## 采购需求

## 1业务需求分析

公共安全视频监控建设联网应用根据业务模式可分为社会治理应用与行业主管部门视频服务应用，通过技防设施前端数据采集及联网应用、视频大数据分析、前后端结合智能应用及应急通信指挥联动构建多位一体、主动智能、集约高效、调度迅速、处置有力的现代化技防能力，作为社会治安防控体系建设的重要手段。

### 1.1社会治理应用

以加强社会公共安全管理，提高城市应急指挥能力，创建综治智慧防控信息平台为总体目标，夯实社会治安防控体系的技术基础，使其成为政府应对突发事件和社会面综合防控的重要技术保障。根据已建和新建点位的整体布局，结合各个单位的应用需求，统筹规划指导选择新建视频监控点位；建成覆盖全县的政法委综治办多级信息联网系统，服务于纵向贯通、横向集成、分级应用的社会治安综合治理信息化系统建设需要，促进综治中心建设实体化实战化，最终实现“收集研判、指挥调度、监管考核、群防群治”的应用目标。

在治安管理方面，通过推进视频监控系统的建设和应用，实现全天候、无死角的社会治安防控网，不受时间和天气状况的限制，及时发现异常情况，对辖区的治安和人口管理起到非常重要的作用。

在应急指挥方面，处置重大安保活动、重大警情、群体性事件时，基于公共安全视频图像信息共享平台、启动现场指挥联动机制，第一时间掌握情况，做到指令准确及时、处置恰当。

### 1.2视频联网需求

通过共建共享，扩大各部门的监控范围，避免重复投资和利用。参考国家及地方标准推进视频监控传输、交换、控制建设，积极探索数据共享机制，打破信息壁垒，为政府级大数据打下基础。

公共视频监控联网共享平台建设需遵照国家标准GB/T 28181-2016《公共安全视频监控联网系统信息传输、交换、控制技术要求》、海南标准DB46/T 258-2013《海南省公共安全视频监控系统技术规范》和《海南省公共安全视频监控联网共享应用建设方案》（琼信组办[2018]30 号）。

## 2信息资源建设需求分析

### 2.1信息资源内容需求

建设陵水黎族自治县综治智慧防控信息平台，需要建设公共视频监控联网共享平台，汇聚接入陵水县各级政府单位及社会面建设的视频监控资源，并与相关政府单位实现信息的交换共享。

其中公共视频监控联网共享平台按照《海南省公共安全视频监控联网共享应用建设方案》（琼信组办[2018]30 号）要求建设。

与其他政府部门业务系统对接有两种方式：

（1）如单位系统连接了省工信厅数据交换平台，则通过省工信厅数据交换平台进行数据交换，实现横向及纵向部门间数据交换及共享。

（2）没有连接省工信厅数据交换平台的，则数据交换与共享是一个由主中心前置服务器与各个部门的前置服务器通过政务外网连接组成的系统。

根据访问方式的不同，系统提供同步传输、异步传输等数据传输机制：提供跨防火墙的数据库同步。通过数据采集接口软件，将政府各部门的数据通过数据采集与整合统一汇集到综治信息平台，进行整合、处理后，进入数据库。

陵水黎族自治县综治平台数据主要来源于以下几个方面：

（1）现在已经存在的历史数据，包括社会治理网格化基础的“人、地、事、物、组织”相关数据，对于已有的历史数据，在采集时可以根据具体情况采取使用专业的ETL（抽取、转换、加载）工具软件、报盘、填表三种方法。

（2）各级单位上报的相关数据。

（3）日常增量数据采集：需要不断的采集到平台中去。

### 2.2业务协同需求

本期建设陵水县公共安全视频监控联网应用综治共享分平台需要对接综治办前期建设的社会管理综合信息平台，实现业务协同。

# 3信息交换与共享需求

本期建设陵水县公共安全视频监控联网应用综治共享分平台负责本级事权二、三类点（社会面）公共安全视频资源的接入，纵向级联省视频监控联网应用综治共享平台和乡镇（街道）、行政村（社区）视频监控汇聚交换节点，横向对接县公安局视频图像信息联网共享分平台和县已建行业主管部门视频监控管理平台，并负责推送二、三类点公共安全视频监控资源。实现全县监控视频的资源目录、统一调阅、存储、安全、校时、权限、视频图像解析等功能。

