**宁波市残疾人辅具网安全项目设备类招标需求**

# 一、项目总体要求：

1、投标方所投的所有产品序列号对应的最终用户名为：“宁波市康复医院”；

2、本次项目所有产品必须为正规渠道供货，不得提供旧货、假货、水货，项目中涉及的所有产品为三年原厂质保服务，（保修年限以所投产品官网查询的生效时限为准，货物必须在投标产品厂商官网和厂商400电话（或官网电话）同时验证所有设备的序列号核对质保日期和最终用户，质保日期需从到货当日起开始计算，不得少于3年，否则算供应商违约，无条件取消中标资格和合同）；

3、本项目要求在合同签订后10天内完成安全设备的安装调试工作，否则无条件取消中标资格和合同；

4、本项目所涉及的配件和辅料等若干未列，报价包含项目所需的所有人力、物力等相关所有费用、采购方不再为此项目承担额外的任何费用；

# 二、设备产品清单

|  |  |  |
| --- | --- | --- |
| **序号** | **产品名称** | **数量/单位** |
| 1 | WAF | 2台 |
| 2 | 下一代防火墙 | 2台 |
| 3 | 数据库审计 | 1台 |
| 4 | 日志审计 | 1台 |
| 5 | 路由器 | 2台 |
| 6 | 交换机 | 2台 |

