**采购需求**

**1.功能要求**

宿州市数据资源局建设网络安全提升项目，需向数据局管理相关工作区域提供千兆无线 WiFi 网络服务，管理平台需具备跨地域无缝漫游能力，采用皖事通 APP 认证的方式进行互联网访问。

**1.1跨区域无缝漫游**

根据宿州市数据资源局网络建设需求，采取802.11ax 网络协议标准，提供不低于1000Mbps的单个AP的无线带宽接入能力，提供高性能的无线覆盖；跨多个区域部署AP，保证被覆盖需求的网络访问流畅，提供网络接入业务，让工作人员和访客群众同时使用快速上网和办事使用。AP通过将接入用户的终端MAC上传至云端数据库中，当此用户在其他区域接入无线网络时，云平台通过进行终端MAC校验，当一致时，用户可直接接入无线网中，无需二次认证。

**1.2“一次一密”认证接入**

无线网络系统建设依托云无线管理平台，需与“皖事通”进行无缝对接，用户可通过APP完成认证，采取“一次一密”的形式接入无线网络，实现无线网络的实名制连接，从而提升网络安全性。通过多层面的接入准控和网络层的隔离优化，确保宿州市数据资源局的无线网络使用安全。

**2、服务内容**

**2.1网络服务要求：**

提供不低于1000M互联网专线1条，不低于2000M互联网专线1条，服务期2年。

**2.2平台服务要求：**

（1）确保办公区域无线网络全覆盖；

（2）确保接入认证安全性和日志可追溯；

（3）确保管理平台具备设备远程管控、设备部署、增值功能和拓展功能。使用管理过程中，运维人员能做到跨地域统一管控、即插即用上线，后期AP可无限制扩展，方便快捷的进行无线网络维护。

