上海飞机客户服务有限公司

竞争性谈判/询价文件

我公司有以下采购项目，具体要求和联系方式见下表和附录，如有意向请在有效期内提交报价文件。

2023年 4月 20日

|  |  |  |  |
| --- | --- | --- | --- |
| 采购方 | 上海飞机客户服务有限公司 | | |
| 采购实施部门联系人 | 朱虹 | 联系地址 | 上海市闵行区江川东路100号 |
| 联系电话 | 18019195439 | E-Mail | Zhuhong3@comac.cc |
| 项目名称 | 互联网出口安全硬件设备采购项目 | | |
| 供应商资质要求 | 1. 具有独立法人资质，具有企业法人营业执照并具有完成本项目所需的经营范围及资质； 2. 在签署本项目合同及履行本项目义务时无任何法律障碍和重大事件影响继续正常存续和全面履行本项目合同的能力，包括但不限于正在审理或执行完毕的标的金额大于500 万元人民币（含本数）的重大诉讼案件、债权债务纠纷、行政处罚，未被列为失信被执行人； 3. 中国商飞公司及其关联企业的在职人员及其直系亲属享有控制权的企事业单位不得参选。 4. 注册资本金不少于1000万元人民币。 | | |
| 供应商能力要求 | 1、提供企业法定代表人资格证明或提供被授权人身份证明及针对本项目的法人授权委托书、营业执照复印件等相关资料；  2、提供近三年经审计的年度财务报表或公司盖章版财务报表（公司成立若不满三年，则按实际情况提供）；  3、提供防火墙设备、准入控制设备、网络流量控制设备、APT设备、内容过滤设备、日志设备、互联网流量牵引设备、主机防病毒设备厂商针对本项目的项目授权书；  4、提供3份类似案例相关合同证明文件； | | |
| 项目技术要求 | 1、详细技术要求见附件一互联网信息安全设备技术要求。 | | |
| 项目进度要求 | 安装地点位于上海飞机客户服务有限公司闵行紫竹园区和嘉兴园区。合同签订生效后的两个月内完成安装调试工作。设备质保期一年。  付款条件要求：合同金额分二期支付，通过银行转账的方式进行，每期支付的金额和时间如下：  第一期支付合同总金额的95%，支付时间：卖方完成软硬件设备安装调试，验收合格，卖方提供全额的合法有效的增值税专用发票后30个工作日内完成付款；  第二期支付合同总金额的5%，支付时间：质保期结束，无质量问题后30个工作日内完成付款。 | | |
| 响应文件送达截止时间 | 2023年 4月 28日 | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 附录 | ☑详细技术要求 | □报价单 | □报价文件编制要求 | ☑其他：供应商信息采集表 |

注：明确技术标准和要求，不限定或指定唯一品牌，在引用品牌或生产供应商名称前加上“参照”或“相当于”字样，确保品牌的市场可选择性。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 以下由报价供应商填写（盖章） | | | | |
| 供应商性质 | □高校/科研院所 □国有及国有控股企业 □外资企业 □民营企业 □境外单位或个人 | | | |
| 联系人 |  | 联系地址 |  | |
| 联系电话 |  | E-Mail |  | |
| 资质文件  （复印件应加盖单位公章，带\*号的为必备材料） | （一）基本证照 | | | |
| □营业执照\* □组织机构代码证\* □税务登记证\* 或□“三证合一”证书 | □法人代表授权书\* | □设备厂商针对本项目的项目授权书\* | |
| （二）财务资料 | | | |
| □银行基本账户开户许可证\* | □经审计的近三年的年度财务报表或  公司盖章版财务报表\* | |  |
| □资信证明\*（银行开具或查询网页截图） | □其他财务指标证明材料 | |  |
| （三）经营范围资料（包括但不限于依法须经批准的项目，相关部门的批准文件） | | | |
| □批准文件 |  |  | |
| （四）能力证明资料 | | | |
| □相关领域的资质文件 | □行业资质证书 | □质量体系认证 | |
| □拟派出项目组成员的资质文件 | □以往类似项目的合同 或验收报告 | □成功案例\* | |
| 资质情况说明 |  | | | |

注：\*号项目，由采购需求部门按需调整。

|  |  |  |  |
| --- | --- | --- | --- |
| 质量能力说明 |  | | |
| 技术方案说明 |  | | |
| 交付时间（天） |  | | |
| 报价 | 人民币 （大写） | | |
| 附录 | □项目技术方案 | □报价单 | □其他说明资料 |
| 注：报价文件盖章后密封送达采购联系人，内含盖章版电子扫描件（U盘或光盘）。 | | | |

