**网站信息安全建设项目**

**附件一：设备配置要求**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **参数要求** | **数量** | **单价** | **总价** |
| **1** | **智慧防火墙系统** | **网络层吞吐量≥22G，并发连接≥400万，每秒新建连接数≥24万，标准2U机架式机箱，单电源；千兆电口≥6个，≥2个接口板卡扩展插槽，≥1个Console，支持液晶，≥128GB SSD固态硬盘存储，三年IPS功能模块，三年硬件维保服务。**  **支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。（提供功能截图证明材料并加盖制造商公章）**  **支持多个物理口基于热备、802.3ad、轮询变为一个逻辑接口，支持基于TCP/UDP、源目的MAC地址、IP地址和MAC地址组合实现负载备份。**  **支持策略路由、动态多播路由、ISP路由。**  **支持源地址和目的地址均为IPv4地址时，能够把目的地址转换成服务器地址，可探测服务器存活状态。**  **支持DNS代理功能，可将指定范围内的DNS请求自动重定向至管理员指定的DNS服务器。**  **支持IPv6下策略路由、动态路由。**  **支持高可靠性配置，支持主备、主主模式；同时支持接口联动、接口权重配置、链路状态探测。**  **支持基于源目的安全域、源用户、源目的地址、源目的地区、服务、应用、隧道、时间、VLAN等、方式访问控制策略，可对国家和地区对象，支持对冗余的策略进行检查。**  **支持威胁引流功能，威胁引流可以通过开关设置是否开启，通过添加蜜罐地址实现引流，同时支持添加例外域名，做到精细化引流管控。（提供功能截图证明材料并加盖制造商公章）**  **支持基于IPv6安全域、IP地址、应用的会话限制，限制内容包括每IP新建和并发、所有IP新建和并发，同时支持设置方向。**  **支持基于端口和MAC的802.1x认证。**  **针对邮件支持基于发件人、收件人等关键字的过滤，包括接收、发送、双向类型。**  **支持对HTTP/SMTP/POP3/IMAP/SMB /FTP六种协议进行反病毒查杀，可上传、下载、双向，能够进行阻断或日志记录。**  **文件过滤支持对压缩文件进行解压查杀，最大支持6层戒解压层数。**  **反病毒支持MD5的自定义签名、病毒例外。**  **支持SSLVPN功能，支持证书配置，认证方式包括单因子认证和双因子认证，支持对于可访问网络IP地址进行设置。**  **支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持scanner或onvif类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置IP地址、MAC地址、资产类型、生效市场、厂商、位置等信息来制定黑/白名单，方便日常资产管理，支持通过设置IP地址、MAC地址、资产类型、操作系统、应用、开放的端口和访问的端口等信息来制定资产指纹库。（提供功能截图证明材料并加盖制造商公章）**  **支持按照主机和威胁情报统计失陷主机数、风险主机数、威胁情况、告警信息；并在界面能够查看木马后门、窃密木马、远控木马等威胁的排行；失陷主机统计结果包含主机IP地址、威胁类别、命中数、动作、发生时间、情报来源、资产等。**  **支持在一条安全策略中设置行为管控、文件过滤、漏洞防护、邮件过滤、内容过滤、联动终端管控等安全功能选项。支持双系统备份，可记录多个历史配置文件。**  **支持加密的WebUI页面管理以及设备管理界面内的命令行管理。**  **在WEB管理界面内置抓包工具，可设置抓包数量、接口、IP地址，并支持设置表达式。** | **1** | **￥134,000.00** | **￥134,000.00** |
| **2** | **运维安全管理与审计系统** | **产品规格：≥6个千兆电口；≥2个接口扩展槽位；≥4TB硬盘；液晶屏；≥300路图形会话或≥800路字符会话并发；≥50授权许可。**  **支持不间断业务部署，支持物理旁路，逻辑串联模式**  **冗余性：投标产品支持HA双机热备、支持跨数据中心部署等。**  **设备管理方式支持SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、Rlogin等协议**  **支持Linux/Unix、Windows、H3C、Huawei、Cisco等主流设备及系统。**  **支持资源按标签管理，并可以对资源批量添加和删除标签。