# 主要产品技术参数

## 1.1、云智能安全监控系统

### 1.1.1、室内场景安全监控

采用高性能两百万像素1/2.8英寸CMOS图像传感器，低照度效果好，图像清晰度高

可输出200万（1920×1080）@25fps

★支持H.265编码，压缩比高，超低码流

★最大红外监控距离50米

★支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境

支持ROI，SMART H.264/H.265，灵活编码，适用不同带宽和存储环境

★网络断开；IP冲突；移动检测；视频遮挡；区域入侵；绊线入侵；场景变更；音频异常侦测；非法访问；电压检测；安全异常

★支持内置MIC

支持DC12V/POE供电方式，电压值12V，方便工程安装

支持IP67防护等级

### 1.1.2、室外安全巡航监控

采用200万1/2.9英寸CMOS图像传感器，F1.5超大光圈，使夜间监控效果更出色 最大支持1920×1080@30fps/1280×720@60fps/实时视频输出

★低码流传输，资源更节省（25帧1080P码流2M）

★支持GB/T 28181、ONVIF、CGI、PISA等各种网络协议，组网更方便

内置150米红外灯补光，采用倍率与红外灯功率匹配算法，补光效果更均匀

一体化结构设计，铝合金外壳，更坚固、耐用 垂直角度-20°～90°超大旋转范围，支持自动翻转 全铝散热设计，能适应-40～70℃的使用环境

★IP66防护等级，内置6000V防雷、防浪涌和防突破保护

多种网络监控方式相结合(手机、WEB、客户端)，使用更方便

灵活的网络扩展能力，适应各种网络平台监控系统

★SD卡本地存储，解决网络异常状态的监控存储问题,支持 NAS 存储录像，录像可断网续传 选用高性能红外灯，保证长时间稳定使用

### 1.1.3、人员甄别对比系统

★内置GPU芯片，支持深度学习算法，有效提升检测准确率

支持三种智能资源切换：通用行为分析、人脸检测、人数统计

★支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光

★支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图

支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁

★支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计

采用星光级低照度400万像素1/2.7英寸CMOS图像传感器，低照度效果好，图像清晰度高

最大可输出400万(2688×1520)@25fps

支持H.265编码，压缩比高，实现超低码流传输

★内置高效双光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米

支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境

支持ROI，SVC，SMART H.264/H.265，帧前滤波，灵活编码，适用不同带宽和存储环境

★支持一键撤防，可在自定义设置的时间段内对报警输出，邮件，音频，灯光等事件联动项进行统一撤防控制

★内置MIC和扬声器，最大支持256G Micro SD卡

支持DC12V/POE供电方式

支持IP67防护等级

### 1.1.4、人员出入对比系统

★内置GPU芯片，支持深度学习算法，有效提升检测准确率

支持三种智能资源切换：通用行为分析、人脸检测、人数统计

★支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光

★支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图

支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁

★支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计

采用星光级低照度400万像素1/2.7英寸CMOS图像传感器，低照度效果好，图像清晰度高

最大可输出400万(2688×1520)@25fps

支持H.265编码，压缩比高，实现超低码流传输

★内置高效双光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米

支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境

支持ROI，SVC，SMART H.264/H.265，帧前滤波，灵活编码，适用不同带宽和存储环境

★支持一键撤防，可在自定义设置的时间段内对报警输出，邮件，音频，灯光等事件联动项进行统一撤防控制

★内置MIC和扬声器，最大支持256G Micro SD卡

支持DC12V/POE供电方式

支持IP67防护等级

### 1.1.5、智能存储系统

★支持嵌入式Linux系统，工业级嵌入式微控制器

支持WEB、本地GUI界面操作

★可接驳支持ONVIF、PSIA、RTSP协议的第三方摄像机和主流品牌摄像机

支持IPv4、IPv6、HTTP、UPnP、NTP、SADP、SNMP、PPPoE、DNS、FTP、ONVIF（支持2.4版本）、PSIA网络协议

支持最大32路网络视频接入，网络性能接入320Mbps，储存320Mbps，转发320Mbps，开启智能时：接入/存储/转发为：160Mbps

支持16M/12M/4K/6M/5M/4M/3M/1080P/1.3M/720P IPC分辨率接入

支持2×12M/4×4K/6×5M/8×4M/11×3M/16×1080P/32×720P解码，最大支持16路视频回放

支持1路VGA输出，2路HDMI输出，支持VGA 1和HDMI 1同源输出，HDMI 2异源输出，4K分辨率输出

★支持4个内置SATA接口，单盘容量支持8T，可用容量≥29T

支持1个外置eSATA接口，用于录像和备份

