附表 1：

1、删除原招标文件中第 8-9 页的“1.7 项目建设依据”。

2、原招标文件中第 9-77 页中“（二）采购内容**”修改为下文：**

2.1 需求一览表

★为方便系统维护及系统兼容性的考虑，本次项目采购的安全等级保护系统的硬件和软件均为同一品牌。

产品名称	数量	参数要求
交换机	1	以太网交换机，48 个千兆电口，8 个万兆 SFP+光口，1 个 Mini usb 型 Console 口，标配电源 AC220V，增强型全网管，支持三层路由，智能风扇，1U 高度，标准 19 英寸机架式安装，包转发率 252Mpps，交换容量 350Gbps，随机包含支架安装包、防水堵头、文档资料。三年原厂质保服务；
互联网防火墙	1	1U 机箱，6 个千兆电口，8 个 SFP 插槽，标配冗余电源；防火墙吞吐 6Gbps，并发连接 220 万，新建连接数≥6.5 万；IPSECVPN 吞吐 180M，SSLVPN 吞吐 320M；默认含 IPSECVPN 模块，可扩展 SSLVPN 模块；支持扩展 AI 应用识别、IPS 入侵防御及 AV 防病毒功能；三年原厂质保服务；
	1	攻击知识库 3 年升级服务许可
	1	专业版病毒知识库 3 年升级服务许可
专线防火墙	1	1U 机箱，6 个千兆电口，8 个 SFP 插槽，标配冗余电源；防火墙吞吐 6Gbps，并发连接 220 万，新建连接数≥6.5 万；IPSECVPN 吞吐 180M，SSLVPN 吞吐 320M；默认含 IPSECVPN 模块，可扩展 SSLVPN 模块；支持扩展 AI 应用识别、IPS 入侵防御及 AV 防病毒功能；三年原厂质保服务；
	1	攻击知识库 3 年升级服务许可
	1	专业版病毒知识库 3 年升级服务许可
数据中心防火墙	1	1U 机箱，配置为 6 个 10/100/1000BASE-T 接口和 2 个 SFP 插槽，2 个可插拔的扩展槽，双电源，防火墙吞吐率：12Gbps，应用层吞吐率（FW+APP）：6Gbps，并发连接数：300 万；每秒新建连接数：13.5 万；默认包含应用识别功能；三年原厂质保服务；
	1	专业版快速扫描查杀病毒库 1 年升级服务许可；
	1	IDP 攻击规则特征库 1 年升级许可
Web 应用安全防护系统	1	1U 机箱，8 个千兆电口，接口支持 Bypass，2 个 SFP 插槽；整机吞吐量：6Gbps，并发连接：350 万，每秒新建连接数：12.5 万 ；含 3

		年特征库升级服务，内含 SQL 注入、XSS、CSRF 等 WEB 攻击防护功能、URL 访问控制功能、防盗链功能、WEB 漏洞扫描功能、DDoS 攻击防护功能、服务器负载均衡功能、报表分析及告警功能；三年原厂质保服务；
	2	WAF 产品特征库 1 年升级 License
上网行为管理系统	1	1U 机箱，4 个千兆电口，1 个接口扩展槽，接口支持 Bypass；日志存储空间 500GB；建议适配带宽：300M，建议用户数 800；默认含一年系统版本升级、网站知识库及应用知识库升级许可；三年原厂质保服务；
	1	含 2 年系统版本、网站知识库及应用知识库升级服务许可
入侵检测系统	1	1U 机箱，6 个千兆电口，4 个 SFP 插槽，标配冗余双电源；整机吞吐量：5Gbps，IDS 吞吐 2Gbps；最大并发连接数：220 万；每秒新建连接数：8.5 万；默认含 1 年攻击知识库升级许可，1 年网站知识库升级许可。三年原厂质保服务；
	1	攻击知识库 2 年升级服务许可
数据库审计系统	1	1U 机箱，6 个千兆电口，4 个 SFP 插槽，1T 存储空间，标配冗余电源；抓包速度≥1000M/秒，审计系统审计事件每秒入库速度≥10000 条/秒；日审计量≥4 亿条。；默认含 1 年的网站知识库、攻击知识库和应用识别库。三年原厂质保服务；
	1	网站知识库、应用识别库和攻击知识库 2 年升级服务许可
运维安全审计系统	1	1U 机型，1 个 console 口，2 个 USB 口；6 个千兆电口，2 个 SFP 插槽，2 个可扩展插槽；16G 内存，2T 存储空间，单电源；100 个主机/设备许可，用户数不限制。三年原厂质保服务；
网络准入系统	1	1U 机箱，6 个 1000BASE-T 电口，2 个 SFP 插槽，1T 存储空间，配置单电源，接口支持 Bypass，冗余 2 个扩展槽位；可支持 500 个并发客户端，用户数无限制；三年原厂质保服务；
日志审计系统	1	1U 机箱,1 个 console 口,6 千兆电口,有效存储容量 4T,标配 Raid5。最大支持 100 日志源授权。综合处理性能：20000EPS，综合处理峰值：30000EPS；包含日志收集、存储、查询、统计分析等功能。三年原厂质保服务；
终端威胁防御系统	1	终端威胁防御系统基础组件，实现系统的集中管理、策略配置、报表查看等功能。
	300	1 个 Windows PC 客户端防病毒功能授权,含 3 年升级许可,按点数销

		售。防病毒的病毒查杀支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS 病毒等进行查杀，提供主动防御系统防护等功能。客户端系统默认支持 Windows XP/VISTA/WIN7/WIN8/WIN10。
	10	针对服务器操作系统进行病毒查杀，提供主动防御系统防护等功能，含三年升级许可。
安全服务	1	安全加固建设服务：对 PC 终端、服务器、网络设备、安全设备、操作系统、数据库系统进行加固；
	1	管理制度规范建设服务：建立健全管理制度、管理机构、人员管理、建设管理、运维管理进行补充完善；
	1	安全培训服务：对医院全员进行安全意识培训，对技术人员进行安全技术培训；

注：1.全部产品含三年原厂质保服务；

2.达到公安部《网络安全等级保护基本技术要求》标准；

★3.承诺通过网络安全等级保护三级验收测评工作。

2.2 安全产品详细技术要求

2.2.1 交换机

序号	参数要求
1	交换容量≥598Gbps，包转发率≥252Mpps；
2	整机提供 48 个千兆电口，8 个万兆 SFP+光口；
3	▲必须支持 EAPS 协议并出具配置截图证明文件加盖设备生产厂家公章；
4	支持 MAC 地址≥16K，支持 ARP 表项≥2K；
5	支持端口聚合，每个聚合组至少 8 个端口；
6	支持静态配置和动态学习 MAC 地址；
7	支持查看和清除 MAC 地址；
8	MAC 地址老化时间可配置；
9	支持 MAC 地址学习数量限制；
10	支持 MAC 地址过滤功能；
11	支持 4K VLAN 表项；
12	支持 GVRP；
13	支持 QinQ 功能；
14	支持 Private VLAN；
15	支持 802.1D（STP）、802.1W（RSTP）、802.1S（MSTP）；

16	支持 BPDU 保护、根保护、环路保护；
17	支持 IGMP v1/v2/v3；
18	支持 IGMP Snooping；
19	支持 IGMP Fast Leave；
20	支持组播组策略及组播组数量限制；
21	支持组播流量跨 VLAN 复制；
22	支持静态路由、RIP v1/v2、OSPF、BGP；
23	支持基于 L2/L3/L4 协议头各字段的流量分类；
24	支持 CAR 流量限制；
25	支持 802.1P/DSCP 优先级重新标记；
26	支持 SP、WRR、SP+WRR 等队列调度方式；
27	支持 Tail-Drop、WRED 等拥塞避免机制；
28	支持流量监管与流量整形；
29	支持基于 L2/L3/L4 的 ACL 流识别与过滤安全机制；
30	支持防 DDoS 攻击、TCP 的 SYN Flood 攻击、UDP Flood 攻击等；
31	支持对组播、广播、未知单播报文的抑制功能；
32	支持端口隔离；
33	支持端口安全、IP+MAC+端口绑定；
34	支持 DHCP Snooping、DHCP Option 82；
35	支持 IEEE 802.1x 认证；
36	支持 Radius、BDTacacs+认证；
37	支持命令行分级保护；
38	支持静态/LACP 方式链路聚合；
39	支持 EAPS、ERPS 以太环网保护协议；
40	支持 ISSU 业务不中断系统升级；
41	支持 Console、Telnet、SSH 2.0；
42	支持基于浏览器 WEB 方式管理；
43	支持 SNMP v1/v2/v3；
44	支持 TFTP 方式的文件上传、下载管理；
45	支持 RMON 事件历史记录；
46	▲设备厂商通过 ISO45001 职业健康安全管理体系认证证书，投标文件提供证书复印件或扫描件，并加盖公章。
47	▲设备厂商通过知识产权管理体系认证证书，投标文件提供证书复印件或扫描件，并加盖公章。

48	▲设备厂商通过工业信息安全应急服务支撑单位证书，投标文件提供证书复印件或扫描件，并加盖公章。
49	▲设备厂商通过 ISO 14001 环境管理体系认证，投标文件提供中文证书复印件或扫描件，并加盖公章。
50	提供 3 年免费维保服务

2.2.2 互联网防火墙

类别	分项功能	指标参数
基本要求	系统结构	▲为响应产品国产化的号召，产品必须为自主研发（非 OEM），产品需拥有自主知识产权（提供软件著权证书、软件产品登记证书复印件并加盖原厂公章），为自主原创产品（提供证书复印件并加盖原厂公章）；产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理特性（提供相应资质证明并加盖原厂公章）；
	操作系统	▲安全操作系统采用冗余设计（提供产品相关功能页面截图并加盖原厂公章）；出于安全性考虑，多系统需在设备启动过程中进行选择不得在 WEB 维护界面中设置系统切换选项。
	硬件架构	▲1U 机箱，6 个千兆电口，8 个 SFP 插槽，标配冗余电源；默认含 IPSECVPN 模块，可扩展 SSLVPN 模块；支持扩展 AI 应用识别、IPS 入侵防御及 AV 防病毒功能；含 3 年入侵防御规则库升级服务许可；含 3 年防病毒规则库升级服务许可；三年原厂质保服务；
硬件配置	配置性能	防火墙吞吐 6Gbps，并发连接 220 万，新建连接数≥6.5 万；IPSECVPN 吞吐 180M，SSLVPN 吞吐 320M；
网络接入	工作模式	支持路由、交换、混合、虚拟线工作模式；
	路由交换	支持静态路由、ISP 路由及动态路由协议，支持 802.1q、QinQ 模式；
		支持基于源/目的地址、源/目的端口、用户、应用的策略路由，保证关键业务流量通过优质链路转发；
	接入功能	支持 GRE 与 IPSEC VPN 接入，提供标准算法及国密算法；（提供产品相关功能页面截图并加盖原厂公章）；
	链路聚合	▲为提高链路可靠性，需支持手工链路聚合及 LACP 链路聚合，提供不少于 10 种的负载分担算法，灵活实现对聚合组内业务流量的负载分担（提供产品相关功能页面截图并加盖原厂公章）；
	IP/MAC 绑定	支持手动添加绑定，基于 IP、接口的动态探测绑定，支持跨三层 IP/MAC 绑定，IP/MAC 绑定表可导入导出；
	地址转换	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；

		支持 Sticky NAT 开关,使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；
		支持 MAP66 功能，将从内部发往 Internet 的数据包的源 IPv6 地址修改为全球单播源 IPv6 地址，实现 IPv6 网络间的地址转换；
	智能 DNS	▲支持智能 DNS 及 DNS Docting 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（提供产品相关功能页面截图并加盖原厂公章）；
IPv6	双栈模式	支持 IPv4/IPv6 双栈工作模式；
	访问控制	支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；
	安全防护	支持基于 IPv6 的应用层检测（FTP\TFTP）、病毒过滤、URL 过滤、ADS、IPS 检测（提供产品相关功能页面截图并加盖原厂公章）；
虚拟系统	资源虚拟化	▲支持在一台物理设备上划分出相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源;（提供产品相关功能页面截图并加盖原厂公章）；
	功能虚拟化	支持配置文件、系统服务等系统功能虚拟化，支持路由、链路聚合等网络功能虚拟化，支持安全策略、NAT 策略、带宽管理、认证策略、IPV6 功能、URL 过滤、异常行为分析、病毒过滤、内容过滤、审计、报表等安全功能虚拟化；
用户管控	认证方式	内置强大的用户身份管理系统，支持本地认证、证书认证及免认证等方式，同时支持 RADIUS、LDAP、TACACS 等多种第三方外部认证设置;（提供产品相关功能页面截图并加盖原厂公章）；
	用户管控	▲综合运用身份认证与访问控制技术，通过内置智能过滤引擎实现基于用户身份的安全防护策略部署与可视化监控；支持手动创建用户、批量导入导出用户，同时支持设备扫描方式创建用户;（提供产品相关功能页面截图并加盖原厂公章）；
		支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回；–
		支持本地 CA 和第三方 CA，支持作为 CA 认证中心为其他人签发证书，也可采用第三方 CA 为其他人签发证书（提供产品相关功能页面截图并加盖原厂公章）；支持标准 CRL 列表，支持 CRL 手工更新，同时支持 CRL 自动下载，通过 HTTP 或者 LDAP 方式定时自动下载更新 CRL 文件；
应用管控	应用识别	▲内置强大应用识别引擎，综合运用端口识别、行为识别、特征识别、关联识别等技术手段，准确识别传统应用如 P2P（提供 P2P 流量识别技术相关的专利证明）、web 应用、移动应用、云应用、加密应用等；内置独立应用识别特征库，总数 2100 种以上，支持应用特征库在线或本地更新，支持应用特征自定义（提供产品相关

		功能页面截图并加盖原厂公章）；
	带宽管理	支持基于 IP/IP 组、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略（提供产品相关功能页面截图并加盖原厂公章）；，支持带宽策略优先级，可配置包含链路、父通道、子通道的 5 层多级带宽策略，对流量进行细分管理，保证带宽的利用率（提供产品相关功能页面截图并加盖原厂公章）；
	连接控制	▲支持对单条访问控制策略进行最大并发连接数限制（提供产品相关功能页面截图并加盖原厂公章）；
		为保护内部网络资源以及合理分配设备系统资源，需支持对指定的源/目的 IP 地址、MAC 地址、应用制定相应的连接限制策略，策略包含三种限制类型：单个 IP 每秒新建连接限制、单个 IP 连接数限制及连接总数限制；
		支持监控功能，显示最近被拦截的 IP、地址对象及应用的节点信息；同时支持对连接数限制策略匹配信息进行分类统计，方便管理员根据统计分析结果进行相应的防护控制；
访问控制	一体化访问控制	▲内置高度集成的一体化智能过滤引擎技术，实现在同一条访问控制策略中配置传统的五元组信息、用户、域名、应用、服务、时间、安全引擎（入侵防御、URL 过滤、病毒过滤、数据防泄漏 DLP、内容过滤、文件过滤、审计、APT）的识别与控制；（提供产品相关功能页面截图并加盖原厂公章）；
		访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址；
		▲提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在 WEB 界面显示检测结果：红色为冗余策略，绿色为冲突策略；（提供产品相关功能页面截图并加盖原厂公章）；
		支持黑名单功能，可设置多个对象条件，如：五元组信息、地址范围、应用、用户等，实现对特定报文进行快速过滤；（提供产品相关功能页面截图并加盖原厂公章）；
安全防护	入侵防御	▲内置攻击检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持 web 攻击识别和防护，如跨站脚本攻击、SQL 注入攻击；支持超过 4200+攻击特征库（提供产品相关功能页面截图并加盖原厂公章）；,同时支持自定义特征库,且厂商具备强大的漏洞和功放研究能力,为 CNNVD 一级支撑单位（提供官网链接），能够确保每周至少更新 1 次攻击特征库。
	未知威胁防御	支持 APT 防御，不依赖于攻击、恶意代码等特征库进行检测，通过沙箱技术对于未知漏洞攻击（0day/1day 漏洞）、木马、病毒具有检测能力；可根据用户环境，将 APT 工作模式设置为深度模式或者智能模式（提供产品相关功能页面截图并加

		盖原厂公章）；
		▲支持异常行为检测，内置统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；（提供产品相关功能页面截图并加盖原厂公章）；
	DDOS 防御	内置流量检测清洗引擎，支持基于 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等众多协议类型的防护策略；提供丰富的策略模板，且支持策略模板自定义；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于 IP 协议的检测清洗，包括但不限于：IP Flood、IP Frag Flood、端口扫描、IP 地址扫描，以及 Fraggle、icmp redirect、icmp unreachable、land、ping of death、smurf、route record、source route、tcp flag、tracert、winnuke 等异常报文攻击；（提供产品相关功能页面截图并加盖原厂公章）；
		▲支持基于 TCP 协议的检测清洗，包括但不限于：TCP Flood、SYN Flood、SynACK Flood、ACK Flood、FIN Flood、RST Flood、新建 SESSION Flood、SESSION Flood 等；支持 SYN 源认证技术，认证模式可设置为基本模式或者高级模式，以防止虚假源攻击；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于 UDP 协议的检测清洗，包括对源、目的限速，对 UDP 最大及最小报文限制；同时支持 UDP 关联认证，要求所有去往服务器的 UDP 报文，必须首先与该服务器的 TCP 端口建立 TCP 连接，对源地址进行合法性认证；
		支持基于 DNS 协议的检测清洗，包括但不限于：DNS QUERY FLOOD、DNS REPLY FLOOD、DNS 投毒攻击、DNS 格式检查、DNS NX 异常比率检测等；支持 DNS QUERY 源认证、DNS REPLY 源认证，认证方式可选基本源认证或者 cname 认证；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于 HTTP 协议的检测清洗，包括但不限于：HTTP Flood、HTTP 新建连接 Flood、HTTP 并发连接 Flood、HTTP URI CC 等攻击检测，同时支持对 HTTP slow-header 和 HTTP slow-post 设置最大传输时间以及异常会话数阈值，有效防御慢速攻击；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于 NTP 协议的检测清洗，包括 NTP REQUEST FLOOD、NTP REPLY FLOOD 等攻击检测，支持基于 NTP 请求限速、NTP 响应限速、源认证、会话认证的防御策略；（提供产品相关功能页面截图并加盖原厂公章）；
		支持根据 DOS/DDOS 攻击行为自动添加动态黑/白名单功能，可自定义动态黑/白名单超时时间；（提供产品相关功能页面截图并加盖原厂公章）；
	病毒过滤	内置病毒检测引擎，支持 HTTP/SMTP/POP3/FTP/IM 等协议的病毒防御，对每种协议数据流的检测方向可选双向、上传、下载；（提供产品相关功能页面截图并加盖

		原厂公章）；
		▲内置至少 2 种专业反病毒厂商或研究机构的病毒特征库，符合等级保护相关标准对网关防病毒特征库和主机防病毒特征库异构的要求。（提供至少 2 家知名、专业防病毒厂商或研究机构的合作文件复印件）病毒特征库规模超过 400 万（提供产品相关功能页面截图并加盖原厂公章）；
		支持病毒白名单，用户可以根据实际业务需求将特定威胁进行排除（提供产品相关功能页面截图并加盖原厂公章）；
	URL 过滤	内置互联网 URL 分类库，支持超过 80 大类、2500 万的 URL 地址分类库，用户可根据上述网站类别，对自身网络的 WEB 应用实施全面化管控，杜绝非法、违规网站的访问行为，从而净化网络应用环境；
	文件过滤	▲内置文件过滤引擎，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM 文件传输等应用类型以及 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤（提供产品相关功能页面截图并加盖原厂公章）；
	内容过滤	支持基于 http、ftp、telnet、smtp、pop3 等协议的内容过滤策略，可对微博、贴吧上传的内容及附件进行过滤，可对 FTP 上传/下载的文件名进行过滤，同时支持过滤 FTP 信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤；（提供产品相关功能页面截图并加盖原厂公章）；
	DLP	▲内置 DLP 数据防泄漏引擎，可针对发送者或接收者模式配置独立的 DLP 策略，对数据进行监控识别，达到敏感数据防护目的。 为提高产品的可用性，需支持识别的加密文件格式不少于 12 种；压缩文件格式不少于 25 种，如 RAR、ZIP、GZ、TAR 等；支持识别 Linux，Unix 等非 Winodws 的文件类型；支持识别异常文件格式类型；支持识别自定义文件类型；（提供产品相关功能页面截图并加盖原厂公章）；
	配置维护	支持多个配置文件并存，配置文件数量不少于 20 个（提供产品相关功能页面截图并加盖原厂公章）；
	升级维护	▲支持多个系统升级包并存，系统升级包文件数量不少于 5 个（提供产品相关功能页面截图并加盖原厂公章）；
	系统诊断	支持分别针对网络层、传输层和应用层提供诊断系统网络连通性的工具，包括 PING、 TRACEROUTE、 TCP、 HTTP 和 DNS（提供产品相关功能页面截图并加盖原厂公章）； 支持在 WEB 界面进入 CLI 模式，执行系统配置、网络诊断、过滤抓包等命令，提

