# **技术需求**

## 一、采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 单位 | 数量 | 备注 |
| 1 | 路由设备 | 台 | 1 |  |
| 2 | 智能DNS系统 | 套 | 1 |  |
| 3 | 入侵防御设备 | 台 | 1 |  |
| 4 | 数据库 | 套 | 1 |  |
| 5 | 应用服务器中间件 | 套 | 1 |  |

## 二、技术指标功能参数

### 1、路由设备

★1、整机交换容量≥800Tbps，包转发率≥195000Mpps，以官网列出最低值为准。提供产品官网截图证明材料并加盖厂家公章；

★2、为满足自主可控要求，要求设备的关键芯片为国产化，包括CPU、网络处理器（NP），内存，主控板等，其中CPU需满足安全可靠测评目录，需提供中国信息安全测评中心公布的安全可靠测评结果公告并加盖厂家公章；

★3、为实现灵活的新功能扩展及演进能力，设备需支持分布式转发架构，接口板包含NP(NetworkProcessor,网络处理器)芯片，支持单独的业务处理能力，提供产品截图证明材料并加盖厂家公章；

★4、支持ARP协议，ARP表项≥1M，支持ND协议，ND表项≥1M；提供产品截图证明材料并加盖厂家公章；

★5、支持交换网板≥4个，需提供设备面板图并加盖厂家公章；

★6、支持电源个数≥6个，独立风扇框≥3，且支持前后直通式风道，主控、网板、线卡板均支持前后通风，提供产品截图证明材料并加盖厂家公章；

★7、支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合，需提供产品截图证明材料并加盖厂家公章；

★8、为保障网络安全性，要求支持与BRAS设备一体化的安全业务插卡，如防火墙插卡等，需提供产品截图证明材料并加盖厂家公章；

★9、为满足业务硬隔离需求，设备需支持硬件切片技术最小颗粒度可达10Mbps，硬件切片粒度最小可支持10Mbps，支持10G、50G、100G的FlexE接口，支持10M、1G、1.25G、5G颗粒度FlexE切片，提供第三方测试报告并加盖厂家公章；

★10、设备支持确定性网络，端到端确定性时延的抖动范围≤20us；，需提供证明材料并加盖厂家公章；

★11、支持基于IPv4认证后的IPv6地址按需分配，需提供证明材料并加盖厂家公章；

★12、支持基于URL的白名单功能，联动DNS解析结果动态刷新，支持URL模糊匹配功能，需提供证明材料并加盖厂家公章；

★13、支持IPoE+Web认证和802.1x在同一接口下的共存，实现用户认证随选功能，提供第三方测试报告并加盖厂家公章；

★14、支持DHCP 地址池组功能，通过地址池配置不同的DHCP server地址和优先级，实现 DHCP server间灵活备份，当主用server故障不响应时可切换到备用server进行地址分配，提供第三方测试报告并加盖厂家公章；

★15、实配双主控，冗余1600W电源≥4个，万兆业务光口≥30个，万兆堆叠光口≥4个，万兆多模光模块≥10个，万兆单模光模块≥10个，满足≥50K接入用户数；

### 2、智能DNS系统

★1.所投产品符合国产化政策要求，在安全可靠测评名录中，并提供国产化CPU对应提供商出具的兼容性互认证书。标准2U设备，实配冗余电源，实配内存≥16G，实际配置≥8个千兆电口，实际配置≥4个千兆光口，实际配置≥2\*1TB硬盘，实际配置≥2个可扩展插槽。支持≥16万QPS能力。

★2、支持A、AAAA、CNAME、NS、MX、TXT记录； 支持在页面修改SOA配置，至少包括：默认TTL，管理员邮箱、默认NS、刷新时间；允许用户进行全局记录配置搜索；支持批量导入、启用/停用、修改记录；支持为发布的权威域在页面配置DNSSEC，通过页面操作直接生成DNSSEC密钥信息，包括：密钥标签、算法、指纹信息。支持CNAME4记录和CNAME6记录类型，实现在解析同一个域名时，指定不同类型（A/AAAA）时指向不同的CNAME结果；支持显性URL解析、隐性URL解析，将域名解析通过地址跳转和不跳转的方式下解析到任意URL（要求提供产品功能截图证明，加盖原厂公章）。

