第一标段：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **产品参数** | **数量** | **单位** |
| 1 | 应用交付网关 | 性能参数：4层吞吐量≥5Gbps，四层并发连接数≥8000000，4层新建连接数 CPS≥100000，7层新建请求数 RPS≥100000。 硬件参数：电源：冗余电源，接口数量≥6千兆电口+2千兆光口SFP。 功能参数： 1.支持旁路部署、路由模式、三角传输模式。 2.支持在一台设备的情况下链路负载、服务器负载、全局负载等功能，且无需额外的授权费用。 3.支持出口的链路负载，包括入站流量、出差流量等，保障出口链路流量的健壮性。 4.★支持完备的IP地址库，全网IP地址库自动化更新，可查并编辑全国省份及运营商的IP地址。其中内置且自动更新超过100,000条国外的URL地址，实现基于国内外地址的灵活流量调度，提供截图证明材料并加盖厂商公章。 5.支持流量出入站访问自定义功能，通过自定义时间来实现流量的调度。 6.★支持链路负载大屏展示，通过对于设备上连接的链路情况、应用选择情况进行大屏投屏展示。在屏幕上能够直观检测除链路的健壮性、带宽使用情况、并发连接数、吞吐量等，提供截图证明材料并加盖厂商公章。 7.支持多种服务器负载均衡算法，能够实现轮询、加权轮询、主机加权轮询、最快响应时间、主机加权最小流量、源IP/源IP端口哈希、HOST哈希、加权最小连接等多类型的负载均衡算法。 8.支持基于cookie作用域和路径实现对于cookie加密，提升其安全性。 9.支持HTTP模式下的网关部署，可以实现对外服务协议从HTTP1.0/1.1升级至HTTP/2，无需改变web服务器情况，提升终端用户的体验及业务安全。 10.支持服务器负载大屏展示，能够显示设备多类型状态包括CPU使用率、CPU温度、内存使用率、并发连接数、吞吐情况、新建连接数、SSL新建等，除此之外对于服务健康状态、新建连接数、并发连接，节点池的调度算法、健康状态进行投屏展示。 11.★要求具备公安颁发的销售许可证，需提供证书复印件并加盖原厂商公章。 12.★厂商具有中国网络安全审查技术与认证中心颁发的风险评估一级和安全开发一级资质证书、提供证明材料并加盖厂商公章 | 2 | 台 |
| 2 | 国产化防火墙 | 性能参数：网络层吞吐量≥20G，IPS吞吐量≥2G，全威胁吞吐量≥1.5G。 硬件参数：电源：冗余电源，接口：4千兆电口。 功能参数： 1.产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式。 2.支持IPSec VPN与SSL VPN功能，其中IPSec VPN支持AI选路，自动切换最优隧道。 3.★支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于 9000 种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，提供产品功能截图证明并加盖原厂公章。 4.支持FTP协议命令控制：delete、rmdir、rename、mget、dir、mput、get、put，避免业务交互被无控制改动。 5.能够对HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀，以及对15 级压缩文件进行解压查杀。 6.★支持勒索病毒检测及防御，产品有勒索病毒攻击防护模块，提供产品功能截图证明，并提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局之中任意一家检测机构出具关于“勒索病毒”的相关证书佐证，证明材料加盖原厂公章。 7.支持服务器抗恶意扫描功能，产品针对扫描源IP进行日志记录，并对恶意源IP联动封锁。 8.支持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，当前僵尸网络信誉库超过120万种，提供产品功能截图证明并加盖原厂公章。 9.支持安全策略独立管理和审计，可对安全策略变更时间、变更账号、变更类型等内容进行审计，提供产品功能截图证明并加盖原厂公章。 10.★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并加盖原厂公章。 11.★厂商为国家信息安全漏洞共享平台CNVD技术组和用户组成员，提供证明材料并加盖厂商公章。 | 2 | 台 |
