# 等级保护加固项目采购需求

## 一、产品清单

**1．防火墙2台**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **指标要求** | **证明材料要求** |
| 1 | 设备 | 要求采用多核架构，自研操作系统。 | 否 |
| ★1 | 2U机型，提供的产品不能少于6个10/100/1000M以太网电口，1个接口扩展槽位，含交流冗余电源模块。 | 否 |
| 2 | 性能 | 系统吞吐不少于6Gbps，最大并发不少于200万，每秒新建不少于6万。 | 否 |
| 3 | 防火墙 | 支持虚拟线、二层透明、路由、混合、旁路监听、PPPoE等接入方式，适应各种网络环境需求。 | 否 |
| 4 | 支持VLAN划分、VLAN Trunk，支持802.1Q，能进行封装和解封；支持MSTP、RSTP等生成树协议。 | 否 |
| 5 | 支持IPMAC绑定，支持手动和自动探测绑定。 | 否 |
| 6 | 能够在一条策略里配置源/目的IP地址、安全区、应用/应用组、协议/端口、时间、用户、安全模板/模板组。 | 否 |
| 7 | 支持基于策略的双向NAT、动态/静态NAT、端口PAT。 | 否 |
| 8 | 支持基于域名的访问控制。 | 否 |
| 9 | 支持WEB界面设置静态路由及OSPF、RIP、BGP动态路由协议；支持基于源/目的地址、接口的、基于服务的策略路由。 | 否 |
| 10 | 支持内置/自定义ISP路由库。 | 否 |
| #1 | 支持链路探测，能够在每接口上以ICMP/TCP/UDP协议探测目标主机可达性，探测链路是否有效 。 | 否 |
| #2 | 支持基于IPv6的访问控制，并可灵活配置。提供IPv6证书。 | 是 |
| 11 | 支持泛洪类攻击防护：UDP/DNS/SYN/PING 泛洪；支持ARP欺骗类攻击。 | 否 |
| 12 | VPN | 支持IPsec VPN、L2TP VPN。 | 否 |
| 13 | Ipsec VPN支持网关-网关、移动客户-网关部署方式。 | 否 |
| #3 | 识别能力 | 支持对1500+ 种应用平台及2200+种的应用进行识别和控制，至少支持5大类，比如：商业系统、协作应用、一般网络应用、媒体等及28子类，比如：认证服务、数据库、ERP-CRM、软件更新、电子邮件、VOIP视频、游戏等；支持自定义应用。 | 否 |
| #4 | 支持应用过滤器，至少支持4个维度进行过滤，比如：应用类别、实现技术、风险等级、标签。 | 否 |
| 14 | 内网风险管理 | 可识别并分析内网主机的接入数量和资产属性。 | 否 |
| #5 | 可不通过主机扫描等技术，即可识别内网主机的操作系统、杀毒软件、浏览器等信息。 | 是 |
| 15 | HA | 采用双机模式部署。 | 否 |
| 16 | 系统管理 | 支持Web管理、串口管理、SSH管理，并且能够支持IE、firefox、chrome等浏览器管理。 | 否 |
| #6 | 针对事件关联分析，可以提供多种入口，比如基于应用、目的IP、源IP、用户、攻击事件等。 | 否 |
| ★2 | 产品资质及实力 | 产品具备《计算机信息系统安全专用产品销售许可证》增强级（千兆）。提供有效证书的复印件。 | 是 |
| #7 | 产品具备《信息技术产品安全测评证书》，测评级别为EAL4+级别。提供证书复印件。 | 是 |