# 三、详细技术参数

## 3.1 WAF

|  |  |  |
| --- | --- | --- |
| **类别** | **指标项** | **规格要求** |
| 性能要求 | ★硬件规格 | 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。 |
| 提供的产品不能少于4个10/100/1000M电口，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800Mbps，最大并发连接数不能低于3万，每秒新建事务数不可小于3400。 |
| 安全体系 | 基于机器学习和语义分析的智能检测引擎 | 基于机器学习和语义分析的智能检测引擎，提升SQLi和XSS检测精度 |
| IP信誉 | 利用威胁情报建立IP风险画像，提供6类信誉数据（1）DDos攻击；（2）安全漏洞；（3）垃圾邮件；（4）Web攻击； （5）扫描源； （6）Botnet客户端。 |
| 规则体系 | 系统提供可配置的内置规则；且支持自定义规则，规则属性要求支持“检测方向（请求或响应）”、“检测对象（URI/URI-path/Host/参数名/参数/Header-name/Header/Cookie名/Version/请求方法/Request-Body）”、匹配操作、特征签名等丰富要素。 |
| ★智能补丁联动 | 基于专利技术，可以与同品牌SaaS扫描服务或者Web漏洞扫描器产品联动，在WAF上定期自动获取专家级、个性化的《WEB漏洞扫描报告》，并转化为WAF可执行的、有针对性的WEB安全防护策略。支持手动导入扫描结果，也支持在WAF上自动下发扫描任务，扫描完成后扫描结果自动上传WAF，投标时提供配置界面截图证明和专利证书复印件 |
| 安全特性 | 网络层通用防护 | 支持ARP攻击防护，支持MAC地址绑定。 |
| 支持基于五元组（源IP地址、目的IP地址、源端口、目的端口、协议类型）及接口的网络层访问控制功能。提供配置界面截图证明 |
| HTTP协议校验 | 支持对HTTP协议合法性进行验证，提供HTTP协议防护功能，支持对HTTP协议的URI、HOST、UA、Cookie、Referer、Content、Accept、Range、其他头部和参数在内的元素、参数进行检测与处理。且支持非法编码和解码的灵活控制与处理。提供配置界面截图证明 |
| WEB基础架构防护 | 支持针对主流Web服务器及插件的已知漏洞防护。Web服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS等插件应覆盖:dedecms、phpmyadmin、PHPWind、shopex、discuz、ecshop、vbulletin、wordpress等，提供Java反序列化漏洞（Jboss）防护插件。提供配置界面截图证明。 |
| WEB资源授权控制 | 支持HTTP访问控制功能，可以提供针对HTTP元素和客户端的组合访问控制策略。支持对多种HTTP方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS、PROPFIND、PROPPATCH、LOCK、UNLOCK TRACE、SEARCH、CONNECT。提供配置界面截图证明 |
| 提供爬虫防护，规则库至少可以防护100种以上的爬虫。提供配置界面截图证明或者爬虫列表 |
| 提供盗链防护，应采用Referer和Cookie算法。提供配置界面截图证明 |
| WEB应用安全防护 | 支持对注入（包括SQL注入、LDAP注入、XPATH注入及命令行注入）、XSS、SSI指令、路径穿越、远程文件包含、WebShell防护。提供配置界面截图证明 |
| 支持CSRF（跨站请求伪造）防护。提供配置界面截图 |
| 支持非法文件上传防护，有效识别文件上传行为，并对上传行为的内容做安全检测，可以根据需要，禁止上传以下文件类型：PE(windows Executable File)、ELF(linux Executable File)、PHP web shell、Linux shell、Power shell(windows Script File)、Java shell、Asp shell、Perl shell、Python shell及Ruby shell。提供配置界面截图证明 |
| 支持非法下载防护，可以根据文件大小、MIME类型及文件扩展名灵活定义下载限制策略，限制用户非法获取网站的关键数据（比如数据库文件，配置文件等），提供配置界面截图证明 |
| 支持Cookie安全机制，包括Cookie加密和Cookie签名的防护算法。支持过期兼容时间配置以及\*配置。 |
| 支持信息泄露防护，提供针对服务器状态码进行过滤和伪装的安全策略。提供配置界面截图证明 |
| 支持内容过滤，提供恶意代码过滤功能 |
| 支持暴力破解防护，可针对指定URL进行暴力破解防护，支持多种方式的登陆，支持referer检测，支持阈值和检测周期的设置。 |
| 支持敏感信息过滤，对用户的个人隐私信息（信用卡卡号、手机号、身份证号码）泄露进行检测、阻断或替换。 |
| XML防护 | 支持XML基础校验，包括最大树深度、元素名长度、元素个数、子节点个数等参数配置。提供配置界面截图证明。 |
| 支持Schema校验，提供配置界面截图证明。 |
| 支持SOAP校验，提供配置界面截图证明。 |
| Web扫描防护 | 基于专利技术实现的Web扫描防护，支持以统计算法分析扫描行为的扫描防护。提供配置界面截图证明和专利证书复印件 |