# 4网络建设和部署需求

## 4.1整体网络结构

根据陵水县公共安全视频监控联网应用整体发展需求，公共安全视频监控建设联网应用网络平台的设计，采用先进、可靠、安全、经济的技术和设备；建设成支持多业务系统的包括支持数据、语音、视频等多种信息于一体的网络平台系统。

传输网络系统主要作用实现各类视频监控资源的接入和共享，为中心管理平台的各项应用提供基础保障，能够更好的服务于各类用户。

依托电子政务外网承载建设公共安全视频监控联网应用综治共享分平台，平台部署在陵水县政务云平台。在陵水县综治中心部署两台高性能核心交换机作为出口，用于与省级频监控联网应用综治共享平台对接，并与陵水县其他部门相关系统互联，达到信息共享，互联互通的目的。

整体网络结构分为核心层（县综治中心）和汇聚层（乡镇综治中心）两层架构。

## 1.2与其他网络的接口

承载网络层主要是用于提供部署在不同位置的系统各个网元之间的网络传输链路，根据业务传输的不同需求，可包括：视频传输专网、电子政务外网、公安视频专网、互联网和移动互联网等网络。

按海南省对于相关网络的规划定位，即“电子政务外网实现了对政府相关职能部门视频资源的汇聚和共享，公安视频专网实现对公安视频资源的汇聚资源和共享”的要求，政府新建的视频点位都通过电子政务外网或公安视频专网进行接入。

## 4.3网络传输带宽

结合项目实际需求，传输网络带宽设计应能满足前端设备接入和视频监控应用共享的带宽需求，主要包括与各级综治信息化平台、政府其它职能部门、用户终端接入综治中心的带宽要求，并留有余量：

公安局视频共享并发数不低于20路，建议带宽至少100兆以上。

## 4.4IP地址规划

（1）IP地址分配原则：

唯一性：一个IP网络中不能有两个主机采用相同的IP地址；

简单性：地址分配应简单易于管理，降低网络扩展的复杂性，简化路由表的款项；

连续性：连续地址在层次结构网络中易于进行路径叠合（Route Summarization），大大缩减路由表，提高路由算法的效率；

可扩展性：地址分配在每一层次上都要留有余量，在网络规模扩展时能保证地址叠合所需的连续性；

灵活性：地址分配应具有灵活性，可借助变长子网掩码技（VLSM-Variable-Length Subnet Mask），以满足多种路由策略的优化，充分利用地址空间。

（2）IP地址规划：

IP地址规划应遵循唯一性、连续性、可扩充性、结构化、可互连性等原则。

RFC 1597规定了三个专门用于内部网络（Private Network） 的保留IP地址块，即：

A类：10.0.0.0 - 10.255.255.255；

B类：172.16.0.0 - 172.31.255.255；

C类：192.168.0.0 - 192.168.255.255。

综治中心公网地址为202网段，具体施工时IP分配由业主方和施工方共同协商确定，以满足与综治中心现有IP规划对接互通。

## 4.5数据资源需求

本期建设平台需要接入全县公共安全视频监控资源（分期建设）和省级平台，实现全县监控视频的资源目录、统一调阅、存储、安全、校时、权限、视频图像解析等功能。

## 4.6云服务需求

本项目租用陵水县政务云平台资源。

## 5其他需求分析

### 5.1性能需求

#### 5.1.1网络性能要求

网络子系统包括视频资源的接入和应用的共享网络，基层治安综合治理平台包含了视频、图片、数据等数据类型，并同时运行实时视音频查看/编码/传输、视音频存储、历史视频回放等业务，在提供用户更直观的体验及监控手段的同时，也给承载网络带来了巨大压力。

参考GB/T 28181-2016《公共安全视频监控联网系统信息传输、交换、控制技术要求》，网络性能基本要求如下：

（1）网络带宽要求

视频传输的网络带宽设计应能满足前端设备接入监控中心、用户终端接入监控中心的带宽要求，并留有余量。本项目中1080P采用H.265编码方式，4Mbps的码流进行计算。