★3、支持递归解析，提供互联网域名解析服务，并支持DNS缓存功能，缓存解析过的域名记录，加速DNS请求响应；支持指定提供域名解析服务的范围，例如对来自外网的IP地址不提供解析服务；支持结果过滤功能，即当同时存在A和AAAA结果时，过滤掉其中的A结果或AAAA结果。支持对域名解析请求的限速；支持限制域名解析服务提供范围；支持DNSSEC验证。（要求提供产品功能截图证明，加盖原厂公章）

★4、支持DNS攻击防护，防护的攻击种类至少包括：DDoS攻击，DNS隧道攻击，DNS递归攻击，DNS缓存投毒、DNS反射攻击防护。支持对挖矿行为进行拦截，并对拦截记录进行日志记录、统计分析，定位到挖矿者源IP，内置挖矿域名库；支持威胁域名防护，内置威胁域名库；挖矿域名库和威胁域名库可以通过同厂商威胁情报分发平台提供在线更新服务。（以上几项要求逐项提供带有CNAS认可标识和CMA标记的第三方机构功能测试报告，并逐项提供产品功能截图证明，加盖原厂公章）

★5、支持使用标准SQL语句查询DNS日志，至少包括：SELECT语句、WHERE语句、GROUP BY语句；支持多维度复杂聚合查询，实现对DNS结构化日志各个字段的自定义聚合统计分析，提供DNS日志的高性能聚合分析平台。（要求提供产品功能截图证明，加盖原厂公章）

★6、支持DNS请求和响应日志记录，对每一次请求内容可通过日志详细记录和查询；支持日志滚动存储，可按天数滚动存储，可按百分比滚动存储、按绝对体积滚动存储；支持DNS日志、操作日志、运行日志通过Syslog形式输出到第三方。支持DNS响应日志的详细内容记录，字段至少包括：请求时间、用户源地址、域名、域名类型、线路或策略、集群、服务器IP、AA/TC/RD/RA/AD/CD标志位，支持日志字段的动态配置；（要求提供产品功能截图证明，加盖原厂公章）

★7、支持对系统运行状态指标进行监控和告警，指标项至少包括：CPU使用率、磁盘使用率、内存使用率、节点连接情况、节点网卡情况；支持对解析行为进行监控和告警，指标项至少包括：DNS缓存命中率告警、DNS查询超速告警、成功查询占比过低告警、域名解析失败人次/人数告警；支持多种告警方式，至少包括：外部推送，微信、邮件；系统自带微信告警平台，无需本地额外部署，用户提供手机号并关注微信公众号即可使用微信告警平台接收告警。（要求提供产品功能截图证明，加盖原厂公章）

★8、支持管理分析服务器的高可用部署，主管理端故障时，备管理端能够无缝衔接管理功能；用户通过统一虚拟IP进行访问，主备节点间数据自动同步，无需额外操作进行数据同步。（要求提供产品功能截图证明，加盖原厂公章）