**2．入侵防御设备1台**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **指标要求** | **证明材料要求** |
| ★3 | 设备要求 | 2U标准机架式硬件，具有自主知识产权；提供的产品不能少于4个10/100/1000M以太网电口，3个扩展插槽。 | 否 |
| #8 | 设备性能 | 网络吞吐量：11Gbps；Realworld吞吐量≥2Gbps；最大并发连接数≥200万；每秒新建连接≥60000。 | 否 |
| 17 | 入侵防护功能 | 系统应提供覆盖广泛的攻击特征库，能够针对8500以上的攻击行为、异常事件，以及网络资源滥用流量，进行检测和防御。 | 否 |
| 18 | 系统应支持多种抗逃避检测技术。 | 否 |
| 19 | 系统应提供入侵行为和应用软件特征的自定义接口，可根据用户需求定制对其它流量的检测和阻断规则。 | 否 |
| 20 | 系统应能够有效抵御SQL注入、僵尸网络等多种常见的应用层安全威胁。 | 否 |
| 21 | 系统应提供先进的DoS/DDoS攻击防护能力，支持双向阻断TCP/UDP/ICMP/ACK Flooding，以及UDP/ICMP Smurfing等常见的DoS/DDoS的攻击。 | 否 |
| 22 | 系统应提供丰富的响应方式，包括：会话阻断、IP隔离、邮件通知等功能，满足用户各种响应需求。 | 否 |
| 23 | 系统应具备攻击快照功能，详细记录触发告警的数据特征，以便做进一步的事件分析。 | 否 |
| 24 | 应用识别 | 系统应能识别主流的应用程序，识别种类不少于2500种。 | 否 |
| 25 | 数据泄露防护 | 系统应提供服务器异常告警功能，可以自学习服务器正常工作行为，并以此为基线检测处服务器非法外联行为。 | 否 |
| 26 | 系统应提供敏感数据保护功能，能够识别、阻断通过自身的敏感数据信息（身份证号、银行卡、手机号等）。 | 否 |
| #9 | 系统应提供关键文件保护功能，能够识别、阻断通过自身的关键文件，以防止非法外传行为。能识别的关键文件类型应包含至少以下几类：文档类如Excel、PDF、PowerPoint、Word等，压缩文件类如CAB、GZIP、RAR、ZIP、JAR等，图像类如BMP、GIF、JPEG等，音频视频类如MP3、AVI、MKV、MP4、MPEG、WMV等，脚本类如BAT、CMD、WSF等，程序类如APK、DLL、EXE、JAVA\_CLASS等。 | 否 |
| 27 | 系统应提供基于信誉的僵尸网络防护能力，具备可以持续升级的信誉库，IPS通过信誉库内的恶意网站IP、C&C服务器地址的信誉值执行相应的防护动作。 | 否 |
| 28 | 部署能力 | 系统应提供策略模板，减少配置工作量，提高部署效率。 | 否 |
| #10 | 系统须支持IPv6/IPv4双协议栈功能，能同时辨识IPv4和IPv6通讯流量。支持IPv6环境下攻击检测技术和基于IPv6地址格式的安全控制策略，为IPv6环境提供入侵防护。 | 否 |
| ★4 | 产品资质 | 产品具备公安部颁发的《计算机信息系统安全专用产品销售许可证》。 | 是 |
| #11 | 产品具备中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》,提供有效证书的复印件。 | 是 |