（2）网络质量要求

联网系统 IP 网络的传输质量（如传输时延、包丢失率、包误差率、虚假包率等）应符合如下要求：

网络时延上限值为400ms；

时延抖动上限值为50ms；

丢包率上限值为1×10-3；

包误差率上限值为1×10-4。

#### 5.1.2传输协议要求

（1）网络传输协议的要求

视频图像信息系统网络层应支持IP协议，传输层应支持TCP和UDP协议。

（2）媒体传输协议要求

视音频流在基于IP的网络上传输时应支持RTP/RTCP协议；视音频流的数据封装格式应符合GB/T 28181中的要求。

（3）会话协商和媒体信息传输协议要求

第三方视频系统级联的会话协商和媒体协商信息应采用SIP消息的消息体携带传输，SIP消息应支持基于UDP和TCP的传输。具体传输协议要求遵循GA/T669-2008第五部分信息传输、交换、控制技术要求。

#### 5.1.3视频图像要求

（1）视频编解码要求

网络视频镜头编码应支持H.265视频编码标准，视频解码应支持H.265视频解码标准。H.265码流应为符合Constrained Baseline Profile（受限基本档次）的码流。

视音频流采用RTP/RTCP/RTSP协议传输。

（2）图像分辨率与帧率要求

编码、传输和存储的图像数据不低于1080P（1280×720）格式的图像分辨率，重要目标图像应具有不低于1080P（1280×720）图像分辨率。

实时视频图像及存储视频图像帧率不低于25帧/秒（PAL制式）。

（3）视频图像存储

根据相关要求，视频图像存储时间不小于30天。

重要案事件视频图像保存时间更长，关键录像资料可采用刻录方式离线长时间保存，案件的存储时间不小于1年。

#### 5.1.4响应时间要求

（1）视频图像显示：在不高于2秒内，显示调看的相关视频图像。

（2）镜头控制响应：在不高于1秒内，视频镜头响应控制。

（3）监控点资源搜索：在不高于4秒内，完成指定条件视频监控点的搜索。

（4）录像提取时间：录像提取时间要求小于5秒。

（5）前端设备与信号直接接入的监控中心相应设备间端到端的信息延迟时间应不大于2s。

1. 前端设备与用户终端设备间端到端的信息延迟时间应不大于4s。

### 5.2安全需求

按照GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》的要求，暂定本项目的安全定级为等保三级。

保障视频共享平台业务安全、设备安全、网络边界安全、终端安全、应用安全、数据安全等，做到设备可知、入网可信、边界可控、行为可查。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **货物名称** | **功能性能及规格基本要求** | **单位** | **数量** |
| 1 | 综治联网共享平台 | 1. 行业视频资源和社会面视频资源整合，包括视频联网共享基础功能，如视频监控资源接入、传输、共享和视频资源目录、调阅、存储、安全、权限等；具备20000路视频共享接入能力。

