硬件设备参数清单

序号	名称	数量	单位
1	下一代防火墙（增强版）	1	台
2	下一代防火墙	1	台
3	全网行为管理	1	台
4	终端安全管理系统（EDR）	1	套
5	数据库审计	1	套
6	日志审计	1	套
7	漏扫	1	套
8	堡垒机	1	套
9	超融合	3	台
10	存储	3	台
11	业务网交换机	4	台
12	存储网交换机	2	台
13	路由器	1	台

1 下一代防火墙（增强级）

名称	具体要求
下一代防火墙	产品支持不少于 8 个 1000M 以太网电口，2 个 1000M SFP 口，内存大小不少于 8G，硬盘容量不少于 128G SSD，1U 机箱。
	网络层吞吐量≥20Gbps，应用层吞吐量≥9Gbps，防病毒吞吐量≥1.5G，IPS 吞吐量≥1.3G，全威胁吞吐量≥1G，并发连接数≥200 万，HTTP 新建连接数≥9 万。
	产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。
	产品支持 3 种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证。
	产品支持应用管控功能，应用特征识别库数量大于 9160 种。
	产品支持基于网络区域、网络对象、MAC 地址、服务、应用等维度进行访问控制策略设置。
	产品支持异常数据包攻击防御,防护类型包括 IP 数据块分片传输防护、Teardrop 攻击防护、Smurf 攻击防护、Land 攻击防护、WinNuke 攻击防护等攻击类型。
	产品支持 https 解密功能，支持 TCP 代理和 SSL 代理。
	提供 3 年软件升级及硬件质保服务。

2 下一代防火墙

名称	具体要求
下一代防火墙	产品支持不少于 8 个 1000M 以太网电口，2 个 1000M SFP 口，内存大小不少于 4G，硬盘容量不少于 128G SSD，1U 机箱。
	网络层吞吐量≥4Gbps，应用层吞吐量≥2Gbps，并发连接数≥200 万，防病毒吞吐量≥600M，IPS 吞吐量≥600M，全威胁吞吐量≥450M，HTTP 新建连接数≥6 万。
	产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。
	产品支持 3 种以上的用户认证方式,包含但不限于单点登录、本地账号密码、外部账号密码认证。
	产品支持应用管控功能，应用特征识别库数量大于 9160 种。

	产品支持基于网络区域、网络对象、MAC 地址、服务、应用等维度进行访问控制策略设置。
	产品支持异常数据包攻击防御，防护类型包括 IP 数据块分片传输防护、Teardrop 攻击防护、Smurf 攻击防护、Land 攻击防护、WinNuke 攻击防护等攻击类型。
	产品支持 https 解密功能，支持 TCP 代理和 SSL 代理。
	提供 3 年软件升级及硬件质保服务。

3 全网行为管理

项目名称	具体参数
全网行为管理	网络层吞吐量≥3.6 Gbps，应用层吞吐量≥450 Mbps，带宽性能≥300 Mbps，IPSEC VPN 加密性能（最高性能）：100Mb，支持用户数≥800，准入终端数≥400，准入终端数的扩容上限≥800，包转发率≥45Kpps 每秒新建连接数≥4000,最大并发连接数≥150000；
	支持两台及两台以上设备同时做主机的部署模式；
	支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；
	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；用户指定应用上网流速超过预设阈值后，网关自动提醒该用户；
	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；
	支持图形化查看当前内网 IP 使用情况，帮助管理员减少人工维护 IP 表的工作量；
	自动发现网络里面的终端，并获取 IP、Mac、厂商、操作系统等信息，设备必须支持 PC、移动设备、哑终端、专用设备的发现和型号识别：至少支持 Windows、Linux、MAC、瘦客户机等 PC；至少支持手机、平板等移动设备；至少支持服务器、交换机、无线控制器等网络设备；至少支持打印机、投影仪、电视、摄像头、门禁系统等哑终端；支持自定义终端类型
	提供 3 年软件升级及硬件质保服务。

