**附件二：技术要求**

**注：本附件中所有“基本要求”（即实质性响应）必须满足；“其他技术要求”可选择响应。**

**数据中心防火墙 1台**

（一）、基本要求

1. 吞吐量应不低于30Gbps，并发连接数不低于1100万，每秒新建连接数不低于40万，虚拟防火墙数量≥490，配置冗余电源。
2. 实际配置不低于2个40G接口，12个10GE SPF+接口(含4个万兆多模光模块)，12个GE电口，1T硬盘。
3. 提供原厂商针对本项目的3年售后服务承诺函原件并加盖原厂鲜章

（二）、其他技术要求（在以下每项要求后面注明“满足”或“不满足”）：

1. IPV6：支持IPv6协议栈、IPV6穿越技术、IPV6路由协议、IPv6 over IPv4 GRE隧道、6RD隧道 （提供“IPV6 Ready Phase-2”认证证书复印件并加盖原厂商鲜章）
2. 数据安全 ：支持SafeSearch功能，能够过滤掉搜索引擎返回的色情和具有潜在攻击性的不健康内容以规范上网行为。（提供功能截图并加盖原厂商鲜章）
3. 加密流量安全防护 ：支持对HTTPS，POP3S，SMTPS,IMAPS加密流量代理解密后，并进行内容过滤，审计，安全防护。（提供功能截图并加盖原厂商鲜章）
4. 智能威胁防御 ：支持防火墙与云沙箱、本地沙箱混合联动，敏感文件在本地沙箱检测，普通文件上传到云沙箱，及保护了客户敏感数据有提高了云检测能力。（提供功能截图并加盖原厂商鲜章）
5. 产品资质：具有公安部颁发的防火墙《计算机信息系统安全专用产品销售许可证》，且达到增强级级别，提供证书复印件并加盖原厂商鲜章

**数据中心入侵防御 1台**

（一）、基本要求

1. 吞吐量应不低于15Gbps，并发连接数不低于1150万，每秒新建连接数不低于39万
2. 实际配置不低于2个40G接口，12个10GE SPF+接口(含4个万兆多模光模块)，12个GE电口，1T硬盘，3年IPS特征库升级服务。
3. 为保证产品兼容性与后期方便维保，要求与数据中心防火墙同一品牌
4. 提供原厂商针对本项目的3年售后服务承诺函原件并加盖原厂鲜章

（二）、其他技术要求（在以下每项要求后面注明“满足”或“不满足”）：

1. 架构：必须为标准机架的专业IPS设备，不能提供防火墙或UTM的IPS功能
2. 入侵防护功能:配置入侵防护功能模块，能够防范各种应用层攻击，包括但不限于：后门程序，木马程序，间谍软件，蠕虫，僵尸主机，异常代码，协议异常，扫描，可疑行为审计类等，能够对跨站攻击、SQL注入等WEB攻击行为进行有效防护
3. 入侵检测功能：支持SSL加密流量检测(提供功能截图并加盖原厂商鲜章)
4. 环境感知:提供NGIPS能力，能够感知网络环境中的客户端类型和应用，并根据环境的变化，自动调整安全策略(提供功能截图并加盖原厂商鲜章)
5. APT防护:支持与沙箱，云沙箱混合联动，对含有未知威胁的文件进行检测，并能阻断(提供功能截图并加盖原厂商鲜章)
6. 事件分级:系统支持除了基于攻击事件本身进行严重级别划分，还可以根据攻击与资产相关性关联进行风险级别定义，协助管理员关注实际环境中需要紧急处理的安全告警，提升安全事件响应效率

**数据中心Web应用防火墙 1台**

（一）、基本要求

1. 吞吐量应不低于8Gbps，并发连接数不低于60万
2. 实际配置不低于2个10GE SPF+接口模块(含2个万兆多模光模块)，8个GE电口、8个SFP 光口，3年特征库升级服务
3. 为保证产品兼容性与后期方便维保，要求与数据中心防火墙同一品牌
4. 提供原厂商针对本项目的3年售后服务承诺函原件并加盖原厂鲜章