		高管理员运维效率（提供产品相关功能页面截图并加盖原厂公章）；
	管理员	▲支持系统管理员能够通过本地认证及外部认证方式进行登录管理，外部认证失败时可转本地认证（提供产品相关功能页面截图并加盖原厂公章）；支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置（提供产品相关功能页面截图并加盖原厂公章）；
数据中心	报表	内置 15 类预定义报表模板，支持根据通信流量、上网行为、威胁统计等来源数据库自定义报表模板；支持一次性报表及周期性报表，可自定义统计时间；（提供产品相关功能页面截图并加盖原厂公章）；
		支持报表按照 PDF、WORD 及 EXCEL 格式导出；（提供产品相关功能页面截图并加盖原厂公章）；
	审计	支持独立配置审计策略，同时也可将指定的 IP 地址、 URL、 应用加入白名单，不进行数据审计；（提供产品相关功能页面截图并加盖原厂公章）；
		支持网站访问审计：审计指定类别的 URL 地址、审计命中指定关键字的网页标题和网页内容；（提供产品相关功能页面截图并加盖原厂公章）；
		支持邮件内容审计：对接收/发送邮件行为及邮件内容进行审计；FTP 审计：对 FTP 上传/下载行为及文件内容进行审计；（提供产品相关功能页面截图并加盖原厂公章）；
		▲支持网盘审计：对主流网盘应用如 360 云盘、百度网盘、腾讯微云、华为网盘、新浪网盘等上传内容进行审计；（提供产品相关功能页面截图并加盖原厂公章）；
		支持 telnet 审计：对 telnet 协议命令进行审计；（提供产品相关功能页面截图并加盖原厂公章）；
		提供完善的审计数据查询功能，方便管理员对用户的上网行为进行审查和分析。支持对用户上网行为进行完整的审计数据查询，包括访问网站、邮件收发、论坛微博、 FTP、 网盘、 TELNET 等；（提供产品相关功能页面截图并加盖原厂公章）；同时支持对用户上网流量时长进行完整的审计数据查询，包括服务端 IP、用户名、协议、上行流量、下行流量、总流量、时间等；（提供产品相关功能页面截图并加盖原厂公章）；
	日志	支持日志本地存储，可对不同类型日志设置存储空间；（提供产品相关功能页面截图并加盖原厂公章）；同时支持外发至 SYSLOG 服务器，可将多条日志合并成一条日志传送到日志服务器中，可选择对日志传输是否加密，设定 8 位或以上的加密密钥；（提供产品相关功能页面截图并加盖原厂公章）；
		日志查看可划分为管理日志、系统日志、策略日志、应用行为日志等四大模块，具体包含用户、连接、流量、NAT、审计、HA、APT、未知威胁等 20 个日志类别，

		可将日志按照 CSV 或 XML 格式导出；（提供产品相关功能页面截图并加盖原厂公章）；
显示监控	资源监控	▲在 WEB 界面提供资源监控开关，可对 cpu 占用率、内存占用率、磁盘占用率设置阈值；（提供产品相关功能页面截图并加盖原厂公章）；
	流量统计	支持根据应用对通过设备的数据报文流量进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速；（提供产品相关功能页面截图并加盖原厂公章）；
		支持根据用户/用户组对通过设备的数据报文流量进行统计，包括用户总流量排名和各个用户的用户名、认证类型、上行流量、下行流量、新建会话数、当前会话数以及流速；
		支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数；
		支持指定监控时间周期，包括：实时、最近 1 小时、最近 1 天、最近 1 周、最近 1 月等；
	威胁统计	支持根据按照病毒防御、入侵防御、APT 防御、ADS 攻击进行威胁统计，可按照威胁类型/攻击者/受害者三种方式进行威胁排名。（提供产品相关功能页面截图并加盖原厂公章）；
资质要求	▲产品资质（需提供证书复印件加盖厂家公章）	计算机信息系统安全专用产品销售许可证（第二代防火墙增强级）；
		涉密信息系统产品检测证书
		国家信息安全漏洞库兼容性资质证书
		ISCCC 产品认证证书（三级）
		网络关键设备和网络安全专用产品安全认证证书
		防火墙产品密码检测证书
		国家信息安全测评信息技术产品安全测评证书（EAL4+）
		IPV6 金牌认证；
	▲厂商资质（需提供证书复印件加盖厂家公章）	为保障项目的机密性，原厂商须具备涉密信息系统集成甲级资质；
		为保证项目设计及集成能力，设备原厂商须具有通信行业安全设计与集成二级资质证书；
		为保障厂商的售后服务水平，原厂商需获得 ISO27001 信息安全管理体系认证、ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证；
		为保证项目的应急响应能力，原厂商须具备网络安全应急服务支撑单位（国家级）资质；

		为保证项目安全服务能力，设备原厂商须具备国家信息安全认证信息安全服务资质证书（安全工程类三级），信息安全等级保护安全建设服务机构能力评估合格证书；
		为保证本项目后续的厂商培训能力，设备原厂商须具备专业的信息安全技术培训能力，并取得权威的培训资质，应具有国家信息安全测评授权培训机构资质证书；
▲售后服务		产品须由原厂商提供 3 年应急响应服务、定期巡检服务，提供设备原厂商针对本项目的授权及售后服务承诺函，点对点技术响应函并加盖原厂公章；

2.2.3 专线防火墙

类别	分项功能	指标参数
基本要求	系统结构	▲为响应产品国产化的号召，产品必须为自主研发（非 OEM），产品需拥有自主知识产权（提供软件著权证书、软件产品登记证书复印件并加盖原厂公章），为自主原创产品（提供证书复印件并加盖原厂公章）；产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理特性（提供相应资质证明并加盖原厂公章）；
	操作系统	▲安全操作系统采用冗余设计（提供产品相关功能页面截图并加盖原厂公章）；出于安全性考虑，多系统需在设备启动过程中进行选择不得在 WEB 维护界面中设置系统切换选项。
	硬件架构	1U 机箱，6 个千兆电口，8 个 SFP 插槽，标配冗余电源；默认含 IPSECVPN 模块，可扩展 SSLVPN 模块；支持扩展 AI 应用识别、IPS 入侵防御及 AV 防病毒功能；含 3 年入侵防御规则库升级服务许可；含 3 年防病毒规则库升级服务许可；三年原厂质保服务；
硬件配置	配置性能	防火墙吞吐 6Gbps，并发连接 220 万，新建连接数≥6.5 万；IPSECVPN 吞吐 180M，SSLVPN 吞吐 320M；
网络接入	工作模式	支持路由、交换、混合、虚拟线工作模式；
	路由交换	支持静态路由、ISP 路由及动态路由协议，支持 802.1q、QinQ 模式；
		支持基于源/目的地址、源/目的端口、用户、应用的策略路由，保证关键业务流量通过优质链路转发；
	接入功能	支持 GRE 与 IPSEC VPN 接入，提供标准算法及国密算法；（提供产品相关功能页面截图并加盖原厂公章）；
	链路聚合	▲为提高链路可靠性，需支持手工链路聚合及 LACP 链路聚合，提供不少于 10 种的负载分担算法，灵活实现对聚合组内业务流量的负载分担（提供产品相关功能页面截图并加盖原厂公章）；
	IP/MAC 绑定	支持手动添加绑定，基于 IP、接口的动态探测绑定，支持跨三层 IP/MAC 绑定，

		IP/MAC 绑定表可导入导出；
	地址转换	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；
		支持 MAP66 功能，将从内部发往 Internet 的数据包的源 IPv6 地址修改为全球单播源 IPv6 地址，实现 IPv6 网络间的地址转换；
	智能 DNS	▲支持智能 DNS 及 DNS Docting 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（提供产品相关功能页面截图并加盖原厂公章）；
IPv6	双栈模式	支持 IPv4/IPv6 双栈工作模式；
	访问控制	支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；
	安全防护	支持基于 IPv6 的应用层检测（FTP\TFTP）、病毒过滤、URL 过滤、ADS、IPS 检测（提供产品相关功能页面截图并加盖原厂公章）；
虚拟系统	资源虚拟化	▲支持在一台物理设备上划分出相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源；（提供产品相关功能页面截图并加盖原厂公章）；
	功能虚拟化	▲支持配置文件、系统服务等系统功能虚拟化，支持路由、链路聚合等网络功能虚拟化，支持安全策略、NAT 策略、带宽管理、认证策略、IPV6 功能、URL 过滤、异常行为分析、病毒过滤、内容过滤、审计、报表等安全功能虚拟化；（提供产品相关功能页面截图并加盖原厂公章）；
用户管控	认证方式	内置强大的用户身份管理系统，支持本地认证、证书认证及免认证等方式，同时支持 RADIUS、LDAP、TACACS 等多种第三方外部认证设置；（提供产品相关功能页面截图并加盖原厂公章）；
	用户管控	综合运用身份认证与访问控制技术，通过内置智能过滤引擎实现基于用户身份的安全防护策略部署与可视化监控；支持手动创建用户、批量导入导出用户，同时支持设备扫描方式创建用户；（提供产品相关功能页面截图并加盖原厂公章）；
		支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回；–
		支持本地 CA 和第三方 CA，支持作为 CA 认证中心为其他人签发证书，也可采用第三方 CA 为其他人签发证书（提供产品相关功能页面截图并加盖原厂公章）；支持标准 CRL 列表，支持 CRL 手工更新，同时支持 CRL 自动下载，通过 HTTP 或者 LDAP 方式定时自动下载更新 CRL 文件；
应用	应用识别	▲内置强大应用识别引擎，综合运用端口识别、行为识别、特征识别、关联识别

管控		等技术手段，准确识别传统应用如 P2P（提供 P2P 流量识别技术相关的专利证明）、web 应用、移动应用、云应用、加密应用等；内置独立应用识别特征库，总数 2100 种以上，支持应用特征库在线或本地更新，支持应用特征自定义（提供产品相关功能页面截图并加盖原厂公章）；
	带宽管理	支持基于 IP/IP 组、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略（提供产品相关功能页面截图并加盖原厂公章）;，支持带宽策略优先级，可配置包含链路、父通道、子通道的 5 层多级带宽策略，对流量进行细分管理，保证带宽的利用率（提供产品相关功能页面截图并加盖原厂公章）；
	连接控制	▲支持对单条访问控制策略进行最大并发连接数限制（提供产品相关功能页面截图并加盖原厂公章）；
		为保护内部网络资源以及合理分配设备系统资源，需支持对指定的源/目的 IP 地址、MAC 地址、应用制定相应的连接限制策略，策略包含三种限制类型：单个 IP 每秒新建连接限制、单个 IP 连接数限制及连接总数限制；
		▲支持监控功能，显示最近被拦截的 IP、地址对象及应用的节点信息；同时支持对连接数限制策略匹配信息进行分类统计，方便管理员根据统计分析结果进行相应的防护控制；（提供产品相关功能页面截图并加盖原厂公章）；
访问控制	一体化访问控制	▲内置高度集成的一体化智能过滤引擎技术，实现在同一条访问控制策略中配置传统的五元组信息、用户、域名、应用、服务、时间、安全引擎（入侵防御、URL 过滤、病毒过滤、数据防泄漏 DLP、内容过滤、文件过滤、审计、APT）的识别与控制；（提供产品相关功能页面截图并加盖原厂公章）；
		访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址；
		▲提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在 WEB 界面显示检测结果：红色为冗余策略，绿色为冲突策略；（提供产品相关功能页面截图并加盖原厂公章）；
		支持黑名单功能，可设置多个对象条件，如：五元组信息、地址范围、应用、用户等，实现对特定报文进行快速过滤；（提供产品相关功能页面截图并加盖原厂公章）；
安全防护	入侵防御	内置攻击检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持 web 攻击识别和防护，如跨站脚本攻击、SQL 注入攻击；支持超过 4200+攻击特征库（提供产品相关功能页面截图并加盖原厂公章）;，同时支持自定义特征库,且厂商具备强大的漏洞和功放研究能力，为 CNNVD 一级支撑单位（提供官网链接），能够确保每周至少更新 1 次攻击特征库。

	未知威胁防御	▲支持 APT 防御，不依赖于攻击、恶意代码等特征库进行检测，通过沙箱技术对于未知漏洞攻击（0day/1day 漏洞）、木马、病毒具有检测能力；可根据用户环境，将 APT 工作模式设置为深度模式或者智能模式（提供产品相关功能页面截图并加盖原厂公章）；
		▲支持异常行为检测，内置统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；（提供产品相关功能页面截图并加盖原厂公章）；
	DDOS 防御	内置流量检测清洗引擎，支持基于 IP、ICMP、TCP、UDP、DNS、HTTP、NTP 等众多协议类型的防护策略；提供丰富的策略模板，且支持策略模板自定义；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于 IP 协议的检测清洗，包括但不限于：IP Flood、IP Frag Flood、端口扫描、IP 地址扫描，以及 Fraggle、icmp redirect、icmp unreachable、land、ping of death、smurf、route record、source route、tcp flag、tracert、winnuke 等异常报文攻击；（提供产品相关功能页面截图并加盖原厂公章）；
		▲支持基于 TCP 协议的检测清洗，包括但不限于：TCP Flood、SYN Flood、SynACK Flood、ACK Flood、FIN Flood、RST Flood、新建 SESSION Flood、SESSION Flood 等；支持 SYN 源认证技术，认证模式可设置为基本模式或者高级模式，以防止虚假源攻击；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于 UDP 协议的检测清洗，包括对源、目的限速，对 UDP 最大及最小报文限制；同时支持 UDP 关联认证，要求所有去往服务器的 UDP 报文，必须首先与该服务器的 TCP 端口建立 TCP 连接，对源地址进行合法性认证；
		支持基于 DNS 协议的检测清洗，包括但不限于：DNS QUERY FLOOD、DNS REPLY FLOOD、DNS 投毒攻击、DNS 格式检查、DNS NX 异常比率检测等；支持 DNS QUERY 源认证、DNS REPLY 源认证，认证方式可选基本源认证或者 cname 认证；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于 HTTP 协议的检测清洗，包括但不限于：HTTP Flood、HTTP 新建连接 Flood、HTTP 并发连接 Flood、HTTP URI CC 等攻击检测，同时支持对 HTTP slow-header 和 HTTP slow-post 设置最大传输时间以及异常会话数阈值，有效防御慢速攻击；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于 NTP 协议的检测清洗，包括 NTP REQUEST FLOOD、NTP REPLY FLOOD 等攻击检测，支持基于 NTP 请求限速、NTP 响应限速、源认证、会话认证的防御策略；（提供产品相关功能页面截图并加盖原厂公章）；
		支持根据 DOS/DDOS 攻击行为自动添加动态黑/白名单功能，可自定义动态黑/白名

		单超时时间；（提供产品相关功能页面截图并加盖原厂公章）；
	病毒过滤	内置病毒检测引擎，支持 HTTP/SMTP/POP3/FTP/IM 等协议的病毒防御，对每种协议数据流的检测方向可选双向、上传、下载；（提供产品相关功能页面截图并加盖原厂公章）；
		▲内置至少 2 种专业反病毒厂商或研究机构的病毒特征库，符合等级保护相关标准对网关防病毒特征库和主机防病毒特征库异构的要求。（提供至少 2 家知名、专业防病毒厂商或研究机构的合作文件复印件）病毒特征库规模超过 400 万（提供产品相关功能页面截图并加盖原厂公章）；
		支持病毒白名单，用户可以根据实际业务需求将特定威胁进行排除（提供产品相关功能页面截图并加盖原厂公章）；
	URL 过滤	内置互联网 URL 分类库，支持超过 80 大类、2500 万的 URL 地址分类库，用户可根据上述网站类别，对自身网络的 WEB 应用实施全面化管控，杜绝非法、违规网站的访问行为，从而净化网络应用环境；
	文件过滤	▲内置文件过滤引擎，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM 文件传输等应用类型以及 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤（提供产品相关功能页面截图并加盖原厂公章）；
	内容过滤	支持基于 http、ftp、telnet、smtp、pop3 等协议的内容过滤策略，可对微博、贴吧上传的内容及附件进行过滤，可对 FTP 上传/下载的文件名进行过滤，同时支持过滤 FTP 信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤；（提供产品相关功能页面截图并加盖原厂公章）；
	DLP	▲内置 DLP 数据防泄漏引擎，可针对发送者或接收者模式配置独立的 DLP 策略，对数据进行监控识别，达到敏感数据防护目的。 为提高产品的可用性，需支持识别的加密文件格式不少于 12 种；压缩文件格式不少于 25 种，如 RAR、ZIP、GZ、TAR 等；支持识别 Linux，Unix 等非 Winodws 的文件类型；支持识别异常文件格式类型；支持识别自定义文件类型；（提供产品相关功能页面截图并加盖原厂公章）；
	配置维护	支持多个配置文件并存，配置文件数量不少于 20 个（提供产品相关功能页面截图并加盖原厂公章）；
	升级维护	▲支持多个系统升级包并存，系统升级包文件数量不少于 5 个（提供产品相关功能页面截图并加盖原厂公章）；
	系统诊断	支持分别针对网络层、传输层和应用层提供诊断系统网络连通性的工具，包括

		PING、 TRACEROUTE、 TCP、 HTTP 和 DNS（提供产品相关功能页面截图并加盖原厂公章）； 支持在 WEB 界面进入 CLI 模式，执行系统配置、网络诊断、过滤抓包等命令，提高管理员运维效率（提供产品相关功能页面截图并加盖原厂公章）；
	管理员	▲支持系统管理员能够通过本地认证及外部认证方式进行登录管理，外部认证失败时可转本地认证（提供产品相关功能页面截图并加盖原厂公章）；支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置（提供产品相关功能页面截图并加盖原厂公章）；
数据中心	报表	▲内置 15 类预定义报表模板，支持根据通信流量、上网行为、威胁统计等来源数据库自定义报表模板；支持一次性报表及周期性报表，可自定义统计时间；（提供产品相关功能页面截图并加盖原厂公章）；
		支持报表按照 PDF、WORD 及 EXCEL 格式导出；（提供产品相关功能页面截图并加盖原厂公章）；
	审计	支持独立配置审计策略，同时也可将指定的 IP 地址、 URL、 应用加入白名单，不进行数据审计；（提供产品相关功能页面截图并加盖原厂公章）；
		支持网站访问审计：审计指定类别的 URL 地址、审计命中指定关键字的网页标题和网页内容；（提供产品相关功能页面截图并加盖原厂公章）；
		支持邮件内容审计：对接收/发送邮件行为及邮件内容进行审计；FTP 审计：对 FTP 上传/下载行为及文件内容进行审计；（提供产品相关功能页面截图并加盖原厂公章）；
		▲支持网盘审计：对主流网盘应用如 360 云盘、百度网盘、腾讯微云、华为网盘、新浪网盘等上传内容进行审计；（提供产品相关功能页面截图并加盖原厂公章）；
		支持 telnet 审计：对 telnet 协议命令进行审计；（提供产品相关功能页面截图并加盖原厂公章）；
		提供完善的审计数据查询功能，方便管理员对用户的上网行为进行审查和分析。支持对用户上网行为进行完整的审计数据查询，包括访问网站、邮件收发、论坛微博、 FTP、 网盘、 TELNET 等；（提供产品相关功能页面截图并加盖原厂公章）；同时支持对用户上网流量时长进行完整的审计数据查询，包括服务端 IP、用户名、协议、上行流量、下行流量、总流量、时间等；（提供产品相关功能页面截图并加盖原厂公章）；
	日志	支持日志本地存储，可对不同类型日志设置存储空间；（提供产品相关功能页面截图并加盖原厂公章）；同时支持外发至 SYSLOG 服务器，可将多条日志合并成一条日志传送到日志服务器中，可选择对日志传输是否加密，设定 8 位或以上的加密