2、平台门户：支持用户自定义快捷入口；支持支持自定义菜单内容，支持平铺及分类两种菜单展示模式；支持页面元素设置，支持上传页面logo图标、修改网站标题、设置并添加网站外部链接；3、统一认证：支持用户名密码认证方式及PKI认证方式；4、权限管理：支持用户管理、部门管理、角色管理；支持设置用户权限信息；支持设置用户登录认证密码、认证方式、在线策略及登录地址绑定等；5、资源目录管理：支持区域目录管理及资源管理；支持国标目录、模板导入目录、自定义目录等目录类型；6、日志管理：支持操作日志、系统日志的存储和查询；7、时间同步：支持通过NTP服务对前端摄像机、平台服务器进行时间同步。视频基础应用模块8、支持视频预览、视频巡查、录像回放、云台控制；9、支持推荐、历史观看点位，收藏夹和预案设置展示；10、支持画面抓图、录像、电子放大、3D放大、云台控制、打开声音、打开对讲、切换主子码流、打开视频智能信息、一键上墙、点位分享、切换录像回放、关闭画面等功能，抓图时支持上传至暂存架；11、支持实时监控预览上墙、回放上墙、桌面上墙功能。12、▲支持点位周边搜索，在地图上自由选择当前等点位周边点位，并支持对所选点位进行预览、回放、收藏、定位到资源树及查看属性(提供公安部授权检测机构出具的有效检验报告复印件，并加盖厂家公章或投标专用章)13、▲支持录像分段回放功能，可以将录像文件等分成多个片段同时回放，通过分割点的图像差异，快速确定回放关键录像时段。(提供招公安部授权检测机构出具的有效检验报告复印件，并加盖厂家公章或投标专用章)14、▲支持针对一段录像进行标签标注(提供公安部授权检测机构出具的有效检验报告复印件，并加盖厂家公章或投标专用章) | 套 | 1 |
| 2 | 流媒体转发软件 | 1.集成高性能一体化软件平台，集DMS、SS、MTS、ARS、PCPS、MES于一体；2、支持2700Mbps的视频流的接入，支持2700Mbps的视频流的接入；支持HLS(HTTP LIVE STREAM)协议转发；3、支持流媒体负载均衡和N+M备份保护，防止因部分流媒体服务故障影响系统取流业务的稳定性。 | 套 | 1 |
| 3 | 一机一档管理系统 | 1.通过与GIS地图引擎、移动app深入融合，构建了一套便捷、可视、稳定的监控点资产档案管理系统，实现监控点属性采集、录入、管理、查询、展示等功能。 | 套 | 1 |
| 4 | 视频质量诊断软件 | 1.D1、720P、1080P等多种分辨率的视频接入； 2、视频抖动、视频清晰度异常、亮度过高，亮度过低、视频偏色、视频噪声、视频条纹、视频丢失、视频冻结、视频遮挡、场景变化、网络异常、对比度异常等13项视频质量诊断；3、诊断结果异常的自动报警，诊断结果列表和图像展示；4、一键配置诊断，将系统中所有通道自动配置到诊断预案中；5、单套至少可以保证5000路1080P高清一天检测完成。 | 套 | 1 |
| 5 | 联网网关 | 1、多平台多层次级联，跨域互联互通与资源共享；2、可支持不小于100个用户，至少3级级联部署；3、支持ONVIF/PSIA/E-Home/GB/T28181/SDK等各类不同协议视频编码设备的接入；4、具备主流平台接入如宇视、海康、大华、东方网力、互信互通等；5、转发能力：800M 标准H264码流转国标码流：单网口4M\*200路；6、转码能力：支持24路标准H.264的D1码流标准转码（非标准H.264为16路）。7、支持4路1080P码流从H.265转为H.264；或者8路720P码流从H.265转为H.2648、标准H.264 D1的转码性能为24路,或者标准H.265 转码4路1080p;9、标准264降码率和分辨率：24路D1/12路720P/6路1080P10、▲千兆网络环境下，设备单业务板卡应支持800M码流转发(提供公安部授权检测机构出具的有效检验报告复印件，并加盖厂家公章或投标专用章)11、▲设备支持控制协议网关和媒体网关分离的操作模式(提供公安部授权检测机构出具的有效检验报告复印件，并加盖厂家公章或投标专用章)12、▲设备应支持将高分辨率、高码率、高帧率视频流转换至低分辨率、低码率、低帧率视频流(提供公安部授权检测机构出具的有效检验报告复印件，并加盖厂家公章或投标专用章) | 台 | 2 |
| 6 | 存储磁盘阵列 | 1.单设备配置64位高性能多核处理器；4GB内存，内存支持扩展到128GB；单设备标配1个管理口和4个千兆网口，可扩展4个千兆网口或2个万兆网口；2.IPSAN工作模式下，存储带宽不小于2.7Gbps；3.可接入1T、2T、3T、4T、5T、6T，8T，10T磁盘，并支持在线热插拔；4. 可接入硬盘48块，当磁盘处于非工作状态下，进入休眠状态，进行读写操作时可被唤醒，增加磁盘寿命；5. 支持RAID误操作恢复功能，防止磁盘被误操作导致数据丢失，增加数据安全性；6.提供基于WEB的配置管理功能，简单易用；7.支持Onvif、GB28181等标准协议，保障了对不同厂家前端设备的兼容性；8、▲单台存储设备组建网络RAID,允许每组RAID中任意9个磁盘发生故障，数据不丢失，存储服务不中断。(提供公安部授权检测机构出具的有效检验报告复印件，并加盖厂家公章或投标专用章)9、▲业务故障隔离功能检验，存储的业务模块可以放在不同的容器中，一个业务模块故障时，不影响其它业务模块。系统可自动重启业务模块并恢复原有业务(提供公安部授权检测机构出具的有效检验报告复印件，并加盖厂家公章或投标专用章10、▲当开启智能录像时，样机可根据前端接入路数、存储周期、码率等参数，自动选择N+M冗余级别较高的数据保护方式。(提供公安部授权检测机构出具的有效检验报告复印件，并加盖厂家公章或投标专用章） | 台 | 1 |