| DDOS防护 | 支持TCP Flood防护；支持基于阈值及算法配置的HTTP Flood防护。提供配置界面截图证明 |
| 支持对慢速攻击的防护。 |
| 支持与同品牌的抗拒绝服务系统联动，对流量进行按需清洗。提供配置界面截图证明 |
| 会话跟踪 | 可根据会话标识、浏览器标识进行会话跟踪，还原攻击场景。 |
| 安全合规 | PCI-DSS符合性报表 | 提供PCI-DSS V3.0符合性报表。提供配置界面截图证明 |
|  | 默认策略模板 | 提供默认策略模板，方便客户快速对站点组及虚拟站点进行web安全防护策略配置。支持严格模板、标准模板及宽松模板。 |
| 策略防护动作 | 支持多达七种的防护动作，包括了放过、阻断、接受、重定向、伪装、清除和替换。可针对不同安全风险提供多种可选方案。提供配置界面截图证明 |
| 支持对攻击源地址的智能阻断，支持永久封禁或者自定义IP封禁时间（秒/分钟/小时），并且可以手工解除解禁。提供配置界面截图证明 |
| 风险级别策略 | 可自定义修改某一策略的默认风险等级 |
| 例外策略 | 支持对安全策略的一键式例外配置。提供配置界面截图证明 |
| 部署能力 | 部署方式 | 支持透明在线部署，不更改网络或网站配置，且提供完整安全防护功能（如HTTPS防护、Cookie安全、CSRF防护、敏感信息过滤等）。 |
| 支持旁路部署，提供配置界面截图证明；支持流量牵引、二层回注、跨接回注及PBR回注方式。 |
| 支持镜像部署方式（可以包含支持检测https流量） |
| 支持反向代理部署 |
| 支持IPv6 | 满足IPv6环境部署要求，提供第三方资质证明。 |
| SSL支持 | 支持对SSL（HTTPS）加密会话进行分析 |
| 支持SSL卸载及加载 |
| 支持SSLv2, SSLv2/v3, SSLv3、TLS1.0\1.1\1.2 |
| 支持HTTPS国密算法 |
| 虚拟站点支持 | 支持针对虚拟站点的细粒度防护 |
| 集中管理 | 支持集中管理能力（可使用集中管理系统对多台WAF进行策略下发、统一升级、状态监控等能力） |
| 日志系统 | 日志查询 | 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 |
| 日志内容源地址溯源 | 支持在安全日志中带有客户端真实IP地址，便于IP溯源。提供配置界面截图证明 |
| 日志集中管理 | 支持将安全日志、系统日志统一发送到同品牌的安全中心。提供配置界面截图证明 |
| 系统监控 | 安全事件呈现 | 支持不同安全事件类型以不同的颜色区分。提供配置界面截图证明 |
| 系统信息 | 支持显示接口状态，引擎状态、系统CPU、内存及硬盘使用率，系统当前时间及系统运行时间 |
| 监控类型 | 安全事件、业务负载、接口流量、系统负载、封禁IP管理、站点访问量统计的实时和历史数据查看及查询 |
| 管理功能 | 管理方式 | 支持B/S管理 |
| 支持标准SNMP V1/V2c/V3以及 trap；支持Syslog接口 |
| 支持REST API接口，提供接口文档。 |
| 系统管理 | 支持分权管理 |
| 多语言支持 | 管理、操作界面支持多语种自由切换，支持简体中文、英文和日文。提供配置界面截图证明 |
| 升级系统 | 定期升级功能模块和规则库 |
| 配置同步 | 支持配置同步，包括离线同步和在线同步，提供三种维度的备份：整机备份；部分备份（“资产+策略”备份以及仅“策略”备份）。提供配置界面截图证明 |
| 一键接受 | 支持一键接受所有防护策略 |
| 支持代理信息配置 | 支持在CDN代理的环境下，对客户端真实IP进行识别。 |
| 时间同步 | 支持与时间服务器同步。提供配置界面截图证明 |
| 服务器存活状态检测 | WAF提供周期性的主动探测后端服务器状态功能。分四层TCP层探测和七层HTTP层探测。支持对HTTP站点和HTTPS站点提供服务器探测功能。提供配置界面截图证明 |
| ★安全运维管家 | WAF可以和云中心进行联动，客户可通过下载手机APP，对设备进行状态监控，监控信息包括CPU、内存、规则库版本等，投标时提供界面截图证明并盖公章 |
| 设备自身安全性 | 设备网络管理 | 支持自定义HTTPS监听端口，不完全依赖缺省的443端口。提供配置界面截图证明 |
| 登录IP限制 | 可以限制远程管理的登录IP。提供配置界面截图证明 |
| 高可用性 | HA部署能力 | 支持A/S部署模式（链路切换、配置同步） |
| 支持VRRP协议。 |
| ★紧急模式 | 支持紧急模式，可配置并发连接数阈值，当并发连接数超过设置阀值时，WAF自动进入紧急模式，已经代理的连接正常代理，对新增的请求不进行代理，直接转发，防止WAF成为访问瓶颈。当连接数恢复正常时，自动退出紧急模式。提供配置界面截图证明并加盖公章 |
| 产品实力证明 | ★市场成熟度 | 投标产品应该是经过市场考验的成熟产品，产品上市时间不少于8年。须提供销售许可证或软件著作权证书等有效证明材料。 |
| 投标产品应该是被广泛应用的成熟产品，在国内市场具有较高的市场份额，连续7年市场占有率排名不应低于前3名。须提供市场占有率排名有效证明材料。 |
| 2014-2017连续4年入选Gartner WAF魔力象限，须提供相应证明。 |
| 产品资质 | 《计算机软件著作权登记证》，提供证书复印件证明 |
| 具备IPv6证书，提供证书复印件证明 |
| 《国家信息安全漏洞库 兼容性资质证书》（千兆/万兆） |
| OWASP中国WEB应用防火墙认证证书，提供证书复印件证明 |