**3．Web应用防火墙1台**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **指标要求** | **证明材料要求** |
| 29 | 设备要求 | 专用机架式硬件设备，系统硬件为全内置封闭式结构，稳定可靠，用户界面、配置和管理等，均为中文，易于理解，并有详尽的中文技术文档。 | 否 |
| ★5 | 提供的产品不能少于6个10/100/1000M电口，1块接口扩展插槽，硬盘不小于1TB；必须内置硬件Bypass。提供的产品应用层吞吐量不能小于1Gbps，事务处理能力30000。 | 否 |
| 30 | 部署能力要求 | 支持透明部署，旁路部署，反向代理模式以及镜像部署模式。 | 否 |
| 31 | 防护功能要求 | 支持HTTP 0.9/1.0/1.1，完全解析HTTP事务。 | 否 |
| 32 | 支持对SSL（HTTPS）加密会话进行分析。 | 否 |
| 33 | 支持对HTTP协议的异常元素、异常参数、非法编码和解码的灵活控制与处理。 | 否 |
| 34 | 支持对注入、XSS、SSI指令、Webshell防护、路径穿越及远程文件包含的攻击防护。 | 否 |
| 35 | 支持CSRF（跨站请求伪造）防护。 | 否 |
| 36 | 支持爬虫防护，实现对100种以上的爬虫特征进行识别和阻断，防止页面因爬虫而引起信息泄露等问题。 | 否 |
| 37 | 支持盗链防护，有效识别网页盗链行为，避免用户网页资源被滥用。 | 否 |
| #12 | 支持Cookie安全机制。 | 否 |
| #13 | 支持对服务器状态码进行过滤和伪装的安全策略。 | 否 |
| 38 | 支持敏感关键字自定义功能。 | 否 |
| 39 | 支持URL ACL。对多种HTTP方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE等。 | 否 |
| 40 | 支持TCP Flood防护和HTTP Flood防护，并说明HTTP Flood防护的检测算法。 | 否 |
| #14 | 支持网页防篡改。 | 否 |
| #15 | 支持XML防护，包括XML基础校验、Schema校验以及SOAP校验。 | 否 |
| 41 | 日志与报表要求 | 支持不同安全事件类型以不同的颜色区分。 | 否 |
| 42 | 支持基于时间、IP、端口、动作、事件类型、URI、方法等条件的日志查询。 | 否 |
| #16 | 支持在安全日志中带有客户端真实IP地址，便于IP溯源。 | 否 |
| 43 | 支持日志分时段导出、全部导出或者清空。 | 否 |
| ★6 | 产品资质 | 《计算机信息系统安全专用产品销售许可证》，提供证书复印件证明。 | 是 |
| #17 | 《计算机软件著作权登记证》，提供证书复印件证明。 | 是 |
| #18 | 《国家信息安全测评信息技术产品安全测评证书》，级别至少为EAL3+，提供证书复印件证明。 | 是 |

