上网行为管理系统招标公告

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

上网行为管理系统1套

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. 投标人未被“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：投标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(维保)均为三年，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2019年9月23日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 顾晓磊收

商务联系人：顾晓磊

联系方式：021-66988356 [guxl@aaic.com.cn](mailto:guxl@aaic.com.cn)

技术联系人：卫金凯

联系方式：021-66988391 [weijk@aaic.com.cn](mailto:weijk@aaic.com.cn)

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

**产品性能指标**

|  |  |
| --- | --- |
| 吞吐量 | 300Mb |
| 用户规模 | 1500 |
| 设备接口 | 6个千兆网口 |
| 硬盘 | 1TB |
| 多线路 | 2条外网线路 |
| URL库 | 包含URL库 |

**产品技术指标**

|  |  |  |
| --- | --- | --- |
| **项目** | **指标** | **具体功能要求** |
| **部署方式** | 网关模式 | 支持网关模式，支持NAT、路由转发、DHCP、GRE、OSPF等功能； |
| 网桥模式 | 支持网桥模式，以透明方式串接在网络中；支持电口、光口bypass； |
| 旁路模式 | 支持旁路模式，无需更改网络配置，实现上网行为审计；旁路支持主主、主备模式部署； |
| 多路桥接 | 必须支持多路桥接功能，最多可支持32组网桥模式； |
| ★多主模式 | 必须支持两台及两台以上设备同时做主机的部署模式； |
| ★虚拟化模式 | 支持基于虚拟化平台的软件版本，支持的虚拟平台包括：VMware、深信服超融合等平台 |
| ★全面支持IPv6 | 支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置； |
| 所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6；（提供产品界面截图） |
| **网关管理** | 管理界面 | 支持SSL加密WEB方式、SSH命令行方式管理设备； |
| 管理员权限分配 | 支持细致的管理员权限划分，包括对不同用户组的管理权限、对各种主要功能界面的配置和查看权限； |
| 管理员角色及等级 | 可设置四类管理员，分别为配置管理员、查看管理员、日志管理员，以及多种权限的超级管理员；管理员支持分级，高级别管理员的策略配置优先生效，并可修改低级管理员的策略； |
| 管理员账号安全保障机制 | 支持管理员账号登录允许尝试次数可配，并支持管理员用户登录进行双因素认证，密码认证加邮件验证码； 管理员账号支持ACACS+/RADIUS/LDAP协议外部认证； |
| 支持集中管理 | 多台设备支持通过统一平台集中管理、集中配置等； |
| 加入集中管理时，支持身份认证，比如密码正确才能加入 |
| 解除集中管理时，要输入中心端的解控秘钥才允许解控 |
| 支持主备伴随升级 | 支持统一平台设备下发升级包，一次下发，2 台设备连续同时升级成功。升级过程中会进行双机切换来保证业务不中断。 |
| 智能组网 | 支持SDWAN 组网技术，统一平台下发策略邮件到多台设备，一键部署； |
| 支持autoVPN，选定两端设备后智能选路，一键配置VPN； |
| 告警管理 | \*支持攻击、双机切换告警、移动终端管理告警、风险终端发现告警、web关键字过滤告警、杀毒告警、设备流量超限告警、磁盘/CPU/内存异常告警等； |
