采 购 需 求

项目名称：新疆税务2025年网络安全设备采购及服务器

升级扩容项目（第一包：网络安全设备采购）

2025年4月

目录

[1项目概述 1](#_Toc11450)

[1.1项目背景 1](#_Toc23896)

[1.1.1项目目的、意义及背景 1](#_Toc12305)

[1.2项目内容 1](#_Toc9691)

[1.2.1项目建设思路 1](#_Toc26507)

[1.2.2采购内容 1](#_Toc12932)

[1.2.3项目实施要求 2](#_Toc30186)

[1.2.3.1实施范围要求 2](#_Toc375)

[1.2.3.2实施时间要求 2](#_Toc21896)

[1.2.3.3实施地点要求 2](#_Toc19802)

[1.3其他要求 2](#_Toc16703)

[1.3.1采购标的需执行的相关标准规范 2](#_Toc27952)

[2投标/响应要求 2](#_Toc17774)

[2.1对供应商的要求 2](#_Toc4021)

[2.1.1必备资质 2](#_Toc16976)

[无。 2](#_Toc5852)

[2.1.2优选资质/优选指标 2](#_Toc12813)

[2.1.2.1相关证书 2](#_Toc15407)

[2.1.2.2成功案例 2](#_Toc22555)

[2.1.3是否允许联合体 3](#_Toc11537)

[2.1.4是否专门面向中小企业 3](#_Toc27888)

[2.1.5其他要求 3](#_Toc1593)

[2.2技术部分投标/响应内容 3](#_Toc12319)

[2.2.1技术投标/响应总要求 3](#_Toc4062)

[2.2.2投标/响应方案要求 3](#_Toc23616)

[3项目需求 4](#_Toc26731)

[3.1总体要求 4](#_Toc4965)

[3.2采购产品一览表 4](#_Toc31160)

[3.3采购产品详细清单及技术指标 5](#_Toc20454)

[1.WEB应用防火墙（WAF） 5](#_Toc13592)

[2.漏洞基线扫描设备 6](#_Toc1217)

[3.网络回溯分析系统 8](#_Toc13495)

[4.日志审计 12](#_Toc12784)

[5.防火墙 14](#_Toc5414)

[6.交换机 17](#_Toc5206)

[3.4服务要求 18](#_Toc12291)

[3.5其他要求 19](#_Toc5686)

[4人员要求 19](#_Toc26908)

[4.1团队要求 19](#_Toc3160)

[4.1.1基本要求 19](#_Toc2441)

[4.1.2优选资质/优选指标 19](#_Toc27965)

[5管理实施要求 20](#_Toc16509)

[6风险管控要求 21](#_Toc23318)

[7履约验收要求 21](#_Toc24562)

[7.1总体要求 21](#_Toc24155)

[7.2具体要求 21](#_Toc23381)

[（一）到货验收 21](#_Toc24119)

[（二）最终验收 21](#_Toc213)

[8其他要求 22](#_Toc3356)

[8.1必备要求 22](#_Toc27153)

[8.1.1通用必备要求 22](#_Toc29507)

[8.2付款安排建议 22](#_Toc18219)

[8.3其他要求 23](#_Toc19941)

[8.3.1保密要求 23](#_Toc32659)

[8.3.2知识产权要求 24](#_Toc29030)

[8.3.3★供应链安全管理要求 24](#_Toc15876)

[8.3.4税务信息化服务商廉政相关要求 26](#_Toc3543)

# 

# 1项目概述

## 1.1项目背景

### 1.1.1项目目的、意义及背景

随着我局金税四期系统的上线、业务规模的不断扩大，互联网业务流量激增，对互联网出口安全设备造成了很大压力，目前数据中心互联网出口WEB应用防火墙（WAF)已出现运行缓慢现象，尤其在征期，严重影响业务的运行；网络回溯分析系统流量较大，峰值流量已经超过设备处理性能，已经造成采集链路中断、丢包、采集结果不完整等现象，影响分析数据的准确性；区局与地州市局之间2台防火墙，设备运行超过8年，性能严重不足，影响业务运行效率；为有效检测系统漏洞和操作系统合规性，需要一套基于原理的漏洞扫描和基线扫描设备；为做好网络安全日志、应用系统日志、运维日志等日志审计工作，需要一套综合日志审计平台，用以提高日志审计的准确性和效率；我局机关大楼楼层接入交换机运行已达15年，存在老化风险，需要进行逐步替换。为提高我局网络安全系统稳定运行，弥补安全管理系统方面的不足，计划采购一批网络安全设备。