		密钥；（提供产品相关功能页面截图并加盖原厂公章）；
		日志查看可划分为管理日志、系统日志、策略日志、应用行为日志等四大模块，具体包含用户、连接、流量、NAT、审计、HA、APT、未知威胁等 20 个日志类别，可将日志按照 CSV 或 XML 格式导出；（提供产品相关功能页面截图并加盖原厂公章）；
显示监控	资源监控	▲在 WEB 界面提供资源监控开关，可对 cpu 占用率、内存占用率、磁盘占用率设置阈值；（提供产品相关功能页面截图并加盖原厂公章）；
	流量统计	支持根据应用对通过设备的数据报文流量进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速；（提供产品相关功能页面截图并加盖原厂公章）；
		支持根据用户/用户组对通过设备的数据报文流量进行统计，包括用户总流量排名和各个用户的用户名、认证类型、上行流量、下行流量、新建会话数、当前会话数以及流速；
		支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数；
		支持指定监控时间周期，包括：实时、最近 1 小时、最近 1 天、最近 1 周、最近 1 月等；
	威胁统计	支持根据按照病毒防御、入侵防御、APT 防御、ADS 攻击进行威胁统计，可按照威胁类型/攻击者/受害者三种方式进行威胁排名。（提供产品相关功能页面截图并加盖原厂公章）；
资质要求	▲产品资质（需提供证书复印件加盖厂家公章）	计算机信息系统安全专用产品销售许可证（第二代防火墙增强级）；
		涉密信息系统产品检测证书
		国家信息安全漏洞库兼容性资质证书
		ISCCC 产品认证证书（三级）
		网络关键设备和网络安全专用产品安全认证证书
		防火墙产品密码检测证书
		国家信息安全测评信息技术产品安全测评证书（EAL4+）
		IPV6 金牌认证；
	▲厂商资质（需提供证书复印件加盖厂家公章）	为保障项目的机密性，原厂商须具备涉密信息系统集成甲级资质；
		为保证项目设计及集成能力，设备原厂商须具有通信行业安全设计与集成二级资质证书；
		为保障厂商的售后服务水平，原厂商需获得 ISO27001 信息安全管理体系认证、ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环

		境管理体系认证；
		为保证项目的应急响应能力，原厂商须具备网络安全应急服务支撑单位（国家级）资质；
		为保证项目安全服务能力，设备原厂商须具备国家信息安全认证信息安全服务资质证书（安全工程类三级），信息安全等级保护安全建设服务机构能力评估合格证书；
		为保证本项目后续的厂商培训能力，设备原厂商须具备专业的信息安全技术培训能力，并取得权威的培训资质，应具有国家信息安全测评授权培训机构资质证书；
▲售后服务		产品须由原厂商提供 3 年应急响应服务、定期巡检服务，提供设备原厂商针对本项目的授权及售后服务承诺函，点对点技术响应函并加盖原厂公章；

2.2.4 数据中心防火墙

类别	分项功能	指标参数
基本要求	系统结构	▲为响应产品国产化的号召，产品必须为自主研发（非 OEM），产品需拥有自主知识产权（提供软件著权证书、软件产品登记证书复印件并加盖原厂公章），为自主原创产品（提供证书复印件并加盖原厂公章）；产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理特性（提供相应资质证明并加盖原厂公章）；
	操作系统	▲安全操作系统采用冗余设计（提供产品相关功能页面截图并加盖原厂公章）；出于安全性考虑，多系统需在设备启动过程中进行选择不得在 WEB 维护界面中设置系统切换选项。
	硬件架构	▲1U 机箱，配置为 6 个 10/100/1000BASE-T 接口和 2 个 SFP 插槽，2 个可插拔的扩展槽，标配双电源，默认包含应用识别功能；含 3 年入侵防御规则库升级服务许可；含 3 年防病毒规则库升级服务许可；三年原厂质保服务；
硬件配置	配置性能	防火墙吞吐率：12Gbps，应用层吞吐率（FW+APP）：6Gbps，并发连接数：300 万；每秒新建连接数：13.5 万；
网络接入	工作模式	支持路由、交换、混合、虚拟线工作模式；
	路由交换	支持静态路由、ISP 路由及动态路由协议，支持 802.1q、QinQ 模式；
		支持基于源/目的地址、源/目的端口、用户、应用的策略路由，保证关键业务流量通过优质链路转发；
	接入功能	支持 GRE 与 IPSEC VPN 接入，提供标准算法及国密算法；（提供产品相关功能页面截图并加盖原厂公章）；
	链路聚合	▲为提高链路可靠性，需支持手工链路聚合及 LACP 链路聚合，提供不少于 10 种的负载分担算法，灵活实现对聚合组内业务流量的负载分担（提供产品相关功能

		页面截图并加盖原厂公章）；
	IP/MAC 绑定	支持手动添加绑定，基于 IP、接口的动态探测绑定，支持跨三层 IP/MAC 绑定，IP/MAC 绑定表可导入导出；
	地址转换	支持一对一 SNAT、多对一 SNAT、一对一 DNAT、双向 NAT、NoNAT 等多种转换方式；支持 Sticky NAT 开关，使相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同；
		支持 MAP66 功能，将从内部发往 Internet 的数据包的源 IPv6 地址修改为全球单播源 IPv6 地址，实现 IPv6 网络间的地址转换；
	智能 DNS	▲支持智能 DNS 及 DNS Docting 功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（提供产品相关功能页面截图并加盖原厂公章）；
IPv6	双栈模式	支持 IPv4/IPv6 双栈工作模式；
	访问控制	支持 IPv6 安全控制策略设置，能针对 IPv6 的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；
	安全防护	▲支持基于 IPv6 的应用层检测（FTP\TFTP）、病毒过滤、URL 过滤、ADS、IPS 检测（提供产品相关功能页面截图并加盖原厂公章）；
虚拟系统	资源虚拟化	▲支持在一台物理设备上划分出相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源；（提供产品相关功能页面截图并加盖原厂公章）；
	功能虚拟化	▲支持配置文件、系统服务等系统功能虚拟化，支持路由、链路聚合等网络功能虚拟化，支持安全策略、NAT 策略、带宽管理、认证策略、IPV6 功能、URL 过滤、异常行为分析、病毒过滤、内容过滤、审计、报表等安全功能虚拟化；（提供产品相关功能页面截图并加盖原厂公章）；
用户管控	认证方式	内置强大的用户身份管理系统，支持本地认证、证书认证及免认证等方式，同时支持 RADIUS、LDAP、TACACS 等多种第三方外部认证设置；（提供产品相关功能页面截图并加盖原厂公章）；
	用户管控	▲综合运用身份认证与访问控制技术，通过内置智能过滤引擎实现基于用户身份的安全防护策略部署与可视化监控；支持手动创建用户、批量导入导出用户，同时支持设备扫描方式创建用户；（提供产品相关功能页面截图并加盖原厂公章）；
		支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回；–
		支持本地 CA 和第三方 CA，支持作为 CA 认证中心为其他人签发证书，也可采用第三方 CA 为其他人签发证书（提供产品相关功能页面截图并加盖原厂公章）；支持标准 CRL 列表，支持 CRL 手工更新，同时支持 CRL 自动下载，通过 HTTP 或者 LDAP

		方式定时自动下载更新 CRL 文件；
应用管控	应用识别	▲内置强大应用识别引擎，综合运用端口识别、行为识别、特征识别、关联识别等技术手段，准确识别传统应用如 P2P（提供 P2P 流量识别技术相关的专利证明）、web 应用、移动应用、云应用、加密应用等；内置独立应用识别特征库，总数 2100 种以上，支持应用特征库在线或本地更新，支持应用特征自定义（提供产品相关功能页面截图并加盖原厂公章）；
	带宽管理	支持基于 IP/IP 组、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略（提供产品相关功能页面截图并加盖原厂公章）;，支持带宽策略优先级，可配置包含链路、父通道、子通道的 5 层多级带宽策略，对流量进行细分管理，保证带宽的利用率（提供产品相关功能页面截图并加盖原厂公章）；
	连接控制	▲支持对单条访问控制策略进行最大并发连接数限制（提供产品相关功能页面截图并加盖原厂公章）；
		为保护内部网络资源以及合理分配设备系统资源，需支持对指定的源/目的 IP 地址、MAC 地址、应用制定相应的连接限制策略，策略包含三种限制类型：单个 IP 每秒新建连接限制、单个 IP 连接数限制及连接总数限制；
		支持监控功能，显示最近被拦截的 IP、地址对象及应用的节点信息；同时支持对连接数限制策略匹配信息进行分类统计，方便管理员根据统计分析结果进行相应的防护控制；（提供产品相关功能页面截图并加盖原厂公章）；
访问控制	一体化访问控制	▲内置高度集成的一体化智能过滤引擎技术，实现在同一条访问控制策略中配置传统的五元组信息、用户、域名、应用、服务、时间、安全引擎（入侵防御、URL 过滤、病毒过滤、数据防泄漏 DLP、内容过滤、文件过滤、审计、APT）的识别与控制；（提供产品相关功能页面截图并加盖原厂公章）；
		访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行 Web 认证，在策略中可设置用户 Web 认证的门户地址；
		▲提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在 WEB 界面显示检测结果：红色为冗余策略，绿色为冲突策略；（提供产品相关功能页面截图并加盖原厂公章）；
		支持黑名单功能，可设置多个对象条件，如：五元组信息、地址范围、应用、用户等，实现对特定报文进行快速过滤；（提供产品相关功能页面截图并加盖原厂公章）；
安全防护	入侵防御	▲内置攻击检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持 web 攻击识别和防护，如跨站脚本攻击、SQL 注入攻击；支持超过 4200+攻击特征库（提供产品相关功能页面截图并加盖原厂

		公章);,同时支持自定义特征库,且厂商具备强大的漏洞和功放研究能力,为CNNVD一级支撑单位（提供官网链接），能够确保每周至少更新1次攻击特征库。
	未知威胁防御	▲支持APT防御，不依赖于攻击、恶意代码等特征库进行检测，通过沙箱技术对于未知漏洞攻击（0day/1day漏洞）、木马、病毒具有检测能力；可根据用户环境，将APT工作模式设置为深度模式或者智能模式（提供产品相关功能页面截图并加盖原厂公章）；
		支持异常行为检测，内置统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；（提供产品相关功能页面截图并加盖原厂公章）；
	DDOS防御	内置流量检测清洗引擎，支持基于IP、ICMP、TCP、UDP、DNS、HTTP、NTP等众多协议类型的防护策略；提供丰富的策略模板，且支持策略模板自定义；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于IP协议的检测清洗，包括但不限于：IP Flood、IP Frag Flood、端口扫描、IP 地址扫描，以及Fraggle、icmp redirect、icmp unreachable、land、ping of death、smurf、route record、source route、tcp flag、tracert、winnuke等异常报文攻击；（提供产品相关功能页面截图并加盖原厂公章）；
		▲支持基于TCP协议的检测清洗，包括但不限于：TCP Flood、SYN Flood、SynACK Flood、ACK Flood、FIN Flood、RST Flood、新建SESSION Flood、SESSION Flood等；支持SYN源认证技术，认证模式可设置为基本模式或者高级模式，以防止虚假源攻击；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于UDP协议的检测清洗，包括对源、目的限速，对UDP最大及最小报文限制；同时支持UDP关联认证，要求所有去往服务器的UDP报文，必须首先与该服务器的TCP端口建立TCP连接，对源地址进行合法性认证；
		支持基于DNS协议的检测清洗,包括但不限于:DNS QUERY FLOOD、DNS REPLY FLOOD、DNS投毒攻击、DNS格式检查、DNS NX异常比率检测等；支持DNS QUERY源认证、DNS REPLY源认证，认证方式可选基本源认证或者cname认证；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于HTTP协议的检测清洗,包括但不限于:HTTP Flood、HTTP新建连接Flood、HTTP并发连接Flood、HTTP URI CC等攻击检测，同时支持对HTTP slow-header和HTTP slow-post设置最大传输时间以及异常会话数阈值，有效防御慢速攻击；（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于NTP协议的检测清洗，包括NTP REQUEST FLOOD、NTP REPLY FLOOD等攻击检测，支持基于NTP请求限速、NTP响应限速、源认证、会话认证的防御策略；

		（提供产品相关功能页面截图并加盖原厂公章）；
		支持根据 DOS/DDOS 攻击行为自动添加动态黑/白名单功能，可自定义动态黑/白名单超时时间；（提供产品相关功能页面截图并加盖原厂公章）；
	病毒过滤	内置病毒检测引擎，支持 HTTP/SMTP/POP3/FTP/IM 等协议的病毒防御，对每种协议数据流的检测方向可选双向、上传、下载；（提供产品相关功能页面截图并加盖原厂公章）；
		▲内置至少 2 种专业反病毒厂商或研究机构的病毒特征库，符合等级保护相关标准对网关防病毒特征库和主机防病毒特征库异构的要求。（提供至少 2 家知名、专业防病毒厂商或研究机构的合作文件复印件）病毒特征库规模超过 400 万（提供产品相关功能页面截图并加盖原厂公章）；
		支持病毒白名单，用户可以根据实际业务需求将特定威胁进行排除（提供产品相关功能页面截图并加盖原厂公章）；
	URL 过滤	内置互联网 URL 分类库，支持超过 80 大类、2500 万的 URL 地址分类库，用户可根据上述网站类别，对自身网络的 WEB 应用实施全面化管控，杜绝非法、违规网站的访问行为，从而净化网络应用环境；
	文件过滤	▲内置文件过滤引擎，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM 文件传输等应用类型以及 HTTP/FTP/SMTP/POP3 等标准协议进行检测，识别可执行文件、office 文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过 50 种文档类型的文件过滤（提供产品相关功能页面截图并加盖原厂公章）；
	内容过滤	支持基于 http、ftp、telnet、smtp、pop3 等协议的内容过滤策略，可对微博、贴吧上传的内容及附件进行过滤，可对 FTP 上传/下载的文件名进行过滤，同时支持过滤 FTP 信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤；（提供产品相关功能页面截图并加盖原厂公章）；
	DLP	▲内置 DLP 数据防泄漏引擎，可针对发送者或接收者模式配置独立的 DLP 策略，对数据进行监控识别，达到敏感数据防护目的。 为提高产品的可用性，需支持识别的加密文件格式不少于 12 种；压缩文件格式不少于 25 种，如 RAR、ZIP、GZ、TAR 等；支持识别 Linux，Unix 等非 Winodws 的文件类型；支持识别异常文件格式类型；支持识别自定义文件类型；（提供产品相关功能页面截图并加盖原厂公章）；
	配置维护	支持多个配置文件并存，配置文件数量不少于 20 个（提供产品相关功能页面截图并加盖原厂公章）；
	升级维护	▲支持多个系统升级包并存，系统升级包文件数量不少于 5 个（提供产品相关功

		能页面截图并加盖原厂公章）；
	系统诊断	支持分别针对网络层、传输层和应用层提供诊断系统网络连通性的工具，包括 PING、 TRACEROUTE、 TCP、 HTTP 和 DNS（提供产品相关功能页面截图并加盖原厂公章）； 支持在 WEB 界面进入 CLI 模式，执行系统配置、网络诊断、过滤抓包等命令，提高管理员运维效率（提供产品相关功能页面截图并加盖原厂公章）；
	管理员	▲支持系统管理员能够通过本地认证及外部认证方式进行登录管理，外部认证失败时可转本地认证（提供产品相关功能页面截图并加盖原厂公章）；支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置（提供产品相关功能页面截图并加盖原厂公章）；
数据中心	报表	▲内置 15 类预定义报表模板，支持根据通信流量、上网行为、威胁统计等来源数据库自定义报表模板；支持一次性报表及周期性报表，可自定义统计时间；（提供产品相关功能页面截图并加盖原厂公章）；
		支持报表按照 PDF、WORD 及 EXCEL 格式导出；（提供产品相关功能页面截图并加盖原厂公章）；
	审计	支持独立配置审计策略，同时也可将指定的 IP 地址、 URL、 应用加入白名单，不进行数据审计；（提供产品相关功能页面截图并加盖原厂公章）；
		支持网站访问审计：审计指定类别的 URL 地址、审计命中指定关键字的网页标题和网页内容；（提供产品相关功能页面截图并加盖原厂公章）；
		支持邮件内容审计：对接收/发送邮件行为及邮件内容进行审计；FTP 审计：对 FTP 上传/下载行为及文件内容进行审计；（提供产品相关功能页面截图并加盖原厂公章）；
		▲支持网盘审计：对主流网盘应用如 360 云盘、百度网盘、腾讯微云、华为网盘、新浪网盘等上传内容进行审计；（提供产品相关功能页面截图并加盖原厂公章）；
		支持 telnet 审计：对 telnet 协议命令进行审计；（提供产品相关功能页面截图并加盖原厂公章）；
		提供完善的审计数据查询功能，方便管理员对用户的上网行为进行审查和分析。支持对用户上网行为进行完整的审计数据查询，包括访问网站、邮件收发、论坛微博、 FTP、 网盘、 TELNET 等；（提供产品相关功能页面截图并加盖原厂公章）；同时支持对用户上网流量时长进行完整的审计数据查询，包括服务端 IP、用户名、协议、上行流量、下行流量、总流量、时间等；（提供产品相关功能页面截图并加盖原厂公章）；
	日志	支持日志本地存储，可对不同类型日志设置存储空间；（提供产品相关功能页面截

		图并加盖原厂公章）；同时支持外发至 SYSLOG 服务器，可将多条日志合并成一条日志传送到日志服务器中，可选择对日志传输是否加密，设定 8 位或以上的加密密钥；（提供产品相关功能页面截图并加盖原厂公章）；
		日志查看可划分为管理日志、系统日志、策略日志、应用行为日志等四大模块，具体包含用户、连接、流量、NAT、审计、HA、APT、未知威胁等 20 个日志类别，可将日志按照 CSV 或 XML 格式导出；（提供产品相关功能页面截图并加盖原厂公章）；
显示监控	资源监控	▲在 WEB 界面提供资源监控开关，可对 cpu 占用率、内存占用率、磁盘占用率设置阈值；（提供产品相关功能页面截图并加盖原厂公章）；
	流量统计	支持根据应用对通过设备的数据报文流量进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速；（提供产品相关功能页面截图并加盖原厂公章）；
		支持根据用户/用户组对通过设备的数据报文流量进行统计，包括用户总流量排名和各个用户的用户名、认证类型、上行流量、下行流量、新建会话数、当前会话数以及流速；
		支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数；
		支持指定监控时间周期，包括：实时、最近 1 小时、最近 1 天、最近 1 周、最近 1 月等；
	威胁统计	支持根据按照病毒防御、入侵防御、APT 防御、ADS 攻击进行威胁统计，可按照威胁类型/攻击者/受害者三种方式进行威胁排名。（提供产品相关功能页面截图并加盖原厂公章）；
资质要求	▲产品资质（需提供证书复印件加盖厂家公章）	计算机信息系统安全专用产品销售许可证（第二代防火墙增强级）；
		涉密信息系统产品检测证书
		国家信息安全漏洞库兼容性资质证书
		ISCCC 产品认证证书（三级）
		网络关键设备和网络安全专用产品安全认证证书
		防火墙产品密码检测证书
		国家信息安全测评信息技术产品安全测评证书（EAL4+）
		IPV6 金牌认证；
	▲厂商资质（需提供证书复印件加盖厂	为保障项目的机密性，原厂商须具备涉密信息系统集成甲级资质；
		为保证项目设计及集成能力，设备原厂商须具有通信行业安全设计与集成二级资质证书；