4 终端安全管理系（EDR）

项目要求	具体参数
终端安全管理系统	产品以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署，且需要提供软件 3 年升级授权及维保服务。
	PC 端安全软件≥300 套;服务器端端安全软件≥20 套
	支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和终端账户，其中操作系统和监听端口支持从资产和终端两个视角进行统计和展示。
	提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数
	通过智能识别终端环境情况（低配硬件、老旧设备、虚拟化等）和当前终端资源占用，在闲时实时监控和病毒扫描场景，都可智能调整 EDR 的资源占用（CPU、IO 等），为业务让出资源，不卡业务，对业务零摩擦。
	支持 agent 安装目录的文件保护，可以保护 agent 目录和文件实时监控驱动文件，可以保护 agent 的服务/进程/文件不被恶意删除，以免影响正常功能，导致用户的终端受到病毒入侵
	支持展示终端检测到的 WebShell 事件及事件详情，包括：恶意文件名称，威胁等级，受感染的文件，发现时间，检测引擎，文件类型，文件名，文件 Hash 值，文件大小，文件创建时间；可配置 WebShell 实时扫描，一旦发现 WebShell 文件，可自动隔离或仅上报不隔离

5 数据库审计

项目名称	具体参数
数据库审计	产品以纯软件交付并提供软件 3 年升级授权及维保服务。
	数据库流量≥100M，日志检索≥15000 条/s；
	支持主流数据库 Oracle（Tdata）、SQL-Server、DB2、MySQL（Tdsql）、Informix、Sybase、Postgresql、Cache、MongDB、K-DB，虚谷；

	支持时间段、源 IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码等对数据库日志进行精细检索；
	精细化日志秒级查询通过 SQL 串模式抽取保障磁盘 IO 的读写性能；分离式存储 SQL 语句保障数据审计速度快；
	内置大量 SQL 安全规则包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感表、篡改内置敏感表等；
	支持 SNMP 方式，提供系统运行状态给第三方网管系统； 支持 Syslog 方式向外发送审计日志；

6 日志审计

项目名称	具体参数
日志审计	产品以纯软件交付并提供软件 3 年升级授权及维保服务；
	资产授权数量≥50；
	支持主动、被动相结合的数据采集方式，支持通过 Agent 采集日志数据，支持通过 syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka(截图证明)等多种方式完成日志收集；
	支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射；
	支持网站攻击、漏洞利用、C&C 通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到 350 条以上，支持自定义关联分析规则；
	支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等,可提供设备专项分析场景。如防火墙外部攻击场景分析、VPN 账号异常场景分析、Windows 服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析；
	内置主机安全报表（linux）、主机安全报表（windows）、数据库安全报表、网络设备安全报表、应用安全报表五种；支持提供日报、周报、月报和自定义时间导出报表。

7 漏扫

名称	具体参数
漏扫	产品以纯软件交付并提供 3 年软件升级授权及维保服务。
	系统漏扫授权 IP 数≥20，WEB 漏扫授权 URL 数≥10； 性能指标：系统漏扫最大并发 IP 数≥20，WEB 漏扫最大并发 URL 数≥5；
	支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB 漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB 漏洞扫描、弱口令扫描同时执行。
	支持资产发现功能，可基于 IP 地址、IP 网段、IP 范围、URL 等方式进行资产发现扫描，支持 EXCEL 格式批量导入。
	支持国产操作系统的漏洞扫描，包括麒麟（Kylin）、统信（UnionTech OS）、中兴新节点（NewStart CGSL）等。
	支持行业通用标准 OWASP，支持通用 WEB 漏洞检测，如：SQL 注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、命令执行、敏感信息泄露等。

8 堡垒机

项目名称	具体要求
堡垒机	产品以纯软件交付并提供软件 3 年升级授权及维保服务。包含资产授权数量≥50；
	用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、短信认证（移动云 mas)、AD 域/LADP 认证、Radius 认证等认证方式；并支持各种认证方式和静态口令组合认证；
	支持首次使用手机动态口令由用户自行扫码配置；
	支持 unix 资源、windows 资源、网络设备资源、数据库资源、C/S 资源、B/S 资源；
	支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作；
	支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等，并可以实时阻断；
	支持自定义报表，可记录审计报表模板，可生成图形报表，并提供 EXCEL、WORD、PDF、HTML