| 3 | 国产化上网行为管理 | 性能参数：网络层吞吐量≥5Gb，带宽性能≥500Mb，支持用户数：3500，包转发率：90Kpps。 硬件参数：电源：冗余电源，接口：6千兆电口。 功能参数： 1.支持网关模式、路由模式、网桥模式、网桥模式（多路桥接模式）和旁路模式等多种模式的网络部署方式，支持电口bypass。 2.支持导入和通过扫描导入用户/用户组信息，支持以CSV格式文件导入帐户/分组/IP/MAC/描述/密码等信息；用户分组支持树形结构，支持父组、子组、组内套组等。 3.★基于IP网段地址、Vlan划分、MAC地址、SSID标识等实现上网人员差异化自动分组、认证规则，提供相关证明材料包括但不限于包括厂商截图证明材料等。 4.可针对于不同的认证场景提供不同的认证界面，不同上网人员所对应的认证页面支持自定义，可根据需要针对文字、颜色风格、图片等进行编辑，且图片支持轮播。 5.支持radius、AD、POP3、Proxy、PPPOE、 H3C IMC/CAMS、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； 6.支持记录用户信息，第二次上线无需输入用户名密码即可获取上网权限，可配置永久有效或长期有效时间。 7.支持综合网络质量审计，可以对上网人员的访问质量进行分析并进行网络访问质量评级，针对于存在访问质量的上网人员可以以列表形式统一展示并定向分析。 8.★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，提供相关证明材料包括但不限于包括厂商截图证明材料等。 9.支持常见远程控制软件的审计,包括但不限于Teamviewer、向日葵、Anydesk、RDP的的外发文件审计。 10.★要求具备公安颁发的销售许可证，需提供证书复印件并加盖原厂商公章。 11.★产品厂商为互联网应急中心国家级安全应急服务支撑单位，提供证明材料并加盖厂商公章。 | 1 | 台 |
| 4 | 智能语义WEB应用防火墙 | 1.支持15000QPS,可通过增加检测节点数量，实现性能的无缝横行扩容，提供数据可视化大屏,能够以可视化地图方式展示实时请求信息、拦截信息、攻击源IP地理分布、攻击类型分布等； 2.拥有自主知识产权的WAF系统软件，采用容器技术，支持在公有云、私有云和实体服务器部署； 3.★支持嵌入式集群模式与Nginx、tengine集群实现高度耦合，无需改变网络架构，实现旁路检测和阻断,支持k8s环境部署; 4.★具备http协议深层解码能力，支持递归解码，解码方式包括：URL解码、JSON解码、Base64解码、16进制转换、斜杠反转义、XML解析、PHP反序列化解析、UTF-7解码；（提供功能截图，并加盖厂商公章） 5.★具有独立防护能力的具有自主知识产权的智能分析检测引擎（提供软件著作权证明，提供专利证明，并加盖厂商公章） 6.支持SQL注入攻击检测，通过解析http协议中payload内容，识别符合sql语句的特征，评估威胁等级并阻断；（提供功能截图，并加盖厂商公章） 7.支持SQL非注入型攻击检测，如完整SQL语句执行；（提供功能截图，并加盖厂商公章） 8.★支持深度检测功能，可在站点详情中的防护配置页面开启深度检测，即使该请求已在检测过程中已被判断为拦截，仍可继续进行所有攻击检测模块的检测，完整地记录攻击检测信息记录，便于进行更完整的分析（提供功能截图，并加盖厂商公章） 9.支持CC攻击防护，通过限制IP和Session实现对异常访问行为的限制，并内置Session系统；（提供功能截图，并加盖厂商公章） 10.支持自定义规则检测前解码，可根据业务系统编码类型进行配置，快速实现新爆发漏洞的防护。（提供功能截图，并加盖厂商公章） 11.★支持安全策略可视化编排，以树状结构展示安全检测流程。支持在流程树状结构中查看流程详情，并支持在不同的检测点直接插入配置修改规则。（提供功能截图，并加盖厂商公章） 12.★具备0day漏洞防护能力，实现告警和拦截； 13.★支持站点全量访问日志的完整记录功能，属性包括：站点信息、访问地址、源IP、请求方法、响应码、请求开始时间；查看详情功能提供分类查看日志详情，可分为访问日志详情、请求检测信息、响应检测信息、HTTP响应展现。（提供功能截图，并加盖厂商公章） 14.支持设备信息实时监控，监控数据包括CPU使用率、内存使用率、磁盘使用率、网络读写、每秒新建连接数、每秒检测请求数；（提供功能截图，并加盖厂商公章） 15.★支持后端Web服务器集群的负载均衡，支持加权轮训法、最小连接数法和源地址哈希法三种调度策略；（提供功能截图，并加盖厂商公章） 16.支持服务器健康状态检测，至少包括TCP、http、https三种；（提供功能截图，并加盖厂商公章） 17.产品具有中国公安部颁发的《计算机信息系统安全销售许可证》Web应用防火墙（国标-增强级）；提供证明材料并加盖厂商公章。 18.产品具有中国信息安全测评中心《国家信息安全漏洞库（CNNVD）兼容性资质证书》；提供证明材料并加盖厂商公章。 | 1 | 套 |