（提供功能截图证明材料并加盖制造商公章）**  **设备管理支持图形、字符，混合协议下的批量登录**  **支持IPv4、IPv6双栈网络运维审计支持**  **支持对MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client、Radmin、dbisql等应用程序/客户端的扩展支持，且支持图形界面分辨率调整。**  **设备添加支持按IP范围、端口进行资源设备自动发现，快速批量添加资源设备**  **支持Xshell、SecureCRT、putty等第三方客户端运维字符类型资源（交换机、路由器）**  **支持同时对多台被管设备进行管理，批量执行命令。**  **支持多方协同运维工作，可实现运维协助，操作权限回收。支持以网盘形式在堡垒机上存储文件，并自定义云盘大小，实现操作端、堡垒机、目标服务器三者之间文件共享**  **支持SSH、TELNET、RDP等协议文件管理与剪切板控制功能。**  **支持以网盘形式在堡垒机上存储文件，实现操作端、堡垒机、目标服务器三者之间文件共享。**  **支持动态令牌、USBKEY、手机令牌、手机短信等多因子认证**  **支持用户水印功能，避免数据泄露无法追责。**  **支持分组管理，实现不同分组的管理各自资源及日志查看**  **支持按用户、账户组设置多对多的资源访问授权，用户组和账户组内的新增成员自动继承授权关系**  **设备具备预制Linux主机和网络设备的基本命令，支持正则表达式和通配符方式设置匹配规则，自定义命令黑白名单**  **设备支持对MySQL和Oracle数据库的访问操作控制，可基于库、表、命令实现对数据库操作的细粒度访问控制**  **支持从Linux服务器同步账户，实现堡垒机与纳管的资源服务器之间的账户同步。**  **支持精细化的访问控制策略，支持双人授权，针对核心重要设备需要管理员审批才能操作。**  **支持通过工作流申请资源，流程可按多人多级审批模式或会签审批，权限包括文件上传下载、RDP剪切板。**  **支持对高危命令操作的审计与控制，可实现动态审批授权功能。**  **全面的审计功能，支持对运维操作中的详细操作命令、授权、协同、以及剪切板拷贝行为进行记录，并可以通过关键字搜索定位回放，审计日志内容支持导出。** | **1** | **￥85,800.00** | **￥85,800.00** |
| **3** | **日志收集与分析系统** | **事件综合处理性能≥3000EPS。硬件规格：≥6个千兆电口，≥2个扩展插槽，1个Console接口，≥2T硬盘。≥25授权节点。**  **能够对企业和组织的IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、虚拟化、云计算、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。**  **支持审计各种网络设备（路由器、交换机等）配置日志、运行日志、告警日志等；**  **支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防DDOS攻击，Web应用防火墙、等）配置日志、运行日志、告警日志等；**  **支持审计各种主机操作系统（包括Windows\Solaris\Linux\AIX\HP-UX\UNIX\AS400）配置日志、运行日志、告警日志等；**  **支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等；**  **支持通过Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能；**  **支持对资产IP地址（含内网IP）的地理信息进行管理，设置单IP及IP段行政区及经纬度，支持地图显示。（提供功能截图证明材料并加盖制造商公章）**  **支持自定义资产类型及资产属性；支持对资产自定义标签，支持对标签内容进行查询和管理**  **支持对日志进行归一化处理并保留原始日志，方便用户对关键日志快速定位和事后取证；**  **系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化,不需修改系统程序。**  **支持正则表达式、JSON日志解析、日志自动化范化。**  **支持对选中的日志内容自动生成正则表达式来提取日志属性。**  **系统可自动识别收集的日志并自动选择范化策略，也可由人工设置设备的范化策略。**  **针对匹配的多条范化策略，系统支持用户手工设置策略匹配优先级，保证最佳范化策略匹配。**  **对于枚举类型的范化字段，其字典表可根据需要自定义扩展；**  **支持对关联规则进行监控，了解该规则命中历史情况。**  **能够在世界地图上实时定位事件源/目的IP地址（内网IP）的地理位置；**  **对于原始日志的枚举字段，能够将原始的枚举值映射为系统统一的枚举值。**  **能够在世界地图上实时定位事件源/目的IP地址（内网IP）的地理位置；** | **1** | **￥82,000.00** | **￥82,000.00** |