**附件一：互联网信息安全设备技术要求**

1. **防火墙FW/IPS**

一台，对出口流量进行安全防护，与出口流量性能匹配，包含IPS、网络防病毒。与山石品牌E2860型号设备完全兼容。

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 硬件要求 | 管理接口：设备需提供1个Console接口，1个MGT口，2个USB3.0口 |
| 业务接口：在提供管理接口的基础上，提供≥8个千兆电口，提供≥8个千兆光口，≥2个万兆光接口 |
| 提供交流双电源 |
| 性能要求 | 网络层吞吐≥10Gbps |
| 最大并发≥150万，可扩展≥220万 |
| HTTP新建≥13万 |
| IPS吞吐≥5Gbps |
| AV吞吐≥4Gbps |
| IPsec VPN吞吐≥5Gbps |
| 策略数 | policy策略数≥10万条 |
| 特征库 | 配置1年IPS、AV、APP特征库 |
| IPS入侵防御 | 支持旁路和在线两种模式，支持基于安全策略和安全域启用IPS功能，可在不同的攻击方向上启用IPS（至少支持流入\流出\双向等方向） |
| 支持对HTTP、FTP、SMTP、IMAP、POP3、TELNET、TCP、UDP、DNS、RPC、FINGER、MSSQL、ORACLE、NNTP、DHCP、LDAP、VoIP、NETBIOS、TFTP、SUNRPC和MSRPC等常用协议及应用的攻击检测和防御 |
| 具备12000种以上攻击特征库规则列表，至少支持基于协议类型、操作系统、攻击类型、流行程度、严重程度、特征ID等方式的查询；入侵防御特征库为独立文件，支持自动更新和手动更新模式 |
| 支持SQL注入、XSS防护，支持HTTP头域中的URL、Cookie、Referer、POST检查点配置防护策略 |
| NAT功能 | 需支持动态地址转换和静态地址转换，支持多对一、一对多和一对一等多种方式的地址转换 |
| 支持NAT地址池可用性探测 |
| VPN | 要求所投产品支持IPSec VPN\SSL VPN\L2TP VPN等VPN技术 |
| 支持SM2\SM3\SM4算法 |
| 要求且SSL VPN具备USB-KEY认证的能力 |
| 路由协议 | 需支持静态路由、等价路由、策略路由，以及BGP、RIPv1/v2、OSPF等动态IPv4路由协议（非透传） |
| 策略路由需支持基于指定IP地址、指定应用协议、指定时间表生效 |
| 出栈负载 | 支持智能链路负载，基于带宽利用率、延时、抖动、丢包率进行自动切换 |
| 入栈负载 | 支持smartDNS入栈智能负载，支持设备对域名的权威解析，可基于ISP地址簿返回给client不同的IP地址 |
| 黑名单地址库 | 鉴于安全攻防时大量封堵IP的需求，要求设备支持通过非策略方式配置黑名单地址库，避免因为海量地址封堵导致设备性能严重下降 |
| 要求防火墙支持读取外部地址库，例如FTP发布的地址库，且支持周期更新 |
| 访问控制策略 | 需支持基于五元组，基于应用，基于URL的的访问控制策略，防火墙策略命中数统计功能，便于管理员维护防火墙策略 |
| 支持基于国家/地区维度进行流量控制等安全策略，支持自学习生成策略，支持垃圾策略清理，支持聚合策略以及策略导出 |
| DNS代理 | 支持基于策略的DNS代理，DNS策略支持入接口、源地址、目的地址、域名等控制粒度；  支持针对DNS代理的命中数分析及日志记录 |
| 会话控制 | 需支持基于源地址、目的地址、生效时间、应用协议（http、https、mysql、ms-sql、sqlnet、sip、P2P下载、视频、网络游戏等）限制新建连接、并发连接 |
| 系统版本 | 需支持2个系统软件并存，并可在WEB界面上直接配置启动顺序，防止配置不当或系统故障造成的网络中断，充分保证系统的稳定性；支持不少于10个配置文件并存，并支持配置文件的中文备注 |
| API接口 | 要求防火墙支持RESTful API接口，基于GET/POST/PUT/DELETE方法对设备进行增、删、改、查操作 |
| 要求支持基于API获取设备的会话、新建连接数、整机流量及接口流量 |
| 要求支持基于API进行黑名单地址库的下发，例如IP、MAC、Service下发 |
| 要求支持基于API进行策略的增、删、改、查，包括但不限于IP、服务、应用 |
| 监控和统计 | 需支持在WEB界面上显示设备的硬件状态：包括CPU利用率、内存利用率、存储空间利用率、会话利用率、CPU温度、机箱温度、风扇运行等状况 |
| 需支持在WEB界面上显示设备历史时间段内的整机流量、接口流量、新建连接数、并发连接数 |
| 需支持基于IP及应用的流量、并发连接数、最近1小时、最近一天、最近一月类型的统计 |
| 会话控制 | 需支持基于源地址、目的地址、生效时间、应用协议（http、https、mysql、ms-sql、sqlnet、sip、P2P下载、视频、网络游戏等）限制新建连接、并发连接 |
| 流量包统计 | 支持按64字节、128字节、256字节、512字节等数据包流量统计 |
| 资质证书 | 提供公安部颁发的防火墙销售许可证 |

