分支机构部署wifi项目招标书

安信农业保险股份有限公司（以下简称“征集人”）现邀请合格的供应商（以下简称“应征人”）就征集人所需项目进行项目征集，征集人偿付能力符合监管规定,具体可上征集人官网查询[www.aaic.com.cn](http://www.aaic.com.cn)，征集人将择优选定中选人，欢迎符合条件的应征人前来参与方案比选，现将有关事项公告如下。

1. 征集项目内容
2. 设备数量

15家分支机构部署wifi，需要上网行为审计，集中管理，集中认证，每家至少4个ap，报价需包含施工费用。

1. 设备要求

设备及设备附属配件均为原厂提供。

1. 应征人必须具备的条件：
2. 应征人须为原厂商或授权代理商，所投产品品牌为国内外知名品牌，所投服务器产品性能可靠，不少于三年市场应用案例。
3. 应征人必须具有独立法人资格，具有独立承担民事责任的能力，具备相应的经营范围且其注册资金或净资产（所有者权益）必须不小于 1000（含）万元人民币（或等值外币）。须提供有效《企业法人营业执照》副本复印件。
4. 应征人必须具有专业团队，具有较强的售前、售中和售后服务支持能力，提供7\*24报修服务电话及固定的客户服务经理，省会城市、一类城市、直辖市均需要有办事处及备件库。提供全国性服务网点的证明材料。提供人员素质和技术能力资质证明。
5. 应征人未被“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”（www.ccgp.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单;并提供截图证明；
6. 财务状况：应征人应具备良好的财务状况，具有足够的流动资金来承担招标范围各事项,提供近两年的财务状况报告复印件（至少包括资产负债表和利润表）。
7. 近六个月中任一月份的依法缴纳税收和社会保障资金的相关材料。
8. 法定代表人为同一个人的两个及两个以上法人，母公司与全资子公司/由其控股的子公司，不得同时参加本项目。
9. 法律、行政法规规定的其他条件。
10. 应证人需提供厂商对本项目的授权书。
11. 应征人所需提交材料
12. 有效《企业法人营业执照》副本复印件
13. 全国性服务网点的证明材料
14. 人员素质和技术能力资质证明
15. 企业征信证明
16. 近两年的财务状况报告复印件（至少包括资产负债表和利润表）
17. 近六个月中任一月份的依法缴纳税收和社会保障资金的相关材料
18. 以上所有资质证明都需加盖应征人公司公章
19. 售后服务要求
20. 应证人应为征集人提供及时周到的系统技术支持。
21. 应证人应确保为甲方提供7\*24小时技术支持服务，响应时间不应该超过1小时，现场响应支持不应超过4小时。
22. 应证人所提供设备保质期均为至少一年，集成商所提供的设备在保质期内因硬件、软件本身质量问题所造成的损坏或无法正常运行，由此产生的维修、更换硬件和软件故障排除等所需一切费用（包括工程师差旅费用等支出）由集成商负责。
23. 应证人应提供相应的备件支持，以便及时更换损坏硬件。
24. 应证人应在质保期后设备生命周期内有义务继续对系统设备提供维保服务，甲方将支付相应费用。
25. 针对以上要求，应证人可提供具体可行的有吸引力的合作方案。
26. 验收
27. 所有设备均需提供安装服务，所采购设备（包括软件）安装都必须由生产厂商授权集成商执行。
28. 安装前由征集人信息技术部协同征集人行政办公室对货物的品牌、数量、包装等方面进行实物验收。征集人提供的所有包装的货物均应完好无损。如遇交付前已拆封的货物，征集人有权拒绝或要求更换。应证人交货时，必需提供所有产品原厂或总代理出具的供货相关证明。
29. 应证人根据征集人技术要求在征集人信息技术部指导下进行设备安装、调试，并由征集人信息技术部进行使用性能方面的验收。
30. 报名方式