## 3.2 下一代防火墙

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| ★配置要求 | 采用多核架构，自研操作系统，提供“多核分布式安全操作系统”的软件制作权登记证书 |
| ≥1\*RJ45管理口，≥8\*GE（Bypass）接口，配置≥4个千兆光口；支持BYPASS；3年质保 |
| 网络层吞吐量≥8 G，并发连接数≥200万，每秒新建连接数≥20万应用识别功能，含3年应用特征库升级许可 病毒防护功能，含3年企业版病毒特征库升级许可 入侵防御功能，含3年攻击规则库升级许可 网站分类过滤功能，含3年URL网址库升级许可 IPSECVPN功能。 |
| 防火墙功能 | 支持虚拟线、二层透明、三层、混合、旁路监听接入方式，适应各种网络环境需求 |
| 支持Flood防护，包括PING Flood、UDP Flood、SYN Flood、DNS Reply Flood、DNS Req Flood，支持针对以上Flood攻击调整检测阈值(包数)、检测周期（秒）、复位时间（秒）、保护时间（秒）、限制流量（PPS） |
| 在策略匹配时有较高的匹配效率，请提供《网络数据流安全处理方法及设备》的专利 |
| 支持8级流控，可对应用流量实行带宽限制、带宽保证等策略，请提供《一种网络数据流量控制设备及方法》的专利 |
| 具备SSL VPN功能，支持WEB代理和L3-VPN两种实现模式，并提供两种功能模式配置截图证明 |
| 支持策略路由，策略路由可基于应用进行流量控制。提供截图证明 |
| 支持源IP联动封锁。在入侵防御事件中发现源IP存在攻击行为时，可以一键封禁该IP，并设置封禁的时间。提供截图证明 |
| ★资产风险识别 | 支持资产风险识别。可根据用户指定的网络范围，通过自动、手动识别等多种方式，识别资产类型，如PC、移动设备、服务器等等资源类型，提供截图证明 |
| 支持对易受攻击的系统及应用软件进行打分告警、报表分析，如操作系统版本漏洞威胁度、上网浏览器客户端漏洞威胁度等，让用户实时了解当前网络资产资源中的脆弱度，提供截图证明 |
| 支持安全加固指导及实施。针对识别出的资产风险，为用户提供一键安全策略生成的功能，并可实时告警和记录入侵安全事件，形成安全事件报表和趋势图，指导用户及时做出加固防护。提供截图证明 |
| 可自定义操作系统、浏览器、杀毒软件的风险等级，并支持预置风险等级。可提供截图 |
| 可为每个内网主机生成风险指数，通过数字直观展示内网主机的风险状态。可提供截图 |
| 可生成内网资产风险报表，提供高风险资产top10，提供操作系统等相关资产信息的数据统计和报表展示。可提供截图 |
| ★远程安全运维功能 | 支持与堡垒机联动，以VPN模块+堡垒机的方式提供远程运维安全服务。远程维护人员登录VPN后，无需再输入帐号密码即可登录堡垒机，提升运维便捷性；同时，防火墙无需保存任何堡垒机的帐号，保障运维安全性。提供截图证明 |
| 终端防护 | 支持联动终端安全系统，对终端上的安全状态进行检查，确认符合安全要求后才可连网访问，使得防火墙能够提供端到端的安全防护能力。 |
| 在终端安全接入方案的基础上，支持配置白名单（排除范围），如配置一些可以不接收管控的特殊IP地址，或者地址组。便于管理员根据单位的实际情况来进行特殊处理。提供截图证明 |
| 信誉管理 | 支持内置Web信誉库，收录40万+恶意站点，请截图证明 |
| 支持web信誉的白名单配置，请截图证明 |
| 支持僵尸网络、web信誉的本地及云端查询，请截图证明 |
| ★漏洞发现 | 支持联动外部扫描器，外部扫描器定期将漏洞推送至防火墙，通过防火墙可查看扫描器上报的内部资产漏洞的拦截情况。  |
| ★一体化安全 | 入侵防护规则库具有超过5000条攻击规则，每条规则具备详细的攻击规则描述及解决方案。同品牌入侵防护类产品通过国际权威机构NSS Labs的IPS专项测试，提供NSS Labs相关证明复印件 |
| 移动端安全运维 | 可通过移动端实现设备安全运维监控，APP支持安全设备运行状态监控，监控指标包括CPU使用率、内存使用率、设备IP地址，设备状态，查看安全告警等功能，提供APP下载网页和相关链接以及包括APP相关功能界面的截图证明 |
| 产品资质 | 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、万兆）。提供有效证书的复印件 |
| 产品具备《涉密信息系统产品检测证书》（千兆、万兆）。提供有效证书的复印件 |
| 产品具备《中国国家信息安全产品认证证书》（千兆、万兆），并且认证级别为增强级。提供有效证书的复印件 |
| 产品具备《军用信息安全产品认证证书》（军B）（千兆、万兆）。提供有效证书的复印件 |
| ★产品具备《多核分布式安全操作系统》提供有效证书的复印件 |
| 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； |
| 要求获取CVE证书，且类型为下一代防火墙（Next Generation Firewall）,提供截图证明； |
| 参与制定《信息安全技术 第二代防火墙安全技术 要求》，请提供相关证明材料 |
| 提供由中国信息安全测评中心颁发的《自主原创产品测评证书》 |
| 产品拥有IPv6 Ready Phase-2 Logo。提供有效证书的复印件 |