| IPsec VPN | 必须具有IPSec VPN远程加密访问和连接的模块，并能提供IPSec VPN客户端授权远程接入访问； |
| \* IPsec VPN支持多线路功能，支持配置主备线路组和流量分配模式的多线路选路策略； |
| \*支持硬件特征码绑定认证； |
| \*IPsec VPN支持与LDAP服务器、Radius服务器结合认证； |
| （提供产品界面截图） |
| 链路负载 | 支持按剩余带宽、带宽比例、平均分配、前面优先的方式进行多链路负载； |
| 支持使用VPN做专线备份； |
| 支持链路故障检测；（提供产品界面截图） |
| 排障工具 | 提供图形化排障工具，便于管理员排查策略错误等故障； |
| 上网故障排除系统 | 支持开启直通后，流量控制模块依然生效，避免全部数据直通导致线路流量过大； |
| 实时监控 | 设备资源信息 | 提供设备实时CPU、内存、磁盘占有率、在线用户数、系统时间、网络接口等信息； |
| ★首页可视化分析展示 | 支持首页分析显示接入用户人数、终端类型、认证方式；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况；（提供产品界面截图） |
| 流量状态 | 实时提供用户流量排名、应用流量排名、所有线路应用流速趋势、流量管理状态、连接监控信息； |
| 安全状态 | 实时显示当天的安全状况，最后发生安全事件的时间、类型、总次数、源对象，帮助管理员管理上网安全； |
| 上网行为监控 | 实时显示设置过滤条件的用户上网行为监控，支持手动设置刷新时间； |
| ★Web访问质量检测 | 1.     针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级 |
| 2.     支持以列表形式展示访问质量差的用户名单 |
| 3.     支持对单用户进行定向web访问质量检测 |
| （提供产品界面截图） |
| ★支持网络故障排查 | 支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况；（提供产品界面截图） |
| ★支持权限策略故障排查 | 支持针对上网权限策略进行检测分析，查看各个应用是否匹配相关策略；（提供产品界面截图） |
| 用户认证故障排查 | 支持针对用户认证的故障进行分析，给出错误详情以及处置建议；（提供产品界面截图） |
| **用户管理** | 本地认证 | 支持触发式WEB认证，静态用户名密码认证等； |
| 第三方认证 | 支持LDAP、Radius、POP3、Proxy等第三方认证； |
| Radius必须支持GBK和UTF-8编码格式可选； |
| 支持ISA\lotus ldap\novel ldap\oracle、sql server、db2、mysql等数据库等第三方认证； |
| USB-KEY双因素认证 | 必须支持以USB-Key方式实现双因素身份认证；（提供产品界面截图） |
| IP、MAC认证 | 支持绑定IP认证、绑定MAC认证，及IP/MAC绑定认证等； |
| 支持通过SNMP服务器跨三层获取MAC地址； |
| 支持当用户MAC地址变动时，需要重新认证； |
| 多终端自绑定 | 同一个账号，支持与指定数量的多个终端进行自动绑定；（提供产品界面截图） |
| 短信认证 | 支持短信认证方式，用户输入手机号作为用户名，通过短信猫或短信平台发送验证码； |
| 短信认证能够根据不同用户推送不同认证页面，该认证页面可自定义，编辑内容包括文字、颜色风格、图片，且图片支持轮询播放（提供界面证明） |
| 必须支持网关类型为HTTP协议时，发送国家码可配； |
| 微信认证 | 1. 支持与微信结合的认证方式，用户关注微信公众号后即通过身份认证，后台记录用户ID（提供产品界面截图） |
| 2.与第三方微信平台无缝对接，不需要修改第三方微信平台代码； |
| 3、支持不同分支选择不同的微信公众号进行认证； |
| ★二维码认证 | 支持二维码认证，管理员扫描访客的二维码后对其网络访问授权（提供产品界面截图） |
| 新用户认证 | 基于IP网段、VlanID、MAC地址等实现新用户差异化的账户创建、自动分组、认证规则； |
| 支持认证前使用某个组织结构的上网权限； |
| 支持认证黑白名单功能，黑名单是名单中用户不能认证，白名单是只有名单中用户才能认证； |