支持IPC复合音频1路输入，支持语音对讲1路输出，支持PC通过NVR与网络摄像机进行语音对讲

支持16路报警输入、6路报警输出，支持开关量输入输出模式

支持3个USB接口（1个前置USB2.0接口、2个后置USB3.0接口）

★支持2个千兆以太网口，支持2个不同段IP地址的IPC设备接入，支持将双网口设置同一个IP地址，实现数据链路冗余

支持按时间、按事件等多种方式进行录像的检索、回放、备份，支持图片本地回放与查询；

★持标签自定义功能，设备支持对指定时间的录像进行标签并归档，便于后续査看

支持硬盘、外接USB存储设备、DVD刻录等存储方式，支持U盘，eSATA方式，DVD刻录备份方式

支持设备操作日志、报警日志、系统日志的记录与查询功能

★支持断网续传功能，能对前端摄像机断网这段时间内SD卡中的录像回传到NVR

支持即时回放功能，在预览画面下回放指定通道的录像

支持预览图像与回放图像的电子放大

采用通用协议，可以通过鼠标控制云台转动、放大、定位等操作

支持远程管理IPC功能，支持对前端IPC远程升级，支持远程对IPC的编码配置修改等操作

★支持远程零通道预览功能，可将接入的多路视频图像多画面显示在一路视频图像上

支持切片回放功能，将录像切片等分成若干段视频进行多路同时回放

支持走廊模式功能，支持IPC画面旋转90°或270°，成9:16走廊模式

支持客户端、WEB支持客户端和IPC对讲，语音透传

支持网络安全基线，在线网络云升级前端IPC/NVR

支持预览通道拖动保存

支持Smart IPC接入、绊线入侵、区域入侵、场景变化、移动侦测、人脸检测、物品遗留和物品搬移时，可给出报警/联动/上传，同时支持热度图，人数统计，车牌检测（支持卡口ITC、球机）

★支持前智能人脸检测识别、人体检测、视频结构化（目标检测）、通用行为分析、周界防范、双目客流

★支持2路人脸识别（1080p视频流）或8路人脸识别（图片流）比对报警，支持年龄，性别，表情，口罩，帽子，眼镜，面具，胡子人脸属性检测

★支持普通/陌生人糢式：当相似度达到/未达到预设阈值时，在客户端软件给出报警提示、蜂鸣、抓图、录像及日志记录

支持按通道及时间、结构化属性条件高级检索相关图片，可关联录像回放

支持以图搜图，最多8张目标人脸进行相似图片搜索，并设置相似度阈值检索

★支持人脸库，可通过U盘、客户端软件，并为图片编辑姓名、性别、生 日、省份、城市、证件类型、证件编号，最大创建20个人脸库（黑白名单），共导入2万张人脸图片，单库2万人脸实时布控

## 1.2、云智能安全准入系统

### 1.2.1、云智能准入系统

**1、系统层技术参数要求：**

可设置多个时间段，控制门锁启闭，每个时间段起始值任意定义；

数据支持双重备份，上传服务器备份、SD卡备份；

★图像抓拍功能：对于进出功能验证的人员，验证时抓拍现场实时图片，并把图片作为记录保存

★非法开门，强行开门，超时未关门等自动报警，合法人员在授权时间段以外试图开门时，视同非法处理；

★具备互锁、反潜功能

可设置门的不同工作状态；

开门延时可调；

可脱机或联网使用；

可以配置后备电池保证工作正常；

★采用 E²PROM技术，即使在行电状态下，也不会丢失任何数据，最长保存时间10年；

系统软件针对不同级别的操作人员分配多种级别的操作权限，不同的用户可进入不同的控制界面。

2）联动功能

★安防联动：开门动作（包括非法闯入，门锁被破坏）时，启动联动监视系统，发出实时报警信息可连接多个防区，连接的探头具有防撤的功能；

★消防联动：当出现火警时，自动打开相应区域通道；

3）集中管理

★发卡中心统一对人员二维码出入权限设置、更改、取消、恢复；

发卡中心可远程控制开门；

后台管理工作站可建立统一用户二维码资料库；

★实时采集每个出入口的进出资料（时间、人员、是否非法等相关信息），同时可按各用户进行汇总、查询、分类、打印等。

**2、管理控制器技术参数要求：**

★采用高速32位640MHZ高速CPU，配合32MBits RAM，256MBits Flash

嵌入式Linux操作系统。

★硬件平台/固件平台/应用软件平台将RFID与BIOMETRIC技术无缝整合。

强大的联动功能，支持硬件触发及事件触发。如，门状态、卡状态、输入输出点和卡号的组合联动。

插入式SD卡，双重数据备份，如遇系统故障，可恢复持卡人及事件记录。

★支持多人多组刷卡，如1个经理+3个值班员同时刷卡才允许进入。

支持首卡常开功能，在设置的时间段内，第一张刷卡后保持门常开。

采用真正的以太网加RS485工业总线双通讯技术，保证通讯的可靠性，具有自有的MAC地址，永不冲突。

采用B/S架构软件，无需安装客户端，操作更简单。

自带WebServer服务器，无须安装任何软件，即插即用

控制单门双向进出。

支持最多30，000个持卡人及100，000条脱机事件记录。

可灵活设置多个时间组、门状态、节假日和不同用户的各种开门权限。

支持多种Weigand卡格式，支持密码键盘，兼容各种卡片

控制器内置硬件看门狗，杜绝死机。

控制器电源输入具有过流、过压、反压保护

★门禁控制器具有多组辅助输入/输出接口，辅助输入接口可以连接报警前端设备，可以联动设置辅助继电器启动相关报警设备。

### 1.2.2、云智能消费系统

★显 示 屏：4.3寸触摸彩屏

★指纹采集器：LiveID指纹头

★通讯方式：TCP/IP,USB-HOST、RS232/485

面部容量：2500张

指纹容量：2000

录容量：100000条

摄 像 头：高分辨率红外和彩色双摄像头

电 源：12V 3A

### 1.2.3、云智能车辆识别系统

#### 1.2.3.1、系统功能要求

采用高清车牌识别摄像机对进入停车场的车辆进行车牌识别、图像抓拍，将车牌信息传输给专用控制器，再上传给电脑、引导车辆进入，并保存记录；在停车场出口通过高清车牌识别摄像机对驶出的车辆进行车牌识别、图像抓拍，在线状态通过计算机判断，对固定车自动放行，脱机状态有停车场控制器判断，对固定车辆放行，并保存记录，如果系统中有语音和显示屏，会驱动其播报和显示车辆信息。对于临时车根据停车时间进行管理，实现车辆的进出监控和管理。

