**附件1：**

技术参数及安装要求

1. **设备清单**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备 | 单位 | 数量 |
| 1 | 网络汇聚交换机 | 台 | 1 |
| 2 | 网络接入交换机 | 台 | 4 |
| 3 | 无线网络控制器 | 台 | 1 |
| 4 | 无线网络接入点 | 台 | 14 |
| 5 | 网络防火墙 | 台 | 1 |

1. **设备技术参数要求**

|  |  |
| --- | --- |
| **网络汇聚交换机（1台）** | |
| 类别 | 技术规格要求 |
| 交换容量 | 交换容量≥2.56Tbps，转发性能≥720Mpps，以官网所列最低参数为准,提供官网截图及链接。 |
| 硬件规格 | 配置双电源，双风扇模块，支持前后、后前风道,提供官网截图及链接。 |
| 提供的电源模块功率不超过500W。 |
| 支持≥2个扩展插槽，可扩展业务线卡和多功能插卡,提供官网截图及链接。 |
| 软件规格 | 整机最大路由地址表≥64K，整机最大ARP地址表≥64K，整机最大MAC地址表≥128K。 |
| 端口配置要求 | 实配10 GE 光接口≥24个，40 GE光接口≥2个，扩展插槽≥2个，≥14个万兆多模光模块，≥10个千兆电模块。 |
| 三层功能 | 支持IPv4/IPv6静态路由、RIP、OSPF、ISIS、BGP。 |
| 防火墙插卡 | 支持防火墙插卡，防火墙插卡集成多种安全模块，保障网络信息安全。 |
| 网络管理 | 所投产品可纳入客户现有运维管理平台，并提供原厂运维工程师7×24小时远程或现场监控远维服务，每月提供运维报告以及资产报告。 |
| 维保 | 提供3年7x24级别原厂维保,供应商供货时需提供原厂商针对本项目的授权函及售后服务承诺函。 |
| 资质 | 提供工信部入网证。 |

|  |  |
| --- | --- |
| **网络接入交换机（4台）** | |
| 类别 | 技术规格要求 |
| 交换容量 | 交换容量≥672Gbps，转发性能≥207Mpps，以官网所列最低参数为准,提供官网截图及链接。 |
| 硬件规格 | 具有1个USB接口。 |
| 工作环境温度-5ºC～45ºC,提供官网截图及链接。 |
| 软件规格 | 整机最大路由地址表≥3K，整机最大ARP地址表≥2K，整机最大MAC地址表≥16K。 |
| 端口配置要求 | 实配10/100/1000BASE-T PoE+电口≥48个， 1/2.5/10GE SFP+端口≥4个，≥2个万兆多模光模块。 |
| 三层功能 | 支持IPv4静态路由、RIP、OSPF。 |
| 支持IPv6静态路由、RIPng、OSPFv3。 |
| 网络管理 | 所投产品可纳入客户现有运维管理平台，并提供原厂运维工程师7×24小时远程或现场监控远维服务，每月提供运维报告以及资产报告。 |
| 维保 | 提供3年7x24级别原厂维保,供应商供货时需提供原厂商针对本项目的授权函及售后服务承诺函。 |
| 资质 | 提供工信部入网证。 |

