1. 项目介绍

**项目概述：**

本次招标项目是对光明日报社新老办公区域内无线网建设项目进行覆盖及实施,要求满足无线、有线独立运行，并对光明日报社全媒体采编发平台进行网络安全改造。

**建设内容：**

本次招标项目是在光明日报社内建设一套快速稳定、安全可控的无线办公网络，满足光明日报社内部员工的无线办公业务以及访客的上网需求。建设区域包含光明日报社大楼地下1层到5层，以及新办公区的整层区域。无线网络需要达到在上述区域内无死角覆盖，实现终端无缝漫游。同时，对现有全媒体采编发平台增加负载、审计、远程管理等安全设备。

**踏勘安排**

鉴于本项目涉及无线AP部署及工程施工，招标方将在项目招标公示期间组织投标人来项目实施现场踏勘，投标人应在规定时间和地点参加踏勘，并承担自身参与踏勘所发生的交通等相关费用。投标人未参加踏勘的，由此产生的不利后果由投标人自行承担。

1. 总体要求

本部分内容是根据本项目实际情况制定的。

1. 投标人必须仔细阅读本部分的全部条款。对本部分中存在的任何疑问、遗漏或相互矛盾之处，或是对于相关要求不清楚，认为存在歧视、限制的情况，投标人可以向采购中心寻求书面澄清。
2. 本部分所列明的工艺、材料和设备的标准以及参照的品牌或分类号仅起说明作用，并没有任何限制性，投标人在投标中可以选用替代标准，品牌或分类号，但这些替代应当等于或优于文件技术要求。
3. 履约保证金

 中标方应在与采购方签订合同后 30 天内，向甲方提供相当于合同总价百分之五（5%）的履约保证金。

1. 付款方式：
	* 1. 双方签订合同生效后15日内，采购方向中标方支付合同金额的30%；
		2. 中标方将合同货物安装、调试、试运行完成、驻场人员到位，经监理方及采购方验收签发验收书后3个月内，采购方向中标方支付合同金额的70%；
		3. 采购方验收合格后1年内，中标方完成质量保证义务，且无重大质量事故，履约保证金全额返还中标方。
2. 技术要求

A、总体要求

中标人要严格进行项目管理，各阶段都应提交相应的计划、设计方案，并经项目工作组认可后方可进行下阶段工作;并应确保人力、物力的定量投入，定期向项目组提交项目进展情况报告。

投标人提供的投标应答必须是真实可靠的，若发现不真实将导致投标被拒绝，如已签订合同则合同无效，且负相应责任。

投标人提供的产品所有部件、模块和功能特性应具有一定的成熟性，不接受实验室或测试阶段产品，为满足项目管理维护要求，投标人应充分考虑所投各类别产品的兼容性要求。

中标后，若采购推迟，中标人承诺，所投产品按原厂主流型号供货，且不高于原有采购价格。

B、技术支持

技术支持的方式包括：原厂技术服务、电话技术服务、现场技术服务、定期巡查服务和技术升级服务等。

C、售后服务

投标人对投标设备提供5年免费整机保修服务及规则库升级服务。保修期内更换的设备部件和易耗部件须为原厂备件。

1. 参数要求

以下说明中的需求和指标为最低要求，投标人所提供系统所有设备参数及实配应不低于所要求指标；标注“**★**”号为关键技术指标，不满足投标将被拒绝；标注“◆”和“#”为主要、重要技术指标，每有一项标“◆”指标不满足扣3分，每有一项标“#”的指标不满足扣2分，其他指标项不满足扣1分；

系统需求清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目** | **品目号** | **品目名称** | **套数** | **单位** |
| 无线网络设备 | A01-01 | 无线控制器 | 2 | 套 |
| A01-02 | 室内高密无线AP | 160 | 套 |
| A01-03 | 室内面板无线AP | 60 | 套 |
| A01-04 | POE交换机 | 18 | 套 |
| A01-05 | 无线入侵防御系统 | 1 | 套 |
| 网络安全设备 | B01-01 | 防火墙 | 6 | 套 |
| B01-02 | 安全隔离与信息交换系统 | 1 | 套 |
| B01-03 | 数据库安全审计系统 | 1 | 套 |
| B01-04 | VPN安全接入网关 | 2 | 套 |
| B01-05 | 应用交付系统 | 2 | 套 |
| B01-06 | 上网行为管理系统 | 2 | 套 |
| 运维驻场服务 | C01-01 | 运维驻场工程师服务A 1名 | 1 | 年 |
| C01-02 | 运维驻场工程师服务B 1名 | 1 | 年 |