（二）、其他技术要求（在以下每项要求后面注明“满足”或“不满足”）：

1. 功能要求：保护对象网段数不限：支持多条链路数据的防护，最多可防护2路物理链路，防护网段数量不限
2. 功能要求：支持WEB站点服务自动侦测功能(提供功能截图并加盖原厂商鲜章)
3. 功能要求：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 注入等）、跨站请求伪造等应用攻击行为
4. 功能要求：识别服务端响应内容导致的缺陷：敏感信息泄露（银行卡、身份证、电话号码、目录泄露、源码泄露等）、已有的网页后门、错误配置、目录浏览等缺陷
5. 能要求：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(提供功能截图并加盖原厂商鲜章)
6. 功能要求：可以将第三方扫描工具的扫描结果导入到WAF并生成策略规则(提供功能截图并加盖原厂商鲜章)
7. 功能要求：支持网站自学习建模功能，能通过自学习形成网站URL树；通过自学习能生成安全防护策略；通过自学习能发现参数的名称、类型、匹配频率；可配置匹配不到自学习特征直接阻断请求
8. 功能要求：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。

**外网出口上网行为管理、流量管控设备 1台**

（一）、基本要求

1. 吞吐量应不低于8Gbps，应用性能≥1Gbps，并发连接数不低于400万 ，配置至少1T的硬盘
2. 实际配置不低于2个10GE SPF+接口模块，12个GE电口、12个SFP 光口，3年特征库升级服务
3. 为保证产品兼容性与后期方便维保，要求与数据中心防火墙同一品牌
4. 提供原厂商针对本项目的3年售后服务承诺函原件并加盖原厂鲜章

（二）、其他技术要求（在以下每项要求后面注明“满足”或“不满足”）：

1. 4G支持：支持4G扩展网卡作链接备份。支持在4G接口上运行IPSec VPN。(提供功能截图并加盖原厂商鲜章)
2. 应用协议识别：支持BYOD特征库，可识别ios版和安卓版移动互联网软件如微博、微信等特征。(提供功能截图并加盖原厂商鲜章)
3. 应用行为审计：支持即时通讯应用管控的精细化管理，例如微信的“所有行为”、“语音”、“发消息”、“收消息”、“登录”、“发文件”等行为。(提供功能截图并加盖原厂商鲜章)
4. 应用行为审计：支持收集网站访问日志，记录用户所有访问网站行为；支持收集搜索引擎日志，记录用户的搜索内容；支持收集IM通讯软件日志，记录用户登录、注销、收发消息、收发文件等行为；
5. 防私接路由：可识别私接主机个数，并可制定策略分别设置私接终端类型个数为阀值进行封堵，支持自定义阻断时间，同时支持基于IP及IP段配置白名单。(提供功能截图并加盖原厂商鲜章)
6. 应用缓存：支持APP文件缓存在网关设备本地，用户下载时直接从网关下载APP文件，支持针对特定服务器的APP缓存，以减少公网带宽占用。(提供功能截图并加盖原厂商鲜章)
7. 无线非经：至少支持任子行、派博、爱思、虹旭、锐安、网博、华三等主流后端公安平台的直接对接（非额外部署日志服务器方式对接）。（提供功能截图并加盖原厂商鲜章）

**漏洞扫描系统 1台**

（一）、基本要求

1. 配置并发任务数不低于10个，单任务并发IP数不低于60个，不限制授权扫描IP范围
2. 实际配置不低于6个GE电口、1个扩展插槽、 500G硬盘。3年特征库升级服务
3. 为保证产品兼容性与后期方便维保，要求与数据中心防火墙同一品牌
4. 提供原厂商针对本项目的3年售后服务承诺函原件并加盖原厂鲜章