|  |  |
| --- | --- |
| **无线网络控制器（1台）** | |
| 设备指标项 | 设备技术参数及性能（配置）要求 |
| 硬件配置要求 | 所投产品集中转发性能≥10Gbps，配置千兆GE端口≥8个，万兆SFP+端口≥2个，2.5GE端口≥2个，内置双电源，配置≥16个无线AP管理授权，配置≥1个万兆多模光模块,提供官网截图及链接。 |
| 管理AP数 | 所投产品满足常规AP最大数量≥144。 |
| 产品硬件 | 1U高度。 |
| 内置双电源冗余供电,提供官网截图及链接。 |
| 策略转发 | 满足策略转发双网关，方便总部分支网络用户远程办公，同时减少ACAP中间链路资源占用，设备满足同一SSID终端的内网业务AC集中转发处理，外网业务AP本地转发。 |
| 运维 | 管理设备内嵌网管支持整网设备拓扑的可视化呈现。支持基于拓扑配置交换机各端口的VLAN业务。 |
| 管理设备内嵌网管支持基础的WAN配置和无线配置。WAN配置包括WAN口选择、上网方式、多WAN口策略。无线配置包括无线服务模板、AP组、射频、国家码等。 |
| 业务不间断升级 | 支持在集群热备组网下，通过AC ISSU升级，可以实现AC在升级时业务不中断，AP和终端不掉线，终端可持续ping通网关。 |
| 无线运维 | 为了有效排查无线网络中存在的匿名攻击的隐患，所投产品需要具备仿冒终端检查的能力，并且识别仿冒终端所接入SSID、AP以及终端设备型号、终端操作系统等信息。 |
| 组网能力 | 满足标准IETF 5415 CAPWAP协议，AP和AC之间满足L2/L3层网络拓扑，为提高网络安全，AP与控制器之间能够满足DTLS对CAPWAP隧道进行加密处理。 |
| CAPWAP 隧道同时支持 IPv4 和 IPv6 双栈，支持用户地址和隧道地址任意选择使用IPv4或IPv6 ，灵活组合使用。 |
| 可靠性 | 支持MAC认证逃生功能：AC、AP满足MAC认证逃生功能，为提高无线网络认证可靠性，无线控制器满足MAC认证逃生功能。 |
| 支持Portal认证逃生功能：AC、AP满足Portal认证逃生，为提高无线网络认证可靠性，无线控制器满足Portal认证逃生功能。 |
| 网络管理 | 所投产品可纳入客户现有运维管理平台，并提供原厂运维工程师7×24小时远程或现场监控远维服务，每月提供运维报告以及资产报告。 |
| 市场地位 | 产品生产厂商提供2023年全年中国境内无线市场销售量，提供相应IDC证明材料。 |
| 授权要求 | 提供原厂针对本设备的授权函及三年原厂7×24小时售后服务承诺函。 |

|  |  |
| --- | --- |
| **无线网络接入点（14台）** | |
| 设备指标项 | 设备技术参数及性能（配置）要求 |
| 硬件配置要求 | 采用三射频设计，可工作在802.11a/b/g/n/ac/ac wave2/ax模式。 |
| 整机协商速率≥5.375Gbps，且所有5G频段单频段速率≥2.4Gbps,提供官网截图及链接。 |
| 接口要求 | 固化≥2个接口，包括1个固化100/1000M/2.5G电口，1个固化10M/100M/1000M电口。 |
| 安装方式 | 满足壁挂、吸顶和面板安装方式。 |
| 功耗 | 整机最大功耗≤30W,提供官网截图及链接。 |
| WIFI6功能 | 使用WIFI6终端接入测试，接入5GHz频段，在80MHz频宽下，单用户极限性能可达到930Mbps以上。 |
| 使用WIFI6终端接入测试，接入2.4GHz频段，在40MHz频宽下，单用户极限性能可达到400Mbps以上。 |
| 证书 | 要求报价产品为成熟产品，报价设备必须持有国家工信部型号核准证。 |
| 网络管理 | 所投产品可纳入客户现有运维管理平台，并提供原厂运维工程师7×24小时远程或现场监控远维服务，每月提供运维报告以及资产报告。 |
| 授权要求 | 需提供原厂针对本设备的授权函及三年原厂7×24小时售后服务承诺函。 |