技术要求：

无线网络设备

**投标产品指标要求：**

 A01-01无线控制器 2套

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 招标要求 |
| **基本参数** |
| 1 | **★** | AP管理数量 | 集中转发模式下最大可支持管理AP数≥250，本地转发模式下最大可支持管理AP数≥1000；配置250个AP的license； |
| 2 | ◆ | 硬件接口 | 千兆网口≥6；USB接口≥1； |
| 3 | ◆ | 转发性能 | 802.11转发性能≥4Gbps 每秒新建连接数≥7K，最大并发连接数≥200K |
| 4 | ◆ | 在线用户数 | 单台设备在线并发用户数≥10K |
| **功能参数** |
| 5 |  | VLAN | 最大支持VLAN数量≥4K |
| 6 | ◆ | 存储容量 | ≥120GB；保留拆机测验权利；  |
| 7 | ◆ | 认证方式 | 设备具备二维码审核认证、微信认证、短信认证 |
| 8 |  | Portal页面 | 1.支持Portal认证页面自定义； |
| 2.提供多种规则的Portal页面推送方式，具备根据AP/SSID、终端类型、时间计划推送不同的Portal页面，实现不同的区域推送不同的Portal认证页面； |
| 3.具备页面终端自适应，推送合适匹配终端的尺寸Portal页面； |
| 9 |  | 认证后跳转 | 具备认证后跳转，可根据用户/接入AP/终端类型设置不同的跳转页面或URL； |
| 10 |  | 部署模式 | 1.设备支持在WLAN网络使用过程中当设备ip地址发生变化时，无线网络连接不中断，无需重新认证功能，以确保业务的正常进行； |
| 2. 具备在同一个AP上实现部分本地转发部分集中转发；支持跨广域网、NAT部署远程接入点； |
| 3. 具备路由网关功能，具备静态IP、DHCP等上网方式； |
| 4. 具备SNAT、DNAT、PAT、双向NAT、端口映射等； |
| 5. 具备静态路由、策略路由、DNS代理等； |
| 11 |  | 分组管理 | 具备AP分组管理，方便AP设备的管理维护 |
| 12 |  | 终端识别 | 具备智能终端识别，能识别主流安卓、ios、WP、笔记本等接入终端 |
| 13 |  | 配置管理 | 设备可基于接入设备的类型、应用角色、用户位置进行访问策略、速率及QoS的配置管理。 |
| 14 |  | 流量管控 | 1.支持智能通道管理，支持流量父子通道技术，且支持不低于三级父子通道； |
| 2. 具备根据不同的应用、用户、用户组来划分流量通道及优先级设置； |
| 3. 具备流量通道内智能平均分配用户带宽； |
| 4.基于单用户的上下行流量管控，流控粒度1Kbps； |
| 5. 具备上网时长控制和流量配额，时长粒度精细到1分钟 |
| 6. 具备基于时间的流量管控，不同的时间段内分配不同的流量策略，灵活分配带宽资源； |
| 7. 具备基于终端接入位置的流量管控，不同的接入位置分配不同的流量策略； |
| 8. 具备基于终端类型（安卓、ios、windows等）的流量管控； |
| 15 |  | 射频管理 | 具备基于时间段定时开启或关闭射频，并可配置例外SSID |
| 16 |  | 负载均衡 | 具备基于用户数、流量、频段的负载均衡，在双频情况下，实现2.4G和5G的双频负载 |
| 17 | ◆ | 反制 | 具备WIPS，支持对非法接入点的检测、告警及反制，支持防钓鱼AP |
| 18 |  | VLAN划分 | 具备根据用户/用户组、接入AP位置/AP组、终端类型/MAC、RADIUS Class属性值/Group ID、AD属性值、证书属性值自动进行VLAN划分，终端接入时自动分配到相应的VLAN池中 |
| 19 |  | 数据中心 | 具备内置数据中心和外置数据中心两种保留方式；提供日志查询功能；对指定IP/用户组/用户/应用在指定时间段内的上网流量和上网时长进行查询； |
| 20 | ◆ | 分级管理 | 提供分级分域管理功能，不同域的管理员仅能管理特定域的设备，可分别指定各管理员的功能配置和监控权限； |
| 21 |  | 有线无线一体化 | 具备有线无线一体化，具备对有线用户进行认证、访问控制、流量管理等，提供统一中文Web管理界面； |
| 22 |  | 人流统计 | 具备统计每一个AP在最近一天、最近一周、最近一个月的接入用户数和上网流量及趋势变化； |
| 23 | ◆ | 灾备 | 具备 1+1 AC冗余热备；支持AC间AP快速切换； |
| 当AP与控制器的隧道断开后或控制器冗机故障，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； |
| 具备DHCP服务器冗余备份； |
| 具备认证服务器冗余备份，具备认证服务器逃生功能，当所有的第三方认证服务器冗机后，依然能保证新用户也能通过认证连入无线网络； |
| 24 |  | 管理界面 | 具备WEB、CLI、Telnet、SSH等，支持中文界面管理； |
| 25 | ◆ | 微信推广 | 具备支持多微信公众平台，一台控制器上可以同时配置多个微信公众号，实现微信推广； |
| 26 | ◆ | 信息推送 | 具备根据时间段、出现次数、接入位置实现在线间隔、定时、首次接入、终端出现以及接入位置、位置变更的信息推广；  |
| 27 |  | 人流分析 | 内置客流分析系统，支持按区域查看总到人数、新到人数、非首次到人数、新接入上网人数、总接入上网人数、平均驻留时间的统计及趋势变化； |
| 支持查看用户驻留时间分布的统计；支持客流分析原始数据的导出，包括终端类型、终端MAC、首次出现时间、最后出现时间、出现次数和接入终端的终端类型、终端MAC、首次接入时间、最后接入时间、接入次数； |
| 28 | ◆ | AP可视化 | 具备导入建筑图、楼层区域分布图，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、在线用户列表、实时流量等信息，方便管理员实时了解网络健康状态； |
| 29 |  | 上网审计 | AC设备具备与第三方上网审计设备组网，能实现AC开启portal服务的同时将用户IP、MAC、用户名、上下线时间等信息实时传递给上网审计设备。 |
| 30 | ◆ | 移动管理软件 | 可以通过手机APP管理所有AP，进行AP上线激活、故障分析、远程管理等工作。 |
| 31 |  | 应用识别 | 实配能识别不低于1900种的网络应用,内置预分类URL库 |
| 32 | ◆ | 销售许可证 | 提供公安部颁发的《计算机信息系统安全专用产品销售许可证》复印件 |
| 33 |  | 互联网公共上网服务(无线接入前端)检测报告 | 提供公安部计算机信息系统安全产品质量监督检测中心出具的《互联网公共上网服务场所信息安全管理系统(无线接入前端)检验报告》 |

 A01-02 室内高密无线AP 160套

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | **重要性** | **指标项** | **指标要求及参考型号** |
| **基本参数** |
| 1 | **★** | 整机性能 | 同时支持802.11a/n/ac和802.11b/g/n工作；3X3 MIMO (2.4G最大传输速率≥300Mbps，5G最大传输速率≥700Mbps，整机最大传输速率≥1000Mbps)；  |
| 2 | ◆ | 硬件 | 以太网口≥1\*10/100/1000Mbps |
| **功能参数** |
| 3 | ◆ | 认证方式 | 具备微信认证、二维码认证； |
| 4 |  | ACL策略 | 具备基于应用/协议/端口/时间段的ACL策略；具备根据AP/SSID/终端类型/终端MAC/用户/用户组的ACL策略下发 |
| 5 |  | 流量管控 | 具备基于应用/AP/用户/用户组的QoS流量通道划分；支持智能流控，根据在线用户总数进行带宽平均分配；支持根据SSID、应用类型进行无线空口资源的带宽划分，并支持802.11e优先级调度； |
| 6 | ◆ | 网关功能 | 具备网关功能，并支持DHCP Server和DNS代理功能 |
| 7 |  | 网络优化 | 具备时间公平算法，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；支持防终端粘滞，AP感知连接到的STA，并智能引导STA接入最佳AP；支持禁止低速率、弱信号的终端接入； |
| 8 | ◆ | 反制 | 具备WIPS，能对非法接入点、钓鱼AP、个人热点进行实时检测、告警及反制 |
| 9 |  | 功耗 | AP满负荷工作功耗≤20W，支持802.3at标准的PoE供电和12V电源适配器本地供电两种方式 |
| 10 |  | 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） |
| 11 |  | 接入人数 | 最大接入用户数≥256 支持基于SSID的接入用户数限制 |
| 12 |  | SSID设置 | 具备虚拟AP(多SSID)之间的隔离，SSID数≥32；支持中文SSID和SSID隐藏 |
| 13 |  | 工作模式 | AP具备集中转发和本地转发两种数据转发模式，同一个AP上支持部分本地转发部分集中转发； |
| 14 | ◆ | 胖瘦一体 | AP可以在没有无线控制器时单独使用；AP无需单独配置，通过无线控制器集中进行配置和管理； |
| 15 | ◆ | SRRC证书 | 提供中国无线电管理委员会颁发的SRRC核准证复印件 |

 A01-03室内面板无线AP 60套

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 招标要求 |
| **基本参数** |
| 1 | ◆ | 整机性能 | 支持802.11a/b/g/n/ac协议，支持802.11ac/a/n和802.11b/g/n双频并发，2X2 MIMO，2.4G最大传输速率≥300Mbps，5G最大传输速率≥700Mbps，整机最大传输速率≥1000Mbps；  |
| 2 | ◆ | 硬件接口 | 千兆以太网口≥1，百兆网口≥2，并需提供至少一个额外的电话扩展口 |
| **功能参数** |
| 3 | ◆ | 接入人数 | 最大接入用户数≥256； 支持基于SSID的接入用户数限制 |
| 4 |  | SSID设置 | 具备虚拟AP技术，SSID数≥32；支持中文SSID和SSID隐藏 |
| 5 |  | 负载均衡 | 具备基于用户、流量的智能负载均衡 |
| 6 |  | 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上支持部分本地转发部分集中转发； |
| 7 | ◆ | 认证方式 | 具备微信认证、二维码认证； |
| 8 |  | ACL策略 | 具备基于应用/协议/端口/时间段的ACL策略；具备根据AP/SSID/终端类型/终端MAC/用户/用户组的ACL策略下发 |
| 9 |  | 流量管控 | 具备基于应用/AP/用户/用户组的QoS流量通道划分；具备智能流控，根据在线用户总数进行带宽平均分配；支持根据SSID、应用类型进行无线空口资源的带宽划分，并支持802.11e优先级调度； |
| 10 |  | 网络优化 | 具备时间公平算法，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；支持防终端粘滞，AP感知连接到的STA，并智能引导STA接入最佳AP；支持禁止低速率、弱信号的终端接入； |
| 11 | ◆ | 反制 | 具备WIPS，能对非法接入点、钓鱼AP、个人热点进行实时检测、告警及反制 |
| 12 |  | 硬件规格 | 满足国家标准面板规格，能直接安装在86盒上 |
| 13 |  | 功耗 | AP满负荷工作功耗≤13W，支持802.3af标准的PoE供电 |
| 14 |  | 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） |
| 15 | ◆ | 产品资质 | 提供中国无线电管理委员会颁发的SRRC核准证复印件 |