★采用可靠自研技术，让月租车不受脱机脱网的影响，正常进出，语音显示屏人性化友好提示。

★临时车辆可脱机计时。

★在系统脱机脱网状态下，所有进场车辆记录保存在出入口控制器中，待网络恢复后，数据自动上传至数据库。

★视频流识别和地感触发识别可选，识别更科学

★模糊计算的应用，进一步提高系统的识别率，配合人性化的操作，系统更方便

#### 1.2.3.2、车辆识别主机

高速DSP嵌入式设备，内嵌识别软件包含了视频采集、图像预处理、车牌检测、车牌切分、字符识别、跟踪和缩、数据传输等模块，系统识别速度快，可靠性高。

★可对输入的两路视频分别进行车牌识别，根据不同的工程路视频可自选为车头或车尾模式识别，相互不受影响。

具有独立的两路视频接口，可同时输入两路不同的视频，输入的两路视频分别进行车牌识别；

★视频流逐帧识别，提取出视频中所存在的车牌号码信息、颜色信息，并同时提供相应的包含车辆的单帧或多帧图、车牌二值化图等信息；

提供车辆附加信息输出，如实时车牌大小以及位置信息；

提供图片预校正与精细校正功能；

★通过动态特征检测技术，实现无牌车的检测与抓拍；

★提供视频监控接口，完成实时视频传送功能；

提供识别结果的输出时间定制功能。

#### 1.2.3.3、车辆检测器

①用于出入口机的控制器

通过检测车辆的有无，来确定显示的内容、自动出卡机的发卡等。

②用于道闸防砸车

当车辆通过道闸的地感线圈后，地感处理器方可给道闸关信号，确保道闸关闸时防砸车的目的。

#### 1.2.3.4、智能道闸

工作电源：AC220V+10% 50HZ

电机功率：70W~150W

工作温度：-40℃ ~ 80℃

环境湿度：5% ~ 95%

配杆长度：≤6米直杆；≤6米曲杆；≤5.5米二栏；≤4.5米三栏

起落杆时间： 3秒，6秒（直杆）， 6秒（曲杆/栅栏杆）

可选配杆类别：直杆类：八角杆、四方杆、伸缩杆，豪华杆、彩光杆、连接杆、胶囊杆、防撞杆栅栏类：二栏杆、三栏杆

曲臂杆类：折杆90度、折叠杆180度

## 1.3、边界防控系统

### 1.3.1、网络防火墙

**基本要求：**

2U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 标配模块化双冗余电源；防火墙吞吐率：25Gbps并发连接数：500万

**性能参数要求：**

★支持路由、透明、混合与虚拟线部署（提供设备管理界面截图）；

支持静态路由、PBR与多播路由，以及RIPv1/2、OSPF、BGP等多种动态路由协议；

支持ISL、802.1Q二层协议封装以及VLAN-VPN功能；

★具有接口联动特性，使同一联动组内所有物理接口的UP/DOWN状态同步变化（提供设备管理界面截图）；

★支持多链路接入环境下的出站多运营商智能选路与入站智能DNS（提供设备管理界面截图）；

★支持服务器负载均衡功能，并至少提供10种以上服务器负载均衡算法（提供设备管理界面截图）；

能够基于访问控制策略对最大并发连接数限制；

★支持策略冲突检测功能（需提供界面截图与相关证明）；

具有防共享接入特性，能够有效识别、报警并阻断局域网网络共享行为；至少支持254个虚拟防火墙，虚拟防火墙支持IPv4/IPv6双栈部署，并能够实现IPv4/IPv6双栈的各种安全控制，

★虚拟防火墙同样支持策略自学习功能；（提供设备管理界面截图）

★支持系统管理员能够通过“用户名＋口令＋图形认证码”方式认证进行登录管理（提供设备管理界面截图）；

支持主备、负载均衡和连接保护等双机或多机的高可用性部署，可实现多心跳接口备份与负载均衡；支持基于接口度量值方式的双机切换条件设置

支持本地多配置文件存储及配置回滚功能，并且可以有选择性的下载“运行配置”、“保存配置”、“备份配置”、配置文件加密下载以及按对象、策略等分类的部分配置文件下载/上传功能；

支持主备、负载均衡和连接保护等双机或多机的高可用性部署（提供设备管理界面截图），可实现多心跳接口备份与负载均衡；支持基于接口度量值方式的双机切换条件设置

★具备WEB攻击防护能力，支持SQL注入攻击防护、XSS攻击防护，对常见的Web服务器环境Web入侵的脚本攻击工具（webshell）的拦截，包含ASPX、ASP、PHP、JSP等（提供设备管理界面截图）；

★为适应不同网络及应用环境，引擎检测模式可选择智能检测或深度检测，数据处理模式可选择应用优先或安全优先，并能够在丢弃报文时发送TCP reset命令（提供设备管理界面截图）；

★生产厂家具备TL9000认证证书

★生产厂家拥有CMMI5认证证书

★防火墙产品密码检测证书

★计算机信息系统安全专用产品销售许可证

国家信息安全测评信息技术产品安全测评证书EAL3+

中国国家信息安全产品认证证书（ISCCC）

★电信设备进网许可证

★计算机软件著作权登记证书

计算机软件著作权登记证书（TOS）

### 1.3.2、入侵检测系统

**基本要求：**

2个USB接口，1个RJ45串口，1个RJ45管理口，6个GE（Bypass）接口，1个接口扩展槽位，硬盘不小于1TB；必须内置硬件Bypass，吞吐量不能小于10Gbps