| **4** | **入侵防御系统** | **网络层吞吐量≥8Gbps，IPS吞吐量≥4Gbps，最大并发连接数≥150万，每秒新建连接数≥8万/秒。标准2U机箱，有液晶面板，1TB硬盘，单电源，标准配置千兆≥6个10/100/1000M自适应电口，≥2个扩展插槽，≥2组bypass，≥1个Console口，≥2个USB接口。IPS特征库升级服务≥三年，硬件质保服务≥三年。**  **支持多种类型接口模式，可配置以太网接口、逻辑桥接口、逻辑链路聚合接口、Vlan子接口、二层Vlan接口等。**  **支持接口配置IPv6地址功能，包括接口名称、IP地址/掩码、地址类型和IPv6路由通告。**  **支持配置向导功能，通过引导用户配置，包括拓扑图、桥接口配置、地址区域流、IPS、可视、概览等多项元素实现快速配置上线。**  **支持配置向导功能，通过引导用户配置，包括拓扑图、桥接口配置、地址区域流、IPS、可视、概览等多项元素实现快速配置上线。（提供功能截图证明材料并加盖制造商公章）**  **支持IP/MAC绑定功能，支持手动添加和自动探测IP/MAC对应关系。**  **支持路由配置功能，支持静态路由、策略路由、多播路由、OSPF、BGP等路由模式。**  **支持一体化安全策略模板功能，通过单条策略既可完成多项策略设置，可以配置源目的地址、国家地区、源目的域、源目的MAC、时间对象、用户、虚拟身份、服务对象、URL分类等对象，同时可在同一策略下，调用入侵防护、一体化防病毒、文件控制、URL过滤、数据过滤防护、威胁情报、口令检测、挂马防护、僵尸网络等应用安全策略进行安全防护。**  **支持DNS解析功能，提供本地DNS解析、DNS自学习安全缓存、DNS静态缓存以及DDNS动态域名功能。**  **支持ISP地址库，提供基于运营商及省份划分的ISP地址库负载均衡分流功能。**  **支持双病毒引擎功能，提供本地病毒引擎与云端第三方病毒引擎功能。**  **支持双机运行保障及支持，提供双机热备、负载均衡、主动共享等模式。**  **支持自定义应用协议，提供除五元组之外的应用技术、应用属性、风险级别、类型、子类、协议、匹配内容、应用层长度等多项设置。**  **支持移动终端对设备的一键黑白名单功能，当突发应急事件时，提供一键黑名单应急处置功能。**  **支持访问控制功能，通过设置源及目的IP、时间调度、用户、网络服务、流入接口、应用对象、源域、目的域等配置项实现访问限制。**  **支持地域访问控制功能，支持根据国家、地区等元素进行地域访问控制。**  **支持自定义服务对象及类型。**  **支持安全态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对威胁趋势图、风险主机TOP10、威胁等级 、最新入侵事件 、设备运行状态 、资源监控、告警总数等信息统计展示。**  **支持检测防逃逸技术，提供缓冲区溢出、SQL注入、扫描刺探、间谍软件、拒绝服务、病毒、木马后门、漏洞攻击、潜在风险的入侵防御特征。**  **支持黑白名单功能，可基于攻击源、攻击目的黑白名单设置。**  **支持暴力破解防御功能。** | **1** | **￥40,000.00** | **￥40,000.00** |
| **5** | **上网行为管理** | **≥1U硬件;标配≥6个千兆电接口;提供≥1个扩展插槽;单电源。最大并发连接数≥16万;最大新建连接数≥24000个/秒；数据防泄漏DLP模块，支持防私接功能，含三年硬件质保服务、三年软件升级服务。**  **支持网关、网桥、旁路、多路网桥模式部署。**  **设备可直路串联在一条或多条原有网络线路上。**  **持IPv6环境下的网址访问审计、生成分析报表等功能。**  **支持标准IPSec协议的VPN功能。**  **支持厂商工程师在线的远程协助和故障排查。**  **设备必须提供物理硬件Bypass按钮。**  **支持远程登录在界面实现Bypass，并可进行切换。（提供功能截图证明材料并加盖制造商公章）**  **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进行反馈。**  **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。