**2．准入控制设备**

两台，对外网接入用户进行准入控制，能够实现公司统一终端准入一键策略下发。与齐安信品牌NAC-1000SX型号设备完全兼容。

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 硬件参数 | 要求支持3000个终端授权,最小支持3G流量，支持Console口，6个自适应电口，3个扩展槽，2TB 硬盘，双电源。 |
| 管理架构 | 系统控制中心采用B/S架构，支持管理员分区分权管理模式，灵活配置管理权限，适应大型分级管理组织架构 |
| 集中管理 | 支持设备集中管理，可在同一管理平台集中管理所有设备，支持设备分组，权限管理，实现分布式部署、集中管理，满足大型网络环境下的部署要求。 |
| 系统监控 | 支持图形化记录和展示最近一小时、最近一天、最近一周、最近四周时间段内的CPU、内存、系统负载、磁盘、网络接口流量的使用率情况 |
| 设备配置采集 | 能够识别设备的设备名称、操作系统、开放网络端口、运行网络应用等配置信息 |
| 识别库管理 | 支持指纹库管理，对于未识别成功的终端，可通过人工录入指纹的方式修正终端信息扫描结果，支持指纹库的外部导入及备份  能够同时根据MAC规则、操作系统、厂商、开放端口、运行服务、主机名、型号来自定义识别规则 |
| 网络设备管理 | 支持可网管型交换机信息的图形化展示，通过面板的形式详尽展现了交换机型号信息、交换机的端口数、各接口状态以及各接口下联的终端详细信息，方便管理员掌握全网网络设备信息 |
| 准入技术 | 产品支持多种认证控制方式，支持802.1x、portal、DHCP、MAB MAC、策略路由、旁路镜像、WebAuth等方式，支持无线和有线环境下的接入控制，适应复杂网络环境下的接入控制 |
| 引导部署 | 检测是否安装客户端，达到入网遵从条件，保障入网终端是安全可信的，未安装客户端的终端禁止访问，将被重定向到客户端安装页面快速引导部署  针对未认证或不合规的设备，当终端访问http、https网站时，支持对其网站访问重定向至引导页面进行身份认证或修复 |
| 身份认证 | 支持使用客户端或portal方式进行设备身份认证，只有合法的用户才可接入网络 |
| 用户管理 | 系统内置用户身份管理系统，支持创建、导入或从第三方系统同步用户身份信息，以便进行身份认证、权限设置等操作 |
| 第三方认证源 | 支持LDAP、Email、Http认证源三种认证源配置，支持第三方认证源的高可用配置  支持在不修改第三方认证源中用户信息的前提下，临时限制特定账号的入网认证请求 |
| 设备身份认证源 | 支持基于终端身份标识的设备身份验证方式  支持同时校验用户身份和设备身份的双重认证 |
| DHCP服务 | 系统内置DHCP服务器，支持动态分配、固定分配、保留地址，设备停用等DHCP常用场景，支持根据设备合规状态动态切换设备IP的DHCP准入控制方式 |
| 黑名单管理 | 支持导入或联动第三方安全系统进行非常设备的加黑处置，对于黑名单中的IP/MAC地址，一律阻断其网络访问流量 |
| 动态授权 | 可基于用户、角色、设备类型、设备分组、设备标签、终端安检结果等动态下发VLAN、acl或厂家属性 |
| 动态ACL | 支持基于不同设备类型定义访问控制规则，特定类型的设备仅允许访问指定的关键服务器，并只允许合法的协议通过  支持基于终端使用用户的用户组、用户角色定义访问控制策略，无论用户使用什么设备还是IP，均可执行对应的访问控制策略 |
| 开放端口检查 | 能检查终端开放端口情况，判断必须是否满足必须开放与禁止开放的安全要求 |
| 指纹仿冒检查 | 能检查终端外在静态指纹特征，支持多种特征维度，支持DHCP动态IP下的设备仿冒检查，无论非法设备修改IP还是修改MAC进行仿冒替换，系统均能快速发现并及时阻断 |
| 协议检查 | 支持基于协议黑白名单的设备协议检查，规范设备行为，防止使用高危协议的设备接入网络 |
| 异常行为 | 能检查终端网络行为模型，支持多种判断模型机器学习，判断终端网络行为是否满足已学习的安全要求 |
| 异常流量 | 检查设备的上下行流量是否在规范范围内，设备流量过大或过小均自动告警 |
| 应用检查 | 支持在不安装客户端安全软件的基础上，判断设备特定软件的安装情况，预置常用应用软件识别规则 |
| 客户端软件 | 为保证使用便捷，需要与现有终端安全管理系统（天擎）使用同一客户端 |
| 认证方式 | 准入客户端提供有线802.1X、无线802.1X，http认证能力，支持用户名密码，主机认证，证书认证多种认证方式 |
| 全静默认证 | 支持全静默的终端身份认证，无需人工参与，终端即可自动完成准入认证，整个过程无弹窗，不影响全屏进程 |
| 合规检查 | 支持健康合规检查策略，采用动态检测技术，需支持多种检查机制，至少支持入网检查、定时检查、周期检查机制，针对接入内部网络的计算机终端实行多种安全检查策略，支持分组策略下发控制，拦截不安全终端接入网络。 |
| 隔离处置 | 支持终端安全检查失败处置措施，可基于协议、特定端口、端口范围、特定地址、IP范围、URL来控制终端访问权限，从而无需操作交换机达到终端网络隔离目的，实现细粒度的访问控制管理 |
| 引导修复 | 支持对不合规的终端提供软隔离，不符合安全策略的计算机终端进行友好提示，提供终端修复向导，需支持引导修复和一键修复功能，并支持不同区域终端的修复区域定义。 |
| 告警信息 | 支持以邮件或短信方式将新设备接入、IP地址变更、接入位置变更、设备仿冒等事件及时告知管理员 |

**3．日志设备**

两台，采集外网流量日志。与齐安信品牌NGSOC-NDS5000-TG35P型号设备完全兼容。

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 硬件规格 | 支持同时开启网络流量采集、威胁数据采集和日志上报功能情况下混合流吞吐量3Gbps，HTTP并发连接数不低于400万，HTTP新建连接速率不低于15万/秒；2U设备，最少配备6个10/100/1000M自适应千兆电口，1个Console口，2个接口扩展板卡插槽。 |
| 旁路部署 | 支持通过流量镜像的方式旁路部署在虚拟化网络中，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产。 |
| 流量采集 | 需支持空载荷过滤，支持对采集的流量的上下行载荷长度设置； |
| 支持离线采集，可通过手动PCAP导入或FTP等协议批量上传导入等方式对离线流量进行采集 |
| 流量识别与解析 | 支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库3000+。 |
| 支持ICMP、DHCP、HTTP、TELNET、DNS、SSL等基础协议的解析 |
| 具有自定义解析流量能力，支持基于正则表达式、TLV格式、固定长度等提取模式对应用流量解析 |
| 文件还原 | 支持还原多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB、TFTP、QQ； |
| 支持多种文件类型的筛选，可执行文件还原格式包含：bin、exe、bat、dll、sys、com、ax、acm、drv等；压缩文件还原格式包含：rar、zip、gz、7z、tar等；文档类型的还原格式包含：doc、docx、xls、txt、pptx、pdf、rtf、ppt等。 |
| 威胁检测 | 系统具备全面的间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理通道、后门程序、远控木马等 |
| 系统具备全面的漏洞检测能力，可检测常见的溢出攻击、跨站脚本、SQL注入、拒绝服务、跨站请求伪造、目录遍历、webshell上传等 |
| 系统支持Flood攻击检测，包括SYN Flood、ICMP Flood、UDP Flood和IP Flood；支持应用层Flood攻击检测，包括DNS Flood和HTTP Flood。 |
| 系统需支持按照协议类型对攻击事件规则的设置检测有效性，协议类型包括HTTP、DNS、FTP、ICMP、IMAP、IRC、Mongodb、NNTP、POP3、RIP、RLOGIN、SMTP、SNMP、TDS、TELNET、TFTP、TNS等 |
| 系统需具备专业的查毒引擎，独立的病毒库，支持通过对HTTP、FTP、SMTP、POP3、IMAP、SMB、TFTP、NFS协议进行恶意文件检测。 |
| 具有云端检测能力，并支持云端沙箱检测 |
| 系统需具备攻击检测能力的扩展功能，支持自定义恶意文件、自定义漏洞、自定义间谍软件、自定义威胁情报； |
| 系统本地需具备攻击告警的过滤能力，能够针对IP地址或端口对攻击告警进行过滤，支持攻击特征高亮展示，方便分析人员事件分析 |
| 数据外发 | 通信模式支持但不限于KAFKA、ZMQ、SYSLOG等协议，需支持多路外发，并支持外发多地址的负载均衡处理 |
| 外发类别支持但不限于流量日志、威胁日志、资产日志、样本文件、威胁相关pcap等 |
| SSL旁路解密 | ☆支持基于SSL协议的SMTPS、POP3S、IMAPS、HTTPS流量进行解密，可添加基于源目的地址及端口的过滤条件。支持解密后的明文流量镜像至下游设备。 |
| 资产识别 | 系统具有资产识别能力，能够根据流量识别资产的操作系统、服务、开放端口、banner信息等；支持资产识别范围配置、支持资产识别展示及导出 |
|  | 支持 资产识别范围配置、支持资产识别展示及导出 |
| 流量及样本取证 | 支持威胁告警的相关pcap数据留存，支持本地下载及外发，外发通信协议包括但不限于KAFKA、FTP、SFTP等 |
| 支持威胁告警的相关文件留存，支持本地下载及外发，外发通信协议包括但不限于FTP、SFTP等 |
| 业务统计和状态监控 | 支持失陷主机、恶意文件检测、漏洞攻击检测的数量统计。 |
| 基于应用维度的TOP5、TOP10的24小时/7天的实时流量统计和可视化展示。 |
| 基于会话维度并发、新建的24小时/7天的统计和可视化。 |
| 网络流量传感器生成的网络流量日志数和威胁检测日志数的实时统计及可视化展示 |
| 安全管理 | 支持HTTP、HTTPS、Telnet、远程SSH等多种管理方式，用户可自定义修改管理端口 |
| 支持可信主机和可信MAC功能，仅可信地址可访问该设备 |
| 对接要求 | 需要与集团核心平台无缝对接 |