**性能参数要求：**

★系统应提供覆盖广泛的攻击特征库，能够针对9000种以上的攻击行为、异常事件，以及网络资源滥用流量，进行检测；系统携带的攻击特征库须获得CVE-Compatible兼容性认证。提供截图和证明

系统应能识别主流的应用程序，识别种类不少于2300种。

系统应提供入侵行为和应用软件特征的自定义接口，可根据用户需求定制对其它流量的检测规则。

★支持基于SCADA等工控协议的相关漏洞攻击检测。提供截图证明。

★系统应提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为。提供界面截图。

系统应支持IP碎片重组、TCP流重组、流量状态追踪技术，基于智能、深入的协议分析，全面检测超过100种以上的应用层协议，能够有效检测运行在非标准端口的协议、数以千记的木马，以及基于Smart Tunnel（智能隧道）的应用协议。

★系统应提供敏感数据外发的检测功能，能够识别通过自身的敏感数据信息（身份证号、银行卡、手机号等）。提供界面截图。

系统应提供关键文件外发防护功能，能够识别通过自身的关键文件，以防止非法外传行为。能识别的关键文件类型应包含至少以下几类：文档类如Excel、PDF、PowerPoint、Word等，压缩文件类如CAB、GZIP、RAR、ZIP、JAR等，图像类如BMP、GIF、JPEG等，音频视频类如MP3、AVI、MKV、MP4、MPEG、WMV等，脚本类如BAT、CMD、WSF等，程序类如APK、DLL、EXE、JAVA\_CLASS等。

★系统应具备攻击快照功能，详细记录触发告警的数据特征，以便做进一步的事件分析。提供界面截图。

★系统应支持“一键巡检”功能，可根据设备运行过程中反馈的数据进行全面分析，并生成图表相结合的安全报告。定时进行巡检可发现异常漏洞与受攻击情况，提供界面截图并加盖公章

系统应提供多种升级方式，至少提供实时在线升级、自动在线升级、离线升级的升级方式。

产品应通过国际权威机构NSS Labs的IPS专项测试，获得Approved认证。须提供有效证明材料。

产品应具有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》，提供有效证书的复印件。

★产品应具有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》，提供有效证书的复印件。

★产品应具有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》，并获得EAL3级别，提供有效证书的复印件。

产品应具有中国信息安全测评中心颁发的《IT产品信息安全认证证书》，提供有效证书的复印件。

★产品应具有IPv6 Ready Logo证书，提供有效证书的复印件。

★厂家应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全安全开发类二级服务资质证书。提供有效证书的复印件

★厂商应具备网络安全应急服务支撑单位证书（国家级）。提供有效证书的复印件

★厂商为微软MAPP成员，并有48小时内发布产品版本响应微软紧急安全公告能力。请提供微软官网截图证明。

### 1.3.3、WAF防火墙

**基本要求：**

系统硬件为全内置封闭式结构，稳定可靠，用户界面、配置和管理等，均为中文，易于理解，并有详尽的中文技术文档。不少于4个10/100/1000M电口(BYPASS)，1个接口扩展槽位，1个GE管理口，1个RJ45口；必须内置硬件Bypass；含交流冗余电源模块, 吞吐量≥2Gbps，应用层吞吐量≥200Mbps。

**性能参数要求：**

支持透明部署，旁路部署，反向代理模式以及镜像部署模式；支持虚拟化环境部署

支持针对主流Web服务器及插件的已知漏洞防护。Web服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS等。插件应覆盖:dedecms、phpmyadmin、PHPWind、shopex、discuz、ecshop、vbulletin、wordpress等，提供Java反序列化漏洞（Jboss）防护插件。

★支持慢速攻击防护。提供配置界面截图证明

支持敏感信息过滤，对用户的个人隐私信息（信用卡卡号、手机号、身份证号码）泄露进行检测、阻断或替换。

支持暴力破解防护，可针对指定URL进行暴力破解防护，支持多种方式的登陆，支持referer检测，支持阈值和检测周期的设置。

★基于自研技术实现的Web扫描防护，支持以统计算法分析扫描行为的扫描防护。提供配置界面截图证明和相关证书复印件

★基于自研技术，可以与同品牌SaaS扫描服务或者Web漏洞扫描器产品联动，在WAF上定期自动获取专家级、个性化的《WEB漏洞扫描报告》，并转化为WAF可执行的、有针对性的WEB安全防护策略。支持手动导入扫描结果，也支持在WAF上自动下发扫描任务，扫描完成后扫描结果自动上传WAF，提供配置界面截图证明和相关证书复印件

支持对攻击源地址的智能阻断，支持永久封禁或者自定义IP封禁时间（秒/分钟/小时），并且可以手工解除解禁。提供配置界面截图证明

★WAF可以和云中心进行联动，客户可通过下载手机APP，对设备进行状态监控，监控信息包括CPU、内存、规则库版本等。提供配置界面截图证明

支持紧急模式，可配置并发连接数阈值，当并发连接数超过设置阀值时，WAF自动进入紧急模式，已经代理的连接正常代理，对新增的请求不进行代理，直接转发，防止WAF成为访问瓶颈。当连接数恢复正常时，自动退出紧急模式。