**4．安全配置核查设备1台**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **指标要求** | **证明材料要求** |
| ★7 | 产品性能 | 允许最大并发扫描≥60个IP地址，允许最大并发任务≥10个任务，单个任务允许扫描的扫描范围不小于一个C类IP地址。 | 否 |
| 44 | 支持无限IP授权。扫描速度可达到800 ip/h。 | 否 |
| 45 | 产品形态 | 1U机架式设备，6个电口，1个RS232串口（RJ45），1个网络扩展板插槽（支持4电、4光、8电、8光），硬盘容量，1TB。 | 否 |
| 46 | 配置核查能力 | 支持**54**种以上常见设备和应用的配置检查，包括操作系统、网络设备（路由器和交换机）、防火墙、应用中间件、WLAN设备、虚拟化设备。 | 否 |
| 47 | 支持主流操作系统配置核查，包括Windows、Linux、AIX、HP-UX、Solaris、Suse、Debian等。 | 否 |
| 48 | 支持主流数据库配置核查，包括DB2、Informix、MySQL、SQL server、Sybase等。 | 否 |
| 49 | 支持应用中间件配置核查，包括Apache、BIND、Jboss、Tomcat、TongWeb、Weblogic、Websphere、Nginx、Resin、IHS等。 | 否 |
| 50 | 支持网络设备配置核查，包括华三路由器和交换机、思科路由器和交换机、Juniper路由器、华为路由器和交换机、中兴路由器和交换机、迈普路由器等。 | 否 |
| 51 | 支持主流防火墙设备配置核查，包括思科ASA防火墙、思科PIX防火墙、CheckPoint防火墙、山石防火墙、Fortigate防火墙、华三防火墙、Juniper NetScreen防火墙、Juniper SRX防火墙、深信服防火墙、华为防火墙、安氏防火墙和迪普防火墙等。 | 否 |
| #19 | 支持主流WLAN设备配置核查，包括邦讯WLAN、思科WLAN、大唐WLAN、国人WLAN、华三WLAN、华为WLAN、中兴WLAN、邦讯WLAN等。 | 是 |
| #20 | 支持虚拟化设备配置彻查，包括Hyper-V、VMWare ESXi、VMWare vCenter、XEN、XenServer配置核查。 | 否 |
| 52 | 报表功能 | 可按IP范围、起止时间、任务名称、任务状态、配置模板、用户账号筛选任务并汇总，并在线查看风险详情和输出离线汇总报表。 | 否 |
| 53 | 报表能提供针对不同角色的默认模板，允许用户选择离线报告的格式，输出HTML、EXCEL、WORD、PDF等格式文件。 | 否 |
| 54 | 支持对检查结果数据进行实时在线报表分析；支持高级数据分析，能够进行历史数据查询、汇总查看、对比分析等，能够进行多个检查任务或多个IP风险对比。 | 否 |
| 55 | 支持扫描任务完成后自动生成报表和发送到指定邮箱或上传到FTP服务器。 | 否 |
| 56 | 提供综述报表和主机报表，综述报表包含资产的分布，风险在资产中的分布，分别细致陈述了配置合规、状态的合规情况，两次扫描结果的对比。主机报表需含配置合规和状态合规信息。 | 否 |
| 57 | 支持报表自定义，可定制报表标题、封面logo、报表页眉和页脚、报表各章节显示内容。 | 否 |
| ★8 | 产品资质 | 产品具有中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，证书显示的产品名称与产品web界面显示名称一致。 | 是 |
| #21 | 产品具有国家版权局颁发的《计算机软件著作权登记证书》 | 是 |

**5．运维安全管理设备1台**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **指标要求** | **证明材料要求** |
| 58 | 产品架构 | 软硬件一体化产品。 | 否 |
| 59 | 网络接口 | ≥4\*100/1000M RJ45自适应以太网口。 | 否 |
| 60 | 静态路由 | 可添加静态路由信息，支持复杂的网络环境堡垒机部署。 | 否 |
| #22 | 手机APP管理 | 可通过手机APP方式进行审批管理、消息通知和系统状态查看。 | 否 |
| ★9 | 性能指标 | 最大可管理设备数不低于500个，实配不低于200个，字符并发数不少于300个，图形并发数不少于100个。 | 否 |
| 61 | 托管设备访问权限控制 | 支持访问策略方式管控不同管理员的托管设备运维权限，即允许不同部门的用户可以访问本部门托管的设备，以便满足部门间托管设备的交叉运维需求。 | 否 |
| #23 | 设备访问授权 | 除用户身份认证外，对特定目标设备访问还需要高级管理员授权才能访问。授权审批方式支持web和手机APP审批。 | 否 |
| 62 | 设备账号自动发现 | 支持自动扫描发现托管设备中的所有设备系统账号，并以列表方式向设备管理员展示托管设备中的所有运维的系统账号。 | 否 |
| 63 | 设备账号自动改密 | 支持自动定期或手动批量修改托管设备账号密码信息，改密完成后支持站内消息、邮件和APP等方式推送改密结果。 | 否 |
| 64 | 设备账号密码备份 | 支持按部门、设备类型、业务类型、设备组等多种方式备份托管设备的设备账号和密码，密码备份文件支持excel和html方式加密保存。 | 否 |
| 65 | 运维实时监控 | 支持实时监控通过SSH、SFTP、RDP、VNC 、Telnet、FTP、X11等协议的操作行为；对监控到的非法操作，可实时手工切断。 | 否 |
| 66 | 支持的协议 | 字符型远程操作协议：SSH(V1、V2)、TELNET， Rlogin。 | 否 |
| 67 | 图形化远程操作协议：RDP、VNC、X11，其支持文件共享；可支持RDP、VNC的客户端直接访问堡垒机。 | 否 |
| 68 | 文件传输协议：FTP、SFTP、SCP、Samba；可支持FTP客户端Wincp直接访问堡垒机。 | 否 |
| 69 | 支持Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、PostgreSQL等数据库。 | 否 |
| 70 | 支持HTTP、HTTPS操作审计，HTTP/HTTPS协议可以直接代理。 | 否 |
| ★10 | 产品资质 | 拥有信息系统安全专用产品销售许可证（身份鉴别类）。 | 是 |
| #24 | 拥有中国国家信息安全产品认证证书（基本级）。 | 是 |
| #25 | 拥有软件著作权证书。 | 是 |