**4.APT 设备**

两台，接收公安部门威胁情报，防御威胁攻击。与公安一所品牌K01型号设备完全兼容。

|  |  |  |
| --- | --- | --- |
| **指标项** | | **参数要求** |
| 硬件规格 | 硬件规格 | 1U机架设备，内存≥16G，硬盘≥1T，1个Console口，2个USB接口，板载千兆电口≥6个，支持2组Bypass，扩展槽≥2 |
| 性能参数 | 新建链接数 | 千兆：≥15000/秒 |
| 并发链接数 | 千兆：1000000 |
| 旁路阻断率 | ≥99%， |
| 串联阻断率 | ≥99% |
| 功能参数 | 网络部署 | 支持串联与旁路部署方式，支持channel、trunk接口模式，并支持802.1Q网络环境 |
| 支持管理口、镜像口、阻断口及业务口分离部署 |
| 阻断拦截 | 支持串联与旁路部署情况下，对流量进行实时检测，并阻断异常访问行为 |
| 支持自动值守和人工研判的攻击阻断方式 |
| 访问控制 | 支持IP黑白名单及访问控制策略配置，支持按照分、时、天、月及永久等不同级别设定生效周期，并支持配置导入导出 |
| 支持IPv6地址格式 |
| 情报源支持 | 系统支持多情报源接入，至少包含正向攻击情报源、受控外联情报源、IP画像情报源及自定义情报源等类型 |
| 多情报源支持冗余设置，可根据网络健康程度进行自由切换 |
| 支持自定义私有情报源，接入方式至少包含FTP、FTPS等类型，且更新频率可自定义设置 |
| 支持IPv6格式情报数据 |
| 攻击监测与阻断 | 支持基于正向攻击类情报的威胁监测与阻断 |
| 系统内置日常和重保策略模板，并支持自定义模板配置 |
| 支持基于不同资产、情报源、情报行业、情报类型、情报碰撞策略及情报威胁等级等维度设置策略匹配条件 |
| 支持配置阻断范围，至少包含单IP和网段 |
| 支持阻断策略优先级配置 |
| 外联检测与阻断 | 支持基于受控外联类情报的外联检测与阻断 |
| 支持针对不同资产设置对应策略 |
| 支持自定义添加外联情报，且支持批量导入、导出、删除等操作，支持精确匹配及正则表达式匹配 |
| 自定义外联情报支持API接入 |
| 弱口令登录检测与阻断 | 支持弱口令登录检测与阻断 |
| 支持针对不同资产设置对应策略 |
| 支持自定义检测强度，至少包含高、中、低3种不同级别 |
| 支持自定义口令字典，可进行批量导入、导出、删除等操作 |
| 溯源画像 | 支持情报源的基础属性画像，至少包含归属地、归属地、经纬度、运营商等属性 |
| 支持情报源的资产属性画像，至少包含资产标签、组件标签、开放端口等属性 |
| 至少支持最近三个月的攻击轨迹溯源，至少包含历史攻击单位、攻击类型、被攻击单位所属行业等属性 |
| 会话取证 | 支持全流量留存取证 |
| 支持基于不同协议的分类流量取证，至少包含HTTP、FTP、SMTP、DNS及SNMP等类型 |
| 统计分析 | 支持攻击监测日志、攻击IP分析及被攻击IP分析等三个维度的统计，可通过丰富的组合筛选条件进行详细风险审计。并支持情报及本地攻击行为的溯源 |
| 支持外联检测日志、外联检测分析以及外联域名分析等三个维度的统计，可通过丰富的组合筛选条件进行详细审计 |
| 支持整体攻击态势可视化展示，并可在地图上直观查看的情报IP的分布情况，同时可直接在数据统计模块进行人工研判 |
| 报表导出 | 支持按照告警模块导出统计报告；报告格式支持HTML和PDF |
| 支持手动和自动导出方式，自动导出周期至少包含天、周、月等时间周期 |
| 日志外发 | 支持Syslog日志外发，支持JSON及字符串两种数据格式 |
| 系统管理 | 支持系统备份及恢复，可选择手动备份或定期自动备份两种方式 |
| 自动备份周期支持按天、按周或按月设置 |
| 支持可视化展示CPU、内存、硬盘资源占用率及网络接口流量情况 |
| 支持自定义远程管理地址段权限设置 |
| 支持账号密码有效期设置，满足等保要求 |
| 支持规则库远程在线升级 |
| 系统内置系统管理员、审计管理员和账号管理员三种角色 |