产品具备《计算机信息系统安全专用产品销售许可证》，提供证书复印件证明。

产品具备《计算机软件著作权登记证》，提供证书复印件证明。

★产品具备《国家信息安全漏洞库-兼容性资质证书》，提供证书复印件证明

★产品具备《IT产品信息安全认证证书》，提供证书复印件证明

★厂商应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国网络安全审查技术与认证中心颁发的信息系统安全运维一级服务资质证书。提供有效证书的复印件

★厂商应获得CNCERT颁发的CNCERT/CC网络安全应急服务支撑单位证书。

### 1.3.4、数据防火墙

**基本要求：**

2U机箱， 最大配置为24个接口， 默认包括2个可插拨的扩展槽，2个SFP插槽和6个10/100/1000BASE-T接口（默认电口具有1组Bypass）， 双电源； 默认含企业版查杀病毒功能，包括企业版快速扫描防病毒查杀和企业版深度扫描防病毒查杀，含3年病毒库升级服务许可（快速+深度）。整机吞吐率：25Gbps最大并发连接数：500W；

**性能参数要求：**

内嵌双引擎杀毒技术，可单独采用流杀毒（快速扫描）引擎或文件型杀毒（深度扫描）引擎，也可同时支持两种杀毒引擎，能够根据不同的被检测协议采用不同杀毒引擎（截图证明）；能够防御病毒、木马、蠕虫，且支持对压缩数据、加壳病毒的查杀；

能够支持对SMTP、POP3、IMAP、HTTP和FTP协议进行病毒扫描和过滤，有效地防止可能的病毒威胁；

支持IPv4和IPv6双栈协议的病毒扫描和过滤；（截图证明）

★支持智能检测应用协议的病毒行为，采用智能方式准确扫描常用协议任意端口的病毒传输行为，而非通过传统手动配置协议端口绑定形式进行病毒扫描；（截图证明）

★支持多接口旁路的病毒传输监听检测方式，可并行监听并检测多个网段内的病毒传输行为，用于高吞吐量、高可靠性要求的旁路应用环境；（截图证明）

★支持通过采用java的 Commons FileUpload或其他类似控件的OA、CRM及其他基于WEB的应用系统（包括WEBMAIL）上传文件时的病毒查杀；（要求测试）

★要求提供病毒检测率不低于98%的第三方证明；（截图证明）

★采用国际国内知名主流品牌病毒库，并提供两家以上专业病毒厂商的授权证明文件，病毒库提供商应通过VB100认证（需能够在病毒库提供商的网站首页可查）；

★要求每种扫描引擎具有独立的病毒库（提供截图），病毒库总数大于600万（提供截图）；

要求具有独立的蠕虫防护规则库，并可通过手动或自动方式进行升级；（截图证明）

采用邮件地址与IP地址的黑、白名单技术实时检测垃圾邮件并阻止其进入企业网络，为企业节省宝贵的带宽；

★生产厂家拥有TL9000认证资质

★生产厂家拥有CMMI5认证资质

### 1.3.5、外网网络防火墙

**基本要求：**

2U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 标配模块化双冗余电源；防火墙吞吐率：25Gbps并发连接数：500万

**性能参数要求：**

★支持路由、透明、混合与虚拟线部署（提供设备管理界面截图）；

支持静态路由、PBR与多播路由，以及RIPv1/2、OSPF、BGP等多种动态路由协议；

支持ISL、802.1Q二层协议封装以及VLAN-VPN功能；

★具有接口联动特性，使同一联动组内所有物理接口的UP/DOWN状态同步变化（提供设备管理界面截图）；

★支持多链路接入环境下的出站多运营商智能选路与入站智能DNS（提供设备管理界面截图）；

★支持服务器负载均衡功能，并至少提供10种以上服务器负载均衡算法（提供设备管理界面截图）；

能够基于访问控制策略对最大并发连接数限制；

★支持策略冲突检测功能（需提供界面截图与相关证明）；

具有防共享接入特性，能够有效识别、报警并阻断局域网网络共享行为；至少支持254个虚拟防火墙，虚拟防火墙支持IPv4/IPv6双栈部署，并能够实现IPv4/IPv6双栈的各种安全控制，

★虚拟防火墙同样支持策略自学习功能；（提供设备管理界面截图）

★支持系统管理员能够通过“用户名＋口令＋图形认证码”方式认证进行登录管理（提供设备管理界面截图）；

支持主备、负载均衡和连接保护等双机或多机的高可用性部署，可实现多心跳接口备份与负载均衡；支持基于接口度量值方式的双机切换条件设置

支持本地多配置文件存储及配置回滚功能，并且可以有选择性的下载“运行配置”、“保存配置”、“备份配置”、配置文件加密下载以及按对象、策略等分类的部分配置文件下载/上传功能；

支持主备、负载均衡和连接保护等双机或多机的高可用性部署（提供设备管理界面截图），可实现多心跳接口备份与负载均衡；支持基于接口度量值方式的双机切换条件设置

★具备WEB攻击防护能力，支持SQL注入攻击防护、XSS攻击防护，对常见的Web服务器环境Web入侵的脚本攻击工具（webshell）的拦截，包含ASPX、ASP、PHP、JSP等（提供设备管理界面截图）；

★为适应不同网络及应用环境，引擎检测模式可选择智能检测或深度检测，数据处理模式可选择应用优先或安全优先，并能够在丢弃报文时发送TCP reset命令（提供设备管理界面截图）；