## 1.2项目内容

### 1.2.1项目建设思路

更新替换现有性能不足的防火墙、WEB防火墙（WAF)、网络回溯分析设备、千兆交换机，改进现有设备的不足、提高系统运行效率；新增漏洞和基线扫描设备、日志审计设备，能够及时扫描系统安全漏洞及基线合规性检查，同时对网络安全日志、应用系统日志、运维日志等进行综合审计，消除现有网络安全系统中存在的风险隐患，确保网络安全系统稳定高效安全运行。

### 1.2.2采购内容

采购WEB应用防火墙（WAF)2台；漏洞基线扫描设备2台；网络回溯分析设备1台；日志审计设备1台；防火墙2台；千兆交换机4台。本项目预算为263万元。

### 1.2.3项目实施要求

#### 1.2.3.1实施范围要求

国家税务总局新疆维吾尔自治区税务局机房。

#### 1.2.3.2实施时间要求

2025年5月至10月。

#### 1.2.3.3实施地点要求

国家税务总局新疆维吾尔自治区税务局指定位置。

### 1.3其他要求

### 1.3.1采购标的需执行的相关标准规范

无。

# 2投标/响应要求

## 2.1对供应商的要求

### 2.1.1必备资质

#### 2.1.1.1供应商应遵守有关国家法律、法规和条例,具备《中华人民共和国政府采购法》第二十二条的规定和本文件中规定的条件。

#### 2.1.1.2本项目的特定资格要求

### 无。

### 2.1.2优选资质/优选指标

#### 2.1.2.1相关证书

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **证书名称** | **颁发部门** | **相关要求** |
| 1 | 无 | 无 | 无 |

#### 2.1.2.2成功案例

无。

### 2.1.3是否允许联合体

否。

### 2.1.4是否专门面向中小企业

本项目专门面向中小企业采购项目。

### 2.1.5其他要求

无。

## 2.2技术部分投标/响应内容

### 2.2.1技术投标/响应总要求

无。

### 2.2.2投标/响应方案要求

以下相关方案，若作为评审因素，则供应商应在满足★关键指标项要求的前提下，根据项目特点和采购需求，制定更为完整、详细、可操作性强的方案。

#### 2.2.2.1 项目需求理解

供应商须提供针对本项目的采购需求理解方案，方案内容要求包括但不限于项目的背景、服务用户、服务系统等方面的理解。

#### 2.2.2.2 项目集成实施方案

供应商须提供针对本项目的集成实施方案，方案内容包括但不限于集成总体方案、集成详细步骤、应急操作方案等内容。

#### 2.2.2.3 安全保障方案

供应商的安全保障方案应具有合理性、可行性等。包括但不局限于信息安全保障措施、安全管理制度等。要求安全保障符合要求，安全管理措施合理规范、安全管理制度细致完善。

#### 2.2.2.4 培训方案

供应商须按照本项目培训要求制定培训方案，内容包括但不限于培训组织、培训计划、课程安排、师资力量及相关保障措施等。

#### 2.2.2.5售后服务方案

供应商提供的售后服务方案内容详尽、完整，内容包括售后服务工作安排、售后服务响应、应急保障方案和措施等。

#### 2.2.2.6 验收方案

供应商必须按照本项目需求，详细阐述项目验收方案。根据需要验收的内容，提出切实可行的验收流程。

# 3项目需求

## 3.1总体要求

所投产品必须是原厂新品，须于合同签定后的50个自然日内全部到货，到货地点为国家税务总局新疆维吾尔自治区税务局指定地点；供应商应按照约定日期完成网络架构设计、综合布线、设备安装部署调试等集成服务。