 A01-04 POE交换机 18套

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 指标 | 指标项 | 指标要求及参考型号 |
| **基本参数** |
| 1 | ◆ | 硬件接口 | 千兆以太网口≥24个（24个POE口），千兆SFP光口≥4个（实配4个多模千兆光模块） |
| 2 | ◆ | 交换容量 | ≥48Gbps |
| 3 | ◆ | 包转发率 | ≥35Mpps |
| **功能参数** |
| 4 |  | 输出功率 | 整机最高POE输出功率不低于310W，能满足至少同时为20台802.3af标准的AP提供电力； |
| 5 |  | 供电标准 | 支持IEEE 802.3af以及802.3at两种供电标准，单端口最高输出功率≥30W； |
| 6 |  | VLAN设置 | 具备VLAN功能，至少支持不低于1000个VLAN；支持802.1Q标准 VLAN； |
| 7 | ◆ | 管理界面 | 支持WEB界面管理 |

A01-05无线入侵防御系统 1套

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | **指标项** | **招标要求** |
| 1 | **★** | **硬件规格** | 要求产品架构由无线入侵防御集中管控平台和无线入侵防御安全探针组成；标准1U机箱，不小于500G存储空间 |
| 2 | ◆ | **授权节点** | 无线入侵防御集中管控平台支持≥50个无线入侵防御安全探针，实际配置34个无线入侵防御安全探针 |
| 3 | ◆ | 热点探测 | 配置发现Wi-Fi网络（使用IEEE 802.11协议的局域网）的热点功能，包括隐藏SSID的热点。 |
| 4 |  | 配置识别所有发现热点的信息，包括热点MAC（BSSID）、热点名（ESSID）、热点频道（CH）、热点加密情况、热点信号强度（RSSI）、WPS状态。 |
| 5 |  | 配置分析热点的基于以下无线协议管理帧的事件：Authentication、Deauthentication、Association、Disassociation、Probe Request等 |
| 6 |  | 配置检测热点是否开启SSID广播、是否无认证或开启WEP认证、是否开启WPS功能。 |
| 7 | ◆ | 配置监视泛洪攻击、热点钓鱼攻击、客户端MAC地址克隆和恶意扫描攻击行为。 |
| 8 |  | 入侵分析 | 系统应对收集的数据包进行分析，发现安全事件。 |
| 9 |  | 系统应具有对高频度发生的相同安全事件进行合并告警，避免出现告警风暴的能力。 |
| 10 |  | 入侵响应 | 当产品检测到入侵事件时，应向用户发出安全警告。 |
| 11 |  | 告警可以采取屏幕实时提示、发送邮件等一种或多种告警方式。 |
| 12 | ◆ | 配置检测到的热点进行阻断，使得该热点不能被任何客户端连接。 |
| 13 | ◆ | 配置检测到的客户端进行阻断，使客户端无法连接任何热点。 |
| 14 |  | 产品应允许管理员定义对被检测网段中指定热点不予检测和告警。 |
| 15 |  | 管理控制 | 产品应提供友好的用户界面用于管理、配置产品的安全功能。管理配置界面应包含配置和管理产品所需的所有功能。 |
| 16 |  | 系统的事件数据库应包括事件定义和分析、详细的解决方案、可采取的对策等。 |
| 17 |  | 产品应能按照事件的严重程度将事件分级，以使授权用户能从大量的信息中捕捉到危险的事件。 |
| 18 |  | 产品应具有升级产品和更新事件库的能力。 |
| 19 | ◆ | 产品应记录并保存检测到的入侵事件。入侵事件信息应至少包含以下内容：事件发生时间、攻击类型、受攻击目标、危害等级、事件详细描述以及解决方案建议等。 |
| 20 |  | 用户应能通过管理界面实时清晰地查看入侵事件。 |
| 21 |  | 系统应能生成反应目标无线网络安全概况的检测防御结果报告。 |
| 22 |  | 用户管理 | 产品应提供创建、修改和删除用户的管理能力。 |
| 23 |  | 用户标识 | 产品应为每个用户规定与之相关的安全属性，包括：标识、鉴别信息、隶属组、权限等。 |
| 24 |  | 产品应提供使用默认值对创建的每个用户的属性进行初始化的能力。 |
| 25 |  | 产品应保证任何用户都具备唯一的标识，用户标识与产品自身审计相关联。 |
| 26 |  | 身份鉴别 | 当用户请求管理产品时，产品应鉴别用户的身份。 |
| 27 |  | 若采用口令鉴别机制，应以非明文显示和存储口令。 |
| 28 |  | 鉴别数据管理 | 产品应根据规定的鉴别机制，提供授权用户鉴别数据的初始化功能，并确保仅允许授权用户使用这些功能。 |
| 29 |  | 产品应保护鉴别数据在传输和存储过程中不被未授权查阅和修改。 |
| 30 |  | 对用户身份进行鉴别时，产品应仅将最少的反馈（如：鉴别的成功或失败）提供给被鉴别的用户。 |
| 31 |  | 鉴别失败处理 | 当用户鉴别尝试失败连续达到指定次数后，产品应阻止用户进一步的鉴别请求，并将有关信息生成审计事件。最多失败次数默认或仅由授权用户设定。 |
| 32 |  | 超时锁定 | 产品应具有访问超时锁定功能。在设定的时间段内授权用户没有对产品进行任何操作的情况下终止会话，需要再次进行身份鉴别才能够重新操作。最大超时时间仅由授权用户设定。 |
| 33 |  | 安全审计 | 产品应对下列可审计事件生成审计日志： |
| 34 |  | a)         所有用户鉴别机制的使用，包括用户的登录和注销； |
| 35 |  | b)        用户操作的行为，包括配置策略、查看入侵防御结果等； |
| 36 |  | c)         对用户进行增加、删除和属性修改的操作。 |
| 37 |  | 对于每一条审计日志，产品应至少记录以下信息：事件发生的日期和时间，事件的类型，主体身份和成功或失败事件。 |
| 38 |  | 支持按照一定条件对审计日志进行检索或排序。 |
| 39 |  | 审计日志安全 | 具有明确的访问权限的授权用户员之外，产品应禁止所有其他用户对审计日志的访问。 |
| 40 |  | 支持审计日志存储于掉电非易失性存储介质中，当审计日志的存储容量到达阀值时，应能及时通知授权用户。 |
| 41 |  | 通信安全 | 支持各组件之间传输的数据（如配置和控制信息、审计日志等）非明文传输。 |
| 42 |  | 产品资质 | 提供公安部颁发的有效期内的《无线入侵防御系统产品销售许可证》 |
| 43 | ◆ | 符合国家无线电管理规定和技术标准，提供工业和信息化部颁发的有效期内的《无线电发射设备型号核准证》 |