★生产厂家具备TL9000认证证书

★生产厂家拥有CMMI5认证证书

★防火墙产品密码检测证书

★计算机信息系统安全专用产品销售许可证

国家信息安全测评信息技术产品安全测评证书EAL3+

中国国家信息安全产品认证证书（ISCCC）

★电信设备进网许可证

★计算机软件著作权登记证书

计算机软件著作权登记证书（TOS）

### 1.3.6、外网入侵检测系统

**基本要求：**

2个USB接口，1个RJ45串口，1个RJ45管理口，6个GE（Bypass）接口，1个接口扩展槽位，硬盘不小于1TB；必须内置硬件Bypass，吞吐量不能小于10Gbps

**性能参数要求：**

★系统应提供覆盖广泛的攻击特征库，能够针对9000种以上的攻击行为、异常事件，以及网络资源滥用流量，进行检测；系统携带的攻击特征库须获得CVE-Compatible兼容性认证。提供截图和证明

系统应能识别主流的应用程序，识别种类不少于2300种。

系统应提供入侵行为和应用软件特征的自定义接口，可根据用户需求定制对其它流量的检测规则。

★支持基于SCADA等工控协议的相关漏洞攻击检测。提供截图证明。

★系统应提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为。提供界面截图。

系统应支持IP碎片重组、TCP流重组、流量状态追踪技术，基于智能、深入的协议分析，全面检测超过100种以上的应用层协议，能够有效检测运行在非标准端口的协议、数以千记的木马，以及基于Smart Tunnel（智能隧道）的应用协议。

★系统应提供敏感数据外发的检测功能，能够识别通过自身的敏感数据信息（身份证号、银行卡、手机号等）。提供界面截图。

系统应提供关键文件外发防护功能，能够识别通过自身的关键文件，以防止非法外传行为。能识别的关键文件类型应包含至少以下几类：文档类如Excel、PDF、PowerPoint、Word等，压缩文件类如CAB、GZIP、RAR、ZIP、JAR等，图像类如BMP、GIF、JPEG等，音频视频类如MP3、AVI、MKV、MP4、MPEG、WMV等，脚本类如BAT、CMD、WSF等，程序类如APK、DLL、EXE、JAVA\_CLASS等。

★系统应具备攻击快照功能，详细记录触发告警的数据特征，以便做进一步的事件分析。提供界面截图。

★系统应支持“一键巡检”功能，可根据设备运行过程中反馈的数据进行全面分析，并生成图表相结合的安全报告。定时进行巡检可发现异常漏洞与受攻击情况，提供界面截图并加盖公章

系统应提供多种升级方式，至少提供实时在线升级、自动在线升级、离线升级的升级方式。

产品应通过国际权威机构NSS Labs的IPS专项测试，获得Approved认证。须提供有效证明材料。

产品应具有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》，提供有效证书的复印件。

★产品应具有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》，提供有效证书的复印件。

★产品应具有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》，并获得EAL3级别，提供有效证书的复印件。

产品应具有中国信息安全测评中心颁发的《IT产品信息安全认证证书》，提供有效证书的复印件。

★产品应具有IPv6 Ready Logo证书，提供有效证书的复印件。

★厂家应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全安全开发类二级服务资质证书。提供有效证书的复印件

★厂商应具备网络安全应急服务支撑单位证书（国家级）。提供有效证书的复印件

★厂商为微软MAPP成员，并有48小时内发布产品版本响应微软紧急安全公告能力。请提供微软官网截图证明。

### 1.3.7、外网数据防火墙系统

**基本要求：**

2U机箱， 最大配置为24个接口， 默认包括2个可插拨的扩展槽，2个SFP插槽和6个10/100/1000BASE-T接口（默认电口具有1组Bypass）， 双电源； 默认含企业版查杀病毒功能，包括企业版快速扫描防病毒查杀和企业版深度扫描防病毒查杀，含3年病毒库升级服务许可（快速+深度）。整机吞吐率：25Gbps最大并发连接数：500W；

**性能参数要求：**

内嵌双引擎杀毒技术，可单独采用流杀毒（快速扫描）引擎或文件型杀毒（深度扫描）引擎，也可同时支持两种杀毒引擎，能够根据不同的被检测协议采用不同杀毒引擎（截图证明）；能够防御病毒、木马、蠕虫，且支持对压缩数据、加壳病毒的查杀；

能够支持对SMTP、POP3、IMAP、HTTP和FTP协议进行病毒扫描和过滤，有效地防止可能的病毒威胁；

支持IPv4和IPv6双栈协议的病毒扫描和过滤；（截图证明）

★支持智能检测应用协议的病毒行为，采用智能方式准确扫描常用协议任意端口的病毒传输行为，而非通过传统手动配置协议端口绑定形式进行病毒扫描；（截图证明）

★支持多接口旁路的病毒传输监听检测方式，可并行监听并检测多个网段内的病毒传输行为，用于高吞吐量、高可靠性要求的旁路应用环境；（截图证明）

★支持通过采用java的 Commons FileUpload或其他类似控件的OA、CRM及其他基于WEB的应用系统（包括WEBMAIL）上传文件时的病毒查杀；（要求测试）