	家公章）	为保障厂商的售后服务水平，原厂商需获得 ISO27001 信息安全管理体系认证、ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证；
		为保证项目的应急响应能力，原厂商须具备网络安全应急服务支撑单位（国家级）资质；
		为保证项目安全服务能力，设备原厂商须具备国家信息安全认证信息安全服务资质证书（安全工程类三级），信息安全等级保护安全建设服务机构能力评估合格证书；
		为保证本项目后续的厂商培训能力，设备原厂商须具备专业的信息安全技术培训能力，并取得权威的培训资质，应具有国家信息安全测评授权培训机构资质证书；
▲售后服务		产品须由原厂商提供 3 年应急响应服务、定期巡检服务，提供设备原厂商针对本项目的授权及售后服务承诺函，点对点技术响应函并加盖原厂公章；

2.2.5Web 应用安全防护系统

指标	指标项	规格要求
基本要求	专用的硬件和软件保障	采用专用硬件架构与专用安全操作系统，基于操作系统内核的完全检测技术；硬件设备可以机架安装，产品必须为专业性 WEB 应用防火墙硬件设备，而非下一代防火墙\UTM 类设备集成的 WEB 防护功能。
	硬件模块化设计	硬件采用模块化设计，可以通过扩展卡来增减业务接口，而非软件 WAF
	MTBF	不少于 450000 小时
	端口数量和扩展能力	1U 机箱，8 个千兆电口，接口支持 Bypass，2 个 SFP 插槽；整机吞吐量：6Gbps，并发连接：350 万，每秒新建连接数：12.5 万 ；3 年特征库升级服务，内含 SQL 注入、XSS、CSRF 等 WEB 攻击防护功能、URL 访问控制功能、防盗链功能、WEB 漏洞扫描功能、DDoS 攻击防护功能、服务器负载均衡功能、报表分析及告警功能；三年原厂质保服务；
网络部署	部署方式	无 IP 纯透明模式串联部署、旁路监测模式部署、负载均衡模式部署、反向代理模式部署
		支持基于域名和 IP 的网站防护
		串联部署时防护口不占用 IP 地址
		串联部署时服务器可以看到真实客户端源 IP，而不是 WAF 的业务 IP 地址
	网络适应性	支持 VLAN 划分，支持多 VLAN 环境下 trunk 的部署
		▲支持虚拟线无论任何网络环境可强制数据从一个接口转发到另一个接口（提供产品相关功能页面截图并加盖原厂公章）；
		物理接口支持子接口

		▲支持链路聚合(Channel)部署，提高链路带宽；支持 Trunk 链路防护（提供产品相关功能页面截图并加盖原厂公章）；
		支持自定义配置网络接口 MTU、半双工模式、全双工模式等属性
		支持静态路由及策略路由配置
		支持 ARP 绑定
		支持静态 MAC 地址表配置
		▲支持对防护的 WEB 服务器进行健康检查，可以实时监测服务器的活跃状态，并且可定期备份健康记录（提供产品相关功能页面截图并加盖原厂公章）；
		支持 IPV6 协议
		支持提取客户端真实 IP 头。自动尝试匹配 X-Forwarded-For, X-Real-IP, Cdn-Src-Ip 用以获取真实客户端 IP
		支持网络层防火墙功能，支持源 IP、源区域、目的 IP、目的区域等条件的访问控制
攻击防护	HTTPS 支持	支持 HTTP/HTTPS 站点防护
		▲代理模式下支持 HTTPS 流量解析，支持 SSL 卸载功能（提供产品相关功能页面截图并加盖原厂公章）；
	协议合规检查	支持请求限制配置通过定义最大请求头长度、最大 content-length、最大 body 长度、最大请求行长度、最大 header 行长度、最多 cookies 个数、最多 header 头个数、最大 header 长度等来对请用户数据做合规性检查
	WEB 安全防护	▲支持针对 OWASP TOP10 的攻击进行分类的 WEB 攻击规则库（提供产品相关功能页面截图并加盖原厂公章）；
		▲应能识别和阻断 SQL 注入攻击,Cookie 注入攻击，命令注入攻击（提供产品相关功能页面截图并加盖原厂公章）；
		▲应能识别和阻断跨站脚本(XSS)攻击(提供产品相关功能页面截图并加盖原厂公章)；
		支持 webshell 等后门上传防护、支持对中国菜刀等工具对后门连接的阻断
		▲支持扫描防护：支持扫描智能检测，进行人机识别防护（js 页面识别疑似扫描行为），支持扫描攻击检查和页面扫描检查多种扫描防护方式；支持扫描防护阈值设置和扫描 IP 的阻断周期设置。(提供产品相关功能页面截图并加盖原厂公章)；
		支持远程文件包含、本地文件包含、目录遍历、信息泄露等攻击防护
		支持 HTTP 参数污染攻击、00 截断、Struts2 命令执行等常见攻击防护
		▲支持多种爬虫攻击防护：支持自定义爬虫，支持导入或者下载后端服务器

		robots.txt,来限制爬虫访问。支持通过导入服务器的目录结构对静态网页进行爬虫防护配置。（提供产品相关功能页面截图并加盖原厂公章）；
		▲支持盗链防护，且支持攻击源盗链例外配置，及目的服务器 URI 例外配置（提供产品相关功能页面截图并加盖原厂公章）；
		支持 CSRF 跨站请求伪造攻击防护：应能识别和阻断跨站请求伪造(CSRF)攻击，支持 HTTP token 防护和 referer 匹配防护等多种防护方式
		支持 IP 黑白名单
		▲支持暴力登录防护（提供产品相关功能页面截图并加盖原厂公章）；
		▲支持对身份证、信用卡、手机电话号码、座机电话号码、邮箱地址等敏感信息做检查，当检查到此类数据后可通过配置特殊字符予以替换隐藏，防止信息泄露（提供产品相关功能页面截图并加盖原厂公章）；
		支持对 URL 编码、多次编码等方式绕过 WAF 的编码方式进行识别，防止绕过
		▲可对文件上传做控制，包括最多上传文件数、最大文件上传大小、可以通过对上传文件的扩展名、MIME 类型及允许请求体编码类型等做上传控制，可对文件做下载控制，包括最大下载文件大小、禁止下载文件的扩展名、MIME 类型等，支持上传文件的病毒检测功能；（提供产品相关功能页面截图并加盖原厂公章）
		支持 API 接口防护：包括 XML 基础校验，XML schema 校验，WSDL 校验
		▲检测到攻击后支持阻断、只检测等动作且动作为阻断时用户可自定义阻断页面（提供产品相关功能页面截图并加盖原厂公章）
		支持 URI 例外配置，包括对指定 URI 地址进行协议合规性检查，防御类型设置，参数设置，上传下载设置
		支持 URI 的访问控制功能，支持 HTTP 请求字段的访问控制，包括（地理位置，HTTP 协议版本，请求方法，cookie 等）
		▲支持自学习建模功能，可以通过学习正常 URL 参数的长度、参数类型、请求方法等数据特点创建白名单模型，如果参数违反白名单模型则认为是非法流量直接阻断，开启自学习建模功能后可生成自学习网站参数的自学习结果报告（提供产品相关功能页面截图并加盖原厂公章）
		▲支持虚拟补丁功能，支持导入 appscan、w3af 等第三方扫描器的扫描结果生成 WAF 的规则，对此类网站漏洞直接防护（提供产品相关功能页面截图并加盖原厂公章）
		可停用或启用任意一条规则，当触发规则后可以制定针对该条规则的动作，包括阻断记录日志、阻断不记录日志、继续、警告、临时或永久跳转到某一

		重定向页面等动作
		▲支持区域访问控制，能够按照指定某一区域进行访问控制，限制该地区的业务访问。（提供产品相关功能页面截图并加盖原厂公章）
		https 证书支持直接将证书内容填充到 waf 内使用，不用再上传或者转换证书使用
	配置易用性	可以针对服务器 IP 地址进行防护，而不需要配置需要防护的网站域名
		▲支持安装向导式部署，引导用户完成防护策略配置（提供产品相关功能页面截图并加盖原厂公章）
		▲支持域名自学习,可以自动学习网络中网站服务器的 IP 地址及此地址下的域名（提供产品相关功能页面截图并加盖原厂公章）
	DDoS 攻击防护	▲支持基线学习，可以自动学习用户 http 正常流量阈值模型，并给出推荐阈值配置项（提供产品相关功能页面截图并加盖原厂公章）
		对 ddos 流量支持检测清洗和强制防御两种模式,检测清洗根据是否到达阈值对流量进行清洗，强制清洗对所有流量直接进行流量清洗判断
		支持 HTTP/HTTPS 的 DDoS 攻击威胁检查，支持对慢速攻击，CC 攻击进行防护。
		▲支持对发起 DDoS 攻击的 IP 加入动态黑白名单（提供产品相关功能页面截图并加盖原厂公章）
	网页防篡改	▲网关型网页防篡改，无需在服务器中安装任何插件，可以对动态网站及静态网站文件内容进行防篡改，当检测到篡改后可以实时恢复篡改内容（提供产品相关功能页面截图并加盖原厂公章）
		▲支持对已篡改页面返回缓存页面或者返回固定页面（提供产品相关功能页面截图并加盖原厂公章）
	WEB 漏洞扫描	▲支持多种 WEB 应用漏洞的安全扫描检测，如 SQL 注入、跨站脚本、目录遍历等（提供产品相关功能页面截图并加盖原厂公章）
		支持自定义 WEB 漏洞扫描任务，支持对需要认证登录的 web 系统进行漏洞扫描，支持自定义每日、每周、每月等扫描周期设置
		可导出 web 漏洞扫描报告，报告支持 pdf,html,txt,xml 等格式导出
	负载均衡	▲支持多服务器的负载均衡，支持轮叫、加权轮叫、原地址散列、最小连接等多种负载均衡算法（提供产品相关功能页面截图并加盖原厂公章）
		能配合现有的负载均衡设备协同工作，支持任意部署，而不影响客户现有拓扑
	应用交付	支持 HTTP header 修改，URL 重写；WEB 缓存；HTTP 压缩等功能
数据分	网络数据分析	▲Web 界面可以直观查看接口、USB 口、管理口、HA 口及业务口的运行状态

析		（提供产品相关功能页面截图并加盖原厂公章）
		可以查看使用业务接口的上下行实时流量
		▲可以查看通过 WAF 的所有 IPV4 及 IPV6 客户端和服务器 IP 地址及端口连接数及状态（提供产品相关功能页面截图并加盖原厂公章）
		▲可以实时查看设备并发连接数、每秒事务数及 HTTP 应用层吞吐率等数据并以可视化的方式展示（提供产品相关功能页面截图并加盖原厂公章）
	设备运行数据分析	可以实时查看设备 CPU、内存、硬盘等自身使用率情况
	日志报表数据分析	▲日志支持以 syslog 和 welf 两种格式向远端日志服务器发送日志（提供产品相关功能页面截图并加盖原厂公章）
		▲日志传输可加密，且管理员可以配置加密密码（提供产品相关功能页面截图并加盖原厂公章）
		支持系统日志、管理员登录日志、调试日志、流量日志，攻击日志，篡改日志 DDoS 攻击日志等日志类型的记录。
		支持日志敏感信息脱敏，记录日志时将敏感数据替换为某个特定字符
		日志支持多条件与查询，支持 CSV 及 XML 格式的日志导出，日志支持清空配置
		支持每种攻击时间类型及次数的统计并以柱状图等形式直观展现
		支持最近一小时、一天、三十天等多种条件内攻击源 IP 攻击次数及攻击分布 TOPN 的统计
系统管理	系统管理	支持 SSL 的 WEB 界面、SSH、Console 多种方式管理
		支持手工设置时间、本地同步时间、和 NTP 服务器同步时间
		▲支持通过 WEB 界面直接跳转到控制台 console 界面（提供产品相关功能页面截图并加盖原厂公章）
		支持 ping、TRACEROUTE、TCP、HTTP、DNS、抓包工具等多种故障诊断方式
		支持 SNMP 的 V1、V2、V3 管理，支持 SNMP 陷阱主机功能
		支持 WAF 本机 DNS 域名解析
		支持 WAF 配置文件导入、导出及恢复出厂配置
		支持操作系统 WEB 方式升级及命令行等方式的离线升级
		支持规则库的在线升级和离线升级
		支持攻击日志邮件告警，可以定时将特定攻击类型的攻击日志间隔定一定时间后定时发送至指定邮箱
		▲支持攻击报表邮件告警，可以定时将攻击报表间隔定一定时间后定时发送

		至指定邮箱（提供产品相关功能页面截图并加盖原厂公章）
	账号及认证管理	支持帐号创建、帐号授权、帐号属性修改、帐号删除等账号管理功能
		支持用户身份认证，用户切换角色时，必须进行重新认证
		▲支持超时重新认证机制并能够定义用户认证尝试的最大允许失败次数（提供产品相关功能页面截图并加盖原厂公章）
		▲支持账号策略自定义，支持定义允许最大登录失败次数、密码错误账号锁定时间、最大在线管理员数、对其他非法在线管理员强制下线、防管理员账号暴力破解（提供产品相关功能页面截图并加盖原厂公章）
高可用性	双机热备	▲支持双机热备，主备模式、主主负载均衡模式、连接保护模式(主主模式下一边断了，会话表会同步到另一边数据不丢包） （提供产品相关功能页面截图并加盖原厂公章）
		支持两台 WAF 配置同步
		支持同一台 WAF 上下接口状态联动(一个接口 down 另外一个接口也同步 down)
		两台 WAF 路由模式接入、两台 WAF 纯透明交换模式接入
	硬件 Bypass	支持开机及断电 bypass 模式，光口支持外置 bypass 模块
联动	防火墙联动	▲支持与防火墙进行联动（提供产品相关功能页面截图并加盖原厂公章）
资质要求	▲产品资质（需提供证书复印件加盖厂家公章）	中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》
		中国信息安全认证中心颁发的《IT 产品信息安全认证证书》
		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》(专业 WAF 类)
		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》
		OWASP 颁发的《web 应用防火墙认证证书》
		IPV6 金牌证书(专业 WAF 类)
	▲厂商资质（需提供证书复印件加盖厂家公章）	为保障项目的机密性，原厂商须具备涉密信息系统集成甲级资质；
		为保证项目设计及集成能力，设备原厂商须具有通信行业安全设计与集成二级资质证书；
		为保障厂商的售后服务水平，原厂商需获得 ISO27001 信息安全管理体系认证、ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证；
		为保证项目的应急响应能力，原厂商须具备网络安全应急服务支撑单位（国家级）资质；
		为保证项目安全服务能力，设备原厂商须具备国家信息安全认证信息安全服务资质证书（安全工程类三级），信息安全等级保护安全建设服务机构能力评

		估合格证书；
		为保证本项目后续的厂商培训能力，设备原厂商须具备专业的信息安全技术培训能力，并取得权威的培训资质，应具有国家信息安全测评授权培训机构资质证书；
售后服务	▲产品须由原厂商提供 3 年应急响应服务、定期巡检服务，提供设备原厂商针对本项目的授权及售后服务承诺函，点对点技术响应函并加盖原厂公章；	

2.2.6 上网行为管理

指标项	指标	具体功能要求
产品要求	软硬件要求	1U 机箱，4 个千兆电口，支持 Bypass；1 个接口扩展插槽，日志存储空间 500GB；建议适配带宽：300M，建议用户数 800；含 3 年系统版本升级、网站知识库及应用知识库升级许可；三年原厂质保服务；
网络适应性	部署模式	支持路由模式，旁路模式、网桥模式、混合模式部署；
	系统存储空间	▲系统 CF 卡≥4G，设备本身的操作系统单独存放在 CF 中，要与日志存储分开。（需要厂家提供证明并加盖原厂公章）
	即插即用	▲支持即插即用功能。不管电脑的 IP 如何配置，开启即插即用功能后，只要插上网线，即可上网。（提供产品相关功能页面截图并加盖原厂公章）
	网络功能	支持基于应用层服务的策略路由；（提供产品相关功能页面截图并加盖原厂公章） ▲支持 ISP 自动地址表（电信、移动、网通、铁通等）的策略路由的选路方式； （提供产品相关功能页面截图并加盖原厂公章） 支持 PPPoE 拨号以及负载均衡； ▲支持支持基于轮询的多链路负载均衡算法；（提供产品相关功能页面截图并加盖原厂公章） 支持基于链路的上行、下行、总流量自动均衡的多链路负载均衡算法，基于固定指派链路的自动均衡算法，基于最佳路径的多链路负载均衡算法； 支持 DHCP Replay/Server； ▲支持智能 DNS,对内部服务器负载均衡，按应用服务的负载均衡多链路冗余切换；（提供产品相关功能页面截图并加盖原厂公章） 支持静态路由、gre、vlan 透传、单臂路由。
	双机模式	支持两台及设备同时做主机的部署模式；

		桥模式下必须支持接口联动，配置同步；
	代理功能	▲要求支持 http 代理、https 透明代理、二级代理、DNS 代理、dns 缓存（提供产品相关功能页面截图并加盖原厂公章）
	链路聚合	▲支持将多个以太网物理端口捆绑成一条逻辑端口（即将多个端口捆绑成一个逻辑的端口以增加带宽，同时增加链路备份）支持基于 mac、轮循、主备、哈希、广播、802.3ad、发送自适应、双向自适应等等多种负载方式。（提供产品相关功能页面截图并加盖原厂公章）
	vpn	▲支持 l2tp、gre vpn、pptp、ipsec。（提供产品相关功能页面截图并加盖原厂公章）
	支持链路健康检查	支持 DNS 链路健康检查算法；支持 ICMP 链路健康检查算法； ▲支持 TCP 链路健康检查算法；支持自定义的链路健康检查算法；（提供产品相关功能页面截图并加盖原厂公章）
设备管理	设备登录	必须支持 ssl 加密方式登录设备，支持 ssh 管理。
	操作界面	系统能够支持简体中文、繁体中文/英文操作界面
	网关策略	支持基于 ip 的网管策略，防止恶意 ip 探测攻击设备，增加网关的安全性。
	管理认证	▲支持管理员通过 Radius 认证后才能登录设备。（提供产品相关功能页面截图并加盖原厂公章）
	排障工具	提供图形化排障及抓包工具，便于管理员排查策略错误等故障；
	分级管理	不同用户组的管理权限支持分配给不同管理员
	Dkey 登录	支持管理员基于硬件 key 登录方式
	集中管理	行为管理支持分布式部署，通过部署集中管理平台，加入集中管理设备之后，可以实现策略下发、设备状态监控、设备日志、用户日志上传。
	APP 集中监控功能	▲支持行为管理设备接入集中管控平台，并通过 APP 管理集中管理平台并查各个局点的 ACM 的状态和告警信息。（提供产品相关功能页面截图并加盖原厂公章）
	特征库自动升级	必须支持 URL 分类库、应用识别库基于域名方式自动在线升级。
实时监控	设备资源	能够提供一小时内 cpu 使用率、内存使用率、活跃会话数、在线认证用户数以及最新的磁盘占用情况。
	物理接口	▲能够实时展现每个接口接收发送流量、字节数、包个数以及错误、丢弃、帧冲突个数。（提供产品相关功能页面截图并加盖原厂公章）
	服务监控	能够提供服务趋势图、服务组趋势图、活跃服务以及所有服务趋势。