| 7 | 监控企业级硬盘（6T) | 企业级3.5英寸硬盘；6TB 7200转 2568MB SATA接口 | 块 | 48 |
| 8 | 万兆防火墙 | 1、2U机箱，6个10/100/1000BASE-T接口和4个SFP插槽，2个万兆接口，1个可插拔的扩展槽，双电源；防火墙吞吐率：20Gbps，并发连接数：500万；提供3年设备原厂保修服务；2、采用双安全操作系统，防止配置不当或防火墙系统故障造成的网络中断，充分保证了系统的稳定性； 3、支持静态路由、ISP路由及动态路由协议，支持802.1q、QinQ模式；4、▲支持手动和LACP链路聚合，可根据源/目的mac、源/目的IP、源/目的端口、五元组、端口轮询等条件提供不少于10种链路负载算法（要求提供功能界面截图进行证明并加盖厂家章）；5、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；6、支持智能DNS及DNS Doctoring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；7、▲支持一体化安全策略配置，可以通过一条策略实现五元组信息源MAC、域名、地理区域、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、WAF、邮件安全、数据过滤、文件过滤、审计、防代理、APT等功能配置,简化用户管理。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（要求提供功能界面截图进行证明并加盖厂家章）；8、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；9、支持在一台物理设备上划分出128个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；10、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； 11、支持针对IP、ICMP、TCP、UDP、DNS、HTTP、NTP等协议进行DDOS防护； 12、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；13、▲内置静态黑名单功能，可设置多个对象条件，如：五元组信息、源MAC、地址范围、应用、用户，实现对特定报文进行快速过滤；内置动态黑名单功能，可与URL过滤、病毒过滤、防代理功能实现联动封锁；支持静态和动态黑名单命中统计和监控（要求提供功能界面截图进行证明并加盖厂家章）；14、所投产品具有公安部颁发的第二代防火墙产品计算机信息系统安全专用产品销售许可证，要求提供复印件并加盖厂家章；15、▲所投产品具备防火墙密码检测证书，要求提供复印件并加盖厂家章；16、▲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，市场占有率排名近连续三年不应低于前3名。须提供知名第三方机构（如IDC）出具的市场占有率排名有效证明材料，并加盖厂家章； | 台 | 3 |
| 9 | 漏洞扫描系统 | 1、2U机箱，双电源，含6个千兆电口，4个千兆光口，1个console；接口数量:11;扩展槽位:2,,包含3年漏洞规则库升级，任务不限制IP数量；并发扫描320个IP地址；并发扫描20个扫描任务；3年漏洞规则库升级服务；提供3年设备原厂保修服务；2、支持IPv4/IPv6双协议栈地址场景漏洞扫描；3、支持资产自动发现功能，支持利用历史扫描过程中所发现的在线主机信息，来添加资产；支持手动添加资产；支持对已有资产的直接扫描；4、产品漏洞库涵盖目前的安全漏洞和攻击特征，漏洞库具备至少CVE、CNNVD、CNCVE、CNVD、BUGTRAQ 编号；5、产品扫描信息包括主机信息、用户信息、服务信息、漏洞信息等内容。