|  |  |
| --- | --- |
| **网络防火墙（1台）** | |
| 功能项 | 功能要求说明 |
| 硬件规格要求 | 产品不少于14千兆电口；不少于12个千兆光口；不少于4万兆光口SFP+；不少于2个扩展槽位；提供不少于2个USB口，提供不少于2个硬盘槽位，提供不少于2块1.92TB SATA SSD硬盘；提供冗余电源，1U机箱。 |
| 产品性能要求 | 网络层吞吐量≥8Gbps，应用层吞吐量≥8Gbps，并发连接数≥500万，每秒新建连接数≥8万。 |
| 授权与服务要求 | 要求防火墙开启IPS、AV功能模块。提供硬件三年维保服务，软件与特征库六年升级服务。 |
| 存储 | 支持SSD硬盘不小于480G，HDD硬盘不小于1T。 |
| 支持双硬盘，双硬盘支持Raid0和Raid1，实现硬盘数据存储的高可靠,提供官网截图及链接。 |
| 工作模式 | 产品提供路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。 |
| 路由特性 | 产品提供静态路由、策略路由和多播路由协议。 |
| 支持静态路由、策略路由、RIP、OSPF、BGP、IS-IS等路由协议。 |
| NAT功能 | 支持一对一、多对一、多对多等多种形式的NAT，支持DNS、FTP、H.323、RTSP、ILS、PPTP、SIP、SQLNET、MGCP、RSH、ICMP差错报文、TFTP、RTSP、SCTP、XDMCP、NBT、SCCP、HTTP等多种NAT ALG功能。NAT地址池支持动态探测和可用地址分配。 |
| 支持NAT44、NAT46、NAT64、NAT66。 |
| VPN功能 | 产品提供IPsec VPN和SSL VPN功能。 |
| 支持IPsec VPN智能选路，根据隧道质量调度流量。 |
| SSL VPN支持IPv6接入方式，包括TCP/WEB接入和IP接入。 |
| 攻击防护 | 实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC 和 IP 绑定功能，基于MAC的访问控制列表，802.1q VLAN 透传等功能。 |
| WEB应用防护 | 支持为Web应用提供基于 HTTP 和 HTTPS 的流量防护。对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站进行有效防护。 |
| 支持CC攻击防护，可基于检测请求报文头的X-Forwarded-For字段，以获取真正的源IP地址。 |
| 支持SQL注入、跨站脚本、远程代码执行、字符编码等攻击的防护，支持对网络设备、网页服务器、数据库等设备的专属特征分类。 |
| 入侵防御 | 支持超过18000条以上特征的攻击检测和防御。 |
| 支持对检测到的攻击行为的前后报文进行自动化抓包功能，方便用户对攻击行为进行取证。 |
| 防病毒 | 可基于病毒特征进行检测，实现病毒库手动和自动升级，实现病毒日志和报表；防病毒本地库数量600万+。 |
| 支持云端防病毒，为保证检测时效性，特征缓存数至少保证20万条且缓存保留时间不应少于700分钟。 |
| 网络管理 | 所投产品可纳入客户现有运维管理平台，并提供原厂运维工程师7×24小时远程或现场监控远维服务，每月提供运维报告以及资产报告。 |
| 产品资质 | 报价产品具备中国国家信息安全产品认证证书，提供有效证书复印件。 |

1. **设备安装要求**

|  |  |
| --- | --- |
| 指标项 | 技术参数及性能（配置）要求 |
| 服务内容 | 1、供货商须先发货到南方日报社在广州的总部，按要求完成设备的调试，测试通过后，供货商再将设备运到深圳现场进行上架调试；  2、供货商须将产品接入现有运维管理平台，提供产品服务方案，必须适应采购人在现有系统可能带来的网络安全方面的调整，配合完成与现有平台的网络及网络安全联调联测工作；  3、网络防火墙设备应实现与广州总部现有防火墙设备实现VPN互联； |
| 服务要求 | 1、供货商应在整个实施计划执行过程中对采购人予以充分协助，完全满足服务内容要求，并且提供详细的服务方案；  2、在系统联调、测试、验收阶段和质保期内，供货商应提供原厂商7×24小时现场、电话技术支持服务，如果不能解决问题，必须提供原厂商现场服务；  3、供货商应在最短时间内对采购人所提出的要求做出反应，供货商保证在接到采购人故障报修或咨询后1小时内给予响应，供货商售后服务工程师在4小时内到达用户现场；  4、供货商应满足安全事件应急响应；制定出网络、安全设备及网络安全应急响应方案，并且提供7×24小时电话服务；质保期内如发生网络安全事件，必须2小时内到达服务现场，启动应急方案并进行安全事件分析和解决问题；  供货商应满足备件服务；针对本项目所投软、硬件产品，质保期内如设备发生故障无法恢复时，可以在4小时内备件到达客户现场，确保业务系统运行不受影响； |

1. **报价说明**

供应商报价时须保证报价产品技术参数的真实性，必要情况下需向采购单位出具第三方权威机构的检测报告。