**  **支持对以下几类网络应用传输的文件进行病毒云查杀：HTTP/FTP/IMAP/SMTP/POP3。**  **支持对Windows百度网盘客户端的文件标题和内容审计。**  **支持对QQ、微信和百度网盘的PC客户端外发文件进行关键字过滤和封堵。**  **内置常用应用标签，分类至少包含内容外发风险、期货行业合规、证券行业合规、高安全风险、影响工作效率、消耗带宽6大类。**  **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。**  **支持与云端杀毒平台联动，对网络中传输的文件进行特征比对，以便减少对本地计算资源的消耗。**  **支持基于云端大数据安全平台，对恶意URL访问进行封堵和记录日志。**  **支持通过恶意软件特征检测方式识别失陷主机并记录日志。**  **支持与威胁情报大数据平台对接，能够快速识别、封堵失陷主机、记录日志。**  **能够实时提供产品CPU、内存、磁盘使用率、网口状态、授权状态、系统情况等信息。**  **可监控到设备运行的天数，确保设备中间无重启，无宕机。** | **1** | **￥32,000.00** | **￥32,000.00** |
| **6** | **WEB应用防火墙系统** | **产品规格：网络吞吐量≥1Gbps，应用层处理能力≥500Mbps， 1U机箱，有液晶面板，≥1TB硬盘，≥2个扩展插槽。≥6个10/100/1000M自适应电口，≥2组bypass，≥1个Console口，≥2个USB口.Web安全保护≥16个站点。≥一个网站目录防篡改客户端授权,≥三年WAF软件特征库服务，≥三年硬件维修服务。**  **产品具备串联和旁路部署方式，串联部署方式支持透明在线部署，不改名网络或网站配置，无需配置IP地址，实现即插即用。**  **产品具备对HTTP、HTTPS协议的代理网关功能，支持透明代理、反向代理、负载均衡等模式。**  **产品具备虚拟补丁功能，支持导入扫描器的扫描结果生成WAF的规则，对此类网站漏洞直接防护。**  **产品具备Web业务控制防御功能，提供针对爬虫、黑链、内网代理以及盗链的防护功能。（提供功能截图证明材料并加盖制造商公章）**  **产品具备防暴力破解功能，可支持频率阈值。**  **支持动态令牌以及频率阈值与动态令牌组合的三种方式实现暴力破解防护。**  **产品具备敏感信息检测防护，检测类型包括：中间件信息保护，数据库信息保护，敏感文件保护，代码错误信息保护，隐私信息保护。**  **产品具备轻量级蜜罐防御功能，提供伪造的后台管理系统页面防御功能。**  **产品具备协议合规检测，可根据实际网络状况自定义协议参数合规标准，过滤非法数据。**  **产品具备日志一键响应功能，针对攻击日志详情具备一键拉黑以及排除规则功能。**  **产品具备支持威胁情报中心联动功能，基于FTP或FTPS协议登录云端获取数据来源。（提供功能截图证明材料并加盖制造商公章）**  **产品具备资产探测功能，提供自动识别资产系统类型和开放端口。**  **产品具备机器学习引擎，针对业务建模，可通过学习URL、host等信息展示网站结构树形图，并支持对URL的访问量和响应健康度进行图形化统计。**  **产品具备旁路部署对镜像流量分析的同时实现阻断功能，产品具备专门的阻断接口设置和对端MAC地址设置功能。**  **可根据源目的IP，端口，协议等进行访问控制处理，并可自定义访问过期时。**  **产品具备安全态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示。**  **产品具备独立的审计日志、安全防护日志、访问控制日志模块。**  **产品具备独立的机器学习日志、入侵防护日志、DDoS防护日志、以及外联日志模块 。**  **产品具备非法URL外联检测功能，针对特定外联URL进行监控或阻断，并且支持自定义URL地址**  **产品具备移动终端管理功能，不需要安装APP和第三方插件，通过手机浏览器即可管理设备，并可查看设备CPU、内存使用情况。** | **1** | **￥88,000.00** | **￥88,000.00** |