需给出各类扫描信息的详细列表，支持56000种以上漏洞，其中数据库漏洞库为500种以上；6、支持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；支持对Cisco、Juniper、华为、F5、Check point等网络设备扫描；支持Android、apple、BlackBerry等移动设备的漏洞扫描；支持通过WLAN进行扫描；支持对VMware、KVM等虚拟化设备检测；支持主流数据库的检测，应包括但不限于：Oralce、Sybase、SQLServer、DB2、Postgres、MySql、MsSql、informix、mongodb等；7、支持数据库登录扫描，至少应包括数据库账号，密码，SYSDBA、SYSOPER、NORMAL认证，SID、数据库名称、实例名称及实例号等登录选项的设置；8、可以并行地检查多个被评估的系统，能够提供扫描策略定制，可以保证扫描的安全性，不影响应用系统和网络业务的正常运行；9、支持对TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP服务与Oracle、MySQL、Postgres、MsSQL、DB2、MongoDB数据库的口令猜解；10、支持每台主机最大并发检测数设置，支持单个任务并发扫描数设置；11、▲支持资产设备漏洞查询，支持根据节点名称、设备名称、设备IP、设备管理员、设备操作系统、风险等级、漏洞名称、端口号、检测时间段等查看设备漏洞情况，并保存导出（要求提供功能界面截图进行证明并加盖厂家章）；12、支持同一任务的两次扫描结果对比，清晰明了的展示出漏洞状态的变更情况，支持不同资产之间的漏洞对比；13、▲导出报表支持自定义报表标题、导出文件名、公司信息、LOGO，其中公司信息包含公司名称、网站地址、服务热线、传真号码、公司地址等。为确保报表安全，支持导出报表加密功能；（要求提供功能界面截图进行证明并加盖厂家章）；14、所投产品具有计算机信息系统安全专用产品销售许可证增强级，要求提供复印件并加盖厂家章；15、所投产品具有国家信息安全漏洞库兼容性资质证书，要求提供复印件并加盖厂家章；16、所投产品具有CVE兼容性证书，要求提供复印件并加盖厂家章； | 台 | 1 |
| 10 | 安全操作审计系统(堡垒机） | 1、2U机型，1个console口，2个USB口； 6个千兆电口，4个SFP插槽，2个可扩展插槽； 32G内存，6T存储空间，双电源； 500个主机/设备许可，用户数不限制；含3年软件升级；提供3年设备原厂保修服务。2、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；3、不限级数的进行分层分级分类管理；4、主帐号支持从AD域内抽取，方便快速建立主账号；5、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；6、支持配置口令策略，达到指定密码有效期和限制主帐号密码强度的目的。支持配置访问锁定策略，达到限制主帐号密码输入错误次数和锁定时间。支持配置访问地址策略，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。支持SSH、TELNET、FTP、SFTP、VNC、XWINDOW、WINDOWS文件共享等协议；7、支持对资源从账号的管理，系统能够将资源上的账号进行自动抽取、推送及属性变更等；8、▲采用动作流方式代填，将单条动作转换为一系列操作并代替人工输入，无需定制即可对各类资源实现代填和审计（要求提供功能界面截图进行证明并加盖厂家章）；9、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。角色权限可以针对组织结构、用户、资源、授权关系和审计等自由结合；10、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；11、支持一键批量登录选中的资源，简化工作量；12、▲内置VPN功能，无需专用VPN硬件支持，即可方便安全地通过远程接入堡垒机（要求提供功能界面截图进行证明并加盖厂家章）；13、支持对RDP实时会话的锁定和解锁，并可以在锁定解锁时发送即时通讯消息，发现危险操作可立即进行锁定操作；14、所投产品具有计算机信息系统安全专用产品销售许可证，要求提供复印件并加盖厂家章；15、所投产品具有IT产品信息安全认证证书，要求提供复印件并加盖厂家章；16、所投产品具有涉密信息系统产品检测证书，要求提供复印件并加盖厂家章； | 台 | 1 |
| 11 | 防病毒系统 | 1、300个Windows PC客户端防病毒功能授权,含3年升级服务。 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；100个Windows Server客户端防病毒功能授权，含3年升级服务。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；2、客户端安装后至多占用50M硬盘资源，日常内存占用不到50M，有效节省PC/Server资源；3、管理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、客户端版本、病毒库版本、IP地址、MAC地址、操作系统版本、高危及功能漏洞、主板信息、显卡信息、内存大小、当前版本信息和物理位置等信息，并支持终端信息导出；4、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。