网络安全设备

**投标产品指标要求：**

 B01-01 防火墙 6套

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 招标指标 |
| **基本参数** |
| 1 | **★** | 硬件规格 | ≥2U机箱，冗余电源； 要求配置1个Console口 、1个HA接口，1个管理网口，实配4口万兆光口（含4个万兆多模光模块）、4个千兆光口（含4个千兆多模光模块）,1个扩展板卡插槽（无占用）；  |
| 2 |  | 管理要求 | 配置液晶管理屏 |
| ◆ | 性能参数 | 网络处理能力≥45G；并发连接数≥600万； 每秒新建连接≥60万/秒； |
| **功能参数** |
| 3 |  | **网络适应能力** | 支持路由、透明、交换、旁路以及混合模式接入，满足各种复杂应用环境的接入需求 |
| 4 |  | 支持物理子接口技术，可虚拟多个逻辑接口，支持安全域配置，含二层安全域和三层安全域 |
| 5 |  | 支持策略路由优先级调整命令行，支持根据安全域、源目的IP、ISP、应用和服务进行智能选 |
| 6 |  | **访问控制能力** | 支持详尽细化的会话超时时间自定义设置，包括：TCP握手、TCP建立、TCP单向关闭、关闭、UDP单向数据、UDP的DNS、UDP的其他、其他协议、GRE协议、TCP长连接、UDP长连接和其他协议的长连接 |
| 7 |  | 支持基于地理区域的安全策略及地理区域对象的导入 |
| 8 |  | 支持会话限制功能，可以根据IP地址、安全域（入、出、双向）、应用对单个IP或所有IP进行新建和并发连接限制 |
| 9 |  | 支持按源目的IP、源目的接口、用户、地理区域及应用进行流量排名，并显示流量统计 |
| 10 |  | **链路冗余能力** | 具备基本网关配置，具备9种均衡方式：源地址目的地址哈希、轮询、源地址哈希、目的地址哈希、源地址轮询、备份、随机、RTT最小、流量均衡 |
| 11 |  | 具备静态路由的负载均衡（最大支持5条），支持基于优先级的链路备份，具有备援网关功能 |
| 12 |  | **网络行为管理** | 具备自定义添加关键字，并设置每一个关键字的权重值。当命中的关键字权重相加超过警戒值之后，将会触发内容过滤策略，数据会依据内容过滤策略的动作判断是允许还是拒绝 |
| 13 |  | **带宽管理能力** | 支持QoS配置向导，支持多层级调度类嵌套进行最大带宽限制、最小带宽保证 |
| 14 |  | 支持优先级设置实现差分服务，实现对剩余带宽的动态分配 |
| 15 |  | **高可用性** | 支持抢占模式和非抢占模式，并支持非抢占模式强制主备切换，支持透明模式非对称主主部署 |
| 16 |  | **抗攻击能力** | 具备对应用层Flood攻击进行五种处理动作：警告、阻断、普通防护、增强防护及授权服务器防护，具备TC反弹技术和ns重定向技术，具备SYN Cookie设置 |
| 17 |  | 支持局域网广播防护，支持全局配置的局域网广播防护及基于二层接口的局域网广播防护，可以防止局域网内广播和多播数据包泛滥，保障网络正常通信 |
| 18 |  | 支持DHCP防护，可进行DHCP服务器检查、DHCP请求检查和DHCP请求限速等功能 |
| 19 |  | **防弱口令扫描** | 支持针对FTP、SMTP、POP3、IMAP协议防弱口令扫描功能，可以帮助用户记录或者拦截网络中猜测FTP用户名密码，邮件用户名密码的行为。并支持生成动态策略，下发给防火墙，再次受到相同攻击时，可指定执行禁止或允许口令猜测的行为 |
| 20 | ◆ | **木马防护** | 通过系统联动及木马云查能生成日志或者动态策略，阻断数据或者记录日志 |
| 21 | ◆ | **动态策略** | 可通过与入侵防护、防弱口令扫描联动，生成动态策略信息，命中动态策略的数据将会被阻断或者记录日志 |
| 22 | ◆ | **安全联动** | 支持系统协同联动，根据不同级别设置动作的情报配置，支持基于协议、本地地址、本地端口、本地证书、状态的情报接收，支持基于协议、远端地址、远端端口、URL地址状态的情报查询 |
| 23 | ◆ | **产品资质** | 提供公安部颁发的防火墙万兆《计算机信息系统安全专用产品销售许可证》防火墙（三级） |
| 24 | **★** | 提供中国信息安全认证中心颁发的《中国国家信息安全认证产品型号证书》（三级） |
| 25 |  | 提供中国信息安全测评中心颁发的有效期内的防火墙万兆《国家信息安全测评信息技术产品安全测评证书》（EAL3+） |

B01-02 安全隔离与信息交换系统 1套

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | **指标项** | **招标要求** |
| **基本参数** |
| 1 | **★** | **产品规格** | ≥2U机箱，配置冗余电源，系统吞吐量600Mbps，内部交换带宽5Gbps，内外网分别配置6个10/100/1000Base-T端口，1个Console口，2个USB口，1个扩展槽位（无占用） |
| 2 |  | **管理要求** | 配置液晶管理屏 |
|  | **安全** | 内、外网分别具有独立的管理接口，而不是通过网络接口管理，也不是通过内网一个管理接口完成全部管理 |
| **功能参数** |
| 3 | ◆ | **管理** | 支持用户名/密码+U-KEY、用户名/密码+数字证书等多种双因子认证方式；  |
| 4 | ◆ | 支持带内管理，可通过业务口进行网闸管理工作；用户可自行选择是否启用带内管理功能；  |
| 5 |  | 管理员及审计员区分并独立，支持分权管理，对管理员角色定制，可以添加多个管理员角色，并定制权限 |
| 6 | ◆ | 支持设备健康状态追踪，通过可视化界面实时显示设备健康状态分布图；  |
| 7 | ◆ | **主模块** | 支持配置管理，能够对单独模块及全部模块配置进行配置导入导出 |
| 8 | ◆ | 当服务器异常重启，客户端可自行启动，无需人员干预；  |
| 9 | ◆ | 支持缓时设置，可根据文件大小设定缓时时间，保证文件传输稳定性和成功率；  |
| 10 |  | 支持客户端、无客户端多种部署方式实现数据库同步； |
| 11 | ◆ | 同步由网闸主动发起并完成，不需要第三方软件支持（无需在数据库安全任何第三方软件），支持windows、linux、unix等多种数据库操作系统类型。 |
| 12 | ◆ | 支持客户端与设备间的认证，认证通过才能进行数据源及任务配置； |
| 13 | ◆ | 支持客户端服务绑定功能，可绑定自定义IP、端口，避免服务端口冲突；  |
| 14 |  | 支持周期复制、实时复制、增量更新等多种同步方式。 |
| 15 |  | **邮件访问** | 邮件模块支持病毒检测功能；支持通过文件大小控制病毒查杀；支持超长邮件限定是否接受； |
| 16 |  | 支持任务运行时间控制 |
| 17 |  | 支持达梦、人大金仓、神通等国产数据库访问 |
| 18 | ◆ | 支持ORCLE数据库命令控制，可对数据库SQL语句进行过滤；  |
| 19 | ◆ | 数据库库名控制、数据库表控制，可以根据用户与数据库表对应关系，进行相应数据库操作过滤；  |
| 20 | ◆ | 支持任务运行时间控制 |
| 21 | ◆ | **FTP模块** | 支持透明模式、代理模式及混合模式 |
| 22 |  | FTP访问模块支持病毒检测功能，支持通过文件大小控制病毒查杀； |
| 23 |  | 支持任务运行标记 |
| 24 |  | 安全浏览模块支持病毒检测功能，支持通过内容长度控制病毒查杀；支持图片文件、媒体文件等文件类型病毒检查；可设定病毒扫描内容最大长度。 |
| 25 |  | **防护设置** | 支持入侵检测功能，可对网页攻击、缓冲区溢出攻击、后门/木马、P2P、病毒/蠕虫、拒绝服务攻击、扫描类攻击等多种攻击类型进行实时检测并记录日志。 |
| 26 |  | 支持双引擎病毒模块，可根据用户需求选择需要的病毒引擎 |
| 27 |  | 支持在线升级、离线升级等病毒库升级方式。可针对文件交换、安全浏览、FTP访问、邮件访问等多种模块进行病毒防护。 |
| 28 | ◆ | **产品资质** | 提供公安部颁发的有效期内的安全隔离与信息交换系统《计算机信息系统安全专用产品销售许可证》网闸（三级） |
| 29 |  | 提供中国信息测评中心颁发的有效期内的安全隔离与信息交换系统《国家信息安全测评信息技术产品安全测评证书》（EAL3+） |
| 30 | **★** | 提供中国信息安全认证中心颁发的有效期内的安全隔离与信息交换系统《中国国家信息安全产品认证证书》（二级） |