| **7** | **数据库审计系统** | **内置≥4TB磁盘存储空间。标准2U机箱，双电源；标配≥6个千兆自适应电口，≥1个Console口，支持≥两个扩展槽位，支持液晶屏。报价中包含≥三年软件升级和硬件维修服务。SQL审计处理能力（速率）≥34000SQL/S**  **系统支持IPv4和IPv6的网络环境下数据库的审计。**  **部署方式：支持端口镜像旁路部署、Agent代理部署。**  **支持使用代理Agent审计回环地址的流量。**  **支持的数据库类型：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用Gbase、神舟通用、Caché、REDIS、等。**  **支持对HTTP、FTP、TELNET、SMTP、POP3、Samba、NFS协议的审计。**  **系统能够添加地址段作为保护对象。**  **内置疑似SQL注入、跨站脚本攻击、字段猜测、代码更改、等近500种风险审计规则库。**  **支持数据库嵌套、函数、脚本访问以及返回内容等审计；**  **支持B/S架构下的业务审计，可提取包括应用系统的人员工号（账号）的身份信息，精确定位到人，并可获取XML返回结果，支持框架：tomcat、apache、weblogic、jboss。**  **支持C/S架构COM、COM+、DCOM组件的审计，可提取应用层工号（账号）的身份信息，精确定位到人。（提供功能截图证明材料并加盖制造商公章）**  **支持白名单管理。**  **支持数据库自动发现公司（支持发现数据库地址、端口、数据库类型等内容），并自动添加成保护对象进行审计，简化操作。**  **支持系统语句的过滤，支持手动添加系统语句。**  **系统可根据全方位对数据库的访问行为，评估被保护数据库的整体安全指数；**  **内置疑似SQL注入、跨站脚本攻击、字段猜测、代码更改、等近500种风险审计规则库，无需单独配置，直接调用。（提供功能截图证明材料并加盖制造商公章）**  **审计规则支持针对访问工具、客户端IP、客户端MAC、操作系统主机名、操作系统用户名、应用账户名、数据库对象、SQL语句执行回应等条件支持设置等于或不等于等条件。**  **审计规则支持针对最大语句操作长度、语句执行时间、返回行数等条件支持设置大于等于或小于等于等条件。**  **支持全库检索、条件检索和关键字检索，快速定位相应的审计会话内容。**  **支持查询结果自定义报表，支持Word、PDF、xls格式报表导出**  **提供用户界面告警、Syslog告警、SNMP告警、邮件告警、短信系统、短信猫等多种告警方式。**  **用户管理支持三权分立，系统提供了审计管理员、系统管理员、安全管理员分权的用户体系。**  **支持旁路阻断功能（非串联方式），阻断两种模式，宽松模式：对单一会话危险操作阻断；严格模式：源IP操作的所有请求直接阻断。**  **支持设置保留天数和占用百分比自动清理功能，清理数据类型支持审计记录（高风险、中风险、低风险、一般行为、关注行为）、报表、后台日志及返回结果。** | **1** | **￥81,000.00** | **￥81,000.00** |
| **8** | **备份一体机** | **标准机架式结构，2U机架式，支持SAS和SATA硬盘混插，支持在线扩容，可通过后期在线添加磁盘和扩展磁盘柜的方式，进行备份介质容量的增加；内存≥32GB，网络端口都可用且可分配不同的备份任务，本次配置2个千兆网口，至少1颗处理器性能不低于2.2G CPU，本次配置单盘容量≥4TB，硬盘数量≥8块。无数量限制备份授权。**  **支持Windows、Linux、UNIX、AIX、Solaris、 HP-UX等主流操作系统，以及龙芯、飞腾架构下中标麒麟、银河麒麟等自主可控操作系统**  **基于linux的备份存储专用系统，支持https方式登录，确保登录安全**  **支持在同一文件备份作业中采用多通道并发备份，提高备份和恢复的速度，并支持文件合成备份（提供产品功能截图）**  **支持linux 和windows操作系统的备份及异机恢复，支持操作系统备份与恢复的UEFI引导方式**  **操作系统恢复过程中提供驱动程序更换界面，允许客户针对不同的驱动程序做调整**  **支持把Windows 操作系统的备份数据直接生成为VMWare、KVM、H3C CAS等虚拟平台支持数据，通过挂载方式实现即时恢复。**  **支持主流及国产主流的数据库备份恢复，包括但不限于Oracle、 SQL Server、MySQL、Sybase、DB2、Informix、PostgreSQL、MongoDB、Exchange、SharePoint、Domino等主流数据库应用**  **支持MySQL基于物理备份的备份数据（非CDP备份数据），实现任意时间点的恢复。（提供产品功能截图）**  **支持MySQL的逻辑备份和物理备份（完全备份、增量备份、日志备份、连续日志备份），通过物理备份实现对数据库的热备份。**  **支持采用ON-Bar方式实现对Informix的任意时间点备份/恢复，并支持自动配置ON-Bar的相关配置文件，以及设置自动日志备份。**  **支持Oracle、SQL Server合成备份，合成数据通过挂载方式实现即时恢复（提供产品功能截图）。