有意者请于2020年7月17日下午17：00之前将标书及相关材料送至以下地址：上海市静安区共和新路3651号

联系人：顾晓磊

联系方式：021-66988356 guxl@aaic.com.cn

1. 投诉邮箱：kehufuwu@aaic.com.cn
2. 设备技术指标

15家分支机构位置

|  |  |
| --- | --- |
| **上海地区（10）** |  |
| 上海闵行支公司 | 闵行区莘潭路122号 |
| 上海嘉定支公司 | 嘉定区墅沟路63号 |
| 上海宝山支公司 | 宝山区牡丹江路1323号 |
| 上海浦东支公司 | 浦东新区新川路835号 |
| 上海南汇支公司 | 南汇区城西路281号 |
| 上海奉贤支公司 | 奉贤区南奉公路6899号 |
| 上海松江支公司 | 上海市松江区光星路1686-1696（双）号1-2层 |
| 上海金山支公司 | 金山区东平南路567,569号 |
| 上海青浦支公司 | 青浦区公园东路1155号1006-1008室 |
| 上海崇明支公司 | 崇明区东门路566号3号楼 |
| **浙江地区（4）** |  |
| 浙江分公司 | 杭州市江干区新塘路72号、76-82号（双号）第五层 |
| 台州中心支公司 | 浙江省台州市椒江区东环大道486号1-3楼 |
| 嘉兴中心支公司 | 嘉兴市新气象路1080号3楼 |
| 绍兴中心支公司 | 浙江省绍兴市越城区延安东路308号国脉大厦三楼 |
| **江苏地区（1）** |  |
| 江苏分公司 | 南京市秦淮区龙蟠中路439号6层 |

1. 上网安全服务平台参数

|  |  |
| --- | --- |
| **指标功能** | **参数要求** |
| 基础能力 | ★支持GRE协议、L2TP协议解析和终结（截图盖章证明） |
| 支持双机高可用，宕机、假死、业务终端可进行双机自动切换 |
| 支持全局bypass功能，自动探测业务单元状态，故障时，自动bypass |
| ★支持与运营平台联动，上报流量吞吐、拨号账号状态，接受运营平台的配置下发 |
| ★租户精简配置：租户支持通过配置向导根据教育、政府、企业等场景简单完成虚拟服务配置 |
| 可靠性 | 平台基于链路状态实时监测物理接口状态的功能，监控到物理接口处于离线状态时，虚拟机能够实现自动迁移； 平台具备实时监测虚拟主机异常，当虚拟主机处于离线，能够自动启动该虚拟主机迁移； ★平台可以通过设置平台可以通过设置数据多副本，数据持久性99.9999%，保障数据不丢失。 |
| 应用识别规则库 | ★支持对每一种应用的定义和解释，帮助客户快速定位应用的分类；  支持给每一种应用列上图标，易于客户了解应用的特征。（提供产品界面截图） |
| ★上网控制 | 设备内置应用识别规则库，支持超过6000条应用规则数，支持超过2800种以上的应用，1000种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率；（提供产品界面截图）  支持根据应用的特征智能识别新更新的应用；  支持根据不同的应用类型或具体的某种应用设置允许或拒绝；  支持开启5类策略：拒绝工作无关的应用、拒绝不安全的应用、拒绝有涉密的应用、拒绝消耗带宽大的应用、拒绝黄赌毒及钓鱼网站。  支持根据用户、用户组、源IP配置免控制用户。  支持基于应用、对象、时间、动作配置自定义策略。 |
| ★上网审计 | 支持开启5类审计策略：网站访问、微博论坛、邮件收发、上网流量与时长、文件上传与下载。  支持根据用户、用户组、源IP配置免审计用户。 |