**5.内容过滤设备**

两台，一台满足100M出口带宽使用需求，一台满足500M出口带宽使用需求。根据公司要求及各自数据文件特点，制定内容传输控制策略。与天空卫士品牌UCSG1100型号设备完全兼容。

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 预置规则 | 系统需预置各类行业及法律法规的规则模版，包括并不限于以下模板：GDPR法案、个人信息保护法规、网络安全法等 |
| 系统需预置开箱即用的权重字典。包括并不限于以下字典：个人用户敏感信息、国家领导人、政治言论、高管信息、技术方案、会议纪要、采购计划、网络安全、投资信息等、简历字典等 |
| 系统需预置常见的正则表达式，包括并不限于以下正则：手机号码、固话号码、姓名、地址、邮箱、身份证号、银行卡号等，支持对数据的有效性进行验证。 |
| 关键字识别技术 | 系统需支持关键字内容匹配的检测规则。支持重复关键字数的统计及关键字的精确匹配模式，并支持自动简繁体自动内容转换的识别技术 |
| 字典识别技术 | 系统应支持关键字组合权重的字典识别技术；支持从外部导入字典 |
| 正则表达式识别技术 | 系统需预置常见的数据识别脚本，包括并不限于以下内容：手机号码、固话号码、姓名、地址、邮箱、身份证号、银行卡号等，支持对数据的有效性进行验证。 |
| 系统应支持标准的正则表达式进行内容检测。 |
| 数据库指纹识别技术 | 系统应支持对数据库（包括并不限于以下数据库类型：CSV文件、Oracle、SQLServer、MySQL、Postgres、DB2等数据库）进行指纹学习，生成敏感数据库数据指纹，从而可以精确识别从数据库源中泄漏的数据。 |
| 文件指纹识别技术 | 系统应支持采用压缩包上传、远程共享学习 的方式对各类Office、PDF等文本文档学习生成 精确数据指纹 和 相似数据指纹，可设置10%-90%的相似度阈值从而防止重要文档泄漏. |
| 系统应支持采用增量 或 全量 的指纹学习 与 定时指纹生成 任务 |
| 系统应支持反向指纹学习，可以将非机密信息如免责声明、内部模版、邮件签名等内容进行例外，降低指纹匹配中误报 |
| 机器学习技术 | 系统应支持机器学习技术，可智能获取指定类型的文件内容特征, 从而识别公司中此类文档中潜在数据泄漏威胁。 |
| 系统应支持正向、反向机器学习 以提高识别能力 |
| 系统应支持 远程目录自动机器 学习，支持机器学习结果导出供其他设备或任务使用 |
| 数据聚类技术 | 系统应支持上传文档并利用数据聚类协助企业进行自动文档分类 , 辅助更有效的DLP策略制定 |
| 系统应支持在线对分类后文档进行机器学习获得文档特征 , 辅助更有效的DLP策略制定 |
| 数据分类技术 | 系统应支持协助企业完成数据安全治理工作，支持设定不同的数据类别，在该类别下可包容不同的检测规则，如 包含 姓名、电话号码 、信用卡号码、地址、邮件地址检测规则均属于用户数据分类 |
| 系统应支持为数据类别设置不同的数据级别，数据级别应可自定名称，不限级别数量，从而协助企业完成数据安全治理工作， |
| 文件特征识别技术 | 系统应支持至少300种以上的主流文件类型真实格式与内容的识别，支持主流Office/PDF加密格式、ZIP/7zip/RAR压缩格式的识别，支持最新的RAR5压缩格式 |
| 系统应支持对文件类型、文件大小、文件名称、文件属性（包括所有者、修改时间、创建时间、访问时间）进行准确的特征识别。 |
| 系统应支持采用文件类型自定义工具，针对企业特定文件进行文件类别特征学习，从而实现后续该类别文件的类别检测 |
| 逃逸技术及用户威胁行为识别技术 | 系统应支持对多层压缩文件、更改文件后缀、更改压缩包后缀、转换文件类型等常见规避手段处理过的文件内容进行检查 |
| 系统应支持对于用户的伪装格式（发送的文件与真实文件格式不符）、文件中有嵌套其他文件等风险行为、点滴式传输的数据 进行审计或保护拦截 |
| 设备部署要求 | 系统应支持旁路审计部署及串联部署，支持在管理界面一键切换运行模式 |
| 系统应支持IPv6环境下的部署和使用 |
| 系统应支持通过ICAP方式与现有代理服务器进行联动配置 |
| 系统OCR识别能力 | 系统应预置高性能高精度OCR图片内容识别引擎，对于图片中的简体、繁体、英文进行高精度的内容识别，无需独立部署或另购 |
| 系统应支持常见图片文件以及嵌套在Office/压缩包中的的图片内容进行检查，包括JPEG、TIF、TIFF、BMP、PNG等常见图片格式 |
| DLP网络协议支持 | 系统应支持HTTP,HTTPS,SMTP,SMB,FTP,IMAP,POP3协议的敏感信息识别与监控 |
| 系统应支持旁路SMTP监控与MTA部署方式对于外发邮件内容进行深度审计与保护 |
| 系统应支持旁路部署下对于简单加密的SSL协议进行解密，内容审计 |
| 数据识别要求 | 产品内嵌预定义数据防泄漏规则模板。 |
| 支持基于关键字、字典库、规则表达式、自然语言处理（NLP）、文件类型／名称／大小、文件及数据库指纹、机器学习、标签、文件分类等方式定义敏感内容。 |
| 支持基于设备的网络监控、阻断功能 |
| SSL解密，内嵌业界领先的HTTPS解密技术，可对SSL解密并对内容进行深层内容分析及根据策略做出响应，以防止企业敏感信息外泄或利用SSL访问不当内容的网站 |
| 支持数据防泄漏事件及报告管理与终端、邮件在同一个管理界面上实现。 |
| 上传敏感数据保护 | 系统应支持对上传给外部网站的数据进行敏感内容检测和阻断 |
| 下载敏感数据保护 | 对从企业内部服务器或云应用Portal中下载到用户电脑中的内容进行敏感内容检测，并对禁止下载的内容进行报警或阻断 |
| 网络传输文件收集 | 系统应支持对网络全流量中的所有常见文件、邮件附件进行自动收集整理与存储，以作为文件全归档、数据梳理与分级分类样本资源 |
| DLP网络协议支持 | 系统应支持HTTP,SMTP,SMB,FTP,IMAP,POP3协议的敏感信息识别与监控 |
| 系统应支持旁路SMTP监控与MTA部署方式对于外发邮件内容进行深度审计与保护 |
| 兼容性要求 | 支持与商飞现有DLP系统联动，并统一接受主控制台管理 |
| 支持与商飞现有DLP系统共用同一套全局DLP策略，全局策略统一由控制台下发，也可以根据需求定制个性化DLP策略应用在本单位 |
| 硬件性能不低于1\*Xeon4C8T，16GB内存，2\*SATA RAID1 硬盘，4\*千兆电口，单电源，1U 机箱；支持100M-200M网络出口带宽； |