| 限制某个新用户只能在某个IP段、MAC段范围内登录； |
| 自定义用户属性 | 支持为用户添加自定义属性（职位、临时项目组、邮件组等），能够根据用户属性自动归类并可以针对用户属性配置上网权限策略、流控策略，审计策略等（提供产品界面截图，） |
| 认证页面管理 | 支持认证页面分权分域管理。启用后，普通管理员只能看到自己有权限的页面，其他管理员页面不可见。 系统管理员可以将某个页面授权给指定的普通管理员管理。 |
| 公用账户 | 支持多人使用同一帐号登录，且支持重复登陆检测机制； |
| 支持限制公共账号的使用人数；（提供产品界面截图） |
| 账户有效期 | 指定账户支持有效期限制，并支持自动过期； |
| 支持自动删除长期不登录账号信息；（提供产品界面截图） |
| 单点登录 | 支持radius、AD、POP3、Proxy、PPPOE、 H3C IMC/CAMS、锐捷 SAM、城市热点等系统进行认证单点登录，简化用户操作； |
| 可强制指定用户、指定IP段的用户必须使用单点登录； |
| 强制AD认证 | 指定用户必须用AD域账户登录操作系统，否则禁止上网； |
| LDAP服务器的域对象的策略管理与同步 | 不需同步AD域用户到本地组织结构中，即可实现配置各种上网管控策略 |
| 认证失败 | 支持为认证失败用户提供DNS等基本网络访问权限机制； |
| 认证后页面跳转 | 认证成功的用户支持页面跳转： |
| 1.     跳转到用户原本输入的URL地址； |
| 2.     跳转到管理员指定的URL地址； |
| 3.     跳转到注销页面; |
| 帐户导入 | 支持从本地导入和扫描导入，支持以CSV格式文件导入帐户/分组/IP/MAC/描述/密码等信息； |
| 组织结构 | 用户分组支持树形结构，支持父组、子组、组内套组等； |
| 用户状态查询 | 支持用户登录时间、注销时间、在线时长的查询； |
| 自动注销 | 支持自动注销指定时间内无流量的已认证用户； |
| 冻结用户 | 支持冻结认证失败次数超过最大值的用户，在冻结时间结束后恢复登录； |
| ★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） |
| **终端管理** | 系统识别 | 支持识别终端操作系统版本、系统补丁安装情况；（必须提供自主知识产权证明）； |
| 文件识别 | 支持识别终端硬盘指定目录下的文件情况； |
| 进程识别 | 支持识别终端系统后台运行的进程信息，防止间谍软件的运行；（必须提供自主知识产权证明）； |
| 注册表识别 | 支持识别终端系统注册表中指定的表项和键值； |
| ★★自定义计划任务 | 支持终端调用管理员指定脚本/程序以满足个性化检查要求，比如检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等；（提供产品界面截图） |
| 终端准入 | 支持win 8 64位操作系统，支持在旁路模式部署下准入生效； |
| 支持禁止不满足终端检查要求的用户访问互联网； |
| ★补丁检测 | 支持检测windows重要补丁的安装情况，并反馈检测结果； （提供产品界面截图） |
| **应用管理** | 应用识别规则库 | 1.     支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类； |
| 2.     支持给每个应用自定义标签； |
| 3.     支持根据标签选择一类应用做控制； |
| 4.     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； |
| 5.     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） |
| ★应用控制 | 1.     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） |
| 2.     支持根据IP、端口、协议等自定义应用规则； |
| 3.     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； |