| 用户管理与认证 | 支持对用户进行分组管理  支持用户上网开启认证策略，包含密码认证、微信认证、短信认证。 |
| QQ白名单 | 支持基于用户组QQ白名单功能。（提供产品界面截图） |
| ★支持与多种网安日志平台对接 | 内置多套日志模板与各省市网安日志平台对接，至少支持以下平台：派博、任子行、网博、云辰、烽火、中新软件、兆物、新网程、美亚柏科、爱思等。（提供产品界面截图） |
| ★加密SMTP邮件过滤 | 支持对加密HTTPS、SMTP-SSL、SMTP的邮件进行关键字过滤；（提供产品界面截图） |
| ★加密SMTP、POP3邮件审计 | 支持对加密HTTPS、POP3-SSL 、POP3、IMAP 、IMAP-SSL、SMTP-SSL、SMTP邮件内容的审计。（提供产品界面截图） |
| ★智能流控 | 支持场景化流控策略，包含政府企业、公共场所、酒店、教育、网吧等场景。每种场景分保障带宽应用、抑制带宽应用、普通应用三种流量管理方法。  支持通过抑制P2P的上行流量，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；  支持根据用户、用户组、源IP配置流控管控-VIP用户。  支持单IP最大带宽限制。 |
| 流控策略 | 流控策略适用对象，适用于以下对象：  一、用户：1、本地组，2、源IP  二、应用类型：访问网站、邮件、办公OA、游戏、P2P、金融行情、微博、论坛、IM、网上银行、网购、网络会议等应用。 |
| ★用户密码强度 | 可对用户密码强度进行限制，如设置用户密码不能等于用户名；  新密码不能与旧密码相同；  可设置密码最小长度；  可设置密码必须包括数字或字母或特殊字符；（提供产品界面截图） |
| 行为趋势报表 | 支持基于时间段/用户/用户组/终端类型/位置等维度的应用行为趋势、网站分类行为趋势报表 |
| 单用户行为分析 | 针对单用户的行为分析（包括：应用流速趋势、应用流量排行、域名流量排行、应用时长排行、域名时长排行、行为汇总排行等）（提供产品界面截图） |
| 离职风险报表 | 从用户上网行为的多个维度（如访问网站、搜索关键字等）分析员工的离职风险 |
| 流速趋势报表 | 支持基于时间段/用户/用户组/终端类型/位置等维度的应用流速趋势、网站分类流速趋势报表 |
| 自定义报表 | 支持从流量分析、时长分析、用户行为分析、网站分类分析、终端接入分析、终端接入安全等多维度下选择具体的基于用户/用户组/终端/网站/域名/应用/通道/搜索关键字等细粒度的排行、趋势等报表，整合成一个自定义报表进行订阅；  支持各细粒度报表直接拖拽进行整合成新报表，支持新建章节和预览功能； |
| 报表订阅 | 支持邮件订阅报告，报表内容包含带宽健康分析，工作效率分析，离职风险分析，合规性分析。 |
| 服务市场 | 平台支持查看服务包和服务内容介绍、提供可扩展的服务市场并持续更新。 |
| 产品资质 | 《网络通讯安全审计产品（国标） 销售许可证》 |
| 中国信息安全认证中心ISCCC《IT产品信息安全产品认证证书》 |
| IPv6 Ready Phase-2认证 |
| 厂商资质 | 售后服务体系通过ISO9001认证  ★★厂商具备CMMI L5认证证书  网络安全应急服务支撑单位证书（国家级）；  ★★★国家标准《信息安全技术信息系统安全审计产品 技术要求和测试评价方法》的主要起草单位; |
| 厂商综合实力 | ★★★有不少于五个网络产品入围全球权威的IT研究与顾问咨询公司GARTNER的魔力象限（提供所有入围Gartner魔力象限产品的报告，以报告数量为准） |