**6．负载均衡设备1台**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标项** | **指标要求** | **证明材料要求** |
| ★11 | 设备性能 | 吞吐量≥11Gbps，并发连接数≥9,000,000 ，4层新建连接数≥CPS350,000 ，7层建连接数≥RPS350,000。 | 否 |
| 71 | 硬件规格 | 采用独立专业负载设备，非防火墙模块或非插卡式扩展的负载均衡设备。本项目要求配置2套。 | 否 |
| 72 | 标准机架式专用设备，高度2U,接口≥6个千兆电口、8个千兆光口，冗余电源。 | 否 |
| #26 | 功能授权 | 单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权。 | 否 |
| 73 | 负载均衡算法 | 支持轮询、加权轮询、加权最小连接、动态反馈、最快响应、最小流量、加权最小流量、带宽比例、哈希、主备、首个可用、优先级等算法。 | 否 |
| #27 | 可编程流量控制 | 通过某种编程语言（如lua）实现自定义的流量编排，对TCP、SSL、HTTP和HTTPS等类型的流量进行分发、修改和统计等操作。 | 否 |
| 74 | 接入方式 | 支持静态IP和PPPOE两种线路接入方式。 | 否 |
| #28 | 支持三明治架构，对防火墙、IPS、行为管理等网络设备进行流量负载均衡和故障切换，使以上网络设备获得Active-Active运行的能力。 | 否 |
| 75 | 流量调度 | 支持基于五元组条件（源IP地址，源端口，目的IP地址，目的端口，传输层协议号）来进行出站访问的流量调度分发。 | 否 |
| 76 | 支持基于管理员自定义的时间计划来进行出站访问的流量调度分发。 | 否 |
| #29 | 内置完备的IP地址库，无需手动导入并支持自动全网更新，可查看并编辑各国家、国内各省份的IP地址段和国内各大运营商IP地址段，并可灵活匹配IP地址库进行流量调度分发，实现链路负载功能。 | 否 |
| #30 | 支持基于URL的链路调度功能，内置目前主流的国外URL网址库，无需手动导入并支持自动更新，管理员可查看并进行编辑。可根据URL将访问国外网站的请求调度到指定线路。 | 否 |
| #31 | 支持基于应用协议的智能选路，能对网银、游戏、视频等流量进行调度。 | 否 |
| 77 | 支持基于域名的流量调度，针对特定网站选择指定的链路转发。 | 否 |
| 78 | DNS功能支持 | 支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。 | 否 |
| 79 | 支持DNS内网记录，包含AAAA、CNAME、MX和TXT等类型，可识别内网用户并对其DNS请求直接返回相应结果。 | 否 |
| 80 | 健康检查 | 支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。 | 否 |
| 81 | SLB能够通过健康检查来获取后端服务器状态，同时将服务可用性、设备CPU、新建并发吞吐等数据上报GSLB，设备之间的联动使得GSLB能根据链路和服务器两者的综合状态实现智能切换，为用户选择最优的数据中心和服务器分配方式。 | 否 |
| #32 | 投屏显示 | 支持链路负载投屏展示，能够分别基于链路监测、应用选路和ISP流量进行投屏展示分析。链路监测展示链路的健康状态、上下行带宽、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；ISP展示基于运营商分类选择链路的示意图。 | 否 |
| #33 | 协议优化 | 支持非对称式部署的TCP协议优化技术，提升远端用户访问应用服务的速度。无需在用户终端或应用服务器上安装任何插件和软件，不受操作系统类型、浏览器版本等兼容性因素限制，并且用户首次访问应用服务即可产生加速效果。 | 否 |
| #34 | 图片优化 | 支持图片优化技术，通过对图片格式的转换，减少传输流量，提升web页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的格式，优化加速效果。 | 否 |
| #35 | 服务器负载均衡 | 支持命令行配置，支持Tab键补全操作，支持界面全部模块通过命令行的模式配置，支持命令批量操作，支持配置导入导出命令行操作。 | 否 |
| #36 | IPv6改造 | IPv6支持双栈模式，支持NAT46、NAT64、NAT66、FTP ALG、DNS64等协议转换。 | 否 |
| 82 | 支持在不增加新域名NS记录和A记录的条件下解决IPv6改造过程中出现的天窗问题，保证客户端不做任何改动，实现平滑解决。 | 否 |
| 83 | IPv6改造方案支持多种模式和部署方案，网络部署清晰可见，不允许通过引流或劫持等不可见的黑盒方式进行改造。 | 否 |
| 84 | IPv6改造方案能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配置的方式解决天窗问题。 | 否 |
| ★12 | 产品资质 | 所投产品具备《计算机软件著作权登记证书》。 | 是 |
| 85 | 所投产品具备《IPv6 Ready Phase-2金色认证证书》。 | 是 |