**  **支持Oracle单个表和多个表在不同时间点上的恢复、支持对Exchange单邮件恢复**  **投标产品必须支持Oracle RAC 在内的多种集群环境的数据备份，支持RAC集群环境向备用机的恢复，只需通过web向导界面即可完成配置，无须手工修改rman脚本；**  **支持 SQL Server Always On Availability Groups 的备份和恢复**  **支持对Oracle、MySQL的日志文件采用连续日志备份方式，持续监控日志文件的变化情况，即时把新增日志的数据块进行备份，实现对数据库变化数据达到秒级以内的备份保护。**  **支持数据库基于日志冗余LR技术的真正数据零丢失技术。**  **数据库采用基于应用层（非物理IO同步方式）数据同步技术实现业务容灾，支持主从切换、继续同步等灵活功能。容灾主机可在线激活，承担业务数据查询等功能，并能够继续同步**  **支持CDP实时容灾功能，可实现秒级内的数据实时容灾。在恢复时支持通过挂载方式实现任意时间点的即时恢复**  **支持VMware、Hyper-V、Xenserver、Xen、KVM、FusionSphere、H3C CAS、OpenStack、CNware等虚拟机的备份恢复（不能采用guest host 操作系统备份恢复方式）。针对Vmware、Hyper-V、H3C CAS平台，支持直接挂载备份集即可实现虚拟机的快速恢复**  **支持VMWare合成备份。**  **Vmware平台虚拟机备份，恢复时可恢复虚拟机网络标签及IP地址**  **可支持共享型存储和镜像型存储的高可用集群，支持一主多备模式集群**  **支持固定块、变长块的数据重删技术，在创建重删存储空间时，需要提供变长和固定数据的数据块大小选择。** | **1** | **￥83,000.00** | **￥83,000.00** |
| **9** | **网站云防护系统** | **提供云端防护账号交付，以 SaaS 的方式为用户提供网站安全防护服务（非硬件盒式WAF、非盒式抗DDoS攻击产品、非集成WAF及抗D功能的防火墙类产品，非虚拟机化WAF）。提供10个同一备案主体域名1年的网站安全云防护。支持Web攻击防护、网站缓存加速、10Gbps的DDoS攻击共享型防护、30Gbps高防DNS、2千QPS正常业务请求并发；提供6TB正常业务流量、10GB的Web访问日志下载流量、10个非标准端口。提供1年售后服务：产品远程技术支持（包含防护接入、防护过程中产品问题支持），7x24小时电话支持，以及防护周期内的防护引擎、防护规则免费升级。**  **支持服务器隐身，使得黑客无法获取服务器真实IP地址，防止黑客对服务器的各种攻击。**  **支持HTTP/HTTPS协议合规性检查，包括畸形报文、HTTP版本检查、报文头缺失、请求方法限制、协议违规等。**  **应能识别和阻断SQL注入攻击、Cookie 注入攻击、命令注入、跨站脚本攻击、文件包含攻击、LDAP注入、XPATH注入、爬虫攻击、Struts2命令执行攻击等常见的WEB攻击，防止网站敏感信息泄露。**  **支持细粒度的WEB防护配置，至少支持对24大类Web安全漏洞类型对设置白名单，当设置生效后，针对某URL的该类WEB攻击不在防护。（提供功能截图证明材料并加盖制造商公章）**  **支持对Appscan、Awvs、Pangolin、Burpsuite、啊D、明小子、Nikto等扫描器的扫描防护。**  **支持对SYN Flood攻击、Frag Flood攻击、ACK Flood攻击、UDP Flood攻击、ICMP Flood攻击等常见的流量型DDOS攻击进行清洗。**  **可以防护针对网站的CC攻击。**  **支持CC白名单功能，可针对IP、URL进行白名单配置。**  **用户可以自定义镜像URL、非镜像URL、开始镜像时间、重保时间段等参数，同时可以格式化镜像数据。**  **支持User-Agent报名单，可针对User-Agent内容进行白名单配置。**  **支持针对DNS的攻击防护，如：DNS Query Flood攻击、DNS replay food攻击等流量型攻击。**  **搜索引擎（百度、谷歌、必应、360、搜狗、神马搜索）及恶意爬虫识别及防护，开启后即有默认防护配置（宽松/中等/严格）。支持针对URL做单独的爬虫防护配置。可使用威胁情报中心的威胁情报信息。**  **支持网站一键配置开启和关闭TSL协议1.0/1.1/1.2版本。（提供功能截图证明材料并加盖制造商公章）**  **支持内置完备的敏感词信息库，开启默认防护策略时，可主动监测网站首页有无敏感词，如果存在便产生告警。