1. 智能网关招标要求：

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| 吞吐量 | 网络吞吐≥100Mb/s |
| 网口 | ≥5个千兆电口 |
| 网络功能 | 支持TCP/IP 协议簇，实现IP、ICMP、IGMP、TCP和UDP等协议 |
| ★支持路由模式、网桥模式部署（提供截图证明） |
| 支持DHCP 自动获取网络地址 、DHCP Server |
| 支持PPPOE Client |
| 支持NAT，实现SNAT和DNAT |
| 支持多LAN和多WAN部署模式，支持DMZ配置 |
| 支持隧道引流技术，支持同时创建多个引流隧道 |
| ★★支持SNMP协议，支持跨三层取MAC地址（提供截图证明） |
| ★支持出口链路负载均衡（提供截图证明） |
| 系统 | 支持管理员密码复杂程度校验如数字、字母、特殊字符。（提供截图证明） |
| ★★支持通过平台联动管控 |

1. 集中管理平台（BBC）

|  |  |
| --- | --- |
| **项目** | **具体功能要求** |
| 交付方式 | 支持软硬件平台一体化交付，以及支持部署在vmvare、超融合等虚拟化平台； |
| 分支展示 | 具备可视化界面，以地图方式通过不同颜色展示全网分支设备健康、离线、告警状态，同时可展开省、市、区等多级分支。 |
| 分支运维 | ★支持Web、SSH； |
| ★支持通过单点登录方式远程接入分支进行配置和管理。 |
| 支持按用户组织结构及地域分布来新建受控网点区域，并实现网点区域的嵌套管理，更符合用户管理习惯。 |
| ★支持快速导入、导出网点信息，方便用户进行快速部署。 |
| ★支持按不同区域来指定不同的管理员，实现细化管理的同时防止管理员越权管理产生的混乱。 |
| 实时监控 | 支持展示所有在线网点的网络吞吐带宽展示、当前用户流量信息、分支设备版本信息； |
| 支持即时查看受控设备状态，包括CPU、内存、磁盘占用等。 |
| 智能监控分支端设备URL、应用识别库，若不是最新版本智能提醒升级。 |
| 分支告警 | 主机网口掉线、数据通信口不通、虚拟机与外部网络不通、直击网口丢包等。 |
| 分支设备离线 |
| 分支设备序列号过期、序列号状态异常、虚拟网络设备序列号过期等。 |
| ★主机CPU、磁盘利用率高，虚拟网络设备CPU、磁盘利用率高等。 |
| 全网分支网络安全告警，如系统漏洞、攻击、木马等安全风险。 |
| 日志 | ★内置日志中心，详细记录管理员操作日志，管理员也可自行设定过滤规则来查看所需日志信息。 |
| 支持同步受控端数据中心的日志到同一个外置数据中心，支持对内网中所有受控端日志的统计、排行和导出； |
| ★管理员通过管理平台远程接入可以查看任何一台受控设备的实时及历史日志信息。 |
| 数据中心 | ★支持展示分支资源利用率排行TOPN、分支带宽利用率TOP排行、分支告警问题总数趋势、分支告警排行TOP5、分支告警数量分布、分支离线市场TOP5等报表。 |