★要求提供病毒检测率不低于98%的第三方证明；（截图证明）

★采用国际国内知名主流品牌病毒库，并提供两家以上专业病毒厂商的授权证明文件，病毒库提供商应通过VB100认证（需能够在病毒库提供商的网站首页可查）；

★要求每种扫描引擎具有独立的病毒库（提供截图），病毒库总数大于600万（提供截图）；

要求具有独立的蠕虫防护规则库，并可通过手动或自动方式进行升级；（截图证明）

采用邮件地址与IP地址的黑、白名单技术实时检测垃圾邮件并阻止其进入企业网络，为企业节省宝贵的带宽；

★生产厂家拥有TL9000认证资质

★生产厂家拥有CMMI5认证资质

### 1.3.8、网络查验交换系统

**基本要求：**

2U机架式设备，含1个RJ45串口，1个GE管理口，6个千兆电口，1个接口扩展槽位，标准配置提供1路授权监听口。

**性能参数要求：**

★支持基于域名、关键字等多种组合的主动内容审计策略，可扫描指定网站，分析网页页面是否含有非法敏感信息。要求提供相关证明。

★通过扫描指定网站，分析检测网页是否被挂马，并实时告警响应记录。提供界面截图证明

★支持审计ORACLE、SQL Server、MY SQL、DB2、Sybase、Informix、Postgresql等各类主流数据库系统。提供界面截图证明

通过对互联网资源（域名、IP地址、URL等）进行威胁分析和信誉评级，将含有恶意代码的网站列入Web信誉库，达到识别含有恶意代码的高风险网站，实现对终端用户的安全评估和保护。

支持HTTP网页浏览及关键字搜索审计：记录用户网站访问行为包括源IP地址、目的IP地址、访问时间、URL、网页浏览时间等，并提供网页还原功能。

★支持无线热点发现功能，能够实时、自动发现办公网络内的无线热点，记录无线热点访问网络时所使用的IP地址、认证用户等信息。提供界面截图证明

★用户身份信息智能关联技术，可将用户各种身份信息与其终端IP地址进行智能关联形成用户身份信息库，从而提高事件定位的精确度。提供界面截图证明

基于B/S的管理架构，灵活方便，适合在任何IP可达地点远程管理

针对接入外网的终端用户，系统提供增强的身份认证功能，支持标准的radius和LDAP接口，及第三方认证平台，实现更灵活、更安全的认证控制。提供界面截图证明

★支持历史版本回滚功能，系统内建历史版本库，可保留最近升级的两个历史版本，并支持回滚到任一历史版本，提高了产品升级过程的可靠性。

产品具备公安部《计算机信息系统安全专用产品销售许可证》 网络安全审计类（增强级）

产品具备中国信息安全认证中心的《中国国家信息安全产品认证证书》（增强级）

产品具备中国信息安全测评中心《国家信息安全测评信息技术产品安全测评证书》（EAL3+）

★厂商为微软MAPP成员，并有48小时内发布产品版本响应微软紧急安全公告能力。请提供微软官网截图证明。

★厂家应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全安全开发类二级服务资质证书。提供有效证书的复印件

★厂商应具备网络安全应急服务支撑单位证书（国家级）。提供有效证书的复印件

### 1.3.9、运维日志交换系统

**基本要求：**

准式机架硬件设备，全内置封闭式结构，具有完全自主知识产权的专用安全操作系统, 包含1个RJ45串口，2个千兆电口，2个接口扩展槽位，含冗系统余电源，系统SATA硬盘容量应不低于4TB；系统授权审计40个日志源接入。

**性能参数要求：**

系统应基于大数据平台架构，具备海量数据收集与快速检索能力

系统应基于B/S架构，支持SSL加密模式访问，可通过web方式直接对系统进行管理

★系统应支持内置采集器，不依赖其他设备即可进行日志采集，请提供截图。

系统支持的数据采集方式包括但不限于SYSLOG、RSYSLOG、SNMP Trap、FTP、ODBC、JDBC、Net flow、WMI、二进制数据、专用Agent等方式采集日志

★系统应支持界面配置即可完成未识别日志接入，无需编写xml，请提供截图。

★系统应支持范式化日志多级提取，请提供截图

★系统应支持正则、KV、格式串等多种灵活的提取方式，请提供截图

系统应能够实现对海量日志数据快速查询。

★系统应能够实现范式化日志的枚举值管理，实现对范式化日志字段的灵活翻译，请提供截图。

★系统应提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源IP信息，请提供截图。

系统应支持日志备份远程服务器，如传送到FTP服务器，请提供截图。

系统应支持实时日志查询、历史日志查询

系统应内置事件分类，并支持自定义事件分类，可定义事件分类的风险级别。

系统应内置丰富的事件规则，应支持自定义事件规则，请提供截图。

★系统应支持告警抑制，请提供截图。

★计算机软件著作权登记证书

★公安部销售许可证-日志分析三级

★国家信息技术产品安全测评证书（EAL3+）

★IPv6 Ready Logo认证

★厂商应具备网络安全应急服务支撑单位证书（国家级）。提供有效证书的复印件

★厂商为微软MAPP成员，并有48小时内发布产品版本响应微软紧急安全公告能力。提供官网截图证明

★厂商应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全服务安全开发类二级服务资质证书。提供有效证书的复印件

### 1.3.10、系统数据扫描交换系统

**基本要求：**

系统使用专门的硬件，基于嵌入式安全操作系统，系统采用B/S架构设计，保证系统的工作效率和自身安全性, 含1个RJ45串口，1个GE管理口，4个10M/100M/1000M自适应以太网电口扫描口，4个千兆SFP槽位，标准配置提供1路授权扫描端口。授权扫描总数量为64个无限制范围的IP地址或域名。