	等格式导出。

9 超融合

项目名称	具体参数
基本要求	提供三台 2U 标准机架设备；每台服务器处理器配置：配置不少于 2 颗 CPU，单颗 CPU 核数≥24（主频不低于 2.2Ghz）；单台内存配置：配置≥512GB；单台硬盘配置：配置≥2*240G SSD +2*960GB SSD 硬盘+4*6T HDD 硬盘；网口配置：配置≥6 个千兆电口+2 个万兆光口（含模块及光纤线）；电源配置：配置冗余电源。本项目需提供计算虚拟化、存储虚拟化、网络虚拟化等授权。
	提供 3 年软件升级及硬件质保服务。
云管平台	1.支持大屏展示便于客户直观查看虚拟化资源池的使用情况和健康状态，包括集群资源情况，各主机资源使用情况，包括内存/CPU/磁盘使用趋势，以及集群故障与告警等。 2.支持可靠中心以提供持续数据保护 CDP、本地备份、异地容灾等高可用服务，当主平台发生故障时，能够切换到备平台，保障云平台稳定运行。 3.弹性 IP 池支持共享带宽，多个弹性 IP 池共用一条带宽，提高带宽资源利用率。 4.应用中心支持常见应用，包括但不限于 MongoDB 、RabbitMQ、Redis、Kafka、ClickHouse、Dipper、Studio、X_HD、X_Search 的快速部署，可对应用进行配置、监控、告警的全生命周期管理。 5.支持上传或利用现有云主机创建镜像，可对镜像进行管理、关联资源池等操作，可通过镜像实现一键快速创建云主机及安全组件。
计算虚拟化	1.虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的 IP 地址、MAC 地址等。 2.支持 UPS 联动，为尽可能保障数据中心断电场景下的业务，可在市电断电时通过 UPS 临时供应电量，当 UPS 电量过低时，按照虚拟机优先级先将不重要的虚拟机进行软关机。 3.可以查看高可用（HA）配置页面信息，包括故障检测敏感度和故障迁移选项，可以对故障检测敏感度进行设置，包括高、中高、中、中低和低，可以查看故障迁移列表项，包括管理通信口、虚拟机直接或间隔一个交换机连接的物理出口、虚拟机所在存储和启用 HA。 4.提供热添加 CPU、内存、磁盘、网卡的功能，无需中断或停机即可实现虚拟资源的在

	线添加。 5.提供基于 PowerShell 的 CLI 命令行功能，通过命令行可以进行管理计算虚拟化、存储虚拟化、网络虚拟化模块，并通过 PowerShell 脚本可简化用户运维操作。 6.为避免主机假死导致系列问题发生，支持识别假死主机并标签化为亚健康主机，通过邮件或短信告警提醒用户进行处理，并限制重要业务在亚健康主机上运行，规避风险。
存储虚拟化	1.采用分布式的软件定义存储架构，在通用 x86 服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点；通过新增物理服务器可以实现存储容量和性能的横向扩展（Scale-Out 架构），扩容过程保证业务零中断。 2.支持数据重建优先级调整，可以查看数据重建任务列表信息，包括对象名称、对象类型、数据量和优先级等信息，可以点击操作中的优先级对数据重建进行优先重建，保证重要的业务优先恢复数据的安全性。 3.支持条带化功能，并且支持以虚拟磁盘为单位设置不同的条带数。 4.支持标准的 iSCSI 协议，允许外部物理主机或应用通过标准的 iSCSI 接口访问虚拟存储。支持 iSCSI 存储、FC 存储、NFS 存储、本地存储。支持通过 iSCSI 透传/非透传指令使虚拟机支持存储裸设备映射（RDM），可以将存储设备上的 LUN 直接映射给虚拟机使用。 5.支持硬盘容量预测功能，并可根据客户设置的阈值进行容量告警，为用户扩容提供指导，并避免使用过程中突然出现容量不足问题。 6.支持物理内存提供读取缓存操作，可以点击高级设置中的读性能优化进行配置占用主机内存比例操作。
网络虚拟化	1.本次配置不限制虚拟路由器创建数量，虚拟路由器支持 HA 功能，当虚拟路由器运行的主机出现故障时，可以实现故障自动恢复，保障业务的高可靠性。 2.网络硬件检测（网络可通、网卡、光模块、网卡掉线、闪断）。 3.在管理平台上可以通过拖拽连线完成网络拓扑的构建，可以在网络拓扑页面通过功能键实现虚拟网络连接、开启和关闭等操作。4.可以支持手动指定虚拟路由器运行在固定的物理主机上，可以自动将虚拟路由器规划到高性能和高吞吐的物理主机上。 5.支持创建分布式虚拟防火墙，可基于虚拟机、虚拟机组、虚拟机标签、IP、IP 范围、IP 组构建安全防火墙。 6.超融合需提供网络可视化组件，可在图形化界面上观察到所有虚拟机的流量走向与访问关系，包括源对象、源 IP、目标对象、目的 IP、访问次数、服务类型、动作等。