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 预置规则 | 系统需预置各类行业及法律法规的规则模版，包括并不限于以下模板：GDPR法案、个人信息保护法规、网络安全法等 |
| 系统需预置开箱即用的权重字典。包括并不限于以下字典：个人用户敏感信息、国家领导人、政治言论、高管信息、技术方案、会议纪要、采购计划、网络安全、投资信息等、简历字典等 |
| 系统需预置常见的正则表达式，包括并不限于以下正则：手机号码、固话号码、姓名、地址、邮箱、身份证号、银行卡号等，支持对数据的有效性进行验证。 |
| 关键字识别技术 | 系统需支持关键字内容匹配的检测规则。支持重复关键字数的统计及关键字的精确匹配模式，并支持自动简繁体自动内容转换的识别技术 |
| 字典识别技术 | 系统应支持关键字组合权重的字典识别技术；支持从外部导入字典 |
| 正则表达式识别技术 | 系统需预置常见的数据识别脚本，包括并不限于以下内容：手机号码、固话号码、姓名、地址、邮箱、身份证号、银行卡号等，支持对数据的有效性进行验证。 |
| 系统应支持标准的正则表达式进行内容检测。 |
| 数据库指纹识别技术 | 系统应支持对数据库（包括并不限于以下数据库类型：CSV文件、Oracle、SQLServer、MySQL、Postgres、DB2等数据库）进行指纹学习，生成敏感数据库数据指纹，从而可以精确识别从数据库源中泄漏的数据。 |
| 文件指纹识别技术 | 系统应支持采用压缩包上传、远程共享学习 的方式对各类Office、PDF等文本文档学习生成 精确数据指纹 和 相似数据指纹，可设置10%-90%的相似度阈值从而防止重要文档泄漏. |
| 系统应支持采用增量 或 全量 的指纹学习 与 定时指纹生成 任务 |
| 系统应支持反向指纹学习，可以将非机密信息如免责声明、内部模版、邮件签名等内容进行例外，降低指纹匹配中误报 |
| 机器学习技术 | 系统应支持机器学习技术，可智能获取指定类型的文件内容特征, 从而识别公司中此类文档中潜在数据泄漏威胁。 |
| 系统应支持正向、反向机器学习 以提高识别能力 |
| 系统应支持 远程目录自动机器 学习，支持机器学习结果导出供其他设备或任务使用 |
| 数据聚类技术 | 系统应支持上传文档并利用数据聚类协助企业进行自动文档分类 , 辅助更有效的DLP策略制定 |
| 系统应支持在线对分类后文档进行机器学习获得文档特征 , 辅助更有效的DLP策略制定 |
| 数据分类技术 | 系统应支持协助企业完成数据安全治理工作，支持设定不同的数据类别，在该类别下可包容不同的检测规则，如 包含 姓名、电话号码 、信用卡号码、地址、邮件地址检测规则均属于用户数据分类 |
| 系统应支持为数据类别设置不同的数据级别，数据级别应可自定名称，不限级别数量，从而协助企业完成数据安全治理工作， |
| 文件特征识别技术 | 系统应支持至少300种以上的主流文件类型真实格式与内容的识别，支持主流Office/PDF加密格式、ZIP/7zip/RAR压缩格式的识别，支持最新的RAR5压缩格式 |
| 系统应支持对文件类型、文件大小、文件名称、文件属性（包括所有者、修改时间、创建时间、访问时间）进行准确的特征识别。 |
| 系统应支持采用文件类型自定义工具，针对企业特定文件进行文件类别特征学习，从而实现后续该类别文件的类别检测 |
| 逃逸技术及用户威胁行为识别技术 | 系统应支持对多层压缩文件、更改文件后缀、更改压缩包后缀、转换文件类型等常见规避手段处理过的文件内容进行检查 |
| 系统应支持对于用户的伪装格式（发送的文件与真实文件格式不符）、文件中有嵌套其他文件等风险行为、点滴式传输的数据 进行审计或保护拦截 |
| 设备部署要求 | 系统应支持旁路审计部署及串联部署，支持在管理界面一键切换运行模式 |
| 系统应支持IPv6环境下的部署和使用 |
| 系统应支持通过ICAP方式与现有代理服务器进行联动配置 |
| 系统OCR识别能力 | 系统应预置高性能高精度OCR图片内容识别引擎，对于图片中的简体、繁体、英文进行高精度的内容识别，无需独立部署或另购 |
| 系统应支持常见图片文件以及嵌套在Office/压缩包中的的图片内容进行检查，包括JPEG、TIF、TIFF、BMP、PNG等常见图片格式 |
| DLP网络协议支持 | 系统应支持HTTP,HTTPS,SMTP,SMB,FTP,IMAP,POP3协议的敏感信息识别与监控 |
| 系统应支持旁路SMTP监控与MTA部署方式对于外发邮件内容进行深度审计与保护 |
| 系统应支持旁路部署下对于简单加密的SSL协议进行解密，内容审计 |
| 数据识别要求 | 产品内嵌预定义数据防泄漏规则模板。 |
| 支持基于关键字、字典库、规则表达式、自然语言处理（NLP）、文件类型／名称／大小、文件及数据库指纹、机器学习、标签、文件分类等方式定义敏感内容。 |
| 支持基于设备的网络监控、阻断功能 |
| SSL解密，内嵌业界领先的HTTPS解密技术，可对SSL解密并对内容进行深层内容分析及根据策略做出响应，以防止企业敏感信息外泄或利用SSL访问不当内容的网站 |
| 支持数据防泄漏事件及报告管理与终端、邮件在同一个管理界面上实现。 |
| 上传敏感数据保护 | 系统应支持对上传给外部网站的数据进行敏感内容检测和阻断 |
| 下载敏感数据保护 | 对从企业内部服务器或云应用Portal中下载到用户电脑中的内容进行敏感内容检测，并对禁止下载的内容进行报警或阻断 |
| 网络传输文件收集 | 系统应支持对网络全流量中的所有常见文件、邮件附件进行自动收集整理与存储，以作为文件全归档、数据梳理与分级分类样本资源 |
| DLP网络协议支持 | 系统应支持HTTP,SMTP,SMB,FTP,IMAP,POP3协议的敏感信息识别与监控 |
| 系统应支持旁路SMTP监控与MTA部署方式对于外发邮件内容进行深度审计与保护 |
| 兼容性要求 | 支持与商飞现有DLP系统联动，并统一接受主控制台管理 |
| 支持与商飞现有DLP系统共用同一套全局DLP策略，全局策略统一由控制台下发，也可以根据需求定制个性化DLP策略应用在本单位 |
| 硬件性能不低于2\*Xeon E5, 32GB内存，2\*SAS RAID1 硬盘，4\*千兆网口, 4\*千兆Bypass网口， 双电源，1U 机箱；支持200M-400M网络出口带宽； |