第二标段：

一、项目概况

本次数据安全防护项目建设以法律要求为依据，以防护为目的，从而最大程度保护数据的安全。需要采购部署防火墙、网闸、数据库审计系统以及终端安全管理系统。

二、招标内容

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **数量** | **单位** | **备注** |
| 1 | 国产化防火墙 | 2 | 台 |  |
| 2 | 国产化网闸 | 1 | 台 |  |
| 3 | 数据库审计 | 1 | 套 |  |
| 4 | 终端安全管理系统 | 1 | 套 | 终端安全管理系统产品控制中心2套（内外网各1套);服务器端点安全软件100套（内网20套、外网80套) |

三、设备清单及技术要求

|  |  |  |
| --- | --- | --- |
| **序号** | **设备名称** | **招标指标要求** |
| 1 | 国产化  防火墙 | **性能参数**：  网络层吞吐量≥20G，IPS吞吐量≥2G，全威胁吞吐量≥1.5G；硬件参数：电源：冗余电源，接口：4千兆电口。  **功能要求：**  1.产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式；  2.★支持IPSec VPN与SSL VPN功能，其中IPSec VPN支持AI选路，自动切换最优隧道，提供产品功能截图并加盖制造厂商公章；  3.★支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于 9000 种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，提供产品功能截图并加盖制造厂商公章；  4.支持FTP协议命令控制：delete、rmdir、rename、mget、dir、mput、get、put，避免业务交互被无控制改动；  5.能够对HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀，以及对15 级压缩文件进行解压查杀，提供产品功能截图并加盖制造厂商公章；  6.★支持勒索病毒检测及防御，产品有勒索病毒攻击防护模块，提供产品功能截图并加盖制造厂商公章；  7.★支持独立的入侵防护规则特征库，规则库支持根据漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等进行分类，特征总数在10000条以上，能对常见漏洞进行安全防护，提供产品功能截图并加盖制造厂商公章；  8.支持独立的入侵防护规则特征库，规则库支持根据漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等进行分类，特征总数在10000条以上，能对常见漏洞进行安全防护，提供产品功能截图并加盖制造厂商公章。  9.支持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，当前僵尸网络信誉库超过120万种，提供产品功能截图并加盖制造厂商公章；  10.支持安全策略独立管理和审计，可对安全策略变更时间、变更账号、变更类型等内容进行审计，提供产品功能截图并加盖制造厂商公章；  11、提供3年原厂质保服务，提供原厂售后服务承诺函；  12.提供所投产品公安IT产品信息安全认证证书EAL4增强级证书；  13.提供所投产品需具备国家信息安全漏洞库兼容性资质证书； |
| 2 | 国产化  网闸 | **性能参数**：  ★1、国产化硬件平台，标准2U机箱，冗余电源；整机配备液晶屏；提供“健康指示灯”。提供HA工作状态监控灯。（提供产品实物面板照片彩页，并加盖制造厂商公章）  2、内网接口：1个HA口，1个管理口，不少于2个千兆电口，不少于10个千兆光口；外网接口：1个HA口，1个管理口，不少于2个千兆电口，不少于10个千兆光口；包含以下功能模块：文件同步，数据库交换、FTP访问、数据库访问、安全浏览、邮件访问、视频传输、定制访问、安全传输、双机热备及负载均衡。  3、文件传输速率不低于800Mbps；文件传输延时不超过0.17ms；  **功能要求**  ★1、内外网主机系统分别支持双系统引导，并可在WEB界面上直接配置启动顺序，在A系统发生故障时，可以切换到B系统（截图证明）；  ★2、支持文件格式特征过滤；并能提供具备图形化界面的文件类型判断工具以帮助用户识别不常见文件类型，提供产品功能截图并加盖制造厂商公章；  3、支持病毒检测；支持Oracle、SQL Server、Sybase、Db2、MySQL、MongoDB等主流数据库；支持达梦、人大金仓、Gbase、神通数据库、博阳等主流国产数据库，提供产品功能截图并加盖制造厂商公章；  4、支持数据库访问用户的过滤和控制；  5、实现安全的FTP访问，支持对访问用户、访问协议命令、上传下载文件类型等访问过滤控制；  6、支持访问时段策略；时间可以设置为一次性或者周循环方式；  7、实现特定TCP、UDP协议的数据隔离交换，可合作定制开发针对特定协议的安全检测；  8、支持多个视频厂商(海康、大华、科达、中兴、迪威、东方网力等协议；  9、内/外网主机系统分别具有独立管理接口，而不是采用低安全的管理方式，如通过业务口管理或通过内网唯一管理接口完成全部管理等；  ★10、支持实时入侵检测功能，并可设置自动阻断响应，提供产品功能截图并加盖制造厂商公章；  11、产品具备国家信息安全测评中心颁发的信息技术产品安全测评证书（EAL3+）；  12、提供3年原厂质保服务，提供原厂售后服务承诺函；  13、所投产品厂家具备信息系统建设和服务能力等级-优秀级（CS4）； |