**  **支持用户自定义URL、敏感词内容，细粒度的对响应方向进行检测，当响应内容包含自定义敏感信息时，则可对内容进行告警、替换\*、阻断和重定向动作。**  **对不同国家和中国的不同省市能否访问保护网站进行访问控制，并能够基于IP地址添加例外访问黑白名单。**  **有全国性的缓存节点机房，按照最小响应时间，最优访问服务等智能缓存算法为用户自动选择缓存节点机房，以提升用户访问效果。**  **支持数据压缩，即对传输的页面文件进行数据压缩以提高传输效率。**  **支持自定义时间段的报表功能，能直观的显示本周及历史周网站遭受的WEB攻击、CC攻击等攻击情况。**  **支持安卓/IOS版手机APP运维客户端，可支持手机接入防护、一键关站（一键处置）、一键回源、WEB防火墙开启/关闭、缓存开关设置、账号管理等功能。** | **1** | **￥75,800.00** | **￥75,800.00** |
| **重保只读模块，提供10个同一备案主体域名1年的重保只读服务。部署该功能，可为客户网站在特殊时期实现网站防篡改。** | **1** | **￥25,400.00** | **￥25,400.00** |
| **10** | **服务器安全管理系统** | **提供资产管理、风险发现、病毒扫描、安全基线等基础检测能力，并额外提供系统防护加固、应用防护等高级防护能力。 含1套管理控制中心软件，增强版客户端≥10个，维保服务≥3年。**  **支持操作系统类型：Windows Server 2003 sp2/R2；Windows Server 2008 sp1及以上/R2；**  **Windows Server 2012~2019 sp1及以上/R2 ；CentOs 5.0及以上；RHEL 5.5及以上 ；Ubuntu 14.04及以上4；SUSE 11及以上版本。**  **支持统一入口查看Windows/Linux系统资产，不应将Windows、Linux系统资产分菜单展示。**  **支持以列表的形式，统一列出Windows/Linux服务器账户资产，并可查看账户的状态、登陆shell、home目录、用户组等信息。**  **支持以列表的形式，统一列出Windows/Linux服务器Web站点资产，并可查看域名、端口号、端口状态、协议、进程等信息。**  **支持全量资产的关键字及语法搜索，支持检索的语法包括但不限于：服务器资产类、进程资产类、账号资产类、软件应用类、web资产类、web服务类、web框架、数据库类、端口资产类、网络连接类、启动服务类、安装包类、计划任务类、环境变量类、内核类、类库资产类、注册表类、证书资产类进行检索。（提供功能截图证明材料并加盖制造商公章）**  **支持以列表的形式，统一列出Windows/Linux服务器端口资产，并可查看端口号、协议、端口状态、绑定IP、监听进程等信息。**  **支持以列表的形式，统一列出Windows/Linux服务器的进程连接资产，并可查看进程名称、协议、IP地址、源端口、目标端口、目标IP、连接状态、同步时间等信息。**  **支持以列表的形式，统一列出Windows/Linux服务器的内核模块，并可查看内核模块名、模块路径、加载地址、模块大小、文件MD5等信息。**  **支持以列表的形式，列出Windows服务器的证书信息，并可查看证书名称、证书路径、颁发者、使用者、有效期开始时间、有效期结束时间等信息。**  **支持以列表的形式，统一列出Windows/Linux服务器基础信息，并在列表中对服务器的关键软硬件进行统计，包括但不限于：CPU数、CPU核数、分区数、账户数、软件应用数、web站点数、web服务数、web框架数、数据库数、端口数、网络连接数、启动服务数、安装包数、计划任务数、环境变量数、内核模块数、证书数、注册表数、类库数等。（提供功能截图证明材料并加盖制造商公章）**  **学习每台服务器的网络外连行为、命令执行行为、文件创建行为，并形成图形化的时间轴行为基线，对于偏离行为以外的动作进行告警。**  **支持以图形化的形式统计展示服务器受到的告警信息/可疑威胁、拦截事件，包括：可疑威胁事件统计、可疑威胁分布、可疑威胁趋势以及具体的威胁事件列表。**  **支持服务器防火墙功能，可对服务器定制访问策略，包括允许本地IP/端口访问指定IP/端口、禁止本地IP/端口访问指定IP/端口，并可设置访问放心，并支持TCP、UDP、ICMP等协议。并根据设置的规则进行访问告警。**  **支持设置端口的暴露控制规则，包括但不限于：禁止/允许外网暴露、禁止/允许内网暴露等策略，并支持例外端口的添加。**  **支持对服务器中的风险账户进行检测，发现可能存在的风险账号，并可对风险账号进行标记修复、加白等操作。