## 3.2采购产品一览表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **产品类别** | **产品名称** | **数量** | **单位** | **备注** |
| 1 | 安全设备 | WEB应用防火墙（WAF） | 2 | 台 | 5年质保 |
| 2 | 安全设备 | 漏洞、基线扫描 | 2 | 台 | 5年质保 |
| 3 | 网络设备 | 网络回溯分析系统 | 1 | 台 | 5年质保 |
| 4 | 安全设备 | 日志审计 | 1 | 台 | 5年质保 |
| 5 | 安全设备 | 防火墙 | 2 | 台 | 5年质保 |
| 6 | 网络设备 | 交换机 | 4 | 台 | 5年质保 |

## 3.3采购产品详细清单及技术指标

采购文件（技术部分）中有标注★号的，为必备服务要求，必须满足，如未作出响应，将导致响应无效；#为重要服务内容、△为一般服务内容。

1.WEB应用防火墙（WAF）

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **指标种类** | **指标名称** | **指标内容** | **重要性** | **是否需要提供证明材料** |
| 1 | 基础参数 | 硬件规格 | ≥2U标准机架式设备，交流双电源，提供接口不少于2个USB口，1个GE管理口，4个千兆电口，4个千兆光口，4个万兆光口，提供1个接口扩展槽位。≥1T机械硬盘。 | ★ | 否 |
| 2 | 产品性能 | 网络层吞吐≥40G，应用层吞吐量≥20G； | ★ | 否 |
| 3 | 产品服务 | 五年产品系统升级、产品保修服务、远程支持服务、硬件故障上门等服务； | ★ | 是 |
| 4 | 产品功能 | 解码能力 | GZIP压缩流量代理。 | △ | 否 |
| 支持自定义规则检测前对请求进行解码，解码类型包括：Base64解码、十六进制解码等不少于5种，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 | △ | 否 |
| 5 | 策略配置 | 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）防护规则。 | △ | 否 |
| 6 | 支持基于WSDL文件来检测webservices请求的soap流量是否符合规则。支持防护XML实体攻击防护和XML DDOS防护。 | △ | 否 |
| 7 | 高可用 | 应支持紧急模式：支持配置CPU使用率、内存使用率、并发连接数阈值，当CPU使用率，内存使用率或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，对新增的请求直接转发；当恢复到阈值以内时，自动退出紧急模式。提供功能截图加盖厂家公章。 | # | 是 |
| 8 | WEB安全 防护 | 支持对XML文件进行基础合规检测，覆盖“节点个数、节点深度、节点名称长度”等；支持基于自定义的schema文件对XML文件进行更加细致的合规检测，能根据定义好的schema文件检测节点类型、属性类型等。提供功能截图加盖厂家公章。 | # | 是 |
| 9 | 同一域名/站点的SSL模块，同时支持国际标准https证书及国密证书，降低针对两种加密标准的国密改造难度。提供功能截图加盖厂家公章。 | # | 是 |
| 10 | 支持盗链防护，能够发现并阻断未经源网站允许的情况下，通过超链接引用源站内容。 | △ | 否 |
| 11 | 支持一键例外策略，降低误报。提供功能截图并且加盖厂家公章。 | △ | 是 |
| 12 | 在WAF上定期自动获取专家级、个性化的《WEB漏洞扫描报告》，自动生成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 | △ | 否 |
| 13 | 支持SSL证书卸载功能，支持国密算法，能够上传证书实现加密协议检测。并可查看SSL证书的有效期、签发者、序列号、域名、使用的站点，可以针对到期证书进行告警。 | # | 是 |
| 14 | 应支持OAS合规检测，支持编辑、导入、导出OAS文件，将OAS合规策略关联到防护站点，可展示OAS文件内容及相关告警。 | △ | 否 |
| 15 | 产品资质 | 产品资质 | 厂商应有成熟的信息安全工程服务资格、水平和能力，获得国家信息安全测评信息安全服务 资质证书-安全运营类二级、风险评估类二级、安全开发类一级资质证书。提供资质证书证明。 | # | 是 |