1. **互联网流量牵引设备**

两台，互联网统一组网。与深信服品牌B1100型号设备完全兼容。

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 硬件参数 | 不少于千兆电口和2个千兆SFP光口 |
| VPN加密性能 | 加密速度不小于450Mbps |
| 防火墙吞吐性能 | 不小于1.5Gbps |
| 部署模式 | 支持网关、单臂等部署模式 |
| 运行状态监控 | 支持实时监控设备运行状态，包括设备CPU占用率、内存占用率、网口运行状态、在线用户数，支持查看最近1小时、最近一天的WAN口流量统计等信息 |
| 应用流量监控 | 支持对应用上行流速、下行流速、总流速进行展示，同时可以设置按5s或者10s的维度设置自动刷新频率。支持查看最近1小时，最近24小时的设备VPN流量传输情况，包括实时发送流量与实时接收流量情况 |
| VPN隧道状态监控 | 支持实时监控VPN隧道状态信息，包括连接状态、对端设备名称、对端设备类型、对端公网IP、对端内网IP、发送流速、接收流速、丢包、时延、抖动、传输类型、加密算法、MTU、最近接入时间等 |
| 故障自动检测 | 设备自带ping包、DNS解析、ARP命令等工具，支持手动设置时间间隔，自动检测线路运行状态。支持业务访问不通或者业务访问慢两个维度进行问题诊断 |
| 硬件特征认证 | 除用户名/密码认证方式外，还支持基于网关硬件特征的高安全身份验证技术 |
| 防火墙 | 具备基于状态监测技术的防火墙功能，可基于网络网络服务、源IP、目的IP、时间自定义防火墙规则，可防范来自外网、内网的DOS攻击，可设置外网访问本机的权限、远程维护、升级维护、SSH维护；检测到数据包不在过滤规则列表中时，可设置默认通过或拒绝；支持规则测试 |
| 应用识别 | 支持智能识别不少于2000种应用及5000条应用识别规则，支持应用分类，支持自定义应用，支持自定义应用类别 |
| 带宽保障通道 | 支持在指定线路或者全部线路上，根据流量保障或者流量限制模式设置带宽百分比，可以匹配全部用户或者指定用户在在特定时间生效，支持设置单用户流量上下行带宽值，避免单用户流量突发情况 |
| 链路丢包优化 | 支持通过FEC前向校验技术优化链路丢包，支持动态自适应以及自定义条件的开启模式，保障在线路高丢包环境下的应用访问体验 |
| 业务优先级编排 | 支持手动编排业务传输的优先级，最高不低于设置4个优先级级别,支持将业务进行自定义服务类型分类，服务类型不低于3类 |
| 最优选路 | 基于DPI和DFI技术智能识别应用并根据应用流量特征将应用划分为多种应用类型根据应用特性与链路探测结果动态匹配，将业务智能负载至最优链路传输，支持基于QOE参数（时延、丢包、抖动）实时检测每条广域网链路的质量，选择质量最佳的链路进行数据转发，支持指定应用（服务）优选指定线路，同时能调整指定线路的优先级顺序 |
| 按剩余带宽比例负载选路 | 支持检测线路剩余带宽容量，并将应用流量按照线路剩余带宽容量比例均匀负载传输，带宽利用比例均衡 |