**  **可对系统防护（包括但不限于：文件监控与防护、操作系统加固、入侵检测）、应用防护（包括但不限于：高级防护、应用漏洞防护）、网络防护（防端口扫描）进行统一的设置及模板管理，并对各类防护策略以模板形式下发。（提供功能截图证明材料并加盖制造商公章）**  **可对服务器杀毒引擎进行综合的设置，支持本地查杀、控制中心查杀的设置与切换，并可对某台服务器的查杀规则进行详细设置。**  **可对服务器的软件漏洞进行综合扫描，并可对扫描方式、扫描周期进行设置，并以报告的形式展示软件漏洞扫描结果，包括：问题机器TOP5、影响最多漏洞TOP5、漏洞发现趋势等。**  **支持以图形化的形式统计展示服务器受到的告警信息/可疑威胁、拦截事件，包括：可疑威胁事件统计、可疑威胁分布、可疑威胁趋势以及具体的威胁事件列表。**  **支持以多种检测方式（实时监控、本地扫描、特征规则、沙箱运行、动态脚本沙箱）检测webshell攻击。**  **支持各类日志、安全报表、资产报表、事件报表、功能状态报表的综合下载导出，并可根据实际情况对报表内容进行自定义导出。** | **1** | **￥85,000.00** | **￥85,000.00** |
| **11** | **以太网交换机** | **48个10/100/1000Base-T电口（其中8个是combo口），4个10G BASE-X SFP+万兆光 [非模块化](https://detail.zol.com.cn/switches/p11716/)432Gbps/4.32Tbps 166Mpps [可堆叠](https://detail.zol.com.cn/switches/p1275/)**  **支持基于端口的VLAN，支持基于MAC的VLAN，基于协议的VLAN，支持QinQ，灵活QinQ，支持VLAN Mapping，支持Voice VLAN，支持GVRP**  **支持对端口接收报文的速率和发送报文的速率进行限制，支持报文重定向，支持CAR（Committed Access Rate）功能，每个端口支持8个输出队列，支持端口队列调度（SP、WRR、SP+WRR），支持报文的802.1p和DSCP优先级重新标记**  **支持用户分级管理和口令保护，支持802.1X认证/集中式MAC地址认证，支持Triple认证，支持Guest VLAN，支持RADIUS认证，支持SSH 2.0，支持端口隔离，支持端口安全，支持MAC地址学习数目限制，支持IP源地址保护，支持ARP 入侵检测功能，支持IP+MAC+端口多元组绑定，支持EAD** | **2** | **￥8,000.00** | **￥16,000.00** |
| **12** | **以太网交换机** | **[三层](https://detail.zol.com.cn/switches/p11711/)[万兆以太网交换机](https://detail.zol.com.cn/switches/s6082/)**  **传输速度: 10000Mbps，**  **交换容量2.56Tbps/23.04Tbps，**  **包转发率1080Mpps**  **48个1/10GE SFP+光接口，2个QSFP+光接口**  **支持基于端口的VLAN（4094个），支持Default VLAN，支持QINQ，支持灵活QINQ，支持VLAN MAPPING，支持PVST+，支持RPVST+**  **支持对端口接收报文的速率和发送报文的速率进行限制，支持CAR功能每个端口支持8个输出队列支持灵活的队列调度算法，可以同时基于端口和队列进行设置，支持SP、WDRR、WRR、WFQ、SP+WDRR等多种模式支持报文的802.1p和DSCP优先级重新标记支持L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源MAC地址、目的MAC地址、源IP(IPv4/IPv6)地址、目的IP(IPv4/IPv6)地址、端口、协议、VLAN的流分类，支持时间段（Time Range）支持WRED**  **支持用户分级管理和口令保护，支持集中MAC认证，支持802.1X，支持storm constrain，支持AAA认证，支持RADIUS认证，支持HWTACACS，支持SSH 2.0，支持端口隔离，支持IP+MAC+端口绑定，支持IP Source Guard，支持HTTPs，支持SSL，支持PKI(Public Key Infrastructure，公钥基础设施)，支持CPU防护** | **1** | **￥22,000.00** | **￥22,000.00** |
| **合计：** | | **大写：捌拾伍万元整** | **小写：850000** | | |