## 3.3 数据库审计

|  |  |  |
| --- | --- | --- |
| **类别** | **参数** | **功能与技术描述** |
| ★配置要求 | 产品架构 | 软硬件一体化产品，2U上架设备。  |
| 部署方式 | 在旁路部署模式下，通过TAP、SPAN等技术将网络流量映射到审计设备，对数据库流量进行审计和告警。 |
| 管理结构 | 中文界面，B/S架构，采用HTTPS方式远程安全管理，无需安装客户端。 |
| 网络接口 | ≥4\*100/1000M RJ45自适应以太网口；2个万兆光口 |
| 数据存储 | 系统自带内部存储，存储空间不低于2TB;并支持外部存储 |
| 性能指标 | SQL语句处理能力：>=20000条SQL每秒  |
| 检索能力：1亿条日志的数据规模，查询响应时间<20秒  |
| 数据库自动发现 | 支持数据库自动发现。设备无需添加、即插即用。支持在目标数据库安装agent解决无法通过旁路镜像获取流量的场景，如同服务器部署数据库和应用系统、云环境、虚拟化环境场景下数据库的审计。提供截图并加盖公章证明。 |
| 数据库类型 | 支持的数据库类型 | 支持主流数据库：Oracle、SQL Server、MySQL、DB2、DM、PostgreSQL、Kingbase、Informix、Oscar、Sybase、Hbase、MongoDB；提供截图证明 |
| 部署方式 | 旁路镜像 | 旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计 |
| 分布式部署 | 支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询。 |
| 分布式部署下，审计引擎和审计中心都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展。 |
| 系统采用大数据架构设计，审计中心支持集群部署，具备平滑升级和扩充存储能力。 |
| 审计能力 | 协议支持 | 支持在IPV6环境中部署，且支持所有数据库IPV6协议的审计。提供截图证明并加盖公章 |
| 审计内容 | 支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小；提供截图证明 |
| 会话的终端信息：IP、MAC、Port、工具名称（程序名） |
| 会话的主机信息、IP、MAC、Port、数据库名（实例名） |
| 会话的其它信息：登录时间、会话时长 |
| 操作信息：操作类型（DDL、DML、DCL等）、操作时间、执行时长、操作成功与失败、操作对象（表、函数、存储过程名称）、SQL语句 |
| 操作影响范围信息：查询、修改、删除操作的影响行数,以及返回行数 |
| ★审计要素 | 执行人who：审计到前端的应用用户、数据库用户名、主机名称、操作系统用户等；提供截图证明并加盖公章 |
| 执行内容what：具体的操作，访问的数据库、表、列、字段、包、存储过程、函数、视图；提供截图证明 |
| 执行时间when：每个操作发生的具体时间，操作时间、登录时间等； |
| 执行地点where：操作的来源和目的，包括IP地址、MAC地址、用户名、端口号、数据库类型；提供截图证明 |
| 执行方式how：通过哪些客户端应用程序或第三方工具执行得操作，如：DDL、DML、DCL；提供截图证明并加盖公章 |
| 影响范围（影响行数）Range：该操作执行的影响范围，如查询、修改或删除的记录行数；提供截图证明并加盖公章 |
| 执行结果ResultSet：执行成功与否的结果以及返回结果集，如查询操作的返回内容；提供截图证明并加盖公章 |
| 复杂SQL语句支持 | 准确审计长SQL语句；提供截图证明 |
| 有效分割、准确审计多SQL语句；提供截图证明 |
| 准确审计绑定变量的SQL语句；提供截图证明 |
| 应用用户关联审计 | 能以完全精确方式，审计到应用端相关信息，包括应用用户等。提供截图证明 |
| 在并发1000个连接的情况下，准确率应达到100%准确。 |
| 支持Weblogic、tomcat、Websphere、Jboss等主流的应用服务器。 |
| 加密链路审计 | 支持MySQL数据库的SSL/TSL加密链路审计 |
| 入侵检测能力 | 数据库漏洞攻击监测 | 能对基于数据库漏洞进行攻击行为监测和告警，默认支持200个以上的数据库漏洞攻击规则库，通过模式匹配的方式对SQL访问进行监测与告警,判断是否为可疑SQL注入；提供SQL注入特征库；提供截图并加盖公章。 |
| SQL注入检测 | 通过模式匹配的方式对sql访问进行监测与告警,判断是否为可疑sql注入；提供sql注入特征库;提供截图证明并加盖公章 |
| 可疑行为识别 | 批量数据导出：对超过特定行数阀值的批量数据导出行为 |
| 高危操作：对超过特定行数阀值的批量数据修改、删除，或全表Update、Delete行为等 |
| 新型语句的识别 |
| SQL注入行为的识别 |
| 规则设置 | 基于数据库设置，从优先级和规则类别两个层面创建并查询审计规则； |
| 根据放行、高风险、中风险、低风险四个层级逐级命中规则； |
| 风险操作支持多条规则逻辑关联，根据排列顺序区分优先级； |
| 支持SQL注入监测：根据IP，sql特征和正则表达式自定义SQL注入 |
| 支持数据库漏洞监测和审计语句统一管理。 |
| 告警能力 | 告警策略 | 支持风险语句告警策略。（黑白名单效果）提供截图证明 |
| 自定义添加风险语句和可信语句（黑白名单效果）； |
| 根据风险操作、SQL注入、漏洞攻击检测、语句管理等模块定义告警规则 |
| 支持高、中、低风险告警。 |
| 支持系统资源监控与告警，支持磁盘使用率监控，当磁盘使用率达到预定的阈值时，系统会发出告警。提供截图证明 |
| 响应方式 | 根据不同的安全级别采用不同的响应方式，包括记录、告警； |
| 告警方式包括：邮件、短信、SYSLOG、SNMP |
| 审计结果展现与查询 | 审计信息显示 | 三个纬度的导航：会话维度、风险纬度、sql分布 |
| 操作记录的信息：审计结果中包括：告警级别、事件发生时间、客户端IP、目标数据库IP、操作类型、客户端MAC地址、客户端端口号、返回状态、结果信息、客户端执行命令等详细信息内容。 |
| 审计查询 | 支持基于时间、IP地址、数据库服务器IP地址、用户名、数据库操作命令、数据库表名，执行结果，应用用户等多种丰富的查询检索条件。 |
| 敏感信息遮蔽 | 对审计结果集敏感内容可进行屏蔽 |
| IP别名 | 支持客户单IP建立别名；提供截图证明 |
| 所有涉及客户端ip页面均显示业务化ip名称；提供截图证明 |
| SQL语句客户化翻译 | 对详细信息中的SQL语句能进行客户化翻译 |
| 报表统计分析 | 自动生成报表 | 支持定时自动生成报表，并发送到指定邮箱 |
| 统计信息 | 风险分析：根据风险语句、sql注入、漏洞攻击、风险操作等维度以时间维度统计数据库分析信息。支持规则命中查询、支持风险查询。语句分析：基于SQL语句的操作类型统计，支持失败sql统计、Top sql统计；支持针对新型语句、语句审计模板检索。会话分析：基于客户端IP、数据库用户、访问程序统计会话、支持会话检索；失败会话和并发会话统计；支持应用层关联会话查询。综合分析：实时统计并展示数据库各类操作及风险状况.支持客户单IP建立别名，所有涉及客户端ip页面均显示业务化ip名称。提供截图并加盖公章 |
| 展现形式 | 提供图表结合的展形式，支持柱状图、饼状图、折线图等多种展示方式 |
| 支持风险语句挖掘和超链接钻取。 |
| 报表展示 | 支持（系统级）多数据库聚合报表展现和单数据库综合性报表展现。 |
| 基于总体概况、性能、会话、语句、风险多层面展现报表。 |
| 支持图表结合展现，支持柱形图、饼状图、条形图，双轴折线图等多种统计图展现形式。 |
| 支持报表定时推动功能，自定义推送周期以邮件形式推送报表文档。 |
| 支持日、周、月 等综合性报表和自定义分析型报表功能。 |
| 文档格式：PDF\HTML |
| 报表自定义 | 支持报表自定义，自定义项不少于10种 |
| 数据维护 | 支持自动数据备份 | 自动备份数据到FTP服务器 |
| FTP服务器可配置 |
| 备份的开始时间、时间间隔可配置 |
| 支持自动清理日志信息 | 达到指定阈值时自动清理日志信息 |
| 阈值、开始清理时间、清理时间周期可配置 |
| 支持手动清理日志信息 | 支持手动清理日志信息 |
| 设备安全性 | 系统自身安全性 | 根据三权分立的原则。提供系统管理员、安全管理员和审计管理员不同的用户身份验证。系统针对产品操作人员的操作行为进行审计记录，可以由审计管理员进行查询，具有自身安全审计功能。提供审计数据管理功能，能够实现对审计数据的自动备份、删除和导入。 |
| 资质要求 | ★产品资产品资质质 | 信息系统安全专用产品销售许可证，须符合行标GA/T相关的技术要求；提供检测报告。 |
| 涉密信息系统产品检测证书； |
| 中国国家信息安全产品认证证书（ISCCC） |
| 国测信息技术产品安全测评证书-EAL3+ |
| 厂商资质 | 厂商应具备足够的信息安全服务技术实力及安全服务保障能力，获得中国信息安全测评中心颁发的信息安全服务安全工程类二级资质证书。 |
| 厂商应具备针对安全事件的远程和现场的紧急响应能力，获得中国信息安全认证中心颁发的信息安全应急处理服务一级资质证书。 |
| 厂商应具备针足够的风险评估服务能力，获得中国信息安全认证中心颁发的信息安全风险评估服务一级资质证书。 |