**7．上网行为管理设备1台**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 指标项 | 指标要求 | 证明材料要求 |
| 86 | 多种部署模式 | 支持网关、网桥、旁路模式部署；网关模式，支持NAT、路由转发、DHCP、GRE、OSPF等功能。 | 否 |
| ★13 | 双机模式 | 用户在用上网行为管理系统为深信服AC-6000，要求能够与在用设备实现双机热备方式部署。 | 否 |
| #37 | 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。 | 否 |
| 87 | 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。 | 否 |
| 88 | 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。 | 否 |
| 89 | 链路负载 | 1.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；  2.支持使用VPN做专线备份。 | 否 |
| 90 | 支持链路故障检测。 | 否 |
| 91 | Web访问质量监测 | 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  支持以列表形式展示访问质量差的用户名单  支持对单用户进行定向web访问质量检测。 | 否 |
| 92 | 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。 | 否 |
| 93 | 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。 | 否 |
| 94 | 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。 | 否 |
| 95 | 用户密码强度 | 可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。 | 否 |
| 96 | 可设置密码必须包括数字或字母或特殊字符。 | 否 |
| 97 | 多终端自定绑定 | 同一个账号，支持与指定数量的多个终端进行自动绑定。 | 否 |
| 98 | 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，和添加信任列表； 2.支持显示以IP或用户名的维度统计一段时间内的趋势图。 | 否 |
| #38 | 支持例外排除功能：如指定例外条件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。 | 否 |
| 99 | 应用标签功能分类管理 | 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；  支持给每个应用自定义标签；  支持根据标签选择一类应用做控制；  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。 | 否 |
| 100 | SSL加密内容审计和过滤 | 针对SSL加密的网站、论坛发帖、web邮箱的内容进行关键字过滤和内容审计；  支持SSL硬件加速卡解密，从而可提高SSL全流量解密性能。 | 否 |
| #39 | 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。 | 否 |
| #40 | 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。 | 否 |
| 101 | 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。 | 否 |
| #41 | 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。 | 否 |
| 102 | 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。 | 否 |
| 103 | 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）。 | 否 |
| 104 | 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。 | 否 |
| 105 | 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。 | 否 |
| 106 | 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；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。 | 否 |
| 107 | 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。 | 否 |
| 108 | 网络安全 | 支持防火墙功能；  支持防DOS攻击，识别并封堵来自于内网或外网的DOS攻击；  支持防ARP欺骗，防范三层网络环境中的ARP欺骗问题。 | 否 |
| #42 | 高性能日志模式 | 支持日志高性能模式处理，精简冗余日志。 | 否 |
| 109 | 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。 | 否 |
| #43 | 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）。 | 否 |
| 110 | 下钻分析 | 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的相关页面支持对统计结果的向下钻取查询。 | 否 |
| 111 | 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。 | 否 |
| 112 | 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。 | 否 |
| 113 | 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。 | 否 |
| 114 | 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。 | 否 |
| 115 | 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。 | 否 |
| 116 | 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。 | 否 |
| 117 | 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。 | 否 |
| ★14 | 投标产品资质 | 公安部颁发的《网络通讯安全审计产品（国标） 销售许可证》。 | 是 |
| ★15 | 公安部颁发的《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》。 | 是 |
| #44 | 国家网络与信息系统安全产品质量监督检测中心《信息技术产品安全分级评估证书-评估保证级3（EAL3级）》。 | 是 |