1. 千兆网络控制器

|  |  |
| --- | --- |
| **项目** | **具体功能要求** |
| 业务端口 | 千兆以太网口数≥4个；并需提供1个RJ-45 Console管理口 |
| 提供USB接口数≥2，用于外接硬件设备（提供官网截图及官网链接证明） |
| 管理AP数 | 集中转发模式下最大可支持管理AP数≥60，单台设备最大可支持管理AP数≥500； |
| 802.11协议 | 支持802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ac、11ac wave2、802.11ax 802.11e、802.11h、802.11i、802.11k、802.11v等协议 |
| 统一准入、阻隔与认证管理 | 支持接入终端操作系统智能识别，能识别安卓、ios、windows移动终端、windows PC、MAC PC等接入终端，基于终端操作系统类型、终端MAC黑白名单库，实现基于终端的准入； |
| ★在无线网络环境中，切断病毒传播的路径，防止主机感染病毒之后横向传播给内网中的其他主机：通过策略实现隔离不同区域的用户；设置黑白名单，对访问源进行差异化拦截或放通；针对一些高风险或通用性服务，可以设置黑白名单对访问源无差别地进行拦截或放通；（提供实际功能截图并加盖软件系统开发商公章，实际功能效果支持现场测试） |
| ★通过网络管理系统可视化查看到网络账号安全状况，感知潜在风险，图形报表直观展示系统安全事件，帮助管理员轻松掌握网络的账号安全，显钓鱼AP、干扰AP、无线泛洪攻击、DDOS攻击等详细数据（提供实际功能截图并加盖软件系统开发商公章，实际功能效果支持现场测试） |
| 支持802.1x、Portal、MAC地址认证、CA证书认证、WAPI、802.1X WEP等企业认证，以及二维码审核认证、微信小程序认证、短信认证、APP认证、临时访客账号、Facebook等外来访客认证方式； 包括微信微信小程序认证、短信认证、二维码审核、802.1X、Web账号密码认证，兼容的软件系统开发商包括但不限于华三、华为、锐捷、思科、Aruba、Ruckus等（提供功能截图证明及第三方权威检测报告并加盖软件系统开发商公章）； |
| 支持关联RADIUS、微软AD域、LDAP、数据库（Oracle、MySQL、MS-SQL）、Portal2.0、AS等外置认证服务器，实现802.1x、Portal等第三方认证； |
| ★支持对接移动办公平台进行用户认证，包括阿里钉钉、微信企业号、口袋助理等主流平台，支持同步组织架构实现不同部门人员分配不同的上网权限策略，同时用户端可以直接通过APP或轻应用即可自助管理账号密码（提供功能截图证明及第三方权威检测报告并加盖软件系统开发商公章）； |
| 支持账号自注册认证方式，通过手机号码白名单来自助设置账号密码，并且支持通过手机号码找回密码 |
| 支持智能PSK技术，不同的终端使用不同的专属密码，并支持移动终端的秘钥与MAC或SN进行绑定，其他终端即使拿到了该秘钥也无法上网，保证终端安全接入要求（提供功能截图证明） |
| 支持Portal认证页面自定义，包括页面展示信息、页面标题、文字描述、免责声明等信息； |
| 支持短信认证的有效期设置和短信验证码的有效期设置，在短信认证有效期内，不用重新认证，在验证码有效期内，不用重新获取验证码 |
| 上网行为管理审计 | ★支持应用识别，能识别不低于4000种的网络应用，能识别邮件、游戏、P2P流媒体、WEB流媒体、金融交易、办公OA、移动终端应用等主流应用（提供功能截图证明及第三方权威检测报告并加盖软件系统开发商公章）； 无线AC支持基于应用层的互联网流量和内网流量双重访问控制；上述内容实现方式包含但不限于无线网络处于本地转发状态下。 |
| 支持多元化基于应用识别管控，包括用户、接入位置、终端类型、终端MAC地址、时间段； |
| ★支持上网行为审计，可审计用户访问的URL、网络应用类型、非加密的邮件正文及其附件内容、Web BBS发帖内容、微博内容、FTP上传和下载的文件名、TELNET执行的命令等（提供功能截图证明及第三方权威检测报告并加盖软件系统开发商公章）； |
| 射频安全 | ★为了预防办公Wi-Fi安全风险，需要支持对防钓鱼Wi-Fi、私接无线路由器的实时检测、告警及反制 |
| 支持基于时间计划定时开启或关闭指定SSID，并可配置例外SSID |
| 缓存加速 | ★支持网络应用智能缓存，自动将无线网络中首次下载的APP，缓存到本地服务器（包括控制器内置硬盘、AP外置U盘或者外挂服务器），实现缓存加速（提供功能截图证明并加盖软件系统开发商公章） |
| ★内置硬盘，硬盘大小≥128GB（提供官网截图及官网链接证明） |
| 负载均衡 | 支持基于用户数、信号强度、信道利用率的智能负载均衡，自动平衡各AP之间的接入压力 |
| 支持射频引导功能，引导无线终端优先接入干扰小的5G频段 |