2.漏洞基线扫描设备

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **指标种类** | **指标名称** | **指标内容** | **重要性** | **是否需要证明材料** |
| 1 | 硬件要求 | 硬件基础要求 | ≥2U标准机架式设备，交流双电源，提供接口不少于2个USB口，2个GE管理口，6\*GE业务口（含3组bypass），4个万兆光口。≥4T机械硬盘。 | ★ | 是 |
| 2 | 分析能力 | 扫描结果分析 | 支持基于系统扫描的结果，下发Web深度扫描任务，能够针对Web和系统扫描的结果深入的进行风险综合分析； | △ | 否 |
| 3 | 漏洞储备 | 漏洞库要求 | 为保证漏扫效果，要求漏洞库数量30万+个，兼容CVE、CNVD、CNNVD、CWE、Bugtrap、微软KB等主流漏洞标准，并提供CNNVD兼容性证明；其中自研PoC漏洞数量 5000+ 个；要求提供截图。 | ★ | 是 |
| 4 | 管理能力 | 资产管理 | 支持对资产进行标签化管理，通过对资产自定义标签的方式，通过标签对资产进行筛选、编辑、下发任务等操作； | △ | 否 |
| 5 | 管理能力 | 任务下发 | 批量任务下发：支持划分不同的下级单位，为每个单位设置不同的用户权限，支持统一的为各下级单位下发资产风险检查任务；要求提供截图并加盖原厂公章。 | △ | 否 |
| 6 | 扫描能力 | 漏洞复测 | 支持对漏洞进行单个或批量复测，且支持查看复测结果；要求提供截图。 | ★ | 是 |
| 7 | 扫描能力 | web扫描 | 支持Web漏洞检查能力，包括但不限于SQL注入、XSS、CSRF、反序列化、LDAP注入、XPath注入、文件上传、水平权限绕过、信息泄露等； | △ | 否 |
| 8 | 扫描能力 | 主机扫描 | 主机扫描：并发主机数、主机存活探测强度（超时等待时长、最小/最大重试次数）、端口扫描强度； | △ | 否 |
| 9 | 扫描能力 | 扫描能力 | 支持漏洞内置为漏洞原理扫描插件，能够有效的提高漏洞检测速度，具有高准确性；具备高质量原理扫描插件，覆盖主机漏洞，Web应用漏洞，虚拟化、物联网、大数据组件、国产化、API等新型环境漏洞，重大保障漏洞，弱口令等；对于匹配到的漏洞，会自动执行相应的脚本，模拟攻击者的行为，触发漏洞。要求提供产品截图。 | ★ | 是 |
| 10 | 分析能力 | 策略模版 | 支持在系统内置的扫描策略基础上自定义扫描策略模板，支持自定义模板增加、删除、编辑、查询功能；支持批量删除自定义扫描策略模板；要求提供产品截图。 | ★ | 是 |
| 11 | 管理能力 | 登录认证 | 支持登录录制认证方式，通过对网站登录操作行为录制，保证录制文件持续登录的有效性，需要开启模拟浏览器爬虫功能； | △ | 否 |
| 12 | 分析能力 | 任务执行 | 支持对指定的IP、IP段、B/C整段、CIDR等形式的扫描任务实现立即执行，定时执行，每天、每周、每月的周期执行扫描任务；支持自定义可扫描和禁止扫描的时段，可分钟级设置允许扫描时间； | △ | 否 |
| 13 | 管理能力 | 断点扫描 | 支持停止、暂停扫描任务（手动/自动），停止后可重启任务，暂停后可断点续扫； | △ | 否 |