## 二、售后服务要求

1. 软硬件产品安装：

投标人提供软硬件的配置安装及集成工作，厂商提供设备安装的技术支持。

1. 软硬件产品技术支持：
   1. 投标人提供硬件产品技术服务期限为3年，从投入使用开始3年内，投标方针对硬件运行过程中出现的技术问题，需要提供7×24小时电话/Email/现场的技术支持，包括问题诊断、提供可行的问题解决方案、技术应答、对硬件的调节/优化提供建议；
   2. 投标人提供软件产品技术服务期限为3年，从投入使用开始3年内，投标方针对软件运行过程中出现的技术问题，需要提供7×24小时电话/Email/现场的技术支持，包括问题诊断、提供可行的问题解决方案、技术应答、对软件的调节/优化提供建议。3年服务支持期内发现的软件功能缺陷或安全漏洞，投标方应免费修补。
2. 驻场服务要求：
   1. 投标人提供1名全职项目驻场人员，驻厂时间：设备全部到货之日起半年内，驻场方式：用户现场5×8。
   2. 服务内容：配合原厂商完成本项目采购设备的安装工作；本项目招标的设备的日常管理和维护。

## 三、软硬件安全服务

1、投标人按照采购人要求完成咨询工作，按照采购人要求协助完成一个三级应用系统的等级保护定级、备案、整改、测评等工作；

2、等级保护测评服务内容包括：针对等保对应级别要求的自评估、自评估所发现问题的加固与整改、等保测评的实施及现场配合；

3、投标人承诺协助采购人指定的系统通过等级保护测评机构的测评。

## 四、集成要求：

1、投标人要统筹考虑、协调本项目建设内容及进度，协调各设计方案的关联接口，充分配合项目招标方的工作；

2、投标人应确保其所提供的软硬件都能满足招标文件中规定的技术要求；

3、提供所有中标产品的集成服务，包括但不限于：硬件设备的上架、安装、部署、调试等，并提供所有相关配件；软件产品的安装、部署、开发、对接、调试等。

## 五、培训要求

培训计划内容周详、合理、培训范围广、有二次培训计划和持续培训计划安排，可实施，有针对性，包括但不限于系统管理员培训，安全培训及相关产品培训；

1、设备使用培训，说明培训计划、每种设备培训内容、使用培训达到预期结果；

2、设备维护培训，说明培训计划、每种设备维护项目内容、维护培训达到预期结果；

3、设备培训地点是培训师必须到采购方现场，如个别设备培训必须到供货方去，则费用全部由供货方负责；

4、培训师须为原厂且工龄超三年以上的工程师（提供工程师社保缴纳证明）。