| 大数据分析 | ★★支持认证用户画像描述，支持对认证用户的移动轨迹、来访偏好、高峰时段、来访频次、驻留时长、WiFi使用时长、移动终端类型、上网爱好标签等信息进行收集和分析（提供功能截图证明及第三方权威检测报告并加盖软件系统开发商公章）； 支持网络注册用户量分析，实现每天总注册人数、新注册人数、二次返回率、驻留时长等网络注册用户量分析（提供功能截图证明及第三方权威检测报告并加盖软件系统开发商公章）； ★★支持人流密度分布热图，可直观查看各区域的人群密度分布情况，哪里人员密集、哪里稀疏； 支持记录上网用户在网站访问行为、网络应用使用行为、搜索引擎及APP内搜索行为，并要求能根据使用此次或搜索次数进行TOPN排行（提供功能截图证明并加盖软件系统开发商公章） |
| 网络部署 | Fit模式系列AP通过广域网方式转发时，无线接入设备部署在分支机构，控制器部署在总部，所有用户数据由无线接入设备发送到控制器，再由无线控制器进行集中转发。该型号AP可将数据报文在无线接入设备上直接转化为不经过控制器的报文，而是在本地进行转发，大大节约了有线带宽； 支持基于SSID选择本地转发或者集中转发； |
| ★支持跨互联网进行远程集群部署，通过中心网络控制器可以对所有分支网络控制器进行统一集中管理，包括统一配置和统一查看分支控制器、AP、用户的在线情况，并实现下属分支AC与中心端AC的垂直网络备份，及分支AC与相邻分支AC的水平网络备份（提供功能截图证明并加盖软件系统开发商公章）； |
| ★支持易部署上线，可以通过导入AP的MAC地址或者SN码，AP联网后无需任何配置即可发现AC（提供功能截图证明并加盖软件系统开发商公章） |
| 高可靠性 | 支持网络控制器双机冗余热备；支持AC间AP快速切换； |
| 支持网络控制器跨互联网冗余备份，建立异地备份中心，保证无线网络的不间断使用 |
| 支持网络控制器逃生功能，当网络控制器宕机后，切换成智能转发模式，依然能保证在线用户的正常上网，并保证新用户也能通过认证连入无线网络（提供功能截图证明并加盖软件系统开发商公章）； |
| AP热点分析 | ★支持AP热点地图分析，导入CAD区域分布图，直观显示每个AP的实际部署位置，可实时查看AP状态、接入用户数、实时流量等信息，方便管理员实时了解网络健康状态（提供功能截图证明并加盖软件系统开发商公章）； |
| 支持查看AP CPU和内存占用率，支持统计每一个AP在一段时间内的接入用户数和上网流量及趋势变化；根据用户数、流量查看繁忙AP和空闲AP TOPN; |
| 提供控制器和AP的WEB管理界面，不仅轻松搞定无线配置，更能够整体运营无线网络，通过控制器的WEB界面不仅能够管理AP还能管理AP下联的用户，可以对用户进行限速和限制用户连入网络等行为，方便运维人员对无线的规划和运维。 |
| 配合控制器，AP可以与软件联动，可以实现对网络中所有控制器和AP的管理，包括设备的配置备份，设备状态的查询，提供无线热敏图来显示无线AP在实际环境中的无线信号分布状态。 |
| 支持查看信号质量差的AP TOPN，分析维度包括AP的信号利用率、噪声值、重传率、误码率趋势； |
| 路由 | 支持静态路由、策略路由、地址转换 |
| 支持路由网关功能，支持静态IP、DHCP、PPPoE拨号三种上网方式； |
| 有线网络管理 | 有线网管平台控标参数单独列出，请查看安视交换机控标参数 |
| ★为了更好的管理维护网中POE、接入、汇聚交换机，需要支持通过该系统实现统一的配置管理（非简单的SNMP网管协议），并且支持可视化的运维配置管理，以及多种方式在网管平台自动上线，包括但不限于二三层发现、DHCP Option43、DNS域名（提供功能截图证明并加盖软件系统开发商公章）； |
| 运维管理 | 支持WEB中英文图形化界面管理，支持CLI、Telnet、SSH等； |
| ★支持移动APP运维，通过手机APP即可进行无线状态查看、无线网络管理、告警通知等，提供第三方权威检测报告并加盖软件系统开发商公章； |
| ★支持不低于5级的AP分组管理，方便AP设备的管理维护（提供功能截图证明并加盖软件系统开发商公章） |
| 支持管理员分权分级，不同的管理员拥有不同的管理权限，包括精细的页面修改查看权限和接入点管辖权限以及是否允许登陆数据中心等，方便网络的维护管理（提供功能截图证明并加盖软件系统开发商公章） |
| 支持SNMP v1/v2/v3，SNMP Traps，支持MIB库； |
| 产品资质 | ★无线AC需满足无线安全及公安网监要求，并提供无线AC的《计算机信息系统安全专用产品销售许可证》复印件及检测报告 |
| 品牌要求 | 保证兼容性与统一管理，要求本次招标AC与AP、交换机同一品牌 |
| ★为保证设备扩展性，要求设备制造商软件开发能力达到CMMI五级，提供相应证书复印件并要求设备制造商盖章证明 |
| 为保证设备安全性，要求设备制造商为WAPI产业联盟会员，提供相应证书复印件并要求设备制造商盖章证明 |
| 同频组网 | 支持同频组网技术，可实现将多个物理AP通过虚拟化技术组成同频group，对终端呈现一个虚拟AP，实现终端在移动切换时无缝漫游、无丢包。 |

