证认可监督管理委员会认可的检测机构出具的相关检测（检验）报告复印件，并加盖生产厂家公章或投标专用章）。 21、支持用户、资产、授权的增删改查等 API 接口，允许第三方平台调用堡垒机的 API 接口，实现用户、资产、权限自动同步到堡垒机，简化堡垒机配置工作量（提供功能截图证明并盖生产厂家公章或投标专用章）。 22、堡垒机产品获得中国信息安全测评中心颁发的《信息技术产品	

				安全测评证书》EAL3+级别。（提供证书复印件加盖单位公章） 23、堡垒机产品获得 IPv6 Ready Logo 认证。（提供证书复印件加盖单位公章）	

二、服务标准

售后服务：产品质保期一年，自验收合格之日起计算。质保期内，凡因正常使用出现质量问题，成交供应商应提供免费维修或更换等服务，承担因此产生的一切费用，并从货物或服务正常使用或更换当日起重新计算质保期。成交供应商在接到买方故障通知后 2 小时内响应，24 小时内到达用户现场并排除缺陷，修理相关货物或解决相关问题，质保期结束后，成交供应商仍应负责对货物提供终生维修服务或对服务提供咨询服务，只收取配件成本或服务成本。

三、交货时间、交货地点和交货方式（履约时间、地点和方式）：

1.交货时间（履约时间）：合同签订之日起 30 天内

2.交货地点（履约地点）：采购人指定地点

3.交货方式（履约方式）：按照本竞争性磋商文件和成交供应商响应文件的规定。

四、付款时间、方式及条件：

由成交供应商届时与采购人具体协商。

五、其他：

1．项目的实质性要求：按本竞争性磋商文件要求和成交供应商响应文件的规定。

2．合同的实质性条款：采购人与成交供应商的名称和住所、标的、数量、质量、价款或者报酬、履行期限及地点和方式、验收要求、违约责任、解决争议的方法等内容。

3．安全标准：符合国家、地方和行业的相关政策、法规

4．验收方法及标准：按本竞争性磋商文件和响应文件的内容及国家、地方和行业的相关政策、法规实施。

5．法律法规规定的强制性标准：无。

“★”条款为不允许偏离的实质性条款，如不满足则认定其无效响应。“▲”条款为重要条款。