| 14 | 管理能力 | 消息策略 | 支持针对业务信息的消息策略配置，包含且不限于危险漏洞提醒、复现漏洞提醒、多次暴露漏洞提醒、高权重资产出现漏洞、敏感端口开放等； | △ | 否 |
| 15 | 扫描能力 | 大数据组件扫描 | 支持大数据组件漏洞扫描能力，包含且不限于：Hadoop、ElasticSearch、Redis、Memcache、Ambari、Cassandra、Flume、Hbase、Hive、 Impala、Kafka、Oozie、Spark、Storm、Yarn、Zookeepe等； | △ | 否 |
| 16 | 管理能力 | 消息策略 | 支持针对日志信息的消息策略配置。包含且不限于任务动态、报表动态、升级信息等； | △ | 否 |
| 17 | 管理能力 | 盲打平台 | 支持盲打平台反连配置，fastjson、SSRF、log4j、代理未授权等需要反向连接确定的漏洞； | △ | 否 |
| 18 | 管理能力 | 统计分析 | 支持针对任务的情况进行分析，包括且不限于针对不同扫描策略下发扫描任务的数量分布、最大并发任务数统计、新发现的漏洞数量趋势分析、新发现的资产数量趋势分析、存在漏洞的任务；要求提供截图并加盖原厂公章。 | # | 是 |
| 19 | 管理能力 | 统计分析 | 支持多个任务扫描结果进行统计分析，包括扫描目标数/存在风险的目标数、漏洞总数、待修复的漏洞总数； | △ | 否 |
| 20 | 管理能力 | 统计分析 | 支持基于渠道调用、消息类型、渠道消息发送趋势等维度进行分析； | △ | 否 |
| 21 | 管理能力 | 报表管理 | 内置扫描任务报表、基线检查报表、资产报表、漏洞报表、对比报表和自定义报表模板；自定义的维度包括且不限于资产（主机存活性、主机指纹、端口、Web指纹等）、漏洞（修复方案、CVSS评分、漏洞细节、漏洞描述、漏洞危害、影响范围等）进行筛选； | △ | 否 |
| 22 | 管理能力 | poc管理 | 支持展示自定义 PoC 的概要信息，包含漏洞名称、漏洞等级、漏洞详情；支持单个 PoC 的编辑、删除操作； | △ | 否 |
| 23 | 核查能力 | 基线核查 | 支持基线核查类型包括操作系统、中间件、虚拟化容器、数据库等；  支持覆盖标准包括但不限于CIS、等保等；  应支持基线覆盖范围：  1、支持操作系统基线包括但不限于：Linux、Windows、Windows Server、 Ubuntu、 CentOS、 Red Hat、SUSE、BC-Linux等；  2、支持国产化操作系统基线包括但不限于：统信UOS、银河麒麟、优麒麟、红旗Linux、深度Deepin、中标麒麟（NeoKylin）、华为欧拉（openEuler）、中科方德、鸿蒙HarmonyOS、中兴新支点等；  3、支持中间件包括但不限于：宝兰德、Weblogic、Apache、NGINX、Tomcat、‌东方通TongWeb、‌金蝶云星瀚中间件、‌中创软件(CreateSOFT)、‌中科软SkyForm、‌浪潮Inspur Middleware、‌华为中间件、‌阿里巴巴Cloud Middleware‌等  4、支持数据库包括但不限于：Oracle、MySQL、Mongo DB、Golden DB、‌人大金仓、TDSQL、‌TiDB、‌达梦数据库等。 | # | 是 |