B01-03 数据库安全审计系统 1套

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | **指标项** | **招标要求** |
| **基本参数** |
| 1 | **★** | 硬件规格 | ≥2U机箱，本次要求配置冗余电源、配置16G内存、配置8个热插拔硬盘槽位,存储空间实配4TB，可扩展到16TB ， MTBF≥100,000小时  |
| 2 | ◆ | 产品性能 | 事件采集能力≥16000条/秒，事件存储能力≥4TB硬盘可以在线分析≥3.7TB的事件量； |
| 3 | ◆ | 接口 | 网络口：6个千兆以太网接口，配置1个扩展槽，（无占用）配置七路的监听授权许可，2个USB接口，1个串口,2个VGA接口 |
| 4 | ◆ | 审计许可 | 配置审计数据库数量≥100个 |
| **功能参数** |
| 5 | ◆ | 审计范围 | 审计包括包括MS SQL Server、Oracle、DB2、Sybase、MySQL、Informix、达梦、Postgresql、Cache等在内的多种数据库；支持审计HTTP/HTTPS协议的URL、访问模式、cookie、页面内容、Post内容 |
| 6 | ◆ | 数据库审计 | 支持Cache数据库集成工具terminal、portal、studio、Sqlmanager、MedTrak工具的审计，其中Portal能审计到sql语句、查询Global、返回结果，Terminal能审计到M语句和返回结果（提供审计界面截图；中间件的支持，支持COM、COM+、DCOM组件 |
| 7 |  | 数据库安全 | 支持对SQL注入、跨站脚本攻击等web攻击的识别与告警 |
| 8 | ◆ | 审计策略 | 支持数据库语句执行时间、语句执行回应、最大操作语句长度等作为分项响应条件；数据库审计策略支持数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件；支持超长操作语句审计，针对传统型数据库，支持3万字节的审计而不截断 |
| 9 | ◆ | 审计查询 | 审计数据支持18种以上查询条件，可支持按数据库操作命令（包括select、create等14个命令）、语句长度、语句执行回应、语句执行时间、返回内容、返回行数、数据库名、数据库账户、服务器端口、客户端MAC、客户端IP、客户端端口、会话ID、关键字、时间（包括开始、结束日期）等为条件进行查询,还可以提供客户端操作系统主机名、客户端操作系统用户名、客户端进程名等信息；实现对所有违规事件出现频率进行图形化的汇总统计分析，并提供对汇总结果的实时查询功能；可以对客户端使用的程序、客户端IP、使用频率进行图形化排名展示 |
| 10 |  | 审计安全 | 审计结果隐秘设置，通过\*号对审计结果中的重要信息进行隐秘处理，防止非法权限查看；系统本身具备能发现未知仿冒进程工具、防范非法IP地址、防范暴力破解登录用户密码、设置系统黑白名单等安全功能；管理员登陆支持静态口令认证，支持密码的复杂性管理，比如大小写、数字、特殊字符、长度等；能够对连续失败登陆进行自动锁定，锁定时间可设置 |
| 11 |  | 配置管理 | 采用B/S管理方式，全中文界面；提供系统升级功能，能够通过升级包的方式实现升级；提供审计数据管理功能，能够实现对审计数据的自动备份、手动备份，支持增量、全量备份方式；提供设备自身CPU、内存、磁盘、网口、运行时间、运行状态等信息的监视功能；提供审计策略和配置的导入导出 |
| 12 | ◆ | 产品资质 | 提供公安部颁发数据库安全审计《计算机信息系统专用产品销售许可证》（增强级） |
| 13 | **★** | 提供中国信息安全认证中心颁发的安全审计系统《中国国家信息安全产品认证证书》（增强级）， |
| 14 |  | 提供中国信息安全测评中心颁发的有效期内的安全审计系统《国家信息安全测评信息技术产品安全测评证书》（EAL 3+） |

B01-04 VPN安全接入网关 2套

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | **指标项** | **招标要求** |
| **基本参数** |
| 1 | **★** | 硬件规格 | ≥2U 机箱，配置冗余电源，配置6个10/100/1000M自适应电口，4个千兆SFP接口（含4个千兆多模光模块） |
| 2 |  | 管理要求 | 配置液晶管理屏 |
| ◆ | 产品性能 | SSL加密吞吐量≥800Mbps，新建用户≥3000次/秒，SSL并发连接数≥80000，支持并发用户数≥2000，配置300个远程接入许可和软token身份认证 |
| **功能参数** |
| 3 |  | **完整性支持** | 支持IPSec VPN和SSLVPN两种VPN协议，是SSL VPN和IPSec VPN二合一产品 |
| 4 |  | 支持Windows（Win7、win7 64位、win8）、Macos、IOS、Android、国产化中标麒麟操作系统客户端APP，在Linux系统平台下具备独立的SSLVPN客户端。 |
| 5 |  | 支持动态域名解析，支持希网、花生壳动态域名设置。 |
| 6 | ◆ | 支持预防'syn flood'攻击，忽略icmp回显请求。 |
| 7 |  | 支持在域环境下发布ssl客户端控件，并提供MSI包。 |
| 9 |  | 认证方式支持15种，本地认证、USBKey、短信认证、数据库认证、邮箱认证、证书认证、动态口令认证、LDAP认证、windows AD认证、RADIUS认证，并且支持支持本地用户名密码、证书认证、第三方证书、LDAP、短信验证码、邮箱验证码、SecToken之间的“与”的认证。可实现USBKey认证、LDAP认证、硬件特征码等多种因子绑定认证。 |
| 10 | ◆ | 支持SecToken根据网关配置的安全策略，进行Root、越狱检测，杀毒检测，若不通过，禁止登录和绑定。 |
| 11 | ◆ | 支持SecToken根据网关配置的安全策略，实现一人一机绑定，达到硬件token的安全要求 |
| 12 | ◆ | 为了保证动态密码的安全，要求SecToken不能通过二维码扫描方式获取动态密码，而是通过Token server地址、用户名、密码的方式连接到Token server获取动态密码 |
| 13 | ◆ | 支持LDAP用户动态化和策略化，实现组织单元映射、属性映射，并支持成员组反向映射。 |
| 14 | ◆ | 支持RADIUS双机认证，管理员可定义的Radius 属性组与系统中其他组一样作为授权对象，可实时与RADIUS建立联系，保证用户数据更新，保证认证的高可用性。 |
| 15 |  | 可单独对每个应用发布业务进行负载均衡，具有轮询、加权轮询、最少连接数、静态就近性、动态就近性等算法来实现 |
| 16 |  | 管理员可分为状态管理员，系统配置管理员，VPN管理员，应用安全管理员，防火墙管理员，IPsec管理员,日志管理员，系统维护管理员，创建管理员可以为其分配相应的管理员权限。 |
| 17 |  | 能显示在线用户列表，并能把在线用户以列表形式导出，可以导出为txt、HTML文件。 |
| 18 |  | 具备用户访问业务的详细日志记录，如账号、密码、提交POST内容 |
| 19 |  | 支持显示各模块日志信息，包括SSL VPN、IPSec VPN、防火墙、应用安全、入侵防御等模块；可以用柱型图比较系统日志等级的数量，可以查看用户登录日志和资源访问日志，用户日志可以按照年、月、日、类型查询。 |
| 20 | ◆ | 支持管理员自定义用户登录帮助文档，通过虚拟门户上传到SSLVPN用户的WEB登录界面，文档格式支持word和TXT。用户登录时刻自行下载帮助文档。 |
| 21 |  | 具备CPU告警、具备内存告警、具备用户授权数告警、具备管理员账号登陆锁定告警、具备用户账号登陆锁定告警，告警方式为邮件、短信、邮件和短信。 |
| 22 |  | 虚拟化 | 产品基于虚拟化云平台技术，提供虚拟VPN技术； |
| 23 | ◆ | 具备虚拟化多租户管理机制，可为不同的部门提供不同虚拟化VPN接入口； |
| 24 | ◆ | 支持直连、代理方式与企业服务器相连，为企业用户提供虚拟化业务服务； |
| 25 | ◆ | 支持私有云部署方式，通过在私有云端安装agent，方便员工连接企业私有云； |
| 26 |  | 支持虚拟用户建立，可通过虚拟用户功能建立临时云VPN账号； |
| 27 |  | 支持安全干净桌面，安全桌面后只显示我的电脑、回收站、网上邻居 |
| 28 |  | 支持安全桌面和本地桌面切换功能，确保一机两用 |
| 29 |  | 智能终端实现对WIFI、联通2G/3G/4G、移动2G/3G/4G、电信2G/3G/4g访问控制 |
| 30 |  | Android、iOS操作系统支持二维码方式下载客户端 |
| 31 | ◆ | 根据IOS或Android的状态root、越狱、杀毒结果进行准入控制 |
| 32 | ◆ | 根据IOS或Android的状态root、越狱、杀毒结果进行应用授权 |
| 33 |  | 支持移动应用封装功能，客户上传移动应用APP进行封装、加固 |
| 34 |  | 支持对移动应用本身进行病毒、木马检测，以保证移动应用自身安全 |
| 35 |  | 网关和Android、IOS支持应用下载功能 |
| 36 | ◆ | 针对移动应用在本系统的应用下载分发、运行后，可对移动应用进行下载次数统计 |
| 37 | ◆ | 针对移动应用在本系统的应用下载分发、运行后，可对移动应用进行评价，促进移动应用的改进 |
| 38 |  | 对接入的智能终端可手动设置其状态“禁止”或启动 |
| 39 | ◆ | Android、iOS操作系统具备二维码扫描登陆，自动代填登陆地址和端口 |
| 40 |  | 应用封装后的APP可通过应用下载按照不同分组、权限进行分发 |
| 41 | ◆ | 具备智能终端连接网关后，只能走安全隧道，防止互联网访问 |
| 42 |  | 支持对智能终端进行控制，如摄像头控制、密码策略控制 |
| 43 |  | 支持移动APP数据进行加密，防止数据泄露 |
| 44 | ◆ | 支持移动app工作区数据擦除以及设备整体数据擦除，防止智能终端丢失后造成数据泄密 |
| 45 | ◆ | **资质** | 提供公安部颁发的VPN《计算机信息系统安全专用产品销售许可证》（三级）及检验报告 |
| 46 |  | 提供中国信息安全测评中心颁发的安全接入网关《国家信息安全测评信息技术产品安全测评证书》 |