（二）、其他技术要求（在以下每项要求后面注明“满足”或“不满足”）：

1. 支持并配置系统扫描、Web扫描、数据库扫描、安全基线检测、弱口令扫描在内的五大功能模块
2. 任务管理：支持IPV4、IPV6双协议栈地址扫描
3. 扫描能力：支持漏洞库涵盖标准包含CVE、CVSS、CNVID、CNNVD、CNCVE、Bugtraq5种
4. 扫描能力：支持对Windows系列、苹果操作系统、Linux、AIX、HPUX、IRIX、BSD、Solaris等目标主机的系统进行扫描；
5. 扫描能力：支持对Vmware、KVM、Xen等虚拟机系统的漏洞扫描；
6. 扫描能力：支持自动探测网段的未知站点，并转为资产进行web扫描；
7. 扫描能力：支持特定的基线检查模板，如：等保检测要求、工信部检测要求、中国电信安全配置规范、中国移动安全配置
8. 扫描能力：支持主流数据库漏洞的检测：Oralce、Sybase、SQLServer、DB2、MySQL、Postgres、Informix
9. 扫描能力：支持目前知名的检测协议，TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP、REDIS、Oracle、MySQL、PostgreSQL、MsSQL、DB2、MongoDB；

**终端准入系统 1套**

（一）、基本要求

1. 支持最大准入用户数≥20000个，本次配置接入用户授权≥3000人；
2. 实际配置要求不低于2个Xeon Silver 4110-8Core CPU,2块16GB内存,2块600GB 2.5inch硬盘, 4个GE,双电源）；
3. 为保证产品兼容性与后期方便维保，要求与数据中心防火墙同一品牌
4. 提供原厂商针对本项目的3年售后服务承诺函原件并加盖原厂鲜章

（二）、其他技术要求（在以下每项要求后面注明“满足”或“不满足”）：

1. 支持IP/MAC、802.1x、Portal、短信、微信等准入方式，并支持基于IP、MAC、接入端口、账号等信息鉴别用户身份；
2. 支持多种身份认证源：支持本地账号密码认证，支持AD域服务器、LDAP服务器、第三方RADIUS服务器作为身份认证源进行联动认证
3. 支持AD/LDAP用户同步：支持AD/LDAP服务器逃生功能保证AD/LDAP服务器宕机情况下的高可靠性(提供功能截图并加盖原厂商鲜章)
4. Portal页面自定义管理：系统提供超过5套的默认模板，用户可自定义新模板(提供功能截图并加盖原厂商鲜章)
5. 多语言支持：推送页面支持简体中文、繁体中文、英文、德文等多种语言(提供功能截图并加盖原厂商鲜章)
6. 支持Portal页面推送策略管理：支持基于终端IP地址段、接入AP、设备类型、接入SSID等条件推送不同的Portal认证页面和注册页面

**堡垒机系统 1台**

（一）、基本要求

1. 磁盘空间不少于1T、至少配备4个100/1000M自适应电口
2. 单台堡垒机字符类并发会话≥200个、图形类并发会话≥50个,管理资产总数≥1000
3. 为保证产品兼容性与后期方便维保，要求与数据中心防火墙同一品牌
4. 提供原厂商针对本项目的3年售后服务承诺函原件并加盖原厂鲜章

（二）、其他技术要求（在以下每项要求后面注明“满足”或“不满足”）：

1. 3、部署模式：采用旁路部署，不得影响业务环境；支持高可用部署，HA秒级切换
2. 认证对接：支持与AD、LDAP、RADIUS系统联动登录堡垒机，支持以Get、Post、SOAP发送方式的HTTP短信网关平台进行联动，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(提供功能截图并加盖原厂商鲜章)
3. 双因子认证：堡垒机须内嵌动态令牌和USBkey认证引擎，可同时使用动态令牌和USBKey，且支持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认证
4. 支持的协议和应用：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、VMware vSphere Client、浏览器等客户端工具
5. 主流数据库运维管理：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
6. 混合云管理：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
7. 自动改密：支持定期自动修改windows服务器、网络设备、LINUX/UNIX等目标设备密码功能；支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、改密后备份、密码文件加密；(提供功能截图并加盖原厂商鲜章)
8. H5运维方式：支持SSH、Telnet、Rlogin、RDP、VNC协议的H5运维，无需本地运维客户端工具(提供功能截图并加盖原厂商鲜章)
9. 日志数据归档：审计数据支持通过SFTP/FTP方式自动归档，并在页面中可以查询哪些数据是否归档，可以设置归档成功之后自动删除数据，归档后的数据可以用专用播放器离线查看