| ★应用细分控制 | 1.能够对新浪微博、腾讯微博、网易微博等进行细分控制，如：登录、浏览、发微博、上传附件等。 |
| 2.能够对teamview、QQ远程桌面等远程控制应用做细分控制，如：接受对方远程控制； |
| 3.能够对Github、百度网盘、百度文库等网络应用的上传动作进行细分控制；（所有功能必须提供产品界面截图） |
| 移动应用的细分控制 | 支持对移动应用的细分权限控制，微信：微信网页版、微信传文件、微信朋友圈、微信游戏。移动QQ：QQ传文件、QQ视频语音等。（提供产品界面截图） |
| 端口控制 | 支持根据端口设定用户不允许访问的目标IP组提供的服务； |
| QQ白名单 | 支持基于用户组、终端类型、位置的QQ白名单功能。（提供产品界面截图） |
| 代理控制 | 1.     不允许使用外部HTTP代理； |
| 2.     不允许使用外部Sock4/5代理； |
| 3.     不允许在HTTP,SSL一些的标准端口上使用其他协议；（比如在80端口上传输非HTTP协议数据，在443端口上传输非HTTPS协议数据等） |
| ★共享接入管理（防共享） | 设备能够发现私接路由（或者共享软件等）共享网络的行为： |
| 1.支持自定义配置终端数量和冻结时间。 |
| 2.支持“仅统计电脑”和“统计所有终端”两种模式。 |
| 3.支持可选“冻结IP”还是“冻结用户名”。 |
| 4.支持添加信任列表 |
| 5.支持显示以IP或用户名的维度统计一段时间内的趋势图。 |
| 6.支持例外排除功能：如冻结条件是2. 指定例外条件1台PC，2个终端。当PC或终端数超过例外条件才会被判定为共享。（提供产品界面截图） |
| 7.支持在数据中心报表中可查询通过共享上网的IP、用户，并能导出报表； （提供产品界面截图） |
| **网页管理** | 静态URL库 | 设备内置海量预分类的URL地址库，支持根据URL类别实现URL过滤； |
| SSL加密网页内容识别 | 识别并过滤SSL加密的钓鱼网站、非法网站等（必须提供自主知识产权证明）； |
| 支持SSL硬件加速卡解密，从而可提高SSL全流量解密性能； |
|  |
| 自定义URL | 设备支持管理者自定义新的URL地址和URL分类； |
| 关键字过滤 | 过滤同时匹配三个以上关键字的搜索行为； |
| 过滤同时匹配三个以上关键字的网页访问行为； |
| 网页过滤 | 支持根据访问的URL、网页关键字进行网页过滤，支持设置拒绝以IP访问网页行为； |
| 支持在放行URL时，自动放行主域名的子链接中被禁止的网站，保证网页显示完整； |
| 发帖管理 | 过滤同时匹配三个以上关键字过滤的网络发帖行为； |
| 必须支持允许用户浏览帖子但不准发帖功能； |
| SSL发帖管理 | 必须支持基于关键字过滤SSL加密的网页、论坛、BBS上的发帖行为； |
| 网页附件管理 | 支持根据文件类型限制http、FTP方式上传、下载行为； |
| **邮件管理** | 邮件地址过滤 | 支持根据源地址和目的地址过滤外发邮件； |
| 邮件附件过滤 | 支持基于扩展名过滤含指定文件类型的邮件外发行为； |
| 支持根据附件大小、附件个数限制外发邮件； |
| 邮件关键字过滤 | 过滤同时匹配三个以上关键字的邮件主题、正文和附件的邮件外发行为； |
| Webmail管理 | 必须支持允许用户登录Webmail收邮件，而禁止发送Webmail邮件的功能； |
| SSL邮件管理 | 必须能基于关键字、发件人地址等识别和过滤使用邮件客户端外发SSL加密邮件的行为； |
| 加密Webmail管理 | 必须能够基于关键字识别和过滤使用SSL加密的Webmail邮箱外发邮件的行为，比如QQ邮箱； |
| ★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） |
| **上网权限管理** | 上网时长控制 | 支持统计和控制用户终端每天上网时间，并支持排除应用或特殊端口后的灵活流量统计方法； |
| 时间配额 | 支持对单个用户/用户组、位置、终端类型等设置一天内总上网时长； |
| 支持将超过配额的用户/用户组添加到低带宽惩罚通道； |
| 外发文件类型过滤 | 支持HTTP上传/FTP/邮件附件等形式的外发文件行为，支持基于扩展名识别并拦截外发文件；（提供产品配置界面） |
| 并发连接控制 | 支持限制指定用户最大并发连接数； |