B01-05 应用交付系统 2套

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | **指标项** | **招标要求** |
| **基本参数** |
| 1 |  | 硬件平台 | 配置双电源；非UTM类设备。 |
| 2 | **★** | 硬件规格 | ≥2U机箱,冗余电源，标配6个千兆电口，具备1个扩展槽（实际配置4个光口、含光模块） |
| 3 | ◆ | 性能指标 | 最大四层整机吞吐≥6G，最大四层并发连接数≥200万，最大四层每秒新建连接数≥10万 |
| **功能参数** |
| 4 |  | 部署模式 | 支持路由、旁路部署，以及三角传输 |
| 5 |  | 高可用性 | 支持AA，AP工作模式，IP地址可在设备间漂移，根据设备状态将流量牵引到主设备。支持包括半连接，全连接会话信息全状态同步； |
| 6 |  | 支持会话保持信息同步；以保障业务不间断切换。 |
| 7 |  | 支持标准VRRP协议。 |
| 8 |  | N+1集群部署：可以实现两台以上设备集群部署，一台设备充当在线备份，各设备可以是不同的软件版本和型号，实现弹性扩展。- |
| 9 | ◆ | 功能 | 实现链路负载均衡、链路特征库、服务器负载均衡，全局负载，应用加速，智能DNS，单边加速功能； |
| 10 |  | L4服务器负载均衡 | 支持SNMP方式动态读取服务器运行状态进行算法调节；支持轮询、加权轮询、加权最小连接、动态反馈、源IP哈希等算法。 |
| 11 |  | SIP负载分担（基于UDP及TCP的负载分担）；流媒体负载分担（RTSP\MMS） |
| 12 |  | 对于源，目的IP相同的UDP访问，可以对每个报文进行分类转发，保证流量负载的均衡性。可以对Radius等接入认证服务器做基于每用户的负载均衡，并且保证每个用户的请求分发到相同的服务器。 |
| 13 |  | 服务器过载保护：支持服务器每秒新建连接和会话数限制，保证分担任务不超过其负载能力。 |
| 14 |  | L7服务器负载均衡 | 通过应用层代理，可解析客户端请求内容， 并根据客户端请求头域做内容分发，将访问不同内容的请求代理到相应服务器上；并将响应数据代理到对应客户端。对图片类、文字类的请求，分别转发到对应的图片、文字服务器，支持基于Cookie、User-Agent、URL、HTTP头的分担模式 |
| 15 |  | 服务器敏感信息保护：HTTP头擦除、重定向信息改写、COOKIE加密 |
| 16 |  | 设备接收到的HTTP流量时，可以按指定的规则对其内容进行管理，完成对出入的HTTP流量的检查、过滤、修改。主要包括：合规性检查、报文内容修改、重定向等功能。 |
| 17 |  | 支持Http协议重写：可以把HTTP请求自动重写为HTTPS协议，实现HTTP到HTTPS的无缝切换 |
| 18 |  | 对于客户端与服务器需要多次交互过程才能完成交易的访问（特别是身份认证系统）；可以根据上一次交互过程的处理结果，分发后续的客户请求，保证相关的客户端请求都由一台服务器完成，支持基于IP地址、Cookie、SSL session id、Server-ID in URL Query、Custermer-ServerID、Rule Based等模式。 |
| 19 |  | 服务器健康检查 | 支持主动式健康检查，包括ICMP、TCP、UDP、FTP、HTTP、HTTPS、LDAP、NTP、POP3、Radius、SMTP、SNMP以及自定义的多重服务器健康检查机制。 |
| 20 |  | 基于业务的状态检查：允许用户自定义检查数据流使之贯穿整个业务系统，允许用户设置GET\POST方法模拟客户提交内容，并自定义服务器返回数据检查点来判断业务系统是否工作正常。 |
| 21 |  | 支持定期生成服务器健康状态报表。 |
| 22 | ◆ | 应用系统加速 | 开通压缩、缓存、TCP连接复用、SSL协议卸载功能的授权。 |
| 23 | ◆ | 通过HTTP协议的增强，实现数据流的多路复用、请求优先级及HTTP报头压缩技术，提升网络速度、优化用户的网络响应速度。 |
| 24 |  | 支持将客户端发送的多个HTTP请求封装在一个TCP数据包内，减少网络负载，避免单个HTTP延迟导致的重传、阻塞。实现http协议加速。- |
| 25 |  | 可自动识别移动终端的访问，并将请求的图片进行优化，将图片进行转码后传输，减少图片传输的流量，并适配移动终端展现。 |
| 26 | ◆ | 通过控制缓存请求连接的速率， 阻止猛增的大量请求进入服务器，从而防止服务器过载，在服务器达到其最大容量时，能够出提示页面，使后续用户自动等待，避免反复刷新。 |
| 27 |  | 全局负载 | 支持标准DNS服务器功能，支持多种DNS 记录 ，包括A ，NS，CNMAE，TXT，MX，PTR记录。支持DNS 授权区域，可将DNS名称空间划分为区域来进行管理。可转发DNS请求，持 forward-only  forward-first 两种DNS转发模式。 |
| 28 |  | 基于DNS方式，在不同地域数据中心之间实现流量牵引； |
| 29 |  | 支持地域优先、静态就近性、动态就近性、基于权重、基于session、基于服务器数量；- |
| 30 |  | 支持配置信息同步、状态信息同步 |
| 31 | ◆ | 多链路负载均衡 | 含10条以上链路进行流量均衡的授权。 |
| 32 |  | 通过TCP丢包预测，快速重传和恢复机制，提高TCP协议的数据传输速度，当广域网链路出现延时和丢包的情况时，可明显改变TCP传输效率，提升传输速率不用在用户终端上安装任何插件和软件，即可提升链路访问速度，节省带宽资源。。 |
| 33 |  | 智能DNS：实现链路智能Inbound访问，避免跨运营商访问。 |
| 34 |  | 支持内网用户上网DNS透明代理，DNS透明代理对内网用户访问外网资源的DNS解析过程进行优化，可以通过对多条链路发起DNS请求探测，根据探测结果结和预先设定的策略，将DNS请求转发到不同的服务器，避免出现因为DNS导向问题导致的某条链路拥塞，某条链路空闲的情况。 |
| 35 |  | 根据用户实时访问情况，动态探测每条链路到用户访问服务的的目标可达性，及延迟信息；并计算出最佳访问链路。并且随着链路质量的变化，可自动调整重新选择最佳发送链路。 |
| 36 |  | 业务的带宽保障：在链路拥塞时，支持对指定业务分配优先级，高优先级的业务优先处理，可以实现对指定业务的带宽保证，链路空闲时，所有业务可以任意使用带宽，链路拥塞时，可保障指定业务使用带宽。  |
| 37 | ◆ | 应用路由：支持常见流媒体，P2P软件，网络游戏， IM ，股票软件的检测识别；可将对相应流量分配到期望的目标链路，可进行速率控制； |
| 38 |  | 网络特性 | 支持动态路由协议RIP，OSPF，BGP，不需要单独授权。 |
| 39 |  | 支持V4/V6双栈，支持V4/V6地址转换,支持前缀地址转换，IVI，地址池，IPv4和IPv6混合环境下的四层服务器负载，链路负载，健康检查。 |
| 40 |  | 支持DNSv6，支持基于IPV6地址的七层内容交换（URL负载、HTTP头擦除、重定向信息改写等功能）。  |
| 41 |  | 支持802.1Q VLAN，STP生成树协议 |
| 42 |  | 支持SNMP V1/V2/V3协议 |
| 43 |  | 可编程脚本语言 | 通过标准的TCL语言实现业务逻辑的可编程控制，通过编程方式支持根据任意数据段内容的负载均衡、HTTP头部内容按需改写等功能。可提供操作界面及工作原理说明 |
| 44 |  | 统计功能 | 支持统计虚拟服务和真实服务器的流量、访问次数、并发连接数。 |
| 45 |  | 安全管理 | 支持全中文的管理界面和HTTPS方式登录、用户角色管理、多级授权管理。 |