**日志审计 1台**

（一）、基本要求

1. 千兆电口不少于4个，内存不少于16GB，磁盘不少于4T ，双电源。支持审计200个日志源；
2. 为保证产品兼容性与后期方便维保，要求与数据中心防火墙同一品牌
3. 提供原厂商针对本项目的3年售后服务承诺函原件并加盖原厂鲜章

（二）、其他技术要求（在以下每项要求后面注明“满足”或“不满足”）：

1. 日志存储：支持日志压缩存储；
2. 日志采集方式：支持通过二进制会话、Syslog、Dataflow、Netflow、FTP；
3. 日志分类：系统能够根据日志特征对防火墙的Syslog日志进行如下分类：攻击防范、流量监控、黑名单、地址绑定、操作命令、防火墙登录、策略命中、内容过滤和其它；
4. 日志查询：支持异步查询和细粒度的查询，查询条件可保存为模板，查询记录提供Excel、CSV、TXT文件导出方式；
5. 多维度Dashboard：入侵防御趋势分析、入侵防御事件排行、攻击防范事件趋势、入侵防御目的IP排行、病毒事件目的IP排行、病毒事件趋势、策略趋势、URL分类排行、日志量趋势、采集器CPU性能、采集器内存性能、分析器CPU性能、分析器内存性能等(提供功能截图并加盖原厂商鲜章)；
6. 多维度日志分析：网络安全分析、会话及NAT溯源分析、流量分析、上网行为分析
7. 用户权限管理：支持基于RBAC和三权分立原则；
8. 自身操作审计：系统能自动对每个用户的操作进行记录，并可由审计员进行审计；
9. 系统日志：系统能自动对运行过程中的故障及重要状态变化进行记录，方便管理员了解系统运行情况；
10. 系统支持语种：支持中文及英文操作界面

**数据库审计 1台**

（一）、基本要求

1. 配置千兆电口不少于4个，内存不少于8GB，磁盘不少于2T，支持不少于12个数据库授权；
2. 为保证产品兼容性与后期方便维保，要求与数据中心防火墙同一品牌
3. 提供原厂商针对本项目的3年售后服务承诺函原件并加盖原厂鲜章

（二）、其他技术要求（在以下每项要求后面注明“满足”或“不满足”）：

1. 部署方式：支持旁路部署,引流插件将流量镜像转发到审计系统；支持 HA部署，实现审计系统高可用性和提高数据安全性，主机系统故障时自动切换到备机连续审计； 支持分布式部署，实现审计策略统一下发，数据集中存储和策略统一管理和下发
2. 数据库协议：支持Oracle、SQL Server、MySQL、DB2、Sybase、PostgreSQL、Cache、Teradata、Informix、达梦（DM）、南大通用（GBASE）、人大金仓（Kingbase）、神通（OSCAR）、MongoDB、Redis数据库的审计
3. 审计策略：支持自定义精确审计规则，可根据账号、IP地址、操作类型、数据库名、数据库表名、返回行数、响应时间、数据库返回码、操作特征设定；
4. 审计策略：系统自带大于200个缺省审计规则库，可使用自带规则库对访问流量审计；
5. 审计策略：支持数据库操作类、表、视图、索引、触发器、游标、事务各种对象的SQL操作审计
6. 审计策略：系统内置高危SQL查询和注入、远程命令执行、跨站脚本攻击、FTP和telnet高危指令等审计规则模板
7. 审计能力：支持双向流量审计，对Select操作返回报文中执行状态（成功/失败）、返回行数、执行时长进行审计，并能够根据返回错误码和返回行数设置审计策略
8. 审计能力：支持DDL语句、DCL语句、DML语句的审计，支持对访问流量中分片包重组后审计，支持绑定变量的审计，并支持记录变量名及变量值，支持数据库并发会话数、并发进程数、并发用户数、并发游标数、并发事务数、数据库锁等超过限制的审计
9. 敏感信息防护：支持对审计日志中敏感数据（帐号、身份证号、手机号、银行卡号）进行掩码处理，进行隐私保护，掩码规则可自定义。(提供功能截图并加盖原厂商鲜章)
10. 报表：提供缺省的报表模板库，包括SOX报表、PCI报表等模板，供用户选择使用。内置报表数量大于20种；
11. 用户行为轨迹：支持根据账号、时间、源IP、操作行为等要素对访问行为轨迹图方式还原数据库访问过程。(提供功能截图并加盖原厂商鲜章)