**性能参数要求：**

★漏洞知识库漏洞信息大于170000条, 提供详细的漏洞描述和对应的解决方案描述。 提供功能截图。

支持扫描国产操作系统、应用及软件的安全漏洞，如红旗、麒麟、起点操作系统。

支持专门针对DNS服务的安全漏洞检测，包括DNS投毒等漏洞检测能力；支持“幽灵木马”检测。

★提供高级漏洞模板过滤器，支持将符合筛选条件的漏洞自动加入到自定义漏洞模板中，及后续插件升级包中的漏洞也可以自动加入到模板中。提供功能截图。

支持扫描时间段控制，只在指定时间段内执行任务，未完成任务在下一时间段自动继续执行，请提供功能截图。

★支持风险告警和风险闭环处理，可在集中告警平台灵活配置告警内容、告警方式、告警资产范围等，支持邮件和页面告警，支持单个或批量修改风险状态，请提供功能截图。

产品提供Web应用扫描能力，提供多种Web应用漏洞的安全检测，如SQL注入、跨站脚本、网站挂马、网页木马、CGI漏洞等。

具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典，请提供功能截图。

★提供与漏洞扫描相关的公开专利，要求数量不少于5个

★投标产品应该是被广泛应用的成熟产品，在国内市场具有较高的市场份额，在IDC市场调查数据中需要在近三年连续市场占有率排名在前3名之内，须提供有效证明材料。

★产品具备中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》，提供有效证书的复印件

产品具备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》, 级别为EAL3+，提供有效证书的复印件

★产品具备全球IPv6测试中心颁发的《IPv6 Ready Logo 认证》证书，提供有效证书的复印件

★厂商为微软MAPP成员，并有48小时内发布产品版本响应微软紧急安全公告能力。请提供微软官网截图证明。

★厂家应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全安全开发类二级服务资质证书。提供有效证书的复印件

★厂商应具备网络安全应急服务支撑单位证书（国家级）。提供有效证书的复印件

### 1.3.11、运维数据审核交换系统

**基本要求：**

1U机箱，6个千兆电口，1TB存储空间，单电源、50个主机许可，用户数不限制

**性能参数要求：**

支持用户多角色划分功能，支持用户的批量导入/导出，按用户类型等分组方式；支持用户安全策略功能，如密码锁定次数、密码有效期、密码复杂度、用户有效期、用户登录时间限制、用户登录IP范围等。

支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP；可通过应用发布的方式进行协议扩展，如数据库Oracle/MSSQL/MySQL/DB2等运维客户端工具、VMware vSphere Client/AS400等远程管理工具。

支持本地静态密码、AD、LDAP、RADIUS等认证方式登录堡垒机，支持同步AD/LDAP用户.

支持单个用户同时使用2种认证方式，如同时使用AD/LDAP用户名+AD/LDAP密码+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

Web访问方式：至少支持使用三种及以上浏览器打开堡垒机的Web页面直接调用mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等运维客户端工具。

支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志。

支持通过基于时间、IP/IP段、用户/用户组、设备/设备组、设备账号、命令关键字、命令关键字正则表达式、危险级别、黑白名单等组合访问控制策略，授权用户可访问的目标设备。

支持系统日志报表统计功能，包括但不限于登录日志统计、配置日志统计、运维访问日志统计等，可以导出报表

产品需获得公安部产品销售许可证

### 1.3.12、网络侦测交换系统

**基本要求：**

千兆电口数量≥10，千兆Combo接口（光电复用）数量≥4，硬盘容量≥500G，支持冗余电源，支持1个存储卡扩展插槽。网络吞吐量≥6Gbps

**性能参数要求：**

支持路由模式、透明（网桥）模式、旁路模式、混合模式，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；

支持静态路由、策略路由、动态路由、ISP路由；

支持IPv6数据包安全检测机制，可有效防御异常包攻击

★支持7元组的链路负载均衡策略，支持基于域名进行链路负载，负载算法包括但不少于优先级和权重，提供web配置截图证明

★支持单用户全天行为分析报表，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息，提供web界面截图；

支持主流P2P、IM、在线视频、网络游戏、网络炒股等应用识别，可识别应用数大于3500种；

支持应用、用户流量统计，应用流量支持趋势图、饼状图呈现，可查看某一应用的流量趋势图和其Top流量用户

★支持Portal逃生，支持选择不逃生、全部用户逃生和已认证用户逃生等方式；可基于PING、TCP、DNS等方式探测认证服务器。以上参数提供web配置界面截图

★支持针对不同的认证方式配置独立的强制重新认证间隔和认证无感知间隔；提供web配置截图证明

规则库超过4000条，支持系统规则库手动、自动升级

★支持本地安全防护，包括但不限于入侵防御、病毒查杀、DDOS、异常包防护等，提供web配置界面截图

支持U盘零配置上线，设备端无需预配置，将U盘插入设备USB接口中，即可实现快速上线实施；支持导入多份配置文件，用于业务需求，变更业务运行，保障可靠性

★产品需具备公安部颁发的《计算机信息系统安全专用产品销售许可证》(国标-增强级)

★产品需具备国家版权局颁发的《计算机软件著作权等级证书》

★厂家应与微软公司合作，具有MAPP合作伙伴资质，应用微软提供的恶意样本信息；提供有效证书的复印件

★厂家应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全安全开发类二级服务资质证书。提供有效证书的复印件

★厂商应具备网络安全应急服务支撑单位证书（国家级）。提供有效证书的复印件

备注：以上性能参数要求提供的相关资质证明文件、截图等材料复印件需加盖原厂鲜章，否则视为未提供。