| 上网时间提醒 | 用户指定应用上网时长超过预设阈值后，网关自动提醒该用户； |
| 上网流速提醒 | 用户指定应用上网流速超过预设阈值后，网关自动提醒该用户；（提供产品配置界面） |
| 策略复用 | 上网策略对象与用户无关联，同一条上网策略可复用、重用； |
| 策略有效期 | 必须支持上网策略对象的自动过期功能； |
| 排除IP | 不控制、不监控目标为排除IP的上网行为； |
| 排除域名 | 不控制、不监控目标为排除域名的上网行为； |
| ★上网策略适用多种对象 | 上网策略适用对象，适用于以下对象和应用类型 |
| （包括上网权限、上网审计、上网安全等上网策略） | 一、用户 |
|  | 1、本地组，2、域安全组，3、域用户(ou和用户)，4、域属性组，5、源IP，6、用户属性组 |
|  | 二、位置 |
|  | 三、终端类型 |
|  | 四、URL类型控制（上网权限） |
|  | 能够针对：网上购物、成人内容、求职招聘、宗教、在线影音及下载、游戏资讯、网上聊天、个人网站及博客、色情、赌博、非法药物、风水命理、娱乐场所、汽车、餐饮、钓鱼及恶意网站、网上银行、在线支付等各种URL类型做识别和分类，同时所有URL类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制。（提供产品界面截图） |
| **流量控制** | 带宽管理 | 必须支持在不同线路上，根据不同的应用、用户/用户组、位置、终端类型来保证或者限制流量； |
| 支持根据百分比或数值设置通道带宽，并支持设置各通道的优先级； |
| ★多线路技术 | 网关必须能同时连接多条外网线路，且支持多条线路流量复用和智能选择流速最快线路的技术(必须提供自主知识产权证明)； |
| ★虚拟多线路 | 必须支持将多条外网线路虚拟映射到设备上，实现对多线路的分别流控；（提供产品界面截图） |
| 父子通道 | 必须支持流量父子通道技术，且至少支持三级父子通道； |
| ★流控通道实时可视化 | 能够实时看到各级流控通道的状态：包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽、优先级，启用状态等。（提供产品界面截图） |
| 应用流控 | 支持基于应用类型、网站类型和文件类型划分与分配带宽； |
| 动态流控 | 支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率； |
| 空闲值可自定义（提供产品界面截图） |
| ★P2P智能流控 | 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；（提供产品界面截图） |
| 流控黑名单 | 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中（提供产品界面截图） |
| 单IP限制 | 支持限制单个IP的最大上行和下行带宽； |
| ★Wan-lan流控 | 支持把每一个外网IP作为通道内的用户，使得通道的用户间公平分配带宽，以及单用户最高带宽属性对外网IP有效； |
| 时间控制 | 支持基于时间段的带宽划分与分配策略； |
| 支持按日期设置流控策略，比如针对节假日设置不同流控策略； |
| 目标IP流控 | 支持基于访问行为的目标IP/IP组实现带宽划分与分配； |
| 流量配额 | 支持对单个用户/用户组、位置、终端类型等设置日流量、月流量配额功能；必须支持流量配额的配置、实时使用量查询； |
| 流控单位 | 支持灵活配置流控单位是IP还是用户名（适用于公共账号：多个IP公用一个账号时，可以对每个IP进行限速，更加灵活准确）（提供产品界面截图） |
| ★流控策略适用多种对象 | 流控策略适用对象，适用于以下对象： |
| 一、用户 |
| 1、本地组，2、安全组，3、域用户(ou和用户)，4、域属性，5、源IP，6、用户属性组 |
| 二、位置 |
| 三、适用终端 |
| 四、文件类型：电影、音乐、图片、压缩文件、应用程序等 |
| 五、URL类型：新闻门户、网上购物、在线影音及下载、非法及不良、网上聊天、软件下载等（提供产品界面截图） |
| ★移动终端管理(非法Wi-Fi热点管控) | 设备必须支持能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型； |