**为确保整个网络达到高性能、智能化、易运维的安全无线网络建设要求，保障系统稳定、有效运行。提供以下配套服务：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **服务**  **名称** | **技术要求** | **数量** | **单位** |
| 1 | 云无线管理平台授权 | 1．▲基于云端管理，采用云无线架构，平台必须可以直接管理AP，不经过AC管理，支持多种AP云管理，零配置上线；（提供官网截图证明，并加盖原厂公章） 2．支持远程升级和云端管理；支持查看平台状态、日志、版本信息；支持B/S架构管理，支持多终端类型登录；支持远程信道、信号强度、优化；支持AP零配置上线； 3．▲支持云端在线一键切换AP工作模式（FAT模式和FIT模式）；（提供功能截图证明，并加盖原厂公章） 4．支持设备的批量导入、导出、批量修改和删除以及批量升级； 5．▲支持与网监对接功能；（提供功能截图证明，并加盖原厂公章） 6．支持弱信号剔除功能； 7．支持智能漫游功能，可根据AP间信号强弱差值，强制用户重新选择更好的AP信号。（提供功能截图证明，并加盖原厂公章） 8．▲AP与平台之间支持广域网连接、可穿越NAT、PPPoE、VPN等网络环境。支持跨广域网漫游，首次认证后，任意范围内无需二次认证；（提供官网截图证明，并加盖原厂公章） 9．支持逃生功能，AP与平台之间连接断开，AP保持正常工作，网络不中断； 10．▲平台支持探针功能，单个AP扫描周边其它AP信号（提供功能截图证明，并加盖原厂公章） 11．▲支持和皖事通联动认证；（提供功能截图证明，并加盖原厂公章） | 20 | 项 |
| 2 | POE交换机 | 1．千兆电端口≥24，1G SPF光口≥4;（提供产品官网截图或产品实物照片，并加盖原厂公章） 2．POE功率≥370W，支持802.3af满载供电； 3．支持网管软件管理 | 1 | 套 |
| 3 | 无线认证网关 | 1．▲配置万兆SFP+口≥2；千兆电口≥5，USB2.0口≥2，console 管理口≥1；（提供产品官网截图或产品实物照片，并加盖原厂公章） 2．网络吞吐率≥3Gbps,并发连接数≥150万； 3．最大支持SSL VPN数400，标配SSL VPN数10； 4．支持支持一键上网、微信认证、短信认证、密码认证等多种认证方式；支持负载均衡、线路备份、在线检测；支持实时的 CPU、内存、接口流量等 | 1 | 项 |
| 4 | 汇聚交换机 | 1．▲千兆光口≥24，复用千兆电口≥8，万兆光口≥4，1个 CLI 控制口；（提供产品官网截图或产品实物照片，并加盖原厂公章） 2．交换容量≥336Gbps，包转发率≥108Mpps（以官网最小值为准）； 3．支持基于端口、协议、MAC的VLAN，最大VLAN数≥4094； 4．支持静态路由，RIP、OSPF 动态路由 ；支持网管软件管理 | 1 | 套 |
| 5 | 上网行为管理 | 1、标准机架式硬件设备；网络接口：千兆电口≥5个，千兆Combo口≥2个，USB2.0接口≥1个，Console口≥1个；整机应用吞吐量≥2Gbps，最大用户数不少于1500IP，并发连接数不少于 50 万，PPS不小于51万（64字节）； 2、工作模式：支持网桥模式，网桥模式，默认未配置策略情况下对用户业务进行透传传输；支持网关模式，包括NAT、DHCP、DNAT等网关模式的功能；支持旁路模式； 3、▲负载均衡：支持基于域名的负载均衡；支持基于应用协议的负载均衡（提供功能截图证明，并加盖原厂公章）； 4、应用协议识别：现网识别准确率在95%以上； 5、行为管理：支持基于IP五元组、VLAN、链路、数据流向、共享用户、移动终端、应用协议/协议组和IP/IP群组的速率和连接数控制，最小颗粒支持Kb；支持针对内网用户进行基于应用层协议、URL的行为管理（提供功能截图证明，并加盖原厂公章）； 6、▲本地镜像：支持专线卫士审计版的同时，支持基于应用协议和应用协议群组的流量镜像；支持基于域名和URL的流量镜像；支持基于时间的流量镜像。（提供功能截图证明，并加盖原厂公章）； 7、VPN：IPSEC性能可达100Mbps；SD-WAN tunnel性能可达900 Mbps；（提供功能截图证明，并加盖原厂公章）； 8、▲远程镜像：支持将镜像流量指定到SD-WAN线路封装和转发到指定的目的地（提供功能截图证明，并加盖原厂公章）； 9、▲业务&网络质量测量：支持应用级被动测量：针对网络流量中每一条会话，进行基于应用级的质量测量；支持对客户端时延、传输时延及应用服务器时延的分段记录与策略（提供功能截图证明，并加盖原厂公章）； 10、▲AC控制器：支持对自有AP的管理，支持AC功能，无需新购置AC控制器（提供功能截图证明，并加盖原厂公章）； 11、威胁情报：系统内置数字货币、C&C节点、APT攻击、网站后门、钓鱼网址、僵尸网络等16种威胁情报，针对网络异常行为进行检测分析；支持对威胁情报的命中监测，支持查看情报命中趋势、情报类型命中分布、以及源IP、目的IP、源MAC等信息（提供功能截图证明，并加盖原厂公章）； 12、▲业务性能日志：支持分析每一条TCP连接的客户时延，服务时延，应用时延，最大包长（提供功能截图证明，并加盖原厂公章）； 13、审计日志：支持1:1全量记录会话日志，并可以按照应用协议、五元组、运营商流向、等信息进行检索和查询；支持HTTP行为审计，以请求方法、状态码、域名、URI、Agent、Cookie等元数据条件进行检索，并支持以时间范围进行查询；（提供功能截图证明，并加盖原厂公章）。 | 1 | 套 |