1. 室内wave2高密AP

|  |  |
| --- | --- |
| **技术指标** | **参数要求** |
| 802.11协议 | ★802.11ac wave 2协议，兼容802.11a/b/g/n/ac协议，支持2.4G和5G同时工作； |
| 接入速率 | 支持2x2 MIMO，2.4G最大传输速率≥300Mbps，5G最大传输速率≥867Mbps，整机最大传输速率≥1167Mbps |
| 天线类型 | 内置矩阵式智能天线 |
| 业务端口 | 以太网口≥2个，并需提供1个RJ-45 Console管理口 |
| ★USB接口≥1个，可拓展物联网模块使用，可外接U盘 |
| 设备供电 | 支持802.3af标准的PoE供电和本地电源适配器供电两种方式 |
| AP满负荷工作功耗≤13W |
| 发射功率 | AP发射功率≤20dBm（最大不超过100mw），且功率可调节（调节粒度为1dBm，调节范围为1dBm~20dBm） |
| 工作环境 | 工作温度：-10~50℃；工作湿度（非凝结）：5%~95% |
| 接入人数 | ★单射频接入人数≥128，整机最大接入人数≥256 |
| 支持基于SSID的接入用户数限制 |
| SSID | 支持虚拟AP技术，单射频SSID数量≥16，整机≥32； |
| 支持SSID隐藏；支持英文SSID、中文SSID或中英文混合SSID |
| 支持SSID与1QVLAN一对一或一对多的映射； |
| 工作模式 | ★支持Fat和Fit 两种工作模式，根据网络规划的需要，可以灵活地在Fat和Fit两种工作模式中切换，同时可以根据应用需求，选择工作模式。 |
| AP支持集中转发和本地转发两种数据转发模式，同一个AP上基于SSID选择本地转发或者集中转发； |
| Fit模式系列AP可将数据报文在无线接入设备上直接转化为不经过控制器的报文，而是在本地进行转发，提升转发效率，降低网络资源开销。 |
| 部署与运维 | ★支持AP零配置，支持二三层发现、DHCP Option43、DNS域名等多种AC自动发现机制 |
| 支持跨三层、跨广域网、NAT部署AP，并支持与AC的管理隧道加密； |
| 可以对Wi-Fi报文进行侦听捕获并实时镜像到本地分析设备供网络管理员进行故障排查、优化分析。 |
| 提供控制器和AP的WEB管理界面，不仅轻松搞定无线配置，更能够整体运营无线网络，通过控制器的WEB界面不仅能够管理AP还能管理AP下联的STA，可以对STA进行限速和限制用户连入网络等行为，方便运维人员对无线的规划和运维。 |
| 认证与准入 | 支持802.1x 认证、MAC 地址认证、PSK 认证、Portal认证等 |
| 二维码认证是另一种方便访客上网的方式，访客接入无线网络后，可获得二维码提示，通过被访者（内部人员）的授权后即可访问网络，访客行为与被访者直接关联，风险行为可快速溯源。 |
| 安全特性 | 支持AES、TKIP等加密方式 |
| 支持WIPS/防钓鱼WIFI，支持对非法接入点的实时检测、告警及反制 |
| ★无线AP支持联动安全策略，通过安全策略可以实现对疑似感染病毒或已感染病毒的无线客户端进行识别、监控与隔离等多种方式的处理，提供功能截图证明，并加盖厂商公章 |
| 认证机制用来对用户的身份进行验证，以限定特定的用户（授权的用户）可以使用网络资源；加密机制用来对无线链路的数据进行加密，以保证无线网络数据只被所期望的用户接收和解析。 |
| 支持将内网终端用于的ARP扫描、IP扫描、端口扫描达到阈值后告警或进入动态黑名单。 |
| 在数据安全方面，通过融合有线无线双重保障，实现全面安全防护。 |
| 1、基于VLAN的STA隔离； 2、基于 SSID 的 STA 隔离； |
| ★支持接入点VPN功能，可以跨互联网与异地的无线控制器建立加密通信隧道，实现加密远程访问 |
| 射频技术 | 支持802.11h 动态频率选择(DFS)、信道自动扫描功能，自动规避干扰 |
| 支持基于时间计划定时开启或关闭指定SSID，并可配置例外SSID |
| ★通过基于特征和协议的射频优化，有效提升无线部署中高密度接入、流媒体传输等场景中的应用加速能力和质量保障效果。其中包含：多用户时间公平调度、混合接入公平、干扰过滤、终端速率管控、频谱导航、组播增强、广播优化、逐包功率控制和智能带宽保障等。 |
| 支持无线带宽平均分配，让不同协商速率的终端占用相等的无线信道时间，防止低速终端拉低网络整体速； |
| 智能负载 | 支持基于STA数、信号强度、信道利用率的智能负载均衡，自动平衡各AP之间的接入压力 |
| 路由功能 | ★支持Fit AP切换成网关模式（非Fat AP模式），支持PPPoE拨号、静态IP、DHCP三种上网方式； |
| 支持DHCP Server和DNS代理功能 |
| 高可靠性 | ★支持逃生模式，AP与控制器连接中断后，原有用户在线、新用户正常接入，业务不中断； |
| 品牌要求 | ★为保证兼容性与统一管理，要求本次招标的系统平台管理软件AP与POE交换机兼容或为同一品牌 |