B01-06 上网行为管理系统 2套

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 指标要求 |
| **基本参数** |
| 1 | ◆ | 产品规格 | ≥2U机箱，要求配置6个千兆电接口、4个千兆SFP插槽（含4个SFP多模模块），1T磁盘空间，流量管理吞吐量≥2200Mbps，最大并发连接数≥100万，最大新建连接数≥50000个/秒 |
| **功能参数** |
| 2 |  | 协议处理 | 支持GRE、L2TP、WLTP、CAACWS、LWAPP、CAPWAP协议下的网络环境 |
| 3 | ◆ | IPv6支持 | 能够支持IPv6环境下的应用识别管控、带宽管理、网址访问审计与管控、生成分析报表等功能；能够在IPv6环境下，正确审计显示用户的IPv6地址；能够正确配置免监控等功能的IPv6地址 |
| 4 |  | Web管理 | 可通过IE、谷歌、火狐浏览器访问设备管理界面 |
| 5 |  | 命令行管理 | 支持采用公开SSH2客户端远程访问设备，配置命令行，支持采用PC自带超级终端通过设备串口管理设备，配置命令行 |
| 6 |  | 账号安全 | 支持管理员账号初始密码检测，如果发现管理员未更改初始密码，能够进行提醒 |
| 7 |  | 审计日志存储 | 支持将多台设备日志集中存储于一台日志中心服务器，便于数据的集中查询与统计。 |
| 8 |  | 访问、日志中心数据必须采用https加密方式访问，避免传输过程被窃取。 |
| 9 |  | 日志中心能够对多台设备的日志进行聚合式搜索，用户执行一次关键字搜索即可在多台设备中搜索出所有具有此关键字的审计日志 |
| 10 | ◆ | 用户识别 | 支持对802.1X、Kerberos、LDAP、POP3、SMTP、Radius、PORTAL、锐捷SAM、H3C CAMS、PPPOE、城市热点等系统的单点登录。 |
| 11 | ◆ | 特权用户 | 支持key免审计、key免管控、key免认证以及三者灵活组合 |
| 12 |  | 认证 | 可以建立认证页面与多个认证跳转成功页面，供不同的Web认证策略引用，并支持用户完全自定义 |
| 13 | ◆ | 分级管理 | 具备分级管理功能功能，1、 超级管理员无权看审计日志；2、 审计员须经过超级管理员授权，才能看日志 3、 审核员仅能审核审计员权限是否合法，不能看日志 |
| 14 |  | 用户自动分类 | 可以为用户添加多属性，并根据用户的属性（如职位、部门、电话、邮件等）自动进行用户分类，根据分类的结果做审计、控制策略 |
| 15 |  | 数据库认证 | 和客户用户管理系统数据库联动进行用户认证 |
| 16 |  | 识别用户设备类型、位置 | 可识别用户上网设备类型作为“工具”对象，并可作为策略条件。可将IP或IP段作为“位置”对象，并可作为策略条件。 |
| 17 | ◆ | URL库大小 | ≥3000万条URL数据，≥150种网页分类 |
| 18 | ◆ | URL分类反馈 | 当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；管理员可查看用户反馈的分类错误，并可以选择向服务器反馈 |
| 19 |  | 阻塞提示 | 不同网页被阻塞后会跳转不同的阻塞页面；支持用户完全自定义 |
| 20 |  | 发帖审计与管理 | 对网站的发帖正文关键字进行管理，一条策略可同时实现控制、记录、告警、便于维护管理； |
| 21 |  | Web页面推送 | 根据用户、终端类型、时间等多个条件为不同的用户推送Web页面。可以建立多个Web推送页面，供不同的推送策略引用，支持用户完全自定义 |
| 22 |  | 邮件延迟预审策略 | 根据邮件标题、正文、附件名、文件触发延迟审计，邮件在通过管理员审核后才能够发送。 |
| 23 |  | 网盘文件外发管理 | 支持百度云、115、华为网盘（DBank）、360云盘等网盘的文件外发审计与过滤，可根据文件大小、文件名、扩展名、传输方向、内容关键字进行审计过滤 |
| 24 |  | QQ审计与管理 | 可针对QQ账号制定策略，对聊天、登录及登出的行为进行记录与控制；  |
| 25 |  | Skype审计 | 支持Skype账号、聊天内容、行为审计与控制。 |
| 26 |  | 支持skype外发文件内容的审计 |
| 27 |  | 百度HI审计 | 支持百度HI账号、内容、行为审计与控制 |
| 28 |  | 应用审计及控制 | 可以对P2P，网络视频，游戏，炒股，期货，即时通讯，移动应用有独立的分类进行识别控制，协议库数量不低于2000，移动协议库数量不低于400 |
| 30 | ◆ | 告警方式 | 支持邮件及语音双重告警 |
| 31 | ◆ | 数据库审计控制 | 可审计、控制Oracle, MySql, SqlServer, PostgreSQL等数据库的访问与操作，包括添加、删除、修改、查询等。 |
| 32 | ◆ | 连接限制 | 可以每个人的并发/新建连接数量进行控制。 |
| 33 | ◆ | 数据分析平台联动 | 数据分析平台采用VMware等主流虚拟化架构部署，支持数据分析能力的可伸缩、可扩展； |
| 34 | ◆ | 设备可将用户上网行为数据上传至数据分析平台，数据分析台基于用户上网行为多维度展现员工、部门、公司的工作效率。包括效率评分、趋势分析、基线对比等，辅助管理者决策； |
| 35 | ◆ | 数据分析平台能够分析用户异常行为，通过风险分数展示用户风险级别，并可以钻取溯源，展示用户威胁过程，包括账号盗窃、数据泄密等风险情况 |
| 36 |  | Bypass功能 | 具备硬件级别光/电口bypass功能 |
| 37 |  | 配置重启 | 必须可以做到在修改任何网络配置后均无需重新启动设备 |
| 38 | ◆ | 产品资质 | 提供公安部颁发互联网控制管理系统《计算机信息系统安全专用产品销售许可证》，  |
| 39 | ★ | 提供中国信息安全认证中心颁发的有效期内的互联网控制网关《中国国家信息安全产品认证证书》 |
| 40 | ◆ | 特征库 | 含5年特征库升级 |