3.网络回溯分析系统

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **指标种类** | **指标名称** | **指标内容** | **重要性** | **是否需要证明材料** |
| 1 | 总体要求 | 信创  要求 | 支持国家信创要求， 系统主要组件为国产化产品（CPU，操作系统）。设备CPU 需在如下范围：海光、鲲鹏、飞腾、龙芯、兆芯、申威；操作系统需在如下范围：麒麟、统信、openEuler。 | ★ | 是 |
| 自主知识产权 | 协议识别和解码技术为自主研发，拥有自主知识产权，具有国家专利和著作权。（提供国家专利证书或软件著作权证书复印件并加盖公章）  系统内置自主产权的数据包解码器。不允许使用国外商用解码器。支持安装在本地国产化操作系统平台进行数据包快速解码分析，支持对国产化平台进行数据包抓包分析，能够详细解码展示2-7层协议的各个字段明细，直观提示数据交互过程中的丢包、重传、乱序、时延等情况。支持Base64、URL、HEX、Unicode编转码功能、IP地址地理位置与经纬度查询功能、MAC地址扫描功能（提供功能截图）。 | ★ | 是 |
| 2 | 性能要求 | 设备性能 | 网络流量分析设备，采集端口：2个万兆光口和4个千兆光口；管理通讯端口：2个10/100/1000M以太网网络接口。  处理性能不得低于:10Gbps，数据包处理能力不低于300万pps，满足至少64TB的数据存储空间。（提供产品正式的技术规格表或规范书等类似材料截图做证明） | ★ | 是 |
| TCP/UDP会话处理能力不低于每秒80万。 | # | 是 |
| 3 | 部署及流量采集方式 | 系统架构及数据采集方式 | 系统为C/S架构或B/S架构，由专用的采集服务器和分析控制台组成，为保证数据安全，控制台和服务器之间数据传输加密（提供产品功能截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | # | 是 |
| 系统支持将物理流量采集接口根据VLAN、MPLS VPN、NETFLOW、GRE、网段、GENEVE、OPCODE创建子接口，并支持将划分的子接口进行逻辑子链路聚合分析。支持在物理采集接口下自定义识别特征。支持是否对物理流量采集接口启用GRE私有格式解码。（提供产品功能截图并加盖供应商公章）。 | # | 是 |
| 支持数据包去重功能，能够将通过镜像引入设备的流量中的重复数据包去除，数据包去重功能不影响设备的处理性能。 | △ | 否 |
| 系统支持对镜像流量数据整形或过滤能力。要求可根据IP地址、端口、应用、IP子网等对特定镜像流量实现丢弃，有效剔除不符合期望的业务流量，减轻设备处理负担。 | △ | 否 |
| 支持原始通讯数据包回放，能够将已捕获的数据包文件在系统上进行回放分析。回放数据包格式包括并不限于：cap、pcap、TRC0、TRC1、dmp等主流数据包格式，且支持的数据包格式不少于14种。 | # | 是 |
| 支持MPLS虚链路分析，能够根据MPLS VRF TAG设定虚链路，实现对特定MPLS链路的分析。支持VLAN虚链路分析，能够根据VLAN ID设定虚链路，实现对特定VLAN流量的分析。 | △ | 否 |
| 支持GRE虚链路分析，能够根据GRE设定虚链路，实现对特定GRE流量的分析。支持IP网段虚链路分析，能够按IP地址范围设定虚链路，实现对特定IP网段的独立流量分析。 | △ | 否 |
| 支持NETFLOW虚链路分析，能够根据NETFLOW设定虚链路，实现对特定NETFLOW流量的分析。支持VxLAN虚链路分析，能够根据VxLAN ID设置虚链路，实现对SDN网络特定VxLAN流量的分析。 | △ | 否 |
| 支持Agent工作模式，当Agent与回溯服务器建立连接时，Agent主动连接回溯服务器Agent网卡主动向回溯服务器进行流量转发。 | △ | 否 |
| 支持分别基于外层VLAN和内层VLAN分别统计数据。统计信息应包括但不限于外层VLAN、内层VLAN、总吞吐量、网络时延、丢包率、响应时间等数据（提供产品功能管理界面截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | # | 是 |
| 4 | 原始数据捕获保存 | 数据采集方式 | 支持对网络通讯流量进行采集存储，实现故障流量的追溯能力，数据包以专用格式存储，只能采用专用的控制台软件读取和导出，不能用其他工具读取并导出，且数据提取过程应支持SSL加密。 | # | 否 |