支持终端策略标签化管理，按需求给终端配置标签，同一标签的终端可配置相同的动态策略，且策略优先级高于分组策略；5、支持远程控制，通过管理中心实现对客户端的远程运维；6、支持管理员操作日志记录可对管理员操作进行追踪。支持客户端与管理中心交互操作日志记录追踪，便于问题定位；7、支持定制磁盘管理规则，对审计日志、系统日志、终端日志、告警日志等即时或定期清理，实现磁盘瘦身；8、支持对webshell后门进行扫描检测 , webshell后门库数量大于100000；9、设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截；10、对系统关键位置进行防护，阻止无文本攻击、流氓、广告程序对系统的恶意篡改等行为。从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护；11、▲支持文档防泄漏功能，针对终端存储的word、pdf、ppt、Excel、rtf、txt等文档的名称、内容进行包含关键字检查，对含有指定关键字的文档进行禁止发送、禁止拷贝等管控，消息提醒的同时将文档违规信息上报管理平台。支持文档跟踪策略，可按照不同文件、压缩包类型跟踪文档内到外、外到内、外到外、内到内等流转方向，并可跟踪文档包括拷贝、压缩、解压缩、修改、删除、重命名、移动等操作（要求提供功能界面截图进行证明）；12、▲支持对移动存储设备采用标签式注册管理，可以区分内外部介质使用，定义禁用、启用只读、启用（只读\_运行）和启用读写、启用（读写\_运行）五种操作，按照文件类型审计在移动存储介质上文件操作记录，并可设置例外USB设备（要求提供功能界面截图进行证明）；13、要求对流行病毒的检测能力必须超过98%的检出率，小于0.1%的误报率，需提供第三方检测报告；14、所投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》，要求提供复印件并加盖厂家章；15、所投产品具有IPv6 Ready Logo Phase-2认证证书，要求提供复印件并加盖厂家章；16、▲所投产品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》（EAL3+级），要求提供复印件并加盖厂家章； | 台 | 1 |
| 12 | 视频安全隔离网闸 | 1、2U，双电源，内外端机双侧液晶屏，各1TB硬盘； 内端机6个10/100/1000Base-T接口，4个SFP插槽，2个SFP+插槽，1个扩展槽位； 外端机6个10/100/1000Base-T接口，4个SFP插槽，2个SFP+插槽，1个扩展槽位；包含安全浏览模块、文件传输模块、文件同步模块、邮件访问模块、VOIP访问模块、数据库访问模块、数据库同步模块、自定义访问模块、数据中心模块；网络吞吐量：7Gbps，并发连接数：40万；含4块万兆多模光口SFPplus模块(850nm，300m，LC)；提供3年设备原厂保修服务。2、提供HTTP页面访问和WEB代理上网功能。支持IP地址、端口、时间以及基于源用户身份的访问控制策略；3、支持基于单一域名的黑白名单访问控制，支持基于URL分类地址库的访问控制，支持允许、阻断、告警三种处理方式；4、内置HTTP安全模块，支持URL过滤引擎、内容过滤引擎、文件过滤引擎、病毒过滤引擎、网页过滤引擎安全防护及单独启停控制；5、内置FTP安全模块，支持内容过滤引擎、文件过滤引擎、病毒过滤引擎安全防护及单独启停控制；6、提供对多种主流数据库,如：MYSQL、SQLSERVER、ORACLE、DB2、SYBASE等系统的安全访问。支持代理、透明、路由三种接入方式。支持IP地址、端口、时间以及基于源用户身份的访问控制策略；7、内置数据库安全模块，支持内容过滤引擎，能够对数据库用户名、命令、关键字等内容进行管控，支持允许、阻断、告警三种处理方式；8、内置邮件安全模块，支持内容过滤引擎、文件过滤引擎、病毒过滤引擎安全防护及单独启停控制；9、▲支持文件名和文件类型的黑白名单过滤，支持不小于50种文件类型识别。支持文件同步信息统计，包括每个任务的开始时间、同步数据量、同步成功数、同步失败数，并能够以图表的方式进行实时可视化展现（要求提供功能界面截图进行证明并加盖厂家章）；10、提供多种主流数据库系统如：ORACLE、SQLSERVER、MYSQL、达梦数据库的同步；11、▲支持网闸同侧数据库之间的数据同步，网闸可旁路部署实现数据库同步（要求提供功能界面截图进行证明并加盖厂家章）；12、支持IPV4/IPV6双栈基础路由配置和邻居学习。提供服务器负载均衡功能，支持轮询、加权轮询、最少连接、加权最少连接等负载均衡算法。13、▲管理端通过独立的管理口与网闸内端机相连，策略统一从内端机下发，不允许采用外端机上的任何网络接口进行管理（要求提供功能界面截图进行证明并加盖厂家章）；14、所投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书（增强级），要求提供复印件并加盖厂家章；15、所投产品具有保密局涉密信息系统产品检测证书，要求提供复印件并加盖厂家章；16、所投产品具有IPv6 Ready Logo认证证书，要求提供复印件并加盖厂家章； | 台 | 1 |