| 支持管理员配置热点信任列表； |
| 支持发现信任列表外非法接入的热点和终端，并阻止该热点/终端上网； |
| 支持将非法热点接入网络的行为通过邮件告警通知管理员，并在数据中心支持行为记录和查询； |
| 支持以图表方式显示移动终端接入趋势； |
| 支持移动终端型号识别，至少识别不少于10种移动终端型号； |
| （提供产品界面截图） |
| DHCP移动终端识别 | 支持DHCP协议增强移动终端识别能力； |
| 防范DOS攻击 | 必须能识别并封堵来自于内网或外网的DOS攻击； |
| 防ARP欺骗 | 必须能防范三层网络环境中的ARP欺骗问题； |
| ★病毒查杀 | 设备必须内置业界知名杀毒引擎； |
| 设备需支持僵尸主机检测； |
| 必须支持HTTP下载、FTP下载、POP3、SMTP杀毒； |
| 支持对HTTP、FTP等下载中启用文件类型杀毒； |
| 病毒库支持通过服务器或本地加载病毒库方式定期升级； |
| （提供产品界面截图） |
| ★https杀毒 | 必须支持https杀毒功能； |
| 防火墙 | 必须具有防火墙功能模块； |
| **上网行为审计** | 网站审计 | 支持记录全部或者指定类别URL、网页标题等信息； |
| 网页内容审计 | 必须能审计记录网页正文内容； |
| 必须支持只记录含有指定关键字的网页正文内容； |
| 必须支持记录SSL加密网页的内容； |
| ★加密证书自动分发 | 审计SSL网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台PC单独安装证书的问题（要求提供产品界面截图） |
| ★加密证书自定义 | 支持用户可以自定义产生根证书，导入包含秘钥的根证书； |
|
| 审计分权限 | 支持对网页过滤和网页审计分开控制； |
| 支持审计指定类型的URL，其他URL类型不予审计，以提高审计效率； |
| 支持在审计时，将行为与内容分离，即可分别设置只审计用户行为还是审计内容； |
| 发帖审计 | 支持审计用户的明文发帖内容； |
| 必须能审计用户在SSL加密论坛、BBS上的发帖内容； |
| ★网页快照 | 支持网页内容审计后的网页快照功能； |
| Webmail审计 | 支持审计用户的Webmail邮件外发行为，支持webmail形式发送的附件审计，并能精准到原始邮件； |
| 必须能审计用户通过SSL加密Webmail网站外发邮件的内容； |
| 邮件审计 | 支持审计用户外发Email邮件的正文及附件； |
| 必须能审计用户使用邮件客户端外发SSL加密邮件的邮件内容； |
| 文件外发审计 | 支持审计用户通过HTTP、FTP、Email当方式外发的文件内容； |
| 必须能对加密文件外发行为识别并记录； |
| Web IM 审计 | 记录Web qq、Web微信的聊天内容、登陆和注销行为，且不需要安装插件； |
| IM审计 | 支持记录QQ、TIM、微信、skype、MSN等主流IM聊天行为和内容； |
| 支持根据QQ、微信账号查询IM聊天行为和内容； |
| IM 传文件内容审计 | 记录QQ、微信传文件动作和所传文件内容，并可指定记录传文件类型和文件长度； |
| 支持同时审计QQ聊天内容和QQ传文件内容。 |
| 移动APP审计 | 支持以下类型的移动APP内容审计： |
| 论坛类（IOS和android）：天涯社区、猫扑社区、百度贴吧、新浪论坛、搜狐社区等 |
| 微博类（IOS和android）: 新浪微博、腾讯微博等 |
| 新闻评论类（IOS和android）：QQ新闻、搜狐新闻、新浪新闻、凤凰新闻等 |
| FTP审计 | 支持审计通过FTP上传的文件名和内容； |
| 支持审计通过FTP下载的文件名； |
| TELNET审计 | 支持审计TELNET执行的命令； |
| 应用审计 | 审计用户使用P2P、流媒体、炒股、网络游戏、FTP、Telnet等应用行为； |
| 时间审计 | 记录用户在指定时间段内的总上网时间； |
| 记录用户在指定时间段内使用指定应用的总时长； |
| 流量审计 | 支持统计在指定时间段内网络应用流量 产生的总流量； |
| 记录用户在指定时间段内使用指定应用的总流量； |