★为保证产品为成熟可靠产品，本次所投产品生产厂家提供以下资质扫描件并加盖原厂公章：

9、软件开发能力认证CMMI 3级或以上资质

10、具备良好的产品质量管理体系，提供ISO 9001认证资质

11、具备良好的信息安全管理体系，提供ISO 27001认证资质

12、具备良好的信息技术服务体系，提供ISO 20000认证资质

13、具备良好的安全管理服务体系，提供ISO 45001 认证资质

14、具备良好的环境管理服务体系，提供ISO 14001 认证资质

### 3、入侵防御设备

1. ★产品为国产品牌，具备自主知识产权，专业性入侵防御设备而非NGAF、NGFW、UTM设备；
2. ★产品内置专业的入侵防御特征库，覆盖勒索、挖矿、webshell、僵尸网络、木马后门、蠕虫、信息泄漏、权限绕过、未授权访问、文件上传、文件读取、文件下载、文件包含、SSRF、XXE、CSRF、反序列化、代码执行、命令执行、XSS攻击、SQL注入、DOS等攻击类型，入侵防御特征数量至少在14000条以上；（提供第三方权威机构出具的CNAS或CMA的检测报告并加盖投标人公章）
3. 产品支持多种规则变更部署模式，至少包括自动防御模式、试运行模式和手动防御模式；（提供功能截图并加盖投标人公章）
4. 产品支持双向检测功能，根据双向流量检测攻击，输出检测结果包含正在利用、攻击成功，应支持HTTP请求/响应缓存；
5. 产品支持基于行为分析的C&C通道（隐蔽通道）检测机制，能够发现网络中的存在的隐蔽通道；
6. 产品内置智能分析能力，具备阻断的活动专项分析和综合威胁告警分析，其中阻断的活动应包括阻断的威胁、阻断的文件和阻断的IP专项分析；（提供功能截图并加盖投标人公章）
7. ★产品支持威胁分析功能，通过与威胁情报、全流取证、网络负载、内置解码工具、事件处理流程、事件性质判定等信息综合对威胁进行分析判断；（提供第三方权威机构出具的CNAS或CMA的检测报告并加盖投标人公章）
8. 产品支持告警处置，包含一键加白和临时封禁，并具备详细的处置记录包含处置时间、处置方式、处置动作等；
9. 产品支持针对网络入侵特征进行全面匹配 ，具备深度解析网络风险的能力；（提供第三方权威机构出具的相关技术证明文件并加盖投标人公章）
10. ★产品支持三权分立，不少于五种认证方式，至少包括密码、双因子认证、超级SIM认证等；（提供功能截图并加盖投标人公章）
11. 产品支持用户密码过期配置，同时在线用户数限制，唯一性检测，防暴力破解等安全访问配置；
12. ★设备制造商须具备数据安全服务能力-数据安全“评估”能力二级证书，能够针对入侵防御设备检测出的风险数据进行全面评估，为用户处置安全风险提供参考依据。

13、★标准2U机架设备，双冗余电源；采用国产化芯片及操作系统，配置不少于1个RJ45串口，1个带外管理口，1个HA接口，2个USB口，4个千兆电口，4个千兆光口，4个万兆光口，1个接口扩展槽位；配置内存不低于16G，内置不低于32G系统盘+128G固态硬盘；整机网络层吞吐量≥30Gbps，应用层吞吐量≥25Gbps，最大并发连接数≥500万，每秒新建HTTP连接数≥20万；提供三年IPS特征库升级授权，三年硬件维保服务。

### 4、数据库

★1、数据库须通过中国信息安全测评中心安全可靠测评，安全可靠等级需≥Ⅰ级，提供测评结果截图加盖原厂公章。

★2、数据库原厂商通过信息系统建设和服务能力CS4级(优秀级)和CNAS中国认可软件过程及能力成熟度评估（SPCA）L3级以上。提供证书复印件加盖公章。

★3、支持多种索引，包括B树索引、聚集索引、唯一索引、非唯一索引、函数索引、分区索引（包括本地分区索引和全局分区索引）、位图索引、位图连接索引、空间索引、数组索引；支持创建索引时指定表空间；支持设置索引可见和不可见；支持设置索引失效；支持重建索引；支持索引监控。提供权威检测机构出具的测试报告并加盖原厂公章。

★4、单表支持创建2048列；支持单表分区数量为65535个；支持分区键包含多列，列数最多达到16列。提供权威检测机构出具的测试报告并加盖原厂公章。

★5、在任意数据库实例出现故障时，集群内服务正常运行，数据不丢失，集群整体业务可用；在实例故障、节点故障等单数据库实例故障时，能实现零数据丢失（RPO＝0）和低于5秒的系统恢复时间（RTO＜5s）。提供权威检测机构出具的测试报告并加盖原厂公章。