## 3.4 日志审计

|  |  |
| --- | --- |
| **指标项** | **规格要求** |
| ★硬件指标 | 系统应为1U标准式机架硬件设备，全内置封闭式结构，具有完全自主知识产权的专用安全操作系统 |
| 系统应支持冗余电源，避免电源硬件故障时设备宕机，提高设备可用性 |
| 系统应包含1个RJ45串口，不少于4个采集口 |
| 系统硬盘容量应不低于4TB，应支持定制扩容 |
| 系统架构 | 系统应基于大数据平台架构，具备海量数据收集与快速检索能力 |
| 系统应基于B/S架构，支持SSL加密模式访问，可通过web方式直接对系统进行管理 |
| 系统应支持内置采集器，不依赖其他设备即可进行日志采集， |
| ★性能指标 | 系统应默认支持审计40以上日志源接入，应可扩展日志源接入数量 |
| 系统应支持每秒2000EPS的日志平均处理能力 |
| 日志采集 | 系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等 |
| 系统支持的数据采集方式包括但不限于SYSLOG、SNMP Trap、FTP、ODBC、JDBC、Net flow、专用Agent等方式采集日志 |
| 系统支持采集的设备厂家包括但不限于：NSFOCUS(绿盟科技)、Venustech(启明星辰)、Topsec(天融信)、DBAPPSecurit(安恒)、SANGFOR(深信服)、Hillstone(山石网科)、东软、瑞星、金山、网康、360网神、Dptech(迪普)、艾科网信、Imperva、Juniper(瞻博网络)、F5、Symantec(赛门铁克)、Deep Security(趋势科技)、MaAfee(迈克菲)、Fortinet(飞塔)、Windows、Linux/Unix、Cisco(思科)、HUAWEI(华为)、H3C(华三)、中兴、Apache、nginx 、IIS、WebLogic、Vmware、Kvm、Xen、OpenStack、Hyper-V、华为FusionSphere、Oracle、MySQL、PostgreSQL、SQL Server、Bind等 |
| 日志管理 | 系统应能实现海量日志数据的采集并保存原始日志数据 |
| 系统应能够对异构日志格式进行统一化处理并保存统一化处理后的日志数据 |
| ★系统应支持界面配置即可完成未识别日志接入，无需编写xml;支持NAT环境下的Agent部署模式.提供截图并加盖公章 |
| 系统应支持范式化日志多级提取,支持正则、KV、格式串等多种灵活的提取方式【提供截图】 |
| 系统应支持自动生成正则以高效的辅助提取【提供截图】 |
| 系统应能够实现对海量日志数据快速查询 |
| 系统应能够实现范式化日志的枚举值管理，实现对范式化日志字段的灵活翻译【提供截图】 |
| 日志转发 | 系统应提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源IP信息【提供截图】 |
| 日志备份恢复 | 系统应支持按类型、按日期(天)，手动、自动备份日志 |
| 系统应支持设置日志存储备份策略，可设置备份周期、备份日志类型 |
| 系统应支持备份日志导入查询 |
| 系统应支持日志备份远程服务器，如传送到FTP服务器 |
| ★系统应支持日志存储扩展，如NFS网络共享存储扩展【提供截图】 |
| 日志查询分析 | 系统应支持实时日志查询、历史日志查询 |
| 系统应支持原始日志、范式化日志查询 |
| 系统应支持自定义查询规则 |
| 系统应支持全文检索、模糊检索、正则检索等多种方式【提供截图】 |
| 系统应支持日志检索结果存储为日志监控视图 |
| 事件告警 | ★系统应内置事件分类，并支持自定义事件分类，可定义事件分类的风险级别,内置丰富的事件规则，应支持自定义事件规则【提供截图】系统应支持查询实时事件，并可以很方便的下钻事件规则以及原始日志信息【提供截图并加盖公章】 |
| 系统应支持基于事件分类的告警规则，支持短信、声音、邮件、界面提示等多种告警方式 |
| 系统应支持告警抑制 |
|  | ★系统应支持资产属性配置,资产标签，且至少6种标签以上，根据标签可快速查询资产【提供截图并加盖公章】 |
| 系统应支持手工注册资产，支持对资产进行修改/删除、批量导入/导出/添加/修改/删除等多种方式的管理； |
| 系统应支持从日志进行资产发现, |
| 系统应支持按资产查看资产日志、事件、资产告警 |
| 报表管理 | 系统应能够按照多种维度统计日志信息 |
| 系统应支持统计分析报表与多种文件格式导出 |
| 系统应能支持用户上传自定义报表模板 |
| 系统应能支持自定义报表目录、LOGO等【提供截图】 |
| 统计项管理 | 系统应支持生成折线图、趋势图、饼图、柱状图、表格等统计项 |
| 系统应支持自定义统计项 |
| 系统应支持统计项分组保存 |
| 系统应支持统计项引用到报表【提供截图】 |
| 用户管理 | 系统应支持用户自定义账号 |
| 系统应支持管理员、审计员、操作员多种权限设置 |
| 系统应支持密码配置策略 |
| 系统应支持超时退出机制 |
| 系统应支持来访IP限制，对暴力猜测IP地址进行锁定 |
| 系统自身安全性管理 | 系统应支持自身日志记录并可查询、自身CPU、内存和磁盘使用率可监控并以图形化方式动态显示，且支持状态监控和主动告警； |
| 系统应支持系统基本参数管理、基本配置管理。 |
| ★资质指标 | 计算机软件著作权登记证书 |
| 公安部销售许可证-行标三级 |
| 涉密信息系统产品检测证书 |
| 产品具有ipv6 ready logo 认证证书 |
| 中国国家信息安全产品认证证书（增强级） |