运维驻场服务

运维驻场工程师服务A 1名

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 招标要求 |
| 1 | ★ | 服务期限 | 1年内5\*8（每周五个工作日，每工作日8小时）； |
| 2 | # | 服务方式 | 驻客户指定现场（不含食宿）； |
| 3 | ★ | 人员要求 | 要求为投标公司在职人员，提供此人员近6个月的社保缴纳证明，在服务期限内不允许更换； |
| 4 |  | 服务地点 | 北京 |
| 5 | # | 技能要求 | 熟练桌面操作系统（Windows/MAC）和Office、专业软件等日常安装、维护、故障排除； |
| 6 | # | 能够熟练搭建和管理、维护基础服务（AD、FTP、DHCP、DNS、Email等）； |
| 7 | # | 掌握主流IT应用架构及部署应用，对网络安全、病毒防护等有一定了解； |
| 8 | # | 有企业邮件系统、WIFI无线网络系统、防毒系统、电话、视频会议、广播、监控系统、电话程控交换机、考勤系统等实施管理经验。 |
| 9 | # | 动手能力强，工作积极主动，善于表达和沟通，具备良好的服务意识和学习能力 |
| 10 |  | 学历要求 | 本科 |
| 11 |  | **证书要求** | 具备中级以上网络工程师认证证书 |

运维驻场工程师服务B 1名

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 招标要求 |
| 1 | ★ | 服务期限 | 1年内5\*8（每周五个工作日，每工作日8小时）； |
| 2 | # | 服务方式 | 驻客户指定现场（不含食宿）； |
| 3 | ★ | 人员要求 | 要求为投标公司在职人员，提供此人员近6个月的社保缴纳证明，在服务期限内不允许更换； |
| 4 |  | 服务地点 | 北京 |
| 5 | # | 技能要求 | 熟悉Linux系统原理，熟悉文件系统调优、内核参数优化、系统安全加固等实施方案； |
| 6 | # | 熟悉TCP网络原理，了解网络知识、网络设备、负载均衡产品； |
| 7 | # | 可以熟练使用脚本（shell,python,php）来完成日常系统运维工作 |
| 8 | # | 了解自动化运维平台，了解自动化监控平台及实现方式； |
| 9 | # | 有责任心，能独挡一面，有较强的沟通及协调能力，学习能力强，做事沉稳细致 |
| 10 |  | 学历要求 | 本科 |
| 11 |  | **证书要求** | 具有信息系统运维管理相关工程师证书； |

1. 售后服务要求

|  |  |
| --- | --- |
| **类别** | **招标服务详细说明** |
| **供货服务** | 中标供应商在签订合同后30日内（含设备采购时间），在用户指定地点交付设备。 |
| 中标供应商必须提供优质产品（包括配件），符合国家以及该产品的出厂标准，并提供产品的附件、说明书和技术咨询。 |
| 中标供应商所提供的货物必须成套和完整，在项目需求中未列明但属于设备运行的所需配件必须一并投报。如果在安装运行过程中发现有缺项漏项，且又是设备正常运行所必要的，中标供应商必须无偿提供。 |
| **无线部署** | 中标供应商应在60个工作日内完成新老设备的对接以及安装、调试等工作，并保证设备正常运行。 |
| ◆中标供应商须提供无线部署方案，按照方案完成无线安装调试服务，布线施工服务。中标方应提供施工中所需要的所有人工、线材、材料、工具、设备等，**网线全部采用6类屏蔽网线**。 |
| ◆要求原厂商对整个无线系统进行优化服务，信号覆盖区域要求达到：测试信号强度：RSSI值大于 -65dbm（电脑终端）， RSSI值大于 -75dbm（移动终端）；测试信号平均强度：RSSI值大于 -55dbm（电脑终端），RSSI 值大于-65dbm（移动终端）测试信号稳定度：取单位时间（3分钟内）10组信号值数据（包括最大值和最小值）进行标准差计算，其数值不能大于3.028。 |
| **无线巡检要求** | ◆维保期间至少每三个月原厂工程师提供一次无线巡检服务。 |
| 维保期间至少每六个月原厂工程师提供一次无线系统评估优化服务，对无线系统进行信号强度、稳定性等进行评估和优化服务，保证无线系统安全稳定高效运行； |

1. 用户培训

投标人须在投标文件中给出详细培训方案。

1、培训目标

通过培训，使受培训人员能独立掌握系统的配置、故障诊断、维护管理等技术，使之能适应系统正常运行的需求。

2、技术培训标准和条件

中标人应提供免费的用户现场培训；

中标人具备健全的培训体系，有成熟的培训流程、能够为项目制定完善的培训教材；

中标人在培训期间应提供：

* 培训大纲：其中应注明每次课程的内容和目的；
* 培训计划：其中应注明每次培训课程的时间及课时；
* 培训内容：系统的性能、相关技术原理和操作使用方法，维护管理的技术，实际的操作练习；

3、培训要求

中标人应对甲方人员进行不少于10人天的技术培训，使其能掌握有关系统设备的使用、维护和管理，达到能独立进行管理、故障处理、日常测试维护等工作的目的，以保障中标人所提供的系统能够正常、安全地运行。

中标人负责对相关技术人员进行相关设备及软件的技术培训。培训内容应包括所提供系统的结构、性能、维护、定制和升级等各个方面；主要设备的工作原理，调试、维护诊断技术及相关软件的使用。并提供全套培训教材和培训课程计划表。

培训教材应使用标准中文,为进行有效的技术交流，所有培训教员须具备熟练的中文会话和书写能力。

1. 保密要求

中标人必须对本项目技术文件以及由甲方提供的所有内部资料、技术文档和信息予以保密。中标人必须遵守与甲方签订的保密协议，未经甲方书面许可，中标人不得以任何形式向第三方透露本项目标书以及本项目的任何内容。