		并且支持快速定位使用对应服务的用户。
	用户监控	能够提供流量适用排名，提供前 50 名用户流量适用情况，并支持趋势图、黑名单、显示活跃服务等操作。通过黑名单可以直接强制某个流量异常用户下线或者快速修改带宽。
	在线用户	能够直接显示已认证且在组织结构中、已认证但不在组织结构中、以及未通过的认证的用户状态。支持以用户名、所属组、ip、mac、用户类型、绑定检查、时间等参数查询用户。
安全防护	安全策略	▲支持基于策略方向、源地址、目的地址、服务、生效时间的安全策略。（必须提供产品界面截图）
	Nat 规则	支持内网代理、一对一地址转换、端口映射、服务器池。
	移动终端管理	支持移动终端发现后拒绝移动终端接入并支持启用事件告警。支持移动终端列表添加信任列表。
	防 ARP 欺骗	支持 ARP 欺骗防护，支持 arp 保护对象以及 arp 广播间隔设置。
	加速老化	支持对 TCP、UDP、ICMP、TCP SYN 超时时间，无回应 UDP 超时时间设置，并能支持按照新建会话与总会话比例设置老化开始或者结束。
IPV6	Ipv6 网络配置	支持接口配置 ipv6 地址、支持 ipv6 地址簿、支持 ipv6 策略路由、NAT64、NAT66、DNS64 等相关配置
	Ipv6 审计	支持 ipv6 流量审计
	Ipv6 控制	支持 ipv6 环境下认证、流量控制、行为控制和防火墙策略
无线环境管理	Ap 上线地址分配	支持 dhcp option43/ option138 可以给 ap 分配地址保证 ap 上线
	AP MAC 地址获取	支持 AP MAC 地址获取，支持读取用户真实 MAC
	无线用户	支持无线用户认证、行为控制、流量控制、用户日志收集
用户管理	组织结构	支持按照公司架构创建用户组、用户、支持多层组和用户，分组能继承父组策略，用户能继承组的策略。 认证用户需支持中文用户名
	自动创建用户和绑定	对于未创建的用户，可根据其 IP 地址、MAC 地址、主机名或者 VLAN ID 等作为新用户名自动创建帐户，并可同时绑定 IP、绑定 MAC、绑定 IP+MAC、绑定 VLAN，并自动分配到指定用户组，享有指定网络权限。对于创建好的用户也支持绑定 IP、绑定 MAC、绑定 IP+MAC、VLAN 绑定。
	用户有效期设置	支持临时账户、绑定账户、认证账户等多种用户身份的有效期设置，支持过期冻结、支持无流量自动下线。
	NetbIOS 协议扫描	▲可通过 NetbIOS 协议扫描内网的主机信息，扫描结果将列出每个主

		机的 IP 地址、MAC 地址和主机名等，然后可以将其加入某个用户组中，逐步完善组织结构的管理。
	跨三层 mac 识别	支持通过 snmp 服务读取下层三层设备的 arp 表象获取客户真实的 mac 地址。
	临时账号设置	▲支持临时账号自动申请功能，方便外来的临时用户使用。支持自动审核和管理员手动审核的核定方法将临时帐户加入到组织结构中。支持网页发送和邮件方式通知临时用户账号和密码（提供产品相关功能页面截图并加盖原厂公章）
	导入用户	支持表格手工导入用户、LDAP、ad 个等自动导入用户 支持以 CSV 格式文件导入帐户/分组/IP/MAC/描述/密码等信息；
	本地认证	支持本地设置用户名、密码的 portal 认证；
	第三方服务器认证	支持 Ad 域、LDAP、Radius、POP3、Proxy 等第三方认证服务器；
	单点登录	支持 AD、POP3、Proxy、PPPOE、 H3C IMC/CAMS、锐捷 SAM、城市热点、web 认证等系统进行认证单点登录，简化用户操作；
	短信认证	支持短信认证方式，用户输入手机号作为用户名，通过短信猫或短信平台发送验证码；该认证页面可自定义。并且支持基于 cookie 和 mac 的免认证方式。
	微信认证	支持与微信公众号结合的认证方式，用户关注微信公众号后即通过身份认证。支持点一点、连一连等多种方式。
	二维码认证	临时账号支持二维码扫描接入认证。
	指纹认证	支持通过指纹识别用户身份，并对用户做控制。
	刷卡认证	▲支持通过磁卡识别用户身份，并对用户做控制。
行为管控	静态 URL 库	包含 50 种个以上分类，至少 2000 万条预分类的 URL 地址库；
	URL 库自定义	支持 URL 库接口开放，可以通过自定义方式用户自主创建 url 类和具体 url
	应用特征库	支持 2300 种以上的应用，至少支持 1000 种以上的移动应用
	应用特征自定义	▲支持自定义 ip 和端口的普通服务，支持自定义 ip、协议类型、字符串、端口等组合的服务特征，支持自定义论坛/网评特征（提供产品相关功能页面截图并加盖原厂公章）
	协议剥离	默认支持 L2TP 协议剥离、GRE 协议剥离、LWAPP 协议剥离、CAPWAP 协议剥离，并支持自定义协议剥离。
	加密网站识别和控制	▲支持 https 网站识别，支持加密网站搜索，支持 ssl 论坛加密发帖内容识别，支持基于关键字的控制。(提供产品相关功能页面截图并加

		盖原厂公章） ▲支持基于授权签名的方式实现 https 审计免除告警的行为。（提供产品相关功能页面截图并加盖原厂公章）
	邮件过滤	支持基于支持邮件的“发件人/主题关键字/内容关键字/附件类型”过滤（POP3/SMTP/Web Mail），支持 ssl 加密邮件内容和标题的识别和过滤。
	告警	设备内存、cpu、会话、接口速率支持告警设置； 支持时间告警，支持黑名单告警； ▲支持违规网站、违规搜索、违规帖子、违规上传、违规邮件、还有潜在威胁的告警行为；（提供产品相关功能页面截图并加盖原厂公章） 告警策略要支持 syslog、短信、邮件、日志记录，以及任意的方式组合。（提供产品相关功能页面截图并加盖原厂公章）
	白名单	支持 url 白名单，添加到白名单的 url 不受策略控制和审计。 支持 ip 白名单，添加到白名单的 ip 不受策略控制和审计。
	定义 URL	网关支持管理者自定义新的 URL 地址和 URL 分类；
	关键字过滤	关键字组支持通配符配置，支持论坛、微博发帖关键字过滤，支持搜索引擎关键字过滤，支持邮件内容、正文标题、附件内容的关键字过滤，支持包含制定关键字的页面过滤。
	发帖管理	支持天涯、猫扑、麻辣社区、百度贴吧等常见论坛发帖控制，支持腾讯微博、搜狐社区、凯迪社区等常见微博的发帖控制。
	终端提醒策略	支持基于用户设置终端提醒策略，能够实现公告页面按照策略推送。
	网页附件管理	支持百度文库、百度云盘、华为网盘等常见网盘的文件过滤
流量管理	线路带宽	支持设备在各个工作模式的线路带宽设置
	基于用户的流控	支持基于源 ip、地址薄、用户及用户组的流控策略。支持基于每个人的限速以及整体限速。
	基于连接数限制	支持每个用户的源，目的活跃连接数控制，避免网络滥用
	服务限速	流控行为可以基于应用特征库选择，也可以基于 url、文件类型控制。
	带宽保障	支持基于用户、协议、应用、url、文件类型的带宽保障行为，可以通过队列实现重要业务优先转发。
	黑名单	根据每用户的“每日/每周/每月”使用的流量(上行/下行/双向)总和超过预设阀值，则自动进入黑名单。根据每用户在连续一段时间的“上行速率/下行速率”超过预设阀值，则自动进入黑名单。根据每用户在连续一段时间的并发会话数(上行/下行)超过预设阀

		值，则自动进入黑名单。对进入黑名单的用户可采取强制下线或修改“上行带宽/下行带宽/上行会话数/下行会话数”的方式对用户进行惩罚。惩罚时间到期，可正常上网。对连续进入黑名单多次（如5次，可配置）的用户，可对用户进行加倍惩罚，惩罚时间可以原来的N倍。(提供产品相关功能页面截图并加盖原厂公章)
	生效时间	支持基于时间计划的流控策略。
	防共享	支持防止1拖n共享行为。
	移动终端管理	支持无线环境下，移动终端接入识别，对未添加信任的黑名单支持拒绝加入网络。
上网日志分析	独立报表中心	▲为了日志安全性，设备必须支持独立硬盘存放审计日志，不能与审计系统共用硬盘。（提供产品相关功能页面截图并加盖原厂公章）
	内置报表中心	设备必须支持内置报表中心，默认自带数据库无需再安装数据库。
	日志分级	▲通过配置管理员分组，实现指定分组的管理员只能访问指定用户组上网行为日志。（提供产品相关功能页面截图并加盖原厂公章）
	DKEY管理	日志中心必须支持usb-key接入认证，当日志查看员同时拥有key和用户名密码时才能查看审计日志从而实现日志安全。
	日志备份	支持通过集中管理平台或者ftp方式备份日志。
	虚拟身份	支持记录qq、微信等常见即时通讯账号登录信息，支持天涯、猫扑等常用论坛登录信息，支持记录新浪新闻、搜狐新闻等常见新闻类登录信息。支持短信认证、pppoe等常见认证身份信息记录。
	邮件审计	支持收件人、发件人账号审计（POP3/SMTP/Web Mail）。 支持邮件内容审计（POP3/SMTP/Web Mail）。 支持邮件附件审计（POP3/SMTP/Web Mail）。 支持机密邮箱内容审计。
	即时通讯	支持Windows pc版qq聊天内容审计、支持Windows pc 微信聊天内容审计、支持飞信、msn等IM登录、聊天、文件传输审计。 支持Facebook、line等国外常见加密即时通讯审计
	url审计	能基于组织结构记录用户访问的具体url、标题、网站类型、访问时间、动作等信息，通过详细信息可以查看用户访问的源和目的地址，以及访问的端口。
	网页搜索	能基于组织结构记录用户搜索的关键字、搜索的类型时间、动作等信息，通过详细信息可以查看用户访问的源和目的地址，以及访问的端口

	论坛微博	能记录用户发帖行为，可以记录用户访问的具体 url、访问时间、发帖内容、用户明、对应分组、以及是否被阻断
	Telnet	支持记录用户 telnet 访问行为，记录访问的人员、命令信息。
	http 上传下载	支持 http 上传和下载记录，包括上传人员地址、mac、用户名信息，上传文件还原，下载文件名称记录
	FTP	支持 FTP 的上传和下载记录，包括用户名和文件名，以及上传文件还原，下载的文件名称记录
	阻断记录	▲支持防火墙模块阻断、流量模块阻断、行为管控模块阻断记录（提供产品相关功能页面截图并加盖原厂公章）
	告警日志	支持非法网站、违规帖子、ftp 上传、网页上传、违规邮件、违规 im、以及匹配潜在威胁的记录。(提供产品相关功能页面截图并加盖原厂公章)
	会话日志	支持所有访问的会话日志记录，包括：源 IP、目的 IP、协议类型、七层应用名称、源端口、目的端口、是否进行 NAT 转换(可显示转换后的 IP 和端口)、会话产生的时间和会话持续时间。
	个人统计分析	▲基于个人的所有行为监控报表，包括：网页标题记录、发贴记录、网页评论记录、在搜索引擎上的搜索记录、网页文件上传记录、URL 访问记录、即时通讯的登录信息/聊天内容/文件传输记录、邮件记录（详细内容、附件）、FTP 登录信息/上传记录/下载记录；（提供产品相关功能页面截图并加盖原厂公章）
	递进式查询	能够进行层层深入的递进式查询，获取某应用对应的用户，或某用户使用网络应用的情况，便于对网络使用现状进行深入分析。
	高级检索	支持基于时间、动作、应用类型、具体应用、关键字、目标 ip 等条件的高级检索行为
	报表管理	支持基于统计分类、统计分类、用户及其用户组的自定义报表，通过邮件方式给部分人员发送日报、周报、月报、年报。
	统计分析	支持 cpu、内存、活跃会话、在线用户的统计以及趋势图
	用户统计	支持基于流量、会话、用户及其用户组统计
	服务统计	支持基于服务、服务类型的统计
	url 统计	支持基于 url、url 类型的统计，支持 url 访问量统计，网页文件访问统计
	线路统计	支持都出口情况下，线路统计
	上网时长统计	支持基于用户的上网时长统计。

用户行为分析	上网态势分析	从内网整体网络的宏观角度展现网络使用概况、上网目的地分布、热门应用流量分布、网站类型分析、终端类型分析、在线人群趋势、高风险任人群排名、违规行为统计等多维度全方位展现网络的使用综合态势，给网络管理提供依据
	网络质量分析	通过对网络线路实时流量趋势、以及应用流量、用户流量进行展示，统计分析出每条专线的负载情况，从而实时地掌握校园网络线路的使用情况。
	校园贷分析	针对学生平时上网行为按 URL 地址和 App 应用特征进行分类识别，从学生上网访问网页内容和搜索热词的关键字进行识别，通过对学生涉及网贷行为以及相关网银操作频次等相关性分析，划分出涉及网贷高危群体和潜在风险群体。
	沉迷网络分析	针对学生在使用网络过程中的具体行为和内容进行分类统计，计算出玩游戏、看视频、网聊购物等低效上网行为，根据学生每日上网行为时长和内容有效识别出沉迷网络的学生群体，开展针对性的辅导和教育
	热点事件分析	针对学生平时上网过程中的浏览内容、网页标题、搜索关键词热词等内容进行匹配识别，了解学生对热点事件的关注和舆论倾向。结合学生关注热点，有针对性的进行舆情分析和舆论导向的正向引导
	工作效率分析	针对员工在工作时段的浏览内容、访问应用的特征进行时长统计，根据预定义的规则判定员工的低效工作状态和时长。针对工作效率低下的员工，可以详细查看具体上网的网站和应用，以及时长，判定消极怠工有据可查
	离职倾向分析	针对员工平时上网过程中的浏览内容、网页标题、搜索关键词热词等内容进行匹配识别，了解员工对与招聘、猎头等信息的关注度。结合有离职倾向员工的分析结果，有针对性的进行主管访谈，或者提前进行涉密行为监控，减少因人员流动给企业正常业务带来的影响。
日志外发	Syslog	▲系统能够支持 Syslog 等第三方日志服务器系统。（需要提供截图）
	网安平台对接	支持与任子行、派博、烽火、爱思、新网程、网星传媒、恒邦、白虹网监，中科新业、城安、上海创多、网星传媒、锐捷 ELOG、兆物、亚美、网博、宽广智通、携网科技接口、华博接口、武汉洪旭接口、智开科技等 20 种以上的网安平台对接。
	集中管理	支持将用户行为日志上传到集中管理平台
资质要求	▲产品资质	全球 IPv6 测试中心《“IPv6 Ready Phase-2”认证》

	（需提供证书复印件加盖厂家公章）	公安部公共信息网络安全监察局《计算机信息系统安全专用产品销售许可证》
		公安部信息安全产品检测中心《互联网公共上网服务场所信息安全管理系统检测报告》
		中华人民共和国国家版权局《计算机软件著作权》
		公安部网络安全保卫局颁发的网络通讯安全审计销售许可证
		中国信息安全认证中心颁发《 IT 产品信息安全认证证书》
		中华人民共和国工业和信息化部《电信设备进网许可证》
	▲厂商资质（需提供证书复印件加盖厂家公章）	为保障项目的机密性，原厂商须具备涉密信息系统集成甲级资质；
		为保证项目设计及集成能力，设备原厂商须具有通信行业安全设计与集成二级资质证书；
		为保障厂商的售后服务水平，原厂商需获得 ISO27001 信息安全管理体系认证、ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证；
		为保证项目的应急响应能力，原厂商须具备网络安全应急服务支撑单位（国家级）资质；
		为保证项目安全服务能力，设备原厂商须具备国家信息安全认证信息安全服务资质证书（安全工程类三级），信息安全等级保护安全建设服务机构能力评估合格证书；
		为保证本项目后续的厂商培训能力，设备原厂商须具备专业的信息安全技术培训能力，并取得权威的培训资质，应具有国家信息安全测评授权培训机构资质证书；
售后服务	产品须由原厂商提供 3 年应急响应服务、定期巡检服务，提供设备原厂商针对本项目的授权及售后服务承诺函，点对点技术响应函并加盖原厂公章；	

2.2.7 入侵检测系统

类别	项目	招标要求
产品要求	硬件要求	要求采用 X86 多核硬件平台； ▲内置 SSD 固态硬盘存储日志（提供产品界面截图并加盖原厂公章） ▲具备硬件温度监控能力；（提供相关功能的产品界面截图并加盖原厂公章）； 1U 机箱，6 个千兆电口，4 个 SFP 插槽，标配冗余双电源；含 3 年攻击知识库升级许可，3 年网站知识库升级许可。三年原厂质保服务；
	软件要求	设备采用自主知识产权的专用安全操作系统，采用多核平台并行处理特性安全操作系统（提供相应资质证明并加盖原厂公章）；

		▲支持多操作系统引导，出于安全性考虑，多系统需在设备启动过程中进行选择，不得在 WEB 维护界面中设置系统切换选项（提供相关功能的产品界面截图并加盖原厂公章）； 系统具有良好的可扩展性，能够扩展支持病毒防御、网站防护（WEB 漏洞扫描及网页防篡改）、无线入侵防御功能；
	性能要求	整机吞吐量：5Gbps，IDS 吞吐 2Gbps；最大并发连接数：220 万；每秒新建连接数：8.5 万；
设备部署	接入模式	要求支持直连、路由、VLAN、旁路监听、混合部署等多种接入模式。
		要求支持多端口链路聚合，支持不少于 10 种链路负载均衡算法（提供相关功能的产品界面截图并加盖原厂公章）；
		要求支持基于源/目的地址、接口的策略路由。
	部署环境	要求支持 VLAN、MPLS、PPPoE 网络，能够在该网络环境中检测出攻击事件。
		要求支持 IPv6、IPv6 over IPv4、IPv6 和 IPv4 混合网络，能够在该网络环境中检测出攻击事件。
规则库	攻击规则库	要求攻击规则库单独分开，可支持手动、自动、以及离线升级。
	应用识别规则	▲要求应用识别规则库单独分开，可支持手动、自动、以及离线升级（提供相关功能的产品界面截图并加盖原厂公章）；
	URL 过滤库	要求 URL 过滤库单独分开，可支持手动、自动、以及离线升级。
	病毒库	支持病毒库，单独分开，可支持手动、自动、以及离线升级。
入侵防御能力	入侵检测引擎	系统应具备：融合模式匹配、协议分析、异常检测、会话关联分析，逃逸等多种技术，准确识别入侵攻击行为，为用户提供 2~7 层深度入侵检测。
		要求支持丢弃报文、记录日志、禁止连接、TCP reset 结束 TCP 会话等多种响应动作
		要求支持自定义攻击检测规则。
		要求支持黑名单，将攻击源加入黑名单，一段时间内禁止访问
		要求支持攻击报文取证功能，检测到攻击事件后将原始报文完整记录下来，作为电子证据（提供相关功能的产品界面截图并加盖原厂公章）；
	攻击特征库	应涵盖广泛的攻击特征库、能够针对 3500 种以上攻击的攻击行为、异常事件，以及网络资源滥用流量，进行检测（提供相关功能的产品界面截图并加盖原厂公章）；
	攻击检测类型	要求能够检测包括溢出攻击类、RPC 攻击类、WEBCGI 攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP 攻击类、系统漏洞类等在内的超过 3500 种攻击事件

病毒检测能力	病毒检测引擎	系统应具备独立的病毒检测引擎。
		同时支持文件型和网络型病毒检测。
	病毒特征库	支持 380 万以上病毒检测规则（提供相关功能的产品界面截图并加盖原厂公章）;
	病毒检测类型	要求能够检测主流 FTP、HTTP、SMTP、POP3 协议的病毒。
	病毒统计	系统支持对病毒攻击事件、受攻击主机等做统计排名
URL 监测	URL 监测引擎	系统应具备独立的 URL 监测引擎。
		支持黑白名单，精确匹配和模糊匹配
		支持阻断、URL 重定向、返回默认页面、返回自定义页面等多种动作。
		支持恶意网站、违反国家政策法规、潜在不安全、浪费带宽、大众兴趣、多种论坛、行业、计算机技术、等多种分类的 URL 检测。
	URL 特征库	支持 URL 地址分类库，超过 650 万种（提供相关功能的产品界面截图并加盖原厂公章）;
	URL 统计	系统支持对 URL 访问次数及访问主机等做统计排名
DDOS 防御功能	DDOS 防御	系统应支持独立的 DDOS 检测及检测基线自学习的能力。
		系统支持检测包括 land、Smurf、Pingofdeath、winnuke、tcp_sscan、ip_option、teardrop、targa3、ipspoof、Synflood、Icmpflood、Udpflood、Portscan、ipsweep 等在内的 DOS/DDOS 攻击。
		系统支持 DNS 异常包及 DNS Flood 攻击检测;
		系统支持 DHCP 异常包及 DHCP Flood 攻击检测;
		系统支持 ARP 异常包及 ARP Flood 攻击检测（提供相关功能的产品界面截图并加盖原厂公章）;
		系统支持 CC 攻击防御，且能够对 Web 服务器上的指定 URI 页面进行防护设置（提供相关功能的产品界面截图并加盖原厂公章）;
		系统支持主机并发连接数和半连接数的限制（提供相关功能的产品界面截图并加盖原厂公章）;
		系统支持 DDOS 机器人自学习功能，学习时间可设置（提供相关功能的产品界面截图并加盖原厂公章）;
应用识别功能	应用识别	系统能够根据数据内容而非端口智能识别包括 P2P、即时通讯、电子商务、股票交易、网络游戏、网络电视、移动应用等在内的 23 大类超过 1200 种应用（提供相关功能的产品界面截图并加盖原厂公章）;
	应用管理	系统应支持灵活的应用管理策略配置功能，实现基于主机地址、区域、时间、应用等多维度的全面、细致监控。