| 其他行为审计 | 支持记录其他网络行为，包括IP、端口等信息； |
| 系统日志审计 | 支持审计管理员的操作日志、系统日志等； |
| ★特权DKey | 支持针对特权用户配置免认证key、免审计key、免控制key |
| 免审计IP | 免除审计目标为指定IP的上网行为； |
| 免审计域名 | 免除审计目标为指定域名的上网行为； |
| **上网日志管理** | ★数据中心 | 设备必须支持内置数据中心和独立数据中心（提供产品界面截图）； |
| ★高性能日志模式 | 支持日志高性能模式处理，精简冗余日志（提供产品界面截图）； |
| 日志分级审查 | 管理员登录数据中心只能审计指定用户组的上网行为日志； |
| 日志中心操作安全保障 | 日志中心所有导出都有对应管理员操作日志、系统日志的日志清理中记录数据删除日志、规则库升级有对应升级日志；支持日志中心网关杀毒； |
| ★日志审查Key | 必须支持以USB-Key方式验证接入数据中心的管理员身份； |
| 支持以USB-Key方式分配管理员的日志审计权限； |
| 用户行为报表 | 支持查询和导出基于指定时间段/用户/用户组的文件审计、邮件收发、访问网站、即时通讯、发帖/微博、搜索关键字等详细用户行为的报表 |
| 终端接入日志 | 支持查询和导出基于指定时间段/用户/用户组的防共享接入日志、移动终端发现日志、准入日志、登录注销日志等行为日志 |
| 流量排行报表 | 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量排行、网站分类流量排行 |
| 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（提供产品界面截图） |
| 流控通道趋势报表 | 支持基于通道流速、通道总用户数、通道活跃用户数等维度的流速趋势分析报表（提供产品界面截图） |
| 域名流量排行报表 | 支持基于时间段/用户/用户组/终端类型/位置等维度，针对具体某个域名的访问流量排行； |
| 支持基于时间/用户/用户组/上行/下行/总体等维度的域名流量排行； |
| 时长排行报表 | 支持提供基于时间段/用户/用户组的应用时长排行和网站分类时长排行 |
| 域名时长排行报表 | 支持基于时间段/用户/用户组/终端类型/位置等维度，针对具体某个域名的访问时长排行； |
| 支持基于时间/用户/用户组/上行/下行/总体等维度的域名时长排行； |
| 用户行为次数排行报表 | 支持基于时间段/用户/用户组/终端类型/位置等维度的文件审计、邮件收发、访问网站、即时通讯、发帖/微博、搜索关键字、网站分类等详细的行为次数排行 |
| 热门应用排行 | 支持基于时间段/用户/用户组的热门应用类型或热门具体应用的行为次数排行 |
| 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 |
| 域名行为排行报表 | 支持基于时间段/用户/用户组/终端类型/位置等维度，针对具体某个域名的访问行为排行； |
| 支持基于时间/用户/用户组/上行/下行/总体等维度的域名访问排行； |
| （提供产品界面截图） |
| 热门发帖访问排行 | 支持基于时间段/用户/用户组的热门发帖行为次数排行 |
| 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） |
| 终端接入分析 | 支持共享接入、终端类型、接入用户数的排行和趋势分析 |
| 终端接入安全 | 支持基于用户和病毒等维度的行为次数排行 |
| 搜索中心 | 基于时间、用户/组、终端类型、位置、日志类型等条件下的关键字检索定位功能； |
| 必须支持对日志中OFFICE等附件正文内容关键字的检索； |
| 关键字订阅 | 支持预置几组关键字，当审计日志中出现这些关键字时，将定期以邮件的方式发送报告给指定邮箱（提供产品界面截图） |
| 网络整体状况报表 | 从带宽健康分析、工作效率分析、离职风险分析、合规性分析四个大块对网络整体状况进行说明 |
| 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 |
| 工作效率报表 | 从用户上网行为的多个维度（如访问网站、使用应用等）分析员工的工作效率 |