## 3.5 路由器

|  |  |
| --- | --- |
| **功能类别** | **技术要求及指标** |
| 包转发率 | ★包转发率≥200Mpps  |
| 架构 | ★控制转发物理分离，提供产品物理转发板及主控截图 |
| 接口 | 实配10\*GE+4\*10GE |
| 槽位数 | 槽位数≥6 |
| 板卡种类 | 支持通道化E1、非通道化E1、异步串口、同异步串口、等广域网接口扩展，并提供板卡实物图 |
| 电源 | 电源数量≥2 |
| 接口形态 | 支持E1、155MPOS、CPOS、SAE、VE1等接口 |
| 特性 | 支持零配置开局，设备拨号上网后，可以通过TR069协议实现配置自动上线部署 |
| 特性 | ★支持对系统软硬部件的内部事件、状态进行监控，出现特定事件后能够自动调整网络设备业务和控制策略，实现智能自动化控制支持对系统软硬件的内部事件、状态进行监控，出现问题时收集实时信息并自动修复将实时信息发送到指定服务器权威第三方机构的测试报告 |
| 特性 | 支持划分安全域，用于管理防火墙设备上安全需求相同的多个接口；支持IPS、ADVPN、GDVPN、SSL VPN特性权威第三方机构的测试报告 |
| 虚拟化IRF  | 支持虚拟化特性，将物理上两台设备虚拟化成一台逻辑设备，权威第三方机构的测试报告 |
| 广域网优化 | 支持对HTTP/FTP等TCP业务流量进行优化传输技术，提高广域网带宽利用率，权威第三方机构的测试报告 |
| URL过滤黑名单功能 | 支持对终端用户域名访问控制功能，权威第三方机构的测试报告 |
| 支持openflow功能 | 支持openflow功能，权威第三方机构的测试报告 |
| 基于域的防火墙 | 支持划分安全域，用于管理防火墙设备上安全需求相同的多个接口，权威第三方机构的测试报告 |
| IPS入侵防御功能 | 支持对已知网络攻击进行安全防御，提高网络安全性，权威第三方机构的测试报告 |
| ADVPN功能 | 通过动态VPN技术，实现动态获取对端分支节点当前的公网地址，从而实现两个节点之间动态建立跨越IP核心网络的ADVPN隧道简化VPN网络部署复杂度和提高管理效率，权威第三方机构的测试报告 |
| GDVPN功能 | 支持密钥和IPSEC安全策略集中管理，基于IPSEC安全模型，属于同一组的所有成员共享相同的策略及密钥，权威第三方机构的测试报告 |
| VXLAN功能 | 支持VXLAN数据中心特性，并提供支持此特性权威第三方机构的测试报告 |
| 短信开局 | 支持利用短信下发的方式实现设备开局部署，并提供支持此功能的权威第三方机构的测试报告 |
| U盘0配置部署 | 支持利用U盘0配置方式实现设备开局部署，并提供支持此功能的权威第三方机构的测试报告 |
| 嵌入式自动化（EAA） | 支持对系统软硬部件的内部事件、状态进行监控，出现特定事件后能够自动调整网络设备业务和控制策略，实现智能自动化控制支持对系统软硬件的内部事件、状态进行监控，出现问题时收集实时信息并自动修复将实时信息发送到指定服务器要求支持此功能，权威第三方机构的测试报告 |