		支持对应用协议的阻断和流量管控以及记录应用日志。
	自定义应用	支持应用协议自定义功能。
无线攻击防御功能	无线管理	要求支持无线自动扫描分组
	无线攻击防御	要求支持检测并阻断 Ad-hoc（简单互联）、非法外连、非法内联
		要求支持能检测并阻断钓鱼攻击、无线代理攻击。
		要求支持无线安全区，对区域内的 WIFI 接入进行屏蔽、检测无线 AP 风险配置
	无线定位	要求支持无线定位功能，定位非法、攻击 AP。
增值功能	网站防护功能	支持 WEB 站点漏洞扫描功能，内置爬虫、支持关键字自学习和 HTML 分析（提供相关功能的产品界面截图并加盖原厂公章）；
		▲支持网页防篡改功能（不需要在 WEB 服务器上装载任何软件）（提供相关功能的产品界面截图并加盖原厂公章）；
	防火墙功能	系统应支持设置访问控制规则，实现对三到七层的访问控制（提供相关功能的产品界面截图并加盖原厂公章）；
		系统应支持源、目的地址转换以及双向地址转换（提供相关功能的产品界面截图并加盖原厂公章）；
		系统应支持 IP/MAC 地址绑定，支持设置协议与非常用端口的绑定策略（提供相关功能的产品界面截图并加盖原厂公章）；
	网络冗余	支持双机热备。
日志和报表系统	日志管理	系统应支持多种形式的日志存储,本地存储、发送至日志服务器、本地日志服务器双存储、自动方式判断日志服务器状态自动决定日志的记录方式（提供相关功能的产品界面截图并加盖原厂公章）；
		系统应提供基于告警级别、时间、IP 地址、事件类型、等条件的日志检索功能，具备日志导出备份、清除功能。
		系统应具备日志归并功能，避免日志风暴。
	报表系统	系统应支持按照时间、源 IP、源端口、目的 IP、目的端口、网络接口、风险级别等条件生成统计分析报表，报表内容包括攻击检测、病毒检测、应用识别、URL 检测四大类。
		系统应支持支持生成日报、周报、月报。
		系统应支持报表以 word、html 格式导出。
		系统应提供报表定时通过邮件方式自动发送。
	告警系统	系统应提供全方位的包含管理、系统、策略、安全、流量等告警。
		系统应提供邮件、声音、snmp 多形式的告警方式。
管理监控	管理	系统支持 web、命令行等多形式灵活安全策略配置。

		支持 B/S 或 C/S 管理模式，可实现多级部署。
		支持 SNMP 的 v1 、v2 、v2c 、v3 版本。
		支持规则库手动、自动更新
	监控	应支持系统资源监视。
		应支持 web 页面的实时显示攻击事件。
		▲应支持设备温度监视以及报警，可以自定义温度阀值（提供相关功能的产品界面截图并加盖原厂公章）;
		应支持实时查看网络流量/攻击状况。
		应支持基于主机、区域的攻击与被攻击的统计显示。
		应支持基于协议的应用识别统计监控。
		应支持基于 web 类型分类的统计监控。
资质及服务能力要求	▲产品资质（需提供证书复印件加盖厂家公章）	《计算机信息系统安全专用产品销售许可证》
		《计算机软件著作权登记》
		《国家信息安全测评信息技术产品安全测评证书》EAL3 级
		IPv6 支持等资质证书
		军用产品认证证书
		国家保密局检测报告
		公安部检测报告
		自主创新产品证书
		CVE CompatibilityCertificate
		ISCCC 产品认证证书
	▲厂商资质（需提供证书复印件加盖厂家公章）	为保障项目的机密性，原厂商须具备涉密信息系统集成甲级资质;
		为保证项目设计及集成能力，设备原厂商须具有通信行业安全设计与集成二级资质证书;
		为保障厂商的售后服务水平，原厂商需获得 ISO27001 信息安全管理体系认证、ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证;
		为保证项目的应急响应能力，原厂商须具备网络安全应急服务支撑单位（国家级）资质;
		为保证项目安全服务能力，设备原厂商须具备国家信息安全认证信息安全服务资质证书（安全工程类二级）
		为保证本项目后续的厂商培训能力，设备原厂商须具备专业的信息安全技术培训能力，并取得权威的培训资质，应具有国家信息安全测评授权培训机构资质

		证书；
	技术能力	投标厂商具备专业的攻防研究团队，能够对安全漏洞进行持续的挖掘与跟踪。2015 年向 CNVD(国家信息安全漏洞共享平台)贡献的漏洞数量排名不低于前三名。（提供 CNVD 官网截图证明并加盖原厂公章）
	▲售后服务	产品须由原厂商提供 3 年应急响应服务、定期巡检服务，具体参考服务要求，提供设备原厂商针对本项目的授权及售后服务承诺函，点对点技术响应函并加盖原厂公章；

2.2.8 数据库审计

指标项	功能描述
硬件要求	1U 机箱，6 个千兆电口，4 个 SFP 插槽，1T 存储空间，标配冗余电源；默认含 1 年的网站知识库、攻击知识库和应用识别库。三年原厂质保服务；无数据库实例限制
性能要求	抓包速度≥1000M/秒，审计系统审计事件每秒入库速度≥10000 条/秒；日审计量≥4 亿条。
审计 DB 授权	▲无数量限制
数据库审计	设备可独立完成审计数据采集，不依赖于数据库自身的日志系统，审计结果存储于独立存储空间；
	支持审计 ORACLE、SQL Server、MY SQL、DB2、Sybase、Informix、Postgresql、Kingbase、Cache、Gbase、Dameng、Teradata、Oscar、Mongodb 等各类主流数据库系统（提供相关功能的产品界面截图并加盖原厂公章）；
	系统内置 SQL 语法解析器，可通过正则与非正则方式分析 SQL 语句的操作类型，操作对象等信息；
	▲支持对数据库 DML、DCL、DDL 语句的审计，可审计的事件基本信息包括：源地址、目的地址、源端口、目的端口、源 MAC、目的 MAC、源用户、目的用户、源国家、目的国家、源区域、目的区域、源城市、目的城市、应用协议名、应用协议分组、VLANID、传输协议、时间（提供相关功能的产品界面截图并加盖原厂公章）；
	支持数据库绑定变量审计，可通过分析、提取语句中绑定变量，审计出访问数据库的源主机名、源主机用户，可监测还原 SQL 操作语句包括源 IP 地址、目的 IP 地址、访问时间、MAC 地址、数据库用户名、客户端名称、服务端名称、数据库操作类型、数据库表名、字段名等；
	支持对访问数据库的设备 ID、源地址、目的地址、SQL 操作响应时间、数据库操作成功、失败的审计（提供相关功能的产品界面截图并加盖原厂公章）；
	支持数据库账号登陆成功、失败的审计（提供相关功能的产品界面截图并加盖原厂公章）；

	支持 SQL 操作审计，可审计数据库操作类、表、视图、索引、触发器、存储过程、域、Schema、游标、事物等；
	支持按数据库名、用户名、数据库表名、操作类别、数据库操作命令、SQL 响应时间、操作结果作为查询和统计条件（提供相关功能的产品界面截图并加盖原厂公章）；
	支持双向审计，支持对超长 SQL 语句的审计，支持 Update、Insert、Delete 操作返回行数、返回字段和结果（最低支持 Oracle、SQLServer）、执行状态的审计（提供相关功能的产品界面截图并加盖原厂公章）；
	▲支持和网络审计在同一平台上运行（提供相关功能的产品界面截图并加盖原厂公章）；
	支持数据库事件进行潜在危害分析，对可能潜在的威胁实时告知管理员，支持数据库密码猜错攻击进行告警；
	支持 HTTP、FTP、Telnet、Rlogin 等运维协议（提供相关功能的产品界面截图并加盖原厂公章）；
	支持以数据库客户端软件名称、数据库名、数据库表名、数据库字段名作为过滤响应条件（非正则表达式方式）的数据库审计策略；
数据库防护	支持对针对数据库的 XSS 攻击行为、SQL 注入攻击行为进行审计，并进行实时报警（提供相关功能的产品界面截图并加盖原厂公章）；
审计关联	支持中间件环境下的 SQL 语句关联到 HTTP 操作，HTTP 操作关联到 HTTP-ID，实现中间件环境下的审计追溯（提供相关功能的产品界面截图并加盖原厂公章）；
	支持数据库审计事件与 WEB 业务系统事件的关联功能，可将审计到的数据库事件，与 web 服务器、客户端 IP 地址等信息关联起来（提供相关功能的产品界面截图并加盖原厂公章）；
报表	支持 WORD、PDF、CVS、EXCEL 等格式导出报表（提供相关功能的产品界面截图并加盖原厂公章）；
	支持邮件方式自动发送报表；
	支持频率趋势图、概率统计图、饼图方式进行报表展现，并可导出统计结果报表；
	支持自定义报表，可以根据客户需求定制更多有实际意义的报表；
	支持按照源 IP 地址、客户端工具等源信息生成报表；
	支持审计结果的多条件组合查询，可以事件发生的时间、用户、访问方式（客户端、TELNET、FTP）、用户 IP、服务器等为查询条件进行组合；
告警	支持通过邮件、syslog、SNMP 等方式进行告警；
	支持对告警信息的发送方式进行设置，以防止告警信息过多，增加邮件服务器压力，至少具备单条发送、归并发送两种方式；

	支持告警信息同时发送到多个管理对象；
	支持告警阀值设置，可设置内容包括：连接数值、流量阀值、系统状态阈值（例如：CPU 阀值设置、硬盘空间阀值空间设置、内存空间阀值设置等）；
	支持报警事件插件的配置管理，例如：事件接收、外发、统计分析、存储等插件；
	支持系统报警规则修改，可自定义报警规则，并定义告警级别、处理方式：系统阻断/放行（旁路）、防火墙联动阻断/放行（提供相关功能的产品界面截图并加盖原厂公章）；
	支持根据审计结果的属性配置告警规则，告警规则匹配方式包括：与或关系匹配、正则匹配、范围匹配等；
	支持告警的统计分析功能，可自定义在线查看统计分析结果，并可根据统计结果生成报表；
	支持告警分类，告警类型至少分为三类，例如：审计报警、日志报警、流量报警（提供相关功能的产品界面截图并加盖原厂公章）；
	支持系统报警的自定义查询功能，可自定义查询系统内所有报警事件内容，包括：事件主体、事件客体、报警内容、报警级别、报警触发规则名称等；
系统管理	系统应提供配置向导，简化策略配置过程（提供相关功能的产品界面截图并加盖原厂公章）；
	▲支持 WEB 登录锁定配置，可自定义用户名/密码尝试次数和登录锁定时间（提供相关功能的产品界面截图并加盖原厂公章）；
	支持 WEB 登录超时自动登出功能，可自定义 WEB 端登录超时时间（提供相关功能的产品界面截图并加盖原厂公章）；
	支持静态密码认证，并对密码的复杂性进行强制要求，比如大小写、数字、特殊字符、长度等；
	支持角色自定义功能，可对角色权限进行细粒度划分，权限可控制到菜单级；
	▲支持双操作系统，通过双操作系统进行冷备支持，当常用系统出现故障可以使用备用系统恢复（提供相关功能的产品界面截图并加盖原厂公章）；
	支持系统状态的监控功能，可监控系统的 CPU、内存、磁盘、网口、运行状态等信息（提供相关功能的产品界面截图并加盖原厂公章）；
	支持本地磁盘状态的查询和显示，可查询设备磁盘的空间利用率，可通过饼状图、柱状图显示磁盘空间占用情况；
	支持磁盘规划功能，可通过饼状图、柱状图显示磁盘空间利用率，本地磁盘中的数据可根据对象进行分类并独立进行备份、清理等操作；
	支持系统管理员 IP 黑白名单，对于无权访问的 IP 可以隐藏设备自身 IP 地址（提供相关功能的产品界面截图并加盖原厂公章）；

	支持系统自审计功能，系统可以记录用户登录操作、系统自动操作、CLI 命令操作以及系统状态情况的自审计日志，管理员可以通过查看自审计日志，随时了解系统的操作情况和运行状态；
	▲支持审计系统与管理系统一体化，不需要安装额外的管理软件，不需要单独的管理设备，无需在被审计系统上安装任何代理；
升级方式	提供系统升级功能，能够通过升级包的方式实现升级；
第三方接口	支持 Syslog 方式向外发送审计日志；
	支持 SNMP Trap 方式向外发送审计日志；
	支持 NTP 时间同步；
	支持以 SNMP 方式，将系统运行状态提供给第三方网管系统；
	支持原始数据包留存，可通过 sftp 方式从设备中取得已记录的原始数据包；
	支持基于流的流量分析功能，可对其他设备发送的 Netflow 进行分析，支持对 Netflow v5/v9 版本的流量分析（提供相关功能的产品界面截图并加盖原厂公章）；
	支持自动备份审计日志，可通过 FTP 方式外送到外部设备，备份文件进行加密，且必须导入设备才能够进行恢复查看；
单点部署	支持旁路镜像模式部署，不影响网络性能和网络架构，网络审计产品的故障不影响被审计系统的正常运行；
多点多级部署	上级设备可下发策略；上级设备也可查看下级设备的统计分析结果等； 任一设备可作管理中心，其他设备作为代理点，管理中心负责策略的下发，数据查询等。用户可根据自身情况，决定代理点是将审计事件发送给管理中心还是存储在代理点本地；
IPv6 环境	支持 IPV6 环境部署和 IPV6 环境下数据库的审计；
规则及策略	支持审计规则的优先级的调整，以防止误报、漏报等发生；
	支持审计策略的自定义，可将时间、源 IP、目的 IP、协议、端口、登陆账号、命令作为响应条件进行策略设置；
	支持数据采集规则定义，对于不关心的数据可以不采集，有效保证系统审计的稳定性与针对性。
	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 高危指令等告警规则（提供相关功能的产品界面截图并加盖原厂公章）；
	支持以字段名称和字段值作为分项响应条件进行审计策略设置（非正则表达式方式）；
	系统具备灰名单功能，可将系统自身无法辨别的安全事件纳入灰名单，并可对灰名单中的内容自定义识别模板，实现对事件类型的辨别扩展功能（提供相关功能的产品界面截图并加盖原厂公章）；

▲产品资质 （需提供证书复印件加盖厂家公章）	《计算机信息系统安全专用产品销售许可证》-增强级
	《计算机软件著作权登记》
	中国国家信息安全产品认证证书 ISCCC-增强级
	涉密信息系统产品检测证书
	军用产品认证证书
	公安部检测报告
	国家信息安全测评 EAL3 证书
	ISCCC 信息安全产品认证证书
	IPV6 Ready Logo Phase-2
▲厂商资质 （需提供证书复印件加盖厂家公章）	为保障项目的机密性，原厂商须具备涉密信息系统集成甲级资质；
	为保证项目设计及集成能力，设备原厂商须具有通信行业安全设计与集成二级资质证书；
	为保障厂商的售后服务水平，原厂商需获得 ISO27001 信息安全管理体系认证、ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证；
	为保证项目的应急响应能力，原厂商须具备网络安全应急服务支撑单位（国家级）资质；
	为保证项目安全服务能力，设备原厂商须具备国家信息安全认证信息安全服务资质证书（安全工程类三级）
	为保证本项目后续的制造商培训能力，设备制造商须具备专业的信息安全技术培训能力，并取得权威的培训资质，应具有国家信息安全测评授权培训机构资质证书；
▲售后服务	产品须由原厂商提供 3 年应急响应服务、定期巡检服务，具体参考服务要求，提供设备原厂商针对本项目的授权及售后服务承诺函，点对点技术响应函并加盖原厂公章；

2.2.9 运维安全审计系统

指标	指标项	规格要求
部署方式	工作模式	物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构，不改变运维人员的运维习惯。
设备要求	配置要求	1U 机型，1 个 console 口，2 个 USB 口；6 个千兆电口，2 个 SFP 插槽，2 个可扩展插槽；16G 内存，2T 存储空间，单电源；100 个主机/设备许可，用户数不限制。三年原厂质保服务；
组织结构	分组	▲不限级数的进行分层分级分类管理。（提供产品相关功能页面截图并加盖原厂公章）；
	AD 域同步	▲支持从 AD 域抽取 OU，方便快速建立组织结构。（提供产品相关功能页面

		截图并加盖原厂公章）；
	组定义类型	支持组定义类型（用户、资源、综合）便于管理和快速查找。
用户管理	用户管理	完整的用户帐号生命周期管理，实现帐号的创建、维护、修改、删除的集中管理；自定义用户类型，基于针对用户类型进行用户地址策略。
	AD 域同步	▲主帐号支持从 AD 域内抽取，方便快速建立主账号。（提供产品相关功能页面截图并加盖原厂公章）；
	用户导入导出	支持以组节点进行批量导入导出。
	用户分组管理	分组可以树形方式展现，不限制分组层级数量。
	用户策略	通过配置口令策略，达到指定密码有效期和限制主帐号密码强度的目的。 配置访问锁定策略，达到限制主帐号密码输入错误次数和锁定时间。 配置访问地址策略，达到限制主帐号访问时所在工作站的 IP 地址池。 配置访问时间策略达到限制主帐号只能在规定的时间段内进行资源访问。
资源管理	资源统计	▲支持柱形图方式查看系统中不同资源所占比例。（提供产品相关功能页面截图并加盖原厂公章）；
	资源分组管理	分组可以树形方式展现，不限制分组层级数量。
	资源类型	unix 资源、网络资源、windows 资源、数据库资源、C/S 资源、B/S 资源、中间件资源、大型机资源。
	资源协议	支持 SSH、TELNET、FTP、SFTP、VNC、XWINDOW、WINDOWS 文件共享等协议。
从账号管理（设备账号）	账号管理	▲支持资源从账号的管理，系统具有各种资源类型驱动器能够将资源上的账号进行自动抽取、推送及属性的变更等。（提供产品相关功能页面截图并加盖原厂公章）；
	自动改密	支持对 unix 资源、网络资源、windows 资源、数据库资源、中间件资源进行密码变更；密码变更可以根据密码策略的要求进行变更，变更的密码符合密码策略中关于密码强度的要求。
	密码拨测计划	▲定期检查平台存储的设备账号密码与设备实际密码是否匹配，以便进校验密码一致性，提高设备的安全性避免密码混乱无法登陆现象发生。（提供产品相关功能页面截图并加盖原厂公章）；
	账号导出	从账号按时间计划导出账号口令，支持手动下载或指定 FTP 服务器； 导出的账号口令需要输入密码解密查看。
	访问端口变更	▲提高设备的安全性，不采用标准的协议端口，平台支持 FTP、telnet、ssh、远程桌面等协议服务端口变更。（提供产品相关功能页面截图并加盖原厂公章）；
授权管理	角色管理	▲支持自定义角色。角色可按照组节点进行定义，从而实现分层分级管理模