| 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 | 支持按预置周期将网络整体状况报表、离职风险报表、工作效率报表、以及自定义报表等自动发送到指定邮箱； |
| 报表导出 | 支持导出所有查询和报表都支持导出；必须支持导出csv格式的报表；最大支持导出10万条，外置对大支持导出100万 |
| 下钻查询 | 在流量时长分析、用户行为分析、终端接入分析等纬度相关页面支持对统计结果的向下钻取查询（提供产品界面截图） |
| 递进式统计分析 | 支持在页面上（应用流量排行、网站分类流量排行、应用时长排行、网站分类时长排行）一次统计，能够基于两个维度（提供产品界面截图） |
| 数据分析应用 | 数据中心可以对上网日志进行大数据分析，并支持多个大数据分析模型，包括泄密分析、离职倾向分析、上网态势分析、带宽分析、工作效率分析。（提供产品界面截图） |
| 泄密追溯分析 | 支持分析整体外发风险概括，包括外发敏感文件的总次数、文件类型、外发通路等状况；（提供产品界面截图） |
| 支持泄密行为追溯，可以上传文件和关键词，查询有过相关外发记录的人员，通过相似度匹配给出风险人员排行；（提供产品界面截图） |
| 工作效率分析 | 支持整体工作效率分析，展示整体的日均工作无关时长和怠工总人数，以及工作无关应用时长趋势；（提供产品界面截图） |
| 支持部门分析和具体人员分析，包含影响工作效率因素分析、影响时段分析、工作效率趋势分析、怠工人员分析； |
| 离职倾向分析 | 支持识别组织中有离职倾向的人员，给出风险等级，分为高风险人员和疑似人员； |
| 可查看具有离职倾向人员的判定依据，判定依据从简历投递、访问求职网站等多个维度综合判定；（提供产品界面截图） |
| **网安日志对接** | ★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） |
| **多产品联动** | 支持与同品牌防火墙联动 | 能够与同品牌下一代防火墙系统实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；（提供截图证明文件） |
| 支持与同品牌安全态势感知产品联动 | 能够与同品牌安全态势感知产品实现联动，实现用户同步，以基于用户身份进行威胁分析；（提供截图证明文件） |
| 支持与同品牌认证中心联动 | 1、支持分支与认证中心无缝对接，在总部实现用户认证策略、用户组织结构、在线用户的统一管理、统一认证；（提供截图证明文件） |
| 2、支持同一上网账号可在不同分支实现无感知漫游认证，且在认证后自动获取授权，在不同分支拥有相同的上网权限，匹配相同的上网策略，实现权随人行的漫游认证服务； |
| 3、支持当分支与认证中心通信异常时，可通过认证逃生机制或策略，保证各分支可独立进行认证上网。认证中心恢复时，再对用户重新进行认证，保障用户身份安全。（提供截图证明文件） |
| 支持与同品牌端点安全检测产品联动 | 能够与同品牌EDR产品实现联动，当检测到终端未安装EDR产品时，禁止上网并提示需要安装EDR终端软件；（提供截图证明文件） |

厂商及产品资质要求

|  |  |
| --- | --- |
| 投标产品资质要求 | 公安部颁发的《计算机信息系统安全专用产品销售许可证》如：  ★《网络通讯安全审计产品（国标） 销售许可证》  ★《互联网公共上网场所 信息安全管理系统（无线接入前端）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》 |
| ★国家网络与信息系统安全产品质量监督检测中心颁发的《国家信息安全测评/ 信息技术产品安全测评证书（EAL3级）》 |
| ★★具有工信部颁发的《电信设备进网许可证》 |
| IPv6 Ready Phase-2认证 |
| ★★应为市场成熟产品，最近两年在国内IDC内容安全市场占有率排名都在前5 |
| ★★★产品应具备相当的技术认可度，最近两年产品曾入围Gartner SWG魔力象限 |
| 投标产品生产商资质要求 | ★★★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 |
| ★★公司研发体系通过国际认证CMMI5 |
| ★国家应急中心应急支撑单位CNCERT证书（国家级） |
| 售后服务体系通过ISO9001认证 |