★6、支持基于自主研发统一内核的多集群体系架构，在一套数据库产品内核代码上，实现了包括共享存储集群、分布式集群、大规模并行处理集群、读写分离集群、主备集群。提供权威检测机构出具的测试报告并加盖原厂公章。

★7、支持RAFT协议主备集群，具有主库故障集群自动选主，备库故障不影响业务运行特性，且支持影子副本。提供由工信部下属的专业测评机构出具的带有CNAS标识的测试报告并加盖原厂公章。

★8、产品拥有自主知识产权，完全自主可控，达到《信息技术产品自主原创测评要求》（试行）中的要求，且产品核心功能模块的核心源码自主代码比例不低于98%。需提供权威评测机构出具的核心源代码开源率证明及信息技术产品自主原创性测评证书（加盖原厂商公章）。

★9、兼容Oracle的DBA\_\*、ALL\_\*和USER\_\*开头的数据字典视图、系统包；兼容PL/SQL语法和数据操作；兼容Oracle、Mysql、SQLServer、DB2、PostgreSQL的常用系统函数；实现对数据查询语言（DQL)、数据操纵语言(DML)和数据定义语言(DDL)的兼容。提供权威检测机构出具的测试报告并加盖原厂公章。

★10、支持SM3，并可对秘钥进行集中管理；支持基于SM4算法的存储加密，支持数据加密存储，支持国密算法加密，支持全面加密，数据文件、日志文件、备份文件、导入导出文件等均支持透明加密；支持数据库级、表级、列级等不同级别加密，支持不同用户、不同列设置不同密钥。提供具有CNAS标识的权威检测机构出具的测试报告并加盖原厂公章。

### 5、应用服务器中间件

1、为适应信创需求。产品需通过《GCC 7004-2020-服务器应用场景测试方法 Web应用》性能评测,提供第三方权威机构颁发的《服务器典型应用场景性能评测证书》以及出具的相关测试报告，报告至少包括报告首页、测试关键内容页（含静态资源测试、动态资源测试、Web应用测试等）、测试结论等内容。

2、所提供的应用服务器中间件产品符合GB/T22239-2019《信息安全技术网络安全等级保护测评要求》(四级)身份鉴别、访问控制、安全审计、入侵防范、数据完整性、数据保密性、数据备份恢复、剩余信息保护技术要求。需提供等级保护测评服务认证资质的第三方机构的测评报告。提供的报告关键页需包含上述内容证明。

3、中间件产品提供适合PaaS平台部署的轻量级产品，提供支持SpringBoot内嵌中间件版本，支持SpringBoot1.x版本、SpringBoot2.x版本、SpringBoot3.x版本。提供5年以上中间件轻量级版本软件著作权证明。

4、支持国产化环境，如飞腾、龙芯、鲲鹏、海光、申威、兆芯等平台及麒麟、统信、中科方德等国产操作系统。支持国产数据库，如：神州通用、达梦、人大金仓、华为GaussDB、瀚高数据库等国产数据库，提供兼容互认证书。

5、支持EJB集群，EJB集群需要支持多种负载管理算法（支持简单轮转、加权轮转、随机、备份等负载均衡策略等）和故障EJB自动隔离功能；EJB容器支持除了IIOP之外的自主序列化协议。并取得以上数据传输方法的国家专利，提供专利官方网站网址、网页截图。

6、产品具备应用运行时自我保护安全防御机制，支持依据上下文及关键函数的参数等信息动态判断恶意攻击，实时进行安全阻断，内置常见安全漏洞防御选项，灵活配置防御策略，实现对多种攻击手段如SQL注入、命令注入、文件目录列表等进行检测和拦截，并记录攻击的细节信息备查，同时根据攻击事件，发现应用存在的安全漏洞，并提出修复意见。确保产品安全可靠，规避中间件产品的安全漏洞威胁，需支持用户认证、授权；三员分立；国密算法等。提供截图证明。