		式。角色权限细粒度高，可自由组合。（提供产品相关功能页面截图并加盖原厂公章）；
	岗位授权	资源授权模式基于岗位授权，岗位上绑定资源账号，这样授权可迁移、授权粒度更细；并可针对岗位设置相关安全策略。（提供产品相关功能页面截图并加盖原厂公章）；
单点登录SSO	收藏夹功能	▲运维人员可将经常访问的资源添加到收藏夹。（提供产品相关功能页面截图并加盖原厂公章）；
	批量单点登录	▲支持批量单点登录资源，简化工作量。（提供产品相关功能页面截图并加盖原厂公章）；
	身份切换代填	支持网络设备 enable 和 unix 主机 su 等身份切换的单点登录功能。
	Zmodem 协议访问	运行 rz，sz 等命令，从而可以非常便捷快速的进行两个系统的文件交换。
	自动代填	访问授权资源时不必再输入从帐号和密码
认证管理	身份认证	▲自身提供证书认证服务，也可与第三方 CA、动态令牌、生物识别、短信认证等方式进行结合。支持组合认证，提高访问的安全性。（提供产品相关功能页面截图并加盖原厂公章）；
	RADIUS 和 TACACS+	▲平台在网络设备的认证协议上不仅支持 RADIUS 和 TACACS+协议，而且产品系统自身可以作为 Radius 和 TACACS 服务器。（提供产品相关功能页面截图并加盖原厂公章）；
安全管理	访问时间策略	可以配置成可访问时间段方式，也可以配置成不可访问时间段方式。配置时间段时可以配置日期和小时。
	地址策略	支持配置成可访问 IP 段方式，也支持配置成不可访问 IP 段方式。IP 段由 IP 和掩码构成。
	RDP 策略	▲上下行剪切板控制、共享磁盘控制、控制台登录控制。（提供产品相关功能页面截图并加盖原厂公章）；
	字符命令	支持命令操作的黑白名单设置，命令权限控制规则应支持正则表达式，并可以对命令的参数进行限制并记录日志
	FTP	支持常用命令列表，方便用户指定 FTP 命令策略。
	口令策略	可以配置口令长度，是否包含字母及字母的长度，是否包含数字及数字的长度，是否包含符号及符号的长度，口令时效性。口令策略还可以配置禁止包含的关键字。
	锁定策略	可以配置访问失败几次锁定，也可以配置锁定后多长时间解锁。
	审计策略	▲根据不同设备审计安全需求，客户自定义审计范围，字符（命令、内容、

		录像)、图形（录像、键盘、上下行剪切板、上下行文件传输)、FTP（命令、保留上传文件、保留下载文件)。（提供产品相关功能页面截图并加盖原厂公章）；
	VPN 功能	▲内置 VPN 功能，无需专用 VPN 硬件支持，即可保证远程接入堡垒机的链路安全。（提供产品相关功能页面截图并加盖原厂公章）；
审计管理	图形审计	图形资源访问时，支持键盘、剪切板、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、文件传输记录的指定位置开始回放。
	字符审计	对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出，并且可以展现各命令的执行时间和允许执行情况。
	实时监控	支持实时审计和阻断。操作人员对于资源的访问，审计员可以实施查看。发现高危操作时，支持实时切断当前会话。
	管理审计	支持提供系统内部操作审计，包括管理员和运维用户的登录、登出、对系统的配置操作、账号属性修改等系统管理操作。
	审计报表	系统预设常用统计报表模板，分为基础业务报表、行为审计报表、信息管理报表三大类。报表提供 Word、Excel、PDF 类型下载。
流程管理	流程管理	▲支持设定主副岗账号和双人共管账号，并提供相应授权流程； 支持流程申请人、审批人、执行人的委派。授权需要申请人定义申请单，发起事件申请；事件可以多人审批，审批人收到申请后可以同意或拒绝申请，同意时可以指定执行人进行实际的管理动作的执行；（提供产品相关功能页面截图并加盖原厂公章）；
	消息管理	▲支持消息管理，可通过系统统一给各管理员和运维人员发布消息。（提供产品相关功能页面截图并加盖原厂公章）； 支持工作计划管理，可自维护方式制定运维工作计划，并到期提醒。
系统配置	数据备份、还原	应用备份、管理数据备份、审计数据备份、配置文件备份
	系统状态	包括：cpu 工作情况，内存使用情况，磁盘使用情况，网卡使用情况，系统数据库工作情况， WEB 服务工作情况，其他关键组件工作情况等。
	时间同步	同步 NTP 服务器
	系统维护	对系统服务配置清除、审计日志清理、还原出厂设置；关机重启等功能
	外接存储	▲支持日志数据的外置存储备份，支持 NFS 和 windows 文件共享协议，远程审计存储和本地存储对审计员透明。（提供产品相关功能页面截图并加盖原厂公章）；
高可用性	HA	支持以 Active-Standby 方式部署 ▲支持服务及应用层面的检测（提供产品相关功能页面截图并加盖原厂公

		章）； 支持双网卡冗余（双网卡虚拟单 Ip）
	集群部署	▲支持堡垒机集群模式部署；支持应用发布服务器的集群部署，可以设定自动选择应用发布服务器，或者由用户手动指定；支持集群设备多节点数据实时同步（提供产品相关功能页面截图并加盖原厂公章）；
	分布式部署	实现公司总部与各分公司之间，组织机构分散而需要统一集中管理的问题。
资质要求	▲产品资质（需提供证书复印件加盖厂家公章）	《计算机信息系统安全专用产品销售许可证》
		《涉密信息系统产品检测证书》
		《计算机软件著作权登记证书》
		《IT 产品信息安全认证证书》3C
	▲厂商资质（需提供证书复印件加盖厂家公章）	为保障项目的机密性，原厂商须具备涉密信息系统集成甲级资质；
		为保证项目设计及集成能力，设备原厂商须具有通信行业安全设计与集成二级资质证书；
		为保障厂商的售后服务水平，原厂商需获得 ISO27001 信息安全管理体系认证、ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证；
		为保证项目的应急响应能力，原厂商须具备网络安全应急服务支撑单位（国家级）资质；
		为保证项目安全服务能力，设备原厂商须具备国家信息安全认证信息安全服务资质证书（安全工程类三级），信息安全等级保护安全建设服务机构能力评估合格证书；
		为保证本项目后续的厂商培训能力，设备原厂商须具备专业的信息安全技术培训能力，并取得权威的培训资质，应具有国家信息安全测评授权培训机构资质证书；
▲售后服务	产品须由原厂商提供 3 年应急响应服务、定期巡检服务，具体参考服务要求，提供设备原厂商针对本项目的授权及售后服务承诺函，点对点技术响应函并加盖原厂公章；	

2.2.10 网络准入系统

指标	指标项	详细要求
设备基本要求	专用的硬件和软件保障	▲采用专用硬件架构与专用安全操作系统（非 Windows 平台），硬件设备可以机架安装。
	接口数量	1U 机箱，6 个 1000BASE-T 电口，2 个 SFP 插槽，1T 存储空间，配置单电源，接口支持 Bypass，冗余 2 个扩展槽位；三年原厂质保服务；
	存储与电源	1TB 存储空间，单电源。

指标	指标项	详细要求
性能要求	处理能力	可支持并发 500 个客户端，最大用户数无限制；
系统部署	部署方式	系统部署简单，支持旁路或串联部署，串联部署采取透明网关准入模式时不依赖于交换机、路由器以及防火墙等设备，避免对已有网络进行较大规模的调整。
	可靠性	▲支持双操作系统冷备，当常用系统出现故障可以使用备用系统恢复。(提供产品相关功能截图并加盖原厂公章)；
		支持 ByPass 监控功能，用于对网络紧急情况的处理。
		▲具备单机模式下的系统逃生工具，可添加维护交换机信息，在准入设备故障时进行自动或手动方式逃生。(提供产品相关功能截图并加盖原厂公章)；
	高可用	支持双机热备，主备无缝切换，能够自定义对外提供管理的设备接口及服务的虚拟 IP 地址。支持双机间的数据同步，可同步系统日志，并能够设置同步时间间隔。
	管理方式	▲支持命令行与 B/S 模式管理，提供系统首页图形化展示功能，可展示设备面板状态、CPU 状态、内存状态、硬盘状态、在线用户、报警统计等信息。(提供产品相关功能截图并加盖原厂公章)；
	兼容性	客户端兼容：支持 windows XP、32 位及 64 位 windows7/8/8.1/10/server2008 操作系统。 浏览器：浏览器插件兼容 IE8 及以上版本。
	适应性	支持 PC 有线和智能终端无线认证，可与主流 AC 设备联动，实现智能终端无线准入，无需安装客户端。
准入认证管理	准入模式	▲支持 802.1X、Portal、透明网关、策略路由等多种准入模式选择，单设备情况下可进行混合准入模式应用。(提供产品相关功能截图并加盖原厂公章)；
		对于不同准入模式的介绍、部署拓扑、配置步骤等信息支持在管理界面中进行展示。
	终端通讯管理	支持终端准入前是否能够与其他主机进行网络通信诊断（PING）操作。
	认证方式	提供 Web 认证方式，并可设置重定向页面 URL 地址。
		提供客户端认证方式，采用用户名/密码认证，可与第三方 AD 域、LDAP 服务器进行用户信息同步。
		▲提供手机短信认证方式，可与短信服务器联动，在终端入网认证时下发验证码。(提供产品相关功能截图并加盖原厂公章)；

指标	指标项	详细要求
	多要素绑定校验	支持信息绑定认证，可检查入网终端 IP、终端 MAC、用户名、交换机 IP、交换机端口、终端硬件 ID 等多要素信息。
	访客时效管理	支持临时入网终端有效期管理，可设置在网时限。
	准入管理	▲支持同账户多在线管理，能够对同一用户同时刻允许使用终端数进行限制，处理方式包括：下线第一个、下线最后一个、不处理等。(提供产品相关功能截图并加盖原厂公章)；
		支持 IP 冲突管理，对入网终端与已在线终端 IP 冲突时提供处理方式，方式包括：下线已在线终端及不处理等。(提供产品相关功能截图并加盖原厂公章)；
		▲支持终端健康检查报告展示设置，可提供显示、不显示、失败时显示、成功时显示等多种展示方式。(提供产品相关功能截图并加盖原厂公章)；
		支持黑/白名单管理，可根据所应用的不同准入模式，设置黑/白名单终端 IP、MAC、协议、端口、VLAN 号等信息。(提供产品相关功能截图并加盖原厂公章)；
		▲支持动态终端 IP 分配功能，并可基于 MAC 绑定下发终端 IP 地址。(提供产品相关功能截图并加盖原厂公章)；
	用户管理	支持认证用户管理，可创建组织结构并添加用户信息，信息包括登录名、姓名、密码、单位、电话、办公地址、邮箱、VLAN ID、ACL 规则名等信息，可进行批量导入导出。
		支持在线用户管理，界面展示入网用户信息，信息包括登录名、终端 MAC、终端 IP、准入模式、交换机 IP、交换机端口、上线时间等，并可对在线用户进行强制下线及恢复操作。
合规监控	入网健康检查	▲支持终端健康检查，系统默认检查项： 1) 系统时间检查； 2) 系统运行时长检查； 3) Guest 用户检查； 4) AD 域域名检查； 5) Windows 文件共享检查； 6) Windows 防火墙检查； 7) 必须/禁止运行进程检查； 8) 必须/禁止运行服务检查； 9) 必须/禁止安装软件检查；

指标	指标项	详细要求
		10）Windows 桌面屏保检查； 11）杀毒软件版本（小红伞、瑞星、金山毒霸、卡巴斯基、诺顿、360 杀毒）检查项。(提供产品相关功能截图并加盖原厂公章)；
		检查项策略对象之间可通过评分制的形式对终端的健康状况做最后的评估，根据预先配置好的阈值对终端入网请求作出判断。
		可设置关键检查项与策略权重，并支持自定义修复向导与命令。
	终端外设监控	支持终端设备进行启用禁用监控：光驱、打印机、调制解调器、网络适配器、图像设备、通讯端口、红外设备、蓝牙设备、1394 控制器、PCMCIA 卡、便携设备、USB 设备，对光驱可设置是否允许刻录权限，对 USB 设备可设置例外项，添加 USB 硬件 ID 和设备信息，USB 设备类包括光驱、打印机、调制解调器、网络适配器、通讯端口、图形图像设备，USB 设备子类包括音频、图像、打印、大容量存储、智能卡、视频等。
	非法外联监控	支持终端非法外联监控，可提供包括 http、telnet、ping 三种方式检测主机违规外联行为，可设定检测周期、内网 IP 范围、外联检测地址、连接内外网或仅在外网的违规处理方式（不处理、重启、断网、提示），并支持自定义外联提示信息。
资产管理	入网资产管理	支持资产管理功能，可添加、修改、删除资产信息，资产类型包括：台式机、笔记本、打印机、IP 电话机、服务器、工作站、手机等，并可对不同资产实施 MAC 免认证操作。
	网络设备管理	支持网络设备管理，可添加、修改、删除网络设备，记录网络设备型号、IP 地址、MAC 地址、类型、使用人、登记时间等信息，并可点选查看设备名称、接口状态、接口类型、允许通过 VLAN、是否开启 MAC-VLAN、连接主机数等信息，支持设备接口 802.1X 启停用管理功能。(提供产品相关功能截图并加盖原厂公章)；
	入网资产发现	支持资产发现功能，可扫描发现接入交换机连接设备信息，包括：终端 IP、终端 MAC、终端网卡供应商、终端 VLAN、交换机端口、交换机 IP、绑定用户等信息。
	入网资产审批	▲支持未确认资产审批功能，记录入网终端操作系统、MAC 地址、IP 地址、计算机名、客户端/插件版本、终端 ID 等信息，提供确认或删除操作，终端确认后方可正常入网。(提供产品相关功能截图并加盖原厂公章)；
日志管理	终端解绑记录	记录终端性质、固定用户名、固定用户部门、终端 MAC、临时用户名、

指标	指标项	详细要求
		注册时间、最后接入时间、退出时间等信息，可按照时间周期快速查询。
	资产登录记录	记录终端性质、用户姓名、用户部门、终端 MAC、IP 地址、登录时间、退出时间、操作等信息，可按照时间周期快速查询。
	报警日志	▲记录系统报警类别、报警内容、报警级别、时间等信息，支持导出 Excle 表，可设置外发报警邮件，提供时间、类别、级别、内容等快速查询方式。(提供产品相关功能截图并加盖原厂公章)；
	系统日志	记录日志源、登录用户名、用户 IP、日志内容、事件结果、日志级别、时间等信息，支持导出 Excel 表，提供时间、用户 IP、级别、日志源、内容等快速查询方式。
	终端认证日志	记录终端认证时间、终端 IP、MAC、用户名、交换机 IP、端口、准入模式、认证结果等信息，支持导出 Excel 表，提供时间、终端 MAC、用户名、交换机 IP、交换机端口等快速查询方式。
	健康检查日志	记录终端健康检查时间、终端 MAC、用户名、交换机 IP、端口、检查结果、检查得分/及格分、检查对象、详情等信息，支持导出 Excel 表，提供时间、终端 MAC、用户名、交换机 IP、交换机端口、健康检查结果、检查得分等快速查询方式。
统计与报表	统计分析	可按照时间周期图形化展示终端认证结果、健康检查结果、健康检查项、准入模式等信息，提供折线、柱状、堆叠、平铺等展示方式，可按照终端 IP、终端 MAC、用户名、交换机 IP、交换机端口等信息进行快速查询。(提供产品相关功能截图并加盖原厂公章)；
	自定义报表	▲可添加、删除、修改报表模板，支持模板名称、标题、公司、统计模块（认证结果/检查结果/检查项/准入模式）、生产报表周期（日报/周报/月报）、报表文件类型（PDF/DOC/XLS/HTML/CSV）设置，可添加报表生成的查询条件，条件信息包括：终端 IP、终端 MAC、交换机 IP、交换机端口、用户名等。(提供产品相关功能截图并加盖原厂公章)；
系统管理	系统信息管理	▲展示系统主机名称、管理员、描述、所在位置、运行时长、DNS 配置、系统时间、系统版本等信息，支持系统界面与登录界面 LOGO 的自定义导入，可自由设置产品显示名称。(提供产品相关功能截图并加盖原厂公章)；
	网络管理	支持对网络准入系统的接口管理、路由管理，接口管理可展示设备自身接口名称、IP 地址、MTU、链接状态、模式、配对的接口、启用状态等信息。

指标	指标项	详细要求
	DHCP 服务配置	支持 DHCP 服务的配置功能，可设置设备提供服务的接口、子网、子网掩码、地址池、网关、域名服务器等信息。
	访问控制	支持系统访问控制管理，实施 IP 地址访问系统控制，可自定义界面访问配置，设置超时时间、重试次数、锁定时间等信息。
	系统管理角色	可创建、删除、修改系统管理账户，支持账户对于不同部门的管理权限设定，可设置账户密码长度、字母长度、数字长度、特殊字符长度、必须包含的字符等复杂度要求。
	系统服务管理	对 TopNAC 上的服务进行管理，可以进行的操作有启动服务、禁用服务、重启服务，系统页面展现服务状态，无需后台操作。
	系统维护	图形化显示系统磁盘状态信息，内容包括：资产数据、报警日志、日志文件、用户数据、对象和策略、其他数据、空闲磁盘空间等，并列出所占空间大小，支持系统磁盘数据的备份、恢复、清理，可按照不同数据对象、时间对象进行系统自动备份操作。(提供产品相关功能截图并加盖原厂公章)；
	系统升级	提供系统升级管理功能，可进行安装包上传及升级操作。
	系统配置管理	▲支持系统配置保存、导入及导出，可进行恢复出厂设置、关机、重启操作。(提供产品相关功能截图并加盖原厂公章)；
	诊断分析	▲支持系统当前状态进行诊断分析，展示不同准入模式运行状态、服务是否正常，并提供系统调试、抓包分析等功能(提供产品相关功能截图并加盖原厂公章)；
资质要求	▲产品资质（需提供证书复印件加盖制造商公章）	中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》
		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》
		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》
		中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》（EAL3+级）
	▲厂商资质（需提供证书复印件加盖厂家公章）	为保障项目的机密性，原厂商须具备涉密信息系统集成甲级资质；
		为保证项目设计及集成能力，设备原厂商须具有通信行业安全设计与集成二级资质证书；
		为保障厂商的售后服务水平，原厂商需获得 ISO27001 信息安全管理体系认证、ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证；

指标	指标项	详细要求
		为保证项目的应急响应能力，原厂商须具备网络安全应急服务支撑单位（国家级）资质；
		为保证项目安全服务能力，设备原厂商须具备国家信息安全认证信息安全服务资质证书（安全工程类三级），信息安全等级保护安全建设服务机构能力评估合格证书；
		为保证本项目后续的制造商培训能力，设备制造商须具备专业的信息安全技术培训能力，并取得权威的培训资质，应具有国家信息安全测评授权培训机构资质证书；
▲售后服务		产品须由制造商提供 3 年应急响应服务、定期巡检服务，具体参考服务要求，提供设备制造商针对本项目的授权及售后服务承诺函，点对点技术响应函并加盖制造商公章；

2.2.11 日志审计系统

指标项	参数说明
硬件要求	▲1U 机箱，1 个 console 口，6 千兆电口，有效存储容量 4T，标配 Raid5。最大支持 100 日志源授权。综合处理性能：20000EPS，综合处理峰值：30000EPS；包含日志收集、存储、查询、统计分析等功能。；TopAudit-Log 标准版，含日志收集、存储、查询、关联分析、统计分析、告警响应等功能。三年原厂质保服务；
系统支持	支持 linux（64 位）系统；
部署模式	支持单级部署； 支持代理分布式部署采集日志；
系统性能	▲数据存储能力：压缩加密存储，压缩比不低于 10:1；日志存储不低于 10000 条/M(提供产品相关功能截图并加盖原厂公章)； 支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于 10s；
数据采集	▲支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于 26 类 300 种日志对象的日志数据采集。(提供产品相关功能截图并加盖原厂公章)； 对于尚未支持的设备类型日志进行新增采集支持,在页面上传升级文件或增加配置文件即可； ▲支持主动、被动相结合的数据采集方式；支持 Telnet\SSH、Syslog、SNMP Trap、Netflow、JDBC、SSH、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过 Agent 采集日志数据。(提供产品相关功能截图并加盖原厂公章)； ▲系统内置已支持设备种类清单，提供设备日志外发配置建议指导；(提供产品相关功能截图并加盖原厂公章)；