1. 安视交换机8口POE交换机

|  |  |
| --- | --- |
| **技术指标** | **参数要求** |
| 固定端口 | 千兆POE电口数≥8个，千兆SFP光口≥4个； |
| POE功能 | 支持IEEE 802.3af/at供电标准，单端口最大输出功率≥30W，整机最大输出功率≥135W |
| 管理端口 | Console口≥1个 |
| 交换机性能 | 交换性能≥256Gbps/2.56Tbps |
| 包转发率≥27Mpps/102Mpps |
| 接入方式 | 支持胖瘦一体化，支持智能交换机和普通交换机两种工作模式，可以根据不同的组网需要，随时灵活的进行切换 |
| 访问控制策略 | 支持基于交换机单端口、聚合口的ACL策略； |
| 支持基于源目IP地址、MAC地址的ACL策略； |
| 支持基于协议（例如：OSPF、UDP、ARP），同时支持自定义协议号的ACL策略； |
| 支持基于时间的ACL策略； |
| 支持基于802.1p、IP及服务等级、DSCP的优先级设置； |
| 以上功能需提供平台功能配置截图证明； |
| 服务质量（Qos） | 流量管理：对于匹配ACL的流量进行重标记从而实现流量监管功能； |
| 流量整形：支持基于交换机端口出方向和入方向进行报文转发速率设置； |
| 优先级映射：支持基于交换机组实现COS、DSCP优先级映射； |
| 拥塞管理：支持多种调度模式（例如：轮询模式、严格优先模式等）实现流量基于报文或端口的优先级 |
| 流量镜像 | 支持流量端口镜像及重定向功能； |
| DHCP Snooping | 支持交换机端口设置为信任端口或非信任端口，非信任端口也可设置白名单响应DHCP报文 |
| 交换机零配置上线方式 | ★二层广播自动发现控制器平台 |
| ★配置静态IP地址三层发现控制器平台 |
| ★DHCP Option43方式发现控制器平台 |
| ★DNS域名发现控制器平台 |
| 以上方式提供官网截图证明； |
| 一键替换 | ★支持通过控制器平台一键替换“按钮”即可完成故障设备替换，提供平台功能截图证明； |
| 生成树 | 支持STP、RSTP、MSTP协议 |
| VLAN | 支持4K个VLAN |
| MAC | 支持MAC地址≥16K |
| 支持MAC地址自动学习 |
| 支持源MAC地址过滤 |
| 支持接口MAC地址学习个数限制 |
| 端口聚合 | 支持端口聚合≥64个 |
| 支持手工和静态LACP |
| ARP | ARP表≥512 |
| DHCP | 支持DHCP Server |
| M-LAG | ★支持M-LAG技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面，提供功能配置截图证明； |
| 交换机状态显示 | ★支持通过控制器平台查看交换机端口负载情况，提供平台功能截图证明； |
| 安全特性 | 支持防网关ARP欺骗 |
| 管理员分级管理 |
| 支持端口保护、隔离 |
| 支持防止DOS、ARP攻击功能 |
| 支持CPU保护功能 |
| 网络管理 | ★支持通过APP进行远程管理，并且可以修改交换机网络配置，提供APP软件功能配置截图证明； |
| ★支持通过网管平台跨广域网、NAT远程管理智能交换机，提供截图证明； |
| 交换机画像管理 | ★支持通过在控制器平台的Web页面对交换机进行可视化管理查看，包括交换机的端口状态及配置、vlan信息，提供功能截图证明； |
| ★支持通过控制器平台图形化操作对交换机端口状态的开启与关闭，提供功能截图证明； |
| 运维 | 支持通过控制器平台查看交换机面板端口工作状态，通过端口颜色显示状态即可判断端口是否在线工作； |
| 支持通过控制器平台查看交换机处于工作端口最近5分钟、1小时、最近1天、最近1周发送与接收的流量趋势；提供功能截图证明； |
| 智能终端类型识别 | ★支持终端类型库，基于指纹自动识别PC、路由器、监控终端设备等，提供平台终端类型识别库截图证明； |
| ★支持基于终端类型自动识别结果，禁止非法终端(例如私接路由器)接入 |
| 终端安全策略 | 支持终端IP-MAC绑定，当IP+MAC不对应时，可以将终端加入黑名单实现断开终端流量 |
| 支持终端IP-MAC首次部署自动学习绑定 |
| 支持将交换机的端口进行端口组划分，方便配置管理，提供功能截图证明； |
| 支持预留的特权IP必须由管理员审批才可以使用，同时支持IP白名单免审批，提供功能截图证明； |
| 支持终端的MAC与交换机端口变更检测，提供功能截图； |
| 支持终端发生安全策略事件后，交换机将终端加入黑名单 |
| 支持交换机端口终端类型变更后，通过APP、短信告警，提供功能截图证明； |
| 可以自定义交换机端口接入终端类型，及MAC黑白名单，提供功能截图证明； |
| 终端状态安全分析 | 支持查看终端在交换机端口离线次数、闲置时间、离线趋势，提供功能截图证明； |
| 支持查看安全事件记录、终端类型异常记录、终端在端口迁移次数、终端地址异常记录等安全事件的记录统计，提供功能截图证明； |
| 支持查看终端的的历史接入交换机端口，终端的活跃状态，提供功能截图证明； |
| 厂商资质 | 为保证产品软件成熟度，设备生产厂商需具备CMMI5级证书，提供证书复印件证明，并加盖厂商鲜章 |