1. **网络流量控制设备**

两台，一台满足1500用户数的使用需求，一台满足1000用户数的使用需求。对出口流量进行流控。与深信服品牌H4700型号设备完全兼容。

|  |  |  |
| --- | --- | --- |
| **指标项** | **参数要求** | |
| 硬件要求 | 规格：1U，内存大小≥4G，硬盘容量≥64G SSD+960G SSD，电源：单电源，接口：千兆电口≥6个，千兆光口SFP≥2个 | |
| 性能要求 | 网络层吞吐量（大包）≥3.6Gb，应用层吞吐量≥450Mb，带宽性能≥300Mb，支持用户数≥1500，包转发率≥45Kpps，每秒新建连接数≥4000，最大并发连接数≥150000。 | |
| 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bypass；支持多路桥接功能，最多可支持32组网桥模式； | |
| 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； | |
| 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； | |
| DNS代理 | 支持DNS代理，能够基于用户、域名、目标DNS，指定代理策略生效，代理策略可以设置为：重定向至DNS服务器、解析为IP、丢弃、重定向至指定线路； | |
| 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； | |
| 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；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；带宽质量分析、实时流量排名；泄密风险、工作效率、共享上网等行为风险情况； | |
| 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； | |
| SSL解密故障排查 | 支持解密排障，自动检测解密审计不成功原因； | |
| 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; | |
| 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； | |
| 自注册认证 | 密码登录支持用户自注册，通过Web页面申请注册新账号，管理员审批后新账号可用，自注册同时支持portal认证和802.1x认证； | |
| 支持管理员关联了手机号码，可以通过手机号接受自注册、终端注册、终端绑定的审批通知; | |
| OA认证 | 支持通过OAuth认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证； | |
| IP管理 | 支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量； | |
| 终端分类可视 | 1.对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等 2.支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；3.支持查看终端类型分布; | |
| 静态URL库 | 设备内置海量预分类的URL地址库，能够针对各种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; | |
| URL数量在3000万以上，包含分类数量150个以上; | |
| SSL加密网页识别过滤 | 识别并过滤SSL加密的钓鱼网站、非法网站等，支持将违规https访问重定向到告警页面; | |
| 必须支持https网页全解密和按网站类别分类进行解密配置； | |
| 应用识别规则库 | 1.设备内置应用识别规则库，支持超过9000条应用规则数，支持超过6000种以上的应用，并保持每两个星期更新一次，保证应用识别的准确率；2.支持根据标签选择应用，并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； | |
| SaaS应用规则 | 1.对Saas应用有默认分类标签，帮助客户统一配置策略 2.必须支持超过200种主流网络会议/办公OA/教育等学习应用; | |
| QQ白名单 | 支持基于用户组、终端类型、位置的QQ白名单功能; | |
| 通道化应用流控 | 必须支持在不同线路上，根据不同的应用、目标IP、时间段、日期、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； | |
| 必须支持流量父子通道技术，且至少支持三级父子通道； | |
| P2P智能流控 | 支持通过抑制P2P的下行丢包，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； | |
| 网页访问审计 | 支持记录全部或者指定类别URL、网页标题等信息； | |
| 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。 | |
| 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； | |
| 用户行为日志 | 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、发帖/微博、搜索关键字等详细用户行为的报表; | |
| 单用户行为分析 | 支持针对单用户的整体行为分析，至少包括应用流速趋势、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）; | |
| 产品资质 | 公安部颁发的《网络通讯安全审计产品销售许可证》 | |
|  |  | |
| **指标项** | **参数要求** |
| 硬件要求 | 规格：1U，内存大小：4G，硬盘容量：128G minisata SSD，电源：单电源，接口：6千兆电口+2千兆光口SFP。 |
| 性能要求 | 网络层吞吐量（大包）：3Gb，应用层吞吐量：300Mb，带宽性能：200Mb，IPSEC VPN加密性能（最高性能）：50Mb，支持用户数：1000，包转发率：27Kpps，每秒新建连接数：2400，最大并发连接数：120000。 |
| 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bypass；支持多路桥接功能，最多可支持32组网桥模式； |
| 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； |
| 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； |
| DNS代理 | 支持DNS代理，能够基于用户、域名、目标DNS，指定代理策略生效，代理策略可以设置为：重定向至DNS服务器、解析为IP、丢弃、重定向至指定线路； |
| 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； |
| 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；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；带宽质量分析、实时流量排名；泄密风险、工作效率、共享上网等行为风险情况； |
| 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； |
| SSL解密故障排查 | 支持解密排障，自动检测解密审计不成功原因； |
| 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; |
| 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； |
| 自注册认证 | 密码登录支持用户自注册，通过Web页面申请注册新账号，管理员审批后新账号可用，自注册同时支持portal认证和802.1x认证； |
| 支持管理员关联了手机号码，可以通过手机号接受自注册、终端注册、终端绑定的审批通知; |
| OA认证 | 支持通过OAuth认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证； |
| IP管理 | 支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量； |
| 终端分类可视 | 1.对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等 2.支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；3.支持查看终端类型分布; |
| 静态URL库 | 设备内置海量预分类的URL地址库，能够针对各种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; |
| URL数量在3000万以上，包含分类数量150个以上; |
| SSL加密网页识别过滤 | 识别并过滤SSL加密的钓鱼网站、非法网站等，支持将违规https访问重定向到告警页面; |
| 必须支持https网页全解密和按网站类别分类进行解密配置； |
| 应用识别规则库 | 1.设备内置应用识别规则库，支持超过9000条应用规则数，支持超过6000种以上的应用，并保持每两个星期更新一次，保证应用识别的准确率；2.支持根据标签选择应用，并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； |
| SaaS应用规则 | 1.对Saas应用有默认分类标签，帮助客户统一配置策略 2.必须支持超过200种主流网络会议/办公OA/教育等学习应用; |
| QQ白名单 | 支持基于用户组、终端类型、位置的QQ白名单功能; |
| 通道化应用流控 | 必须支持在不同线路上，根据不同的应用、目标IP、时间段、日期、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； |
| 必须支持流量父子通道技术，且至少支持三级父子通道； |
| P2P智能流控 | 支持通过抑制P2P的下行丢包，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； |
| 网页访问审计 | 支持记录全部或者指定类别URL、网页标题等信息； |
| 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。 |
| 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； |
| 用户行为日志 | 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、发帖/微博、搜索关键字等详细用户行为的报表; |
| 单用户行为分析 | 支持针对单用户的整体行为分析，至少包括应用流速趋势、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）; |
| 产品资质 | 公安部颁发的《网络通讯安全审计产品销售许可证》 |

1. **主机防病毒设备**

两台，普通X86服务器，内存16G，硬盘2TB。

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 机型 | 机架式服务器 |
| 背板 | 机箱 3.5\*4 SAS/SATA 背板 |
| 处理器 | Intel Xeon 3204 (6C 85W 1.9GHz)Processor Option Kit |
| 内存 | 16GB DDR4 RDIMM |
| 硬盘 | 3.5 2TB 7.2K SATA 6Gbps Hot Swap Hard Drive\*2 |
| 网卡 | 板载 双口千兆 |
| 阵列卡 | SAS PM8222-HBA 12Gb Adapter |
| 电源 | 550W Hot Swap Power Supply\*2 |