| 能实时长期保存网络中的所有的网络总体流量统计数据包括比特率（上下行）、数据包率（上下行）、网络中TCP SYN数量、TCP SYN ACK数量、TCP SYN RST数量，总体流量统计数据要求能保存至少1个月。 | # | 否 |
| 能实时分析并长期保存网络中的所有数据流统计数据，包括详细的IP会话流、TCP会话流、UDP会话流数据，数据精度到秒级，数据流统计数据要求能保存至少1个月。 | # | 否 |
| 支持数据包截断存储，可以设定捕获并保存数据包的长度大小，如64bytes，只保存数据包的前64个字节，要求能够按照不同自定义应用分别设置数据包截断长度。在设置数据包截断存储后，系统应按数据包原始长度进行相关统计分析，不能影响流量统计的准确性。 | # | 否 |
| 5 | 网络通讯数据统计分析 | 网络通讯数据统计分析 | 能够对交易性能指标进行1秒级精度统计监控，包括对每秒交易处理数量、交易处理时间、交易响应时间等指标趋势图统计（提供产品功能截图证明并加盖供应商公章）。 | # | 是 |
| 能够对任意时段指定应用的服务质量关键指标进行分析，服务质量关键指标应当包括：总字节数、上行/下行字节数，总数据包、上行/下行数据包，传输效率、上行/下行传输效率，平均/最大用户响应时间，客户端/服务器平均重传时延，TCP数据包（TCP同步包，TCP同步确认，上行/下行TCP重置包），TCP连接请求无响应次数、TCP连接请求被重置次数，RTT（客户端、服务器端RTT），重传率、分段丢失率，会话数量（新建会话数量，关闭会话数量，活动会话数量），TCP 0窗口数量（客户端/服务器TCP 0窗口数量，交易处理数量（TCP交易总数、TCP 交易无响应次数、TCP交易无响应率），响应时间（平均/最大/最小响应时间），adepx指数等，监控指标不得低于180种，所有指标需支持1秒精度刷新。（提供产品功能截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | # | 是 |
| 要求能够统计分析并展示IP地址、IP会话、TCP/UDP详细会话信息，且针对任意时间段内会话信息最大统计分析及展示条目不得低于50万条。 | △ | 否 |
| 6 | 数据流还原分析 | 数据流还原分析 | 提供针对TCP/UDP会话的流重组功能，将会话中的数据流重组显示。 | △ | 是 |
| 支持对链路IP会话进行回溯分析，分析指标包括但不限于以下类型：总字节数、会话创建/持续/结束时间、端点1/端点2发送负载数据包数、连接建立客户端/服务器重置次数、连接建立客户端/服务器无响应率、TCP同步重传包、TCP同步确认重传包、TCP分段丢失率、TCP重复确认包、三次握手次数、三次握手平均时间、上行/下行传输效率、客户端/服务器平均/最小窗口大小、客户端/服务器三次握手最小/平均/最大RTT、客户端/服务器平均/最大重传时延、服务器响应平均/最大传输时间等。分析精度至少支持1秒级。 | # | 是 |
| 全面支持视频监控/视频会议等基于Voip的视频质量分析，能够识别基于RTP协议的通讯流量，能够对H.323、H.264等分析，支持快速统计、展示出选中时间段（1秒级精度）内的总流量、峰值流量、呼叫数量、呼叫时长、视频最大MoS、视频平均MoS、视频最小MoS等。 | △ | 否 |
| 7 | 识别及解码 | 识别及解码 | 内置应用识别库，能够识别的互联网应用数量不少于1500种。 （提供产品功能截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | # | 是 |
| 系统内置自主知识产权的专家分析系统，能够对采集的2～7层数据进行智能分析，能够针对单个TCP会话进行数据流分析，支持根据TCP交易、数据包数、交易处理时间、服务器响应时间、客户端空闲时间、客户端传输时间、重传次数等进行指标排序，支持升序和降序排序。支持根据TCP交易自定定位到相应的数据包时序图。（提供产品功能截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | △ | 是 |
| 系统内置智能诊断功能,能自动诊断包括:HTTP 错误、SMTP/POP3服务器慢响应、SMTP/POP3 服务器返回错误、FTP 服务器慢响应、FTP 服务器错误、TCP 连接被拒绝、TCP 非法校验和、TCP重复的连接尝试、TCP 头部偏移错误、TCP SYN 带数据、IP TTL太小、IP 地址冲突、路由环路、H.323接入拒绝、H.323带宽拒绝、H.323呼叫失败、SIP服务端错误、SIP客户端授权验证错误、SMTP可疑会话、TCP头部偏移错误、TCP SYN风暴、TCP SYN带数据等常见故障场景。（提供产品功能截图并加盖供应商公章） | △ | 是 |