10 存储

项目要求	具体参数
基本要求	节点数量不少于 3 台通用 X86 架构服务器，授权容量不少于 96T，单台配置至少一颗 2.4GHz/10 核 CPU，单台内存配置≥64GB，单台硬盘配置≥1.92TB 固态硬盘，≥32TB SATA 机械硬盘；标配 1 块 240GB 存储容量的 SSD 系统盘，冗余电源。需提供分布式存储授权。
统一存储	使用三个存储节点组建一个存储集群，同一系统中并发提供文件、块、对象及大数据四种存储服务，统一管理，资源灵活分配。
病毒防护	存储内置防病毒能力，免费提供存储杀毒引擎，支持针对目录开启实时防病毒功能，防止病毒通过文件共享进行传播扩散，有效抵御以勒索病毒为典型的各种病毒。
数据保护	配置目录级快照功能，可按时间点策略进行快照，支持快照数≥1024 个。快照重命名，删除快照链上任意快照点，以及快照点任意文件数据回滚，以达到数据的精准恢复。
访问审计	支持文件审计功能，通过该功能可以在管理平台方便的过滤文件创建、删除及元数据修改相关操作的日志，从而在文件状态出现异常时，可以通过此功能进行追溯。
可靠性	支持多副本冗余功能，支持 2 个或以上副本，副本互斥地保存在集群的不同节点，当 1 个或多个主机或者磁盘故障，确保数据依旧正常访问。
数据重建	集群进行扩容操作后，支持数据重建平衡，并对数据重建智能限速，避免数据重建过程中 IO 性能占用导致对业务的性能造成影响，同时也支持配置数据平衡时间策略，在业务空闲时间端执行数据平衡，避免数据平衡对业务产生影响。

11 业务网交换机

序号	指标要求
1	提供 4 台业务网交换机，每台配置不少于 24 个千兆电口+4 个万兆 SFP+光口；交换容量≥432Gbps/4.32Tbps，包转发率≥156Mpps/168Mpps,支持全端口线速转发；支持 aNAC 统一管理、统一查看状态、VLAN 等配置管理；支持终端识别、终端准入、安全防护及安全画像可视。提供证明并加盖厂商公章；

2	支持通过控制器平台图形化操作对交换机端口状态的开启与关闭，提供功能截图证明；
3	支持 M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面；
4	支持通过控制器平台查看交换机端口负载情况；
5	支持通过控制器平台查看交换机处于工作端口最近 5 分钟、1 小时、最近 1 天、最近 1 周发送与接收的流量趋势；
6	支持查看安全事件记录、终端类型异常记录、终端在端口迁移次数、终端地址异常记录等安全事件的记录统计；
7	提供 3 年软件升级及硬件质保服务。

12 存储交换机

序号	指标要求
1	提供 2 台业务网交换机，每台配置不少于 12 个万兆 SFP+光口，12 个千兆电口；交换容量≥1.28Tbps/12.8Tbps，包转发率≥480Mpps，支持全端口线速转发；支持 aNAC 统一管理、统一查看状态、VLAN 等配置管理；支持终端识别、终端准入、安全防护及安全画像可视；冗余电源；
2	支持通过控制器平台图形化操作对交换机端口状态的开启与关闭，提供功能截图证明；
3	支持 M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面；
4	支持通过控制器平台查看交换机端口负载情况；
5	支持通过控制器平台查看交换机处于工作端口最近 5 分钟、1 小时、最近 1 天、最近 1 周发送与接收的流量趋势；
6	支持查看安全事件记录、终端类型异常记录、终端在端口迁移次数、终端地址异常记录等安全事件的记录统计；
7	提供 3 年软件升级及硬件质保服务。

13 路由器

1 台路由器主机，≥16 个电接口；冗余电源