	支持日志归一化处理,将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者；(提供产品相关功能截图并加盖原厂公章)； ▲支持实时自动刷新每个日志源的实时日志列表,支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志；(提供产品相关功能截图并加盖原厂公章)； 支持独立展示每个被采集源最近 24 小时的日志数量趋势,便于掌握设备的安全事件情况，支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态；(提供产品相关功能截图并加盖原厂公章)； ▲支持对每个日志源设置过滤条件规则，自动过滤无用日志；(提供产品相关功能截图并加盖原厂公章)； 支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接受速率，降低对系统资源的占用，保障重要日志的收集，支持限制速率设置为 1000 条/秒、3000 条/秒和 5000 条/秒等； 支持对文本类型日志源进行限速采集，匀速采集日志，防止对系统资源产生突发冲击； ▲支持日志转发给第三方系统平台，支持设置多个日志转发 IP 地址，支持转发格式化日志或仅转发原始日志；(提供产品相关功能截图并加盖原厂公章)；
数据存储	支持对所管理设备的日志原始数据完整存储，支持数据本地集中存储、网络存储； ▲支持根据设备重要程度设置独立设置每个被采集源的数据存储存储时间为 1 个月、3 个月、6 个月和永久保存等参数；(提供产品相关功能截图并加盖原厂公章)； 支持自定义存储位置，支持多盘并行存储，当磁盘满后自动切换存储位置，支持磁盘阵列、SAN、NAS 等外部高性能存储；(提供产品相关功能截图并加盖原厂公章)； 支持存储空间图像化、动态监控，超过阀值进行告警。支持从存储空间、存储时间多维度进行动态监控；(提供产品相关功能截图并加盖原厂公章)； ▲支持日志备份功能，支持本地备份和 FTP 备份方式，支持自动备份和手动备份。(提供产品相关功能截图并加盖原厂公章)；
告警管理	▲内置系统运行相关告警规则，包括检测到新日志源、节点掉线、主动日志源长期不外发日志、存储上限告警、主机认证失败等，可启用/禁用规则； (提供产品相关功能截图并加盖原厂公章)； 支持安全告警概况、安全告警趋势以及实时安全事件的统一展示，实时告警可根据级别、规则类型等进行分类(提供产品相关功能截图并加盖原厂公章)； ▲支持根据级别、规则类型、规则名称、时间范围、事件名、设备 IP、源 IP、目的 IP 等方式快速检索安全事件告警，检索结果支持 Excel 等格式导出；(提供产品相关功能截图并加盖原厂公章)； ▲支持基于时间轴展示数据分布，能够通过时间轴进行查询分析；(提供产品相关功能截

	图并加盖原厂公章)；
告警响应	▲支持邮件、声音、短信、命令行等多种告警方式，支持报警内容引用字段变量参数；(提供产品相关功能截图并加盖原厂公章)； 可以针对不同类型、不同种类以及不同安全级别的安全事件制定不同的告警方式。(提供产品相关功能截图并加盖原厂公章)；
统计报表管理	▲系统支持智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应；(提供产品相关功能截图并加盖原厂公章)； 报表支持基于全国地图、全球地图进行访问源、访问目的追踪。(提供产品相关功能截图并加盖原厂公章)； ▲支持自定义统计报表报告，支持 PDF、word、execl、html 等方式导出报表，支持实时报表、计划报表。(提供产品相关功能截图并加盖原厂公章)； 内置上百种报表模板。
数据查询	▲支持首页以全国地图、全球地图展示最近 24 小时日志访问源和访问目的的分布，能根据颜色区分访问来源和访问目的数据量大小，能够通过首页地图快速下钻查询指定省、市的日志详细信息；(提供产品相关功能截图并加盖原厂公章)； 支持等于、不等于、大于、小于、正则表达式等查询条件；(提供产品相关功能截图并加盖原厂公章)； 支持多条件组合查询；(提供产品相关功能截图并加盖原厂公章)； ▲支持为不同类型日志设置不同的查询条件和显示条件；(提供产品相关功能截图并加盖原厂公章)； 支持原始日志全文检索；(提供产品相关功能截图并加盖原厂公章)； 支持在一个日志源查询结果列表中以 IP 为条件直接跳转到其他日志源类型中进行查询；(提供产品相关功能截图并加盖原厂公章)； ▲支持在查询结果页面上直接下钻二次查询，快速定位关键日志，还可以返回上次查询条件；(提供产品相关功能截图并加盖原厂公章)； 查询结果可将归一化日志和原始日志同屏对比显示；(提供产品相关功能截图并加盖原厂公章)； 查询结果支持分页显示；(提供产品相关功能截图并加盖原厂公章)； ▲支持查询结果格式化日志、原始日志导出；(提供产品相关功能截图并加盖原厂公章)； ▲支持在日志查询结果上针对源 IP、目的 IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源 IP 和目的 IP（公网地址）还支持以中国地图、世界地图方式展示，在统计图上能够进行点击下钻查询对应条件的日志结果；(提供产品相关功能截图并加盖原厂公章)； ▲支持查询结果快速统计，可自定义统计主题规则，支持以分、时、周、月、年定时执行

	自动统计任务，将统计结果报表发送到指定邮箱；(提供产品相关功能截图并加盖原厂公章)； 支持基于时间轴展示数据分布，能够通过时间轴进行查询分析；(提供产品相关功能截图并加盖原厂公章)； ▲支持历史备份文件导入进行查询；(提供产品相关功能截图并加盖原厂公章)；
日志源管理	▲支持手动添加日志源，管理员可以对日志源进行查看、添加、编辑、删除以及启\禁用的操作；(提供产品相关功能截图并加盖原厂公章)； 支持为日志源指定类型、名称、IP 地址、收集节点、收集方式、以及日志源启停状态等属性信息；(提供产品相关功能截图并加盖原厂公章)； ▲支持日志源在线状态监测告警，实时监测日志源的可用性，可显示每个日志源采集日志的最近时间，实时展示每个日志源最近一天日志趋势变化；(提供产品相关功能截图并加盖原厂公章)； 支持以业务角度将日志源进行分组，支持在日志查询时以业务组进行查询，支持在首页拓扑展示时以业务组进行展示。(提供产品相关功能截图并加盖原厂公章)； ▲支持基于拓扑图的日志源相关数据信息快速查看（需提供界面截图）
系统管理	▲支持用户按角色管理，支持三权分立；(提供产品相关功能截图并加盖原厂公章)； 支持将日志源管理权限分配给不同的操作管理员，不同用户管理不同日志源的日志，互不干扰；(提供产品相关功能截图并加盖原厂公章)； ▲支持设置非法用户访问控制策略；(提供产品相关功能截图并加盖原厂公章)； 系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。(提供产品相关功能截图并加盖原厂公章)； ▲支持将常用 IP 地址或 IP 地址网段标记为自定义名称，在日志查询界面可以在 IP 列中对应悬浮显示自定义名称；(提供产品相关功能截图并加盖原厂公章)；
▲产品资质（需提供证书复印件加盖厂家公章）	产品获得公安部计算机信息系统安全产品销售许可证（行标三级）以及公安部信息安全产品检测中心出具产品检验报告。所提供的产品检验报告须符合《信息安全技术 日志分析产品安全技术要求 GA/T 911-2010》检验规范，并提供完整的检测报告复印件（行标三级）； 产品获得国家保密科技测评中心检测并获得涉密信息系统产品检测证书，需符合《涉及国家秘密的信息系统安全监控与审计产品技术要求》中日志收集与分析的相关要求，并提供完整的检测报告复印件； 军用信息安全产品认证证书（军 C+级）； 计算机软件著作权登记证书。
▲厂商资质（需提供证书	为保障项目的机密性，原厂商须具备涉密信息系统集成甲级资质； 为保证项目设计及集成能力，设备原厂商须具有通信行业安全设计与集成二级资质证书；

复印件加盖厂家公章）	为保障厂商的售后服务水平，原厂商需获得 ISO27001 信息安全管理体系认证、ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证；
	为保证项目的应急响应能力，原厂商须具备网络安全应急服务支撑单位（国家级）资质；
	为保证项目安全服务能力，设备原厂商须具备国家信息安全认证信息安全服务资质证书（安全工程类三级），信息安全等级保护安全建设服务机构能力评估合格证书；
	为保证本项目后续的制造商培训能力，设备制造商须具备专业的信息安全技术培训能力，并取得权威的培训资质，应具有国家信息安全测评授权培训机构资质证书；

2.2.12 终端威胁防御系统

类别	指标项	指标要求
安装部署	支持 B/S 管理架构	系统支持全中文界面，B/S 架构。管理员只需通过浏览器登录控制中心，即可对系统进行管理。本次要求配置 10 个服务器许可，300 个终端许可；
	操作系统支持	至少支持 WindowsXP、Windows 7、Windows 8、Windows 10 等 32 位/64 位终端操作系统，支持 Windows2003、Windows2008、Windows2012 等 32 位/64 位服务器操作系统。同时需支持 Linux 操作系统以及中标麒麟、银河麒麟等国产操作系统。
	支持服务端快速恢复	▲服务端采用 Docker 部署方式，能够快速恢复，横向扩展，可移植性强（提供产品相关功能页面截图并加盖原厂公章）；
	轻量级客户端安装	▲客户端安装后至多占用 50M 硬盘资源，病毒库 3M 大小，日常内存占用不到 10M，有效节省 PC/Server 资源。（提供产品相关功能页面截图并加盖原厂公章）；
	客户端安装	客户端安装支持本地安装，WEB 安装。
管理控制	平台管控	能够对客户端进行统一管理，统一下达指令
	可视化展示	支持控制中心直观的展示终端信息、病毒趋势统计、病毒类型排行、病毒排行、终端危险排行等全网统计情况。并随时对网络中威胁发生的情况进行查询，能组合时间、IP、机器名、病毒名称、病毒类型等信息全方位定位、展示。
	终端管理	控制中心支持实时显示客户端的状态及终端基本信息，包括客户端连接状态、服务状态；终端机器名称、IP 地址、MAC 地址、操作系统、显卡信息、内存大小、当前版本信息和物理位置等信息，支持终端信息导出。
		支持对终端进行分组及批量分组，支持分组导入、导出。
		▲支持对终端进行单/多标签标记。（提供产品相关功能页面截图并加

		盖原厂公章）；
		支持终端连接定制，根据定制，主动清除过期离线客户端相关信息，便于管理员清晰管理终端。
		▲控制中心支持全网/以分组、标签为单位/指定某些客户端定制操作，即时/定时实现客户端三种病毒查杀模式、显示通知、关机、重启、升级等操作，并对以上操作配置详情，客户端执行情况跟踪，实现控制中心对客户端的操作监控。支持对客户端上述操作的快速定制。（提供产品相关功能页面截图并加盖原厂公章）；
		▲支持客户端主动升级及平台即时/定时推送升级；支持全网/以分组、标签为单位/指定某些客户端定制不同版本升级包，实现差异管理、灰度升级。（提供产品相关功能页面截图并加盖原厂公章）；
		平台支持客户端升级包上传及配置 http(s)/ftp 远端同步方式，更新客户端升级包 ，可以根据不同网络环境提供在线获取和隔离网获取相应工具。
		产品具备漏洞集中修复，强制修复；可以通过报表形式展示全网补丁情况，分为高危补丁、功能更新等，并展示以做补丁和未做补丁的信息。
		▲支持单/多客户端不同管理中心迁移。（提供产品相关功能页面截图并加盖原厂公章）；
	策略管理	▲控制中心支持全网/以分组、标签为单位/指定某些客户端定制策略，支持指定客户端策略锁定。（提供产品相关功能页面截图并加盖原厂公章）； 定制策略包括病毒防御（文件实时监控、恶意行为监控、U 盘保护、下载保护、邮件监控）、系统防御（系统加固、软件安装拦截、浏览器保护）、网络防御（黑客入侵拦截、对外攻击检测、恶意网站拦截、IP 协议控制、IP 黑名单）等。
		支持策略无限定时间定制，终端开机启动策略生效，
		▲支持设置客户端与控制中心的通讯时间间隔（提供产品相关功能页面截图并加盖原厂公章）；
		支持自定义白名单，可设置路径、哈希，实现信任文件过滤。
	统计分析	支持统计分析客户端上报的威胁日志，包含终端/部门/责任人危险排行统计、防御类型分布统计、病毒类型分布统计、病毒排行统计、病毒趋势统计等，支持图表显示。支持统计图表导出。

	报表功能	▲支持报表内容、周期、推送、输出格式定制，内容设定模板任意组合包含终端/部门/责任人危险排行统计、防御类型分布统计、病毒类型分布统计、病毒排行统计、病毒趋势统计等统计情景及威胁 Top10、Top20、Top30 排行；周期设定任意组合日、周、月周期，定时生成报表；推送设定任意接收报表人员；输出格式设定 Excel、Word、HTML、PDF 等通用格式输出。（提供产品相关功能页面截图并加盖原厂公章）；
		▲多管理员可定制专属报表，数据隔离，报表仅对自己可见及管理。（提供产品相关功能页面截图并加盖原厂公章）；
		支持立即生成报表模板预置时段或自定义时段报表。
	审计告警	▲支持对客户端上报的安全日志进行审计、告警，可预置字段及自定义字段过滤详细日志，快速定位终端安全状况；定制符合企业敏感程度的告警规则，达到告警阈值，产生告警日志并定制推送，保证告警及时性。（提供产品相关功能页面截图并加盖原厂公章）；
	权限控制	支持管理员功能权限划、终端权限划分，实现不同权限人员查看不同功能模块，管理不同终端 。支持超级管理员预置及自定义权限角色。
		支持多管理员管理，同权限管理员共享数据。
		支持控制中心访问控制，包含 WEB 访问控制定制超时时间、登录重试次数、IP 锁定时长及解锁，IP 访问控制指定具体 IP 可访问控制中心。
	系统管理	支持管理员操作，日志记录追踪；支持控制中心-客户端交互操作，日志记录追踪，便于问题定位。
		▲支持定制磁盘管理规则，对审计、系统、终端、告警等日志即时或定期清理，实现磁盘瘦身。（提供产品相关功能页面截图并加盖原厂公章）；
客户端防护	病毒查杀	至少支持对终端内部文件进行全盘扫描、快速扫描，自定义扫描三种扫描能力。并具备空闲查杀、断点查杀、后台查杀等功能
		▲（截图）要求对流行病毒的检测能力必须超过 98%的检出率，超过 98%的清除率，小于 0.1%的误报率，需提供第三方测试证明。（提供产品相关功能页面截图并加盖原厂公章）；
		支持基于行为的检测和防护技术，支持对已知病毒、未知病毒的查杀能力，包括但不限于：木马病毒、变形病毒、勒索病毒、加壳病毒、宏病毒、注册表病毒、内存或服务类病毒等。
		支持对对压缩文件内的恶意文件扫描，包括但不限于对 Arj、bzip2、Lzh、Tar、Zip、Rar 等压缩文件格式类型查杀防护

		支持扫描和清除各种广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等。
		终端支持路径白名单，添加到信任区的文件扫描自动跳过信任目录，不作检测。
		支持病毒自动隔离备份功能，客户端能自动将病毒文件隔离到本地隔离区，同时支持恢复隔离文件。
		支持本地查杀缓存，提高查杀速度
		支持扫描压缩文件层级及大小设定、不扫描指定扩展名文件，提高扫描效率，降低资源占用。
		▲支持基于虚拟沙盒的高效的本地反病毒引擎， 实现极高的本地查杀能力。(提供产品相关功能页面截图并加盖原厂公章)；
		支持对 webshell 后门进行扫描检测 ， webshell 后门库数量大于 90000
	终端防御	▲支持虚拟补丁功能，针对网络数据流的深层分析，检测入站流量并保护应用程序免受攻击，有效阻止勒索病毒等高危威胁的入侵。(提供产品相关功能页面截图并加盖原厂公章)；
		▲支持内容拦截主动防御，当文件被执行、修改、访问时，反病毒引擎对相应文件进行扫描，如扫描到威胁则阻断用户对该恶意威胁的触碰并根据需要进行隔离操作。(提供产品相关功能页面截图并加盖原厂公章)；
		▲支持规则拦截主动防御，程序执行时，规则拦截层开始生效，并根据基础防护或自定义防护规则，对程序产生的违例动作进行拦截。(提供产品相关功能页面截图并加盖原厂公章)；
		▲支持行为拦截主动防御，当发现威胁时，行为拦截层阻止威胁进程及关联进程、线程的执行，并尽可能地回滚已经产生的潜在风险，实现病毒行为监控，软件安装拦截。(提供产品相关功能页面截图并加盖原厂公章)；
		▲支持内容过滤主动防御，解决网络数据包的安全威胁问题，基于内容过滤的防火墙，实现木马 盗号、钓鱼仿冒、虚假欺诈等各类潜在风险网站的拦截及潜在黑客攻击等恶意入侵行为拦截。(提供产品相关功能页面截图并加盖原厂公章)；
		▲支持全方位主机防护，包括防止指定文件项目被篡改、破坏或恶意创建，防止指定注册表项被恶意篡改，监控针对系统的敏感动作，拦

		截高风险动作，防止指定命令行被恶意利用，实时保护系统重要进程，对顽固留下病毒进行智能拦截等，出现破坏行为，根据策略定制进行自动阻止或自动允许或弹窗提示。(提供产品相关功能页面截图并加盖原厂公章)；
		支持 U 盘扫描修复功能，主动对 U 盘中的文件进行扫描，对 U 盘传播类恶意软件常见恶意修改操作进行修复，防止病毒通过 U 盘在终端传播有效保护终端不受病毒侵扰。
		支持下载保护功能，在下载过程中对文件进行检测，发现恶意程序立即弹窗阻止，并记录安全日志。防止病毒通过网络传播。
		支持 IP 黑名单能力，设为黑名单的 IP 将无法访问被策略保护的主机。
		支持终端对外攻击检测，根据网络攻击检测，自动阻止或记录攻击行为，避免用户的利益受到损害。
		支持终端防火墙功能，支持包括但不限于通过协议（TCP、UDP、ICMP、IGMP、GGP、PUP、IDP、ND、ESP、AH、RDP、GRE、SKIP、RAW），端口号，IP 地址、进出口方向等控制规则对终端进行防护，从网络层保护终端安全。
		支持基于 SMTP/POP3 协议的邮件监控，防止病毒通过邮件在终端传播，有效保护终端不受病毒侵扰。
		支持对终端内文件、邮件、网页一体化实时监控，防止病毒、木马、恶意程序等各途径传播运行；
		支持丰富扩展工具，有效管理文件、桌面、IE 的右键菜单；强制删除或彻底粉碎文件；轻松管理开机启动项目；扫描修复系统漏洞；全面清理系统垃圾文件；拦截程序的各类骚扰弹出；管理网络流量情况等，实现终端最优状态设置。
	客户端管理	能够设置终端卸载或脱离管理中心时要输入的密码，防止终端用户随意脱离保护
		客户端提供控制中心管理所需的相关数据信息，通讯加密
		支持客户端安全日志详细追踪及导出
资质要求	▲产品资质 （需提供证书复印件加盖厂家公章）	具有《计算机信息系统安全专用产品销售许可证》
		具有《信息技术产品安全测评证书,级别:EAL3+》
		具有《计算机软件著作权登记证》
	▲厂商资质 （需提供证书复印件	X 年软件支持服务和 X 年升级服务（X 由销售自定义）
		为保障项目的机密性，原厂商须具备涉密信息系统集成甲级资质；

	加盖厂家公章）	为保证项目设计及集成能力，设备原厂商须具有通信行业安全设计与集成二级资质证书；
		为保障厂商的售后服务水平，原厂商需获得 ISO27001 信息安全管理体系认证、ISO9001 质量管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证；
		为保证项目的应急响应能力，原厂商须具备网络安全应急服务支撑单位（国家级）资质；
		为保证项目安全服务能力，设备原厂商须具备国家信息安全认证信息安全服务资质证书（安全工程类三级），信息安全等级保护安全建设服务机构能力评估合格证书；
		为保证本项目后续的厂商培训能力，设备原厂商须具备专业的信息安全技术培训能力，并取得权威的培训资质，应具有国家信息安全测评授权培训机构资质证书。