| 3 | 数据库安全  审计系统 | 性能参数：  标准机架式2U，含交流冗余电源，J45串口≥1个，RJ45管理口≥2个，USB接口≥2个，电口≥4个，千兆光口≥4个，扩展板卡≥2个，支持扩展万兆光口。硬盘容量≥8T，内存≥32G， SQL峰值吞吐量≥20000条/秒，在线会话上限≥6000个，日志存储在线日志量≥25亿条语句，归档日志量≥260亿条语句，配置≥30个审计授权。  功能参数：  1、支持Oracle、SQL Server、Db2、Informix、PostgreSQL、Sybase ASE、Sybase IQ、MySQL、MongoDB、SAP HANA、MariaDB、Percona、Teradata、Cache、人大金仓、神通、南大通用等数据库审计；支持Hive、HBase、Sentry、Impala、HDFS、ES（Elasticsearch）、GP（Greenplum）、Redis等大数据平台的审计；★支持国产华为Guass DB 100、Guass DB 200、达梦、oceanbase数据库的审计；提供产品功能截图并加盖制造厂商公章；  2、★支持SSH或者KVM登录Oracle、MySQL、SQL Server数据库服务器后，直接执行的SQL操作的审计，不依赖于数据库自身审计功能；  3、支持按照策略进行结果集审计，可以指定敏感表审计结果集，支持通过返回行数和内容大小控制返回结果集大小，降低系统开销，支持基于结果集的关键字检索；提供产品功能截图并加盖制造厂商公章；  4、规则可关联数据库，也可关联数据库类型；关联数据库类型后，可选择自动关联后续添加的数据库；提供产品功能截图并加盖制造厂商公章；  5、★为保证产品易用性，支持自定义业务化语言，可将SQL语句翻译为业务化的语句进行展现，提供产品功能截图并加盖制造厂商公章；  6、★为保证事件处理的即时性，需支持告警方式包括：邮件、短信、SYSLOG、SNMP、企业微信、钉钉、审计系统前台界面；支持短信平台对接，发起告警操作，提供产品功能截图并加盖制造厂商公章；  7、所投产品生产厂商需具备挖掘国际品牌和国内品牌数据库漏洞能力，所挖漏洞被CNNVD、CNVD或CVE承认且具有编号， CVE组织收录且具有编号不少于10个，CNNVD或CNVD承认且具有编号不少于30个，提供证明截图并加盖制造厂商公章；  8、提供3年产品质保服务，提供原厂售后服务承诺函；  9、所投产品的制造厂商在Gartner技术成熟度曲线报告的DAP（数据库审与保护）领域中属于被推荐厂商；  10、为保障安全审计的服务响应效果及时性，要求所投产品制造厂商本地支撑人员同时具备CISP和OCP认证，并且提供不少于6个月社保； |
| 4 | 终端安全  管理系统 | **性能参数**：  终端安全杀毒具有安全策略模板一体化设置，全网资产盘点与风险可视，自动化日志可视化报表一键导出，管理账号分权分域，总分平台级联控制；本次配置包含：终端安全管理系统产品控制中心2套（内外网各1套);服务器端点安全软件100套（内网20套、外网80套);软件升级(\*3年)。  **功能参数**：  1.软件要求在中华人民共和国境内开发，具备自主知识产权，提供软件著作权证书；  2.★支持勒索病毒专项防护展示，直观展示勒索病毒的防护效果，展示内容需要包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数等，提供产品功能截图并加盖制造厂商公章；  3.★支持用户直接对勒索病毒的家族名、病毒名、加密文件后缀名执行链接查询，可通过直接上传加密文件的方式确定勒索病毒类型，如果能解密可以提供必要的解密工具，提供产品功能截图并加盖制造厂商公章；  4.支持客户端的错峰升级，可设置同一时间升级的最大数量，避免大量终端程序同时更新造成网络拥堵，提供产品功能截图并加盖制造厂商公章；  5.★支持对RDP暴破做全方位保护，可开启RDP远程登录二次认证，提供产品功能截图并加盖制造厂商公章；  6.支持对Windows已停更的系统提供专项防护（如Windows 7等），防护类型包括0day漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等，提供产品功能截图并加盖制造厂商公章；  7.★支持与安全态势感知平台进行安全联动，支持管理员在安全感知管理平台管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，提供产品功能截图并加盖制造厂商公章；  8.支持防火墙共享情报，提供C&C通信检测，对僵尸网络实现联合举证溯源，提供产品功能截图并加盖制造厂商公章；  9.提供国际权威机构AV-Test 2022年针对勒索专项，满分测试报告或截图；  10. 提供3年原厂软件升级服务，提供原厂售后服务承诺函； |