**杀毒软件 1套**

（一）、基本要求

1、配备Windows服务器防病毒与补丁功能授权数60个以及3年升级服务，Linux服务器防病毒授权数5个以及3年升级服务，Windows PC防病毒、补丁功能与运维管控功能授权数1000个以及3年升级服务。

2、配置两套管控服务器软件。

3、配备两台机架式服务器硬件平台（CPUE5-2603V4及以上、内存8G及以上、硬盘1T及以上）。

（二）、其他技术要求（在以下每项要求后面注明“满足”或“不满足”）：

4、产品采用B/S架构管理，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能，可支持在Windows、Windows Server、Linux系统环境上部署；要求；

5、操作系统支持：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10、Windows Server 2003\_SP2/Windows Server 2008/Windows Server 2012、SUSE Linux/Red Hat Linux/CentOS/Ubuntu、中标麒麟/Deepin/银河麒麟/普华桌面等操作系统；

6、支持终端保护密码，设置密码后，终端退出或卸载杀毒、或安装控制中心，都需要输入正确的密码方可执行；要求客户端程序具备自保功能，避免被恶意篡改；

1. 支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置；对敲诈者病毒提供防护机制，同时提供解密工具，解密工具应为自主研发；（提供功能截图并盖厂商公章）
2. 支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）设置使用权限；
3. 支持按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；可监控CPU温度、硬盘温度和主板温度；支持冗余有线网卡、无线网卡、3G网卡、MODEM、ADSL、ISDN等设备的外联控制；违规外联发生时可针对内外网连接状态分别设置违规处理措施；
4. 支持正版化管理，系统支持软件的正版序列号读取功能，并导出详细报表集中管理；（提供功能截图并盖厂商公章）
5. 支持中标麒麟/Deepin/银河麒麟/普华桌面操作系统、云桌面产品杀毒；（提供功能截图并盖厂商公章）
6. 支持U盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马；
7. 支持通过数字签名或者文件名的方式分别显示文件，方便管理员管理全网终端上报的文件；（提供功能截图并盖厂商公章）
8. 支持文件解压缩病毒查杀，支持对zip、rar、7z等多种格式的压缩文件查杀能力；
9. 支持漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端P2P补丁分发加速，有效节省外网带宽资源；（提供功能截图并盖厂商公章）
10. 支持漏洞利用防御，尤其对通过文件漏洞（尤其是0day漏洞）的攻击行为进行有效检测与防御；且生产厂商2017年入库国家信息安全漏洞共享平台漏洞库共享原创漏洞不少于30000条，提供入库单位证明文件复印件并加盖生产厂商公章。
11. 支持按病毒、木马、终端等维度统计全网病毒感染状况；支持漏洞集中修复，强制修复，自动修复，具备蓝屏修复功能；（提供功能截图并盖厂商公章）
12. 支持根据需求可扩展数据价值评估功能，通过双彩虹图、雷达图、面积图、柱状图等形式查看配置脆弱程度变化对比、配置脆弱程度变化趋势图、配置风险终端和配置危险终端的比例分布；（提供功能截图并盖厂商公章）
13. 产品具有公安部颁发的《计算机信息系统安全专用产品销售许可证》（提供证书复印件，并盖原厂商鲜章）；
14. 产品具有国家保密科技测评中心颁发的《涉密信息系统产品检测证书》（提供证书复印件，并盖原厂商鲜章）；
15. 产品生产厂商须具备ISO9001:2015、ISO20000:2011、ISO27001:2013体系认证证书；（提供证书复印件，并盖原厂商鲜章）
16. 产品生产厂商须为云安全联盟成员(CSA)成员；（提供证明文件，并盖原厂商鲜章）