## 3.6 交换机

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| ★产品架构 | 支持多级交换架构，能够配置独立的交换网板与独立的主控板，交换网板与主控板硬件槽位分离 |
| 业务板卡与交换网板采用完全正交设计（槽位互相垂直），跨线卡业务流量通过正交连接器直接上交换网板，背板走线降低为零，极大规避信号衰减，具备平滑演进能力。提供官网证明和实物正反面图片，指明槽位物理位置关系。 |
| 空间要求 | 采用紧凑型机框设计以达到更高的机房空间利用率，节约空间成本。 |
| ★业务插槽数 | 业务插槽数≥6 |
| 交换容量 | 153.6Tbps |
| 转发能力 | 36000 Mpps |
| 主控引擎 | 主控槽位与交换网板槽位宽度相同的全宽槽位，提供更好的扩展性和可靠性 |
| 电源冗余 | 电源模块冗余 |
| 关键部件热插拔 | 主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔 |
| ★接口要求 | 以太网支持千兆电口，千兆光口，万兆光口、万兆电口、40G端口、100G端口，提供官网链接 |
| 单槽位万兆端口密度≥48，提供官网链接 |
| 单槽位万兆电端口密度≥24，提供官网链接 |
| 单槽位40G端口密度≥ 24，提供官网链接 |
| 单槽位100G端口密度≥16，提供官网链接 |
| 单槽位能够同时提供千兆光口、千兆电口、万兆光口，且实际可用端口总数≥48，提高槽位利用率和业务可靠性，提供商用板卡公开手册的官网截图证明（24电+20光+4万兆） |
| 支持RPR接口，提供工信部权威第三方测试报告，提供官网配置手册截图和链接 |
| 支持POE+，满足新一代园区网以太网供电需求 |
| 支持FCoE接口 |
| 链路聚合 | 聚合组数≥128组，每组成员≥8个 |
| 支持跨设备链路聚合 |
| 支持对广播、组播、单播报文的均匀分担 |
| 支持链路聚合+ECMP情况也可以对报文均匀分担，即等价路由的链路是由聚合链路组成情况下的报文分担 |
| QOS | 每端口支持8个优先级队列，3个丢弃优先级，支持SP、WRR、SP+WRR三种队列调度算法 |
| 支持精细化的流量监管，粒度可达8K |
| 支持流量整形Shapping |
| 支持WRED拥塞避免 |
| 支持802.1p、TOS、DSCP、EXP优先级映射 |
| 可靠性 | 双引擎快速倒换，主备切换时候板内转发无丢包  |
| 支持NSF/GR for OSFP/BGP/IS-IS |
| 支持热补丁功能，可在线进行补丁升级 |
| 支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由。 |
| MAC | MAC表≥288K |
| MAC表≥1M，学习速率≥130K/S，提供工信部权威第三方测试报告证明 |
| 路由表 | 路由表≥256K |
| IPv4 FIB表项≥3M，IPv6 FIB表项≥1M，提供工信部权威第三方测试报告证明 |
| ARP | ARP表≥170K |
| ARP表项≥180K，学习速率≥1.1K/S，提供工信部权威第三方测试报告证明 |
| ★虚拟化 | 多虚一技术(N:1)，支持4框虚拟化技术，提供工信部权威第三方测试报告，提供官网配置手册截图和链接 |
| 一虚多技术（1:N），提供工信部权威第三方测试报告，提供官网配置手册截图和链接 |
| 支持多虚一技术和一虚多技术的配合使用，提供工信部权威第三方测试报告，提供官网配置手册截图和链接 |
| 支持远程端口扩展，作为控制设备（Controlling Bridge,CB）实现对端口扩展模块（Port Extender,PE）的集中控制，提供工信部权威第三方测试报告，提供官网配置手册截图和链接支持和配套的端口扩展模块虚拟成单一的逻辑设备，在管理层面实现单一节点管理；虚拟化能力≥30：1，即通过单一管理节点可实现超过30台物理设备的统一管理。整机支持的最大PE设备台数≥30 |
| 网络安全一体化 | 支持安全业务插卡FW、IPS、NSM、ACG、LB |
| ★有线无线一体化 | 支持AC板卡，POE，POE+，提供官网链接 |
| 支持WLAN配置，提供官网配置手册截图和链接支持原生的无线AC功能，无需独立的AC板卡或带AC功能的接口板，即支持无线AP管理功能。 |
| 支持有线无线一体化的终端准入认证 |
| MPLS | 支持L3 VPN |
| 支持VLL |
| 支持VLPS |
| 支持MCE |
| FCoE | 支持FCF模式转发，VSAN的创建及配置，支持FC地址的分配及WWN地址和FC地址的绑定等功能支持FLOGI/PLOGI和DCBX功能 |
| ★SDN/OPENFLOW | 支持OPENFLOW 1.3，提供工信部权威第三方测试报告，提供官网配置手册截图和链接支持普通模式和Openflow 模式切换支持多控制器（EQUAL模式、主备模式）支持多表流水线支持Group table支持Meter |
| 跨三层互联技术 | 支持主流的MAC in IP技术，如EVI/EVN/OTV等，实现跨三层网络的二层互联，提供工信部权威第三方测试报告，提供官网配置手册截图和链接 |
| VxLAN | 支持VxLAN 网关，提供工信部权威第三方测试报告，提供官网配置手册截图和链接 |
| 安全特性 | 支持IPv4 uRPF |
| 支持DHCP Snooping |
| 支持ARP防攻击 |
| 支持IP Source Guard |
| 支持CoPP |
| 支持广播风暴抑制 |
| 支持EAD |
| 支持IEEE 802.1ae介质访问控制安全技术，提供工信部权威第三方测试报告，提供官网配置手册截图和链接 |
| 支持端口隔离 |
| 支持IP+MAC+VLAN+PORT的绑定 |
| 支持报文过滤功能，黑洞路由、黑洞MAC |
| 管理特性 | 支持Console/AUX/Telnet/SSH2.0 |
| 支持风扇管理 |
| 支持电源管理 |
| 支持在线诊断 |
| 支持SNMPv1/v2 |
| 支持 SNMPv3 |
| 支持RMON(RFC2819) |
| 支持端口镜像 |
| 支持VLAN镜像 |
| 支持RSPAN |
| 支持流镜像 |
| NAS | 支持802.1x |
| 支持mac认证 |
| 支持Portal |
| 支持本地认证 |
| 支持Radius认证 |
| 支持Tacacs+认证 |
| ★配置要求 | 配置:千兆万兆混合单板（24电+20光+4万兆） |

# 四、商务要求

(1).技术需求中的要求，“★”的参数为实质性参数，不可负偏离

（2）.投标报价时需要提供原厂商针对本项目的授权、原厂商三年售后服务承诺书以及详细技术参数中所需要提供的各类截图并加盖原厂商公章的扫描件（签订合同前提供原件且必须与扫描件一致），否则视为无实质性响应。

 (2).供货的设备须进行安装调试，调试后保证设备能正常使用。