| 13 | 核心交换机 | 1、交换容量≥19Tbps；包转发率≥3200Mpps2、主控引擎≥2；整机业务板槽位数≥63、支持每槽位带宽≥320Gbps4、整机万兆端口密度≥288个5、设备支持模块化风扇框，可热插拔，独立风扇框数≥26、支持颗粒化电源，整机电源槽位数>27、支持独立的硬件监控模块, 控制平面和监控平面物理槽位分离，支持1+1备份，能集中监控板卡、风扇、电源、环境，调节能耗8、支持横向虚拟化技术，将多台设备虚拟为一台设备，支持长距离集群，且用于虚拟化的板卡与业务板卡物理槽位分离，单向虚拟化集群带宽≥80Gbps9、支持整机MAC地址≥1M；MAC学习速率>8000/s；▲支持整机ARP表项≥256K；ARP学习速率≥1000/s；（提供权威第三方检测报告复印件并加盖厂商公章或投标专用章）10、支持4K VLAN；支持1：1，N：1 VLAN mapping支持端口VLAN，协议VLAN，IP子网VLAN；支持Super VLAN；支持Voice VLAN11、支持IEEE 802.1d(STP)、 802.w(RSTP)、 802.1s(MSTP)支持VLAN内端口隔离；支持1:1, N:1端口镜像；支持流镜像；支持远程端口镜像（RSPAN）；支持ERSPAN, 通过GRE隧道实现跨域远程镜像；支持DHCP Client, DHCP Server，DHCP Relay；12、支持IPv4路由转发FIB表项≥512K支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；支持路由协议多实例13、支持IGMP Snooping V1,V2,V3；支持PIM-SM/DM/SSM；支持MLD V1，V214、支持IPv6过渡技术，IPv4/IPv6双栈、6over4隧道、4 over6隧道支持IPv6 DHCP SERVER, IPv6 DHCP Relay, DHCP Snooping，支持IPv6 Souce Guard15、▲支持整机ACL表项≥256K；（提供权威第三方检测报告复印件并加盖厂商公章或投标专用章）16、支持基于第二层、第三层和第四层的ACL支持双向ACL；支持VLAN ACL和IPv6 ACL；支持IP/Port/MAC的绑定功能17、▲支持真实业务流的实时检测技术，秒级快速故障定位。（提供权威第三方检测报告复印件并加盖厂商公章或投标专用章）支持硬件BFD/OAM，3.3ms稳定均匀发包检测，提高设备的可靠性，提供权威第三方测试报告18、▲支持业务板集成AC功能，实现对AP的接入控制和管理，实现对有线无线用户的统一认证管理、用户数据报文的隧道集中转发。（提供权威第三方检测报告复印件并加盖厂商公章或投标专用章） | 台 | 2 |
| 14 | 应用和存储交换机 | 1、交换容量≥590Gbps；包转发率≥250Mpps2、48个千兆SFP，4个万兆SFP+ 3、为了提高设备可靠性，支持模块化可插拔双电源支持1个扩展插槽，可扩展支持业务插卡4、支持64K MAC地址容量，提供权威第三方测试报告5、支持4K个VLAN支持Guest VLAN、Voice VLAN支持MUX VLAN功能或类似技术支持STP(IEEE 802.1d)，RSTP(IEEE 802.1w)和MSTP(IEEE 802.1s)协议5、支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv66、支持基于源IPv6地址、目的IPv6地址、四层端口、协议类型等ACL7、支持MPLS L3VPN、MPLS L2VPN(VPLS，VLL)、MPLS-TE8、三层组播组数≥2048 ；支持VLAN内组播转发和组播多VLAN复制；支持基于端口的组播流量统计；支持IGMP v1/v2/v3、PIM-SM、PIM-DM、PIM-SSM9、支持多个物理端口的流量镜像到一个端口；支持流镜像；支持远程端口镜像（RSPAN）。10、支持防止DOS、ARP攻击功能、ICMP防攻击；支持IP、MAC、端口、VLAN的组合绑定；支持黑洞MAC地址支持CPU保护功能11、支持堆叠，主机堆叠数不小于9台12、▲支持G.8032标准以太环网协议。（提供权威第三方检测报告复印件并加盖厂商公章或投标专用章）13、▲支持纵向虚拟化，作为纵向子节点零配置即插即用。（提供权威第三方检测报告复印件并加盖厂商公章或投标专用章）纵向虚拟化的子节点交换机支持堆叠14、支持SNMPv1/v2/v3；支持网管系统、支持WEB网管特性；支持零配置部署15、支持Openflow 1.3标准 | 台 | 2 |
| 15 | 机柜 | 材质:42U 机柜，前后网眼门，黑色，600mmx1000mm | 台 | 1 |
| 16 | 操作电脑 | 规格:英特尔I5处理器；4GB内存；1TB硬盘；显示器≥22英寸宽屏 | 台 | 11 |
| 17 | 辅材 | 六类双绞线、RJ45水晶头、尾纤、设备标签、电源线、机柜PDU等。 | 批 | 1 |
| 18 | 系统集成费 |  | 项 | 1 |