| 8 | 应用自定义 | 应用自定义 | 支持灵活的应用自定义，可通过IP、IP范围、IP+端口、端口、URL、数据流特征值、网络协议等方式自定义应用并对其性能指标进行1秒级精度流量监测及性能指标分析。（提供产品功能截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点。） | # | 是 |
| 支持以IP地址/地址组/地址范围、端口组或端口范围定义应用。 | △ | 否 |
| 支持对应用添加标识/备注信息。标识/备注信息可以被数据检索、过滤和应用告警时调用，提升数据使用效率。且支持批量修改应用定义存包长度。提供产品功能管理界面截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | # | 是 |
| 支持根据不同业务响应快慢特点，自定义应用响应快和慢时间。 | △ | 否 |
| 支持自动化应用定义，可通过对接CMDB信息，DNS设备、负载均衡、Nginx代理服务等设备配置数据，实现自动更新、维护、定义应用，支持通过特定字段标识出自动定义的应用配置，需要与手动添加的配置做区分（提供产品功能管理界面截图并加盖供应商公章）。 | # | 是 |
| 支持重复和包含关系。业务对外提供多个端口服务时，能独立定义每个服务，也能同时组合多个服务定义一个全应用。重复和包含定义不影响数据统计，可以多维视角剖析业务运行状态，为故障定位和分析提供数据支撑提供产品功能管理界面截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | △ | 是 |
| 支持将多个应用定义为应用组。应用组自行计算指标，流量，连接数等累计指标自动进行累加，响应时间，丢包率等平均指标。 | △ | 否 |
| 9 | 应用监控分析 | 应用监控分析 | 能够对任意时段指定应用的服务质量关键指标进行分析，分析指标包含如下内容：总流量（总流量、上行流量、下行流量）、数据包（总数据包、上行数据包、下行数据包）、TCP数据包（TCP SYN，TCP SYN ACK，上行TCP重置包、下行TCP重置包）、TCP连接请求无响应次数、TCP连接请求被重置次数、RTT（客户端、服务器端RTT）、TCP ACK时延（客户端ACK时延、服务器ACK时延）、重传数量（上下行重传数量、上下行TCP分段丢失数量、上下行TCP重复确认数量）、重传率、分段丢失率、会话数量（新建会话数量，关闭会话数量，活动会话数量）、TCP 0窗口数量（客户端TCP 0窗口数量、服务器TCP 0窗口数量）、交易/应用/业务处理数量（总数、请求数量、响应数量）、响应时间（平均响应时间，最大响应时间，最小响应时间），支持的服务关键指标项至少100个。 | △ | 否 |
| 10 | TCP应用交易分析 | TCP应用交易分析 | 提供数据库交易分析，可以通过图形化界面对Oracle、Redis、Mongo、Mysql、PGsql、cache等数据库进行[自动识别交易](mk:@MSITStore:C:\\Program%20Files%20(x86)\\Colasoft%20CSRAS%20Console%205.3\\mui\\zh_cn\\csrasc.chm::/html/db_auto)、[响应时间](mk:@MSITStore:C:\\Program%20Files%20(x86)\\Colasoft%20CSRAS%20Console%205.3\\mui\\zh_cn\\csrasc.chm::/html/db_response)、[交易时间](mk:@MSITStore:C:\\Program%20Files%20(x86)\\Colasoft%20CSRAS%20Console%205.3\\mui\\zh_cn\\csrasc.chm::/html/db_db_transtime)、[自定义交易](mk:@MSITStore:C:\\Program%20Files%20(x86)\\Colasoft%20CSRAS%20Console%205.3\\mui\\zh_cn\\csrasc.chm::/html/db_define)和[字段配置](mk:@MSITStore:C:\\Program%20Files%20(x86)\\Colasoft%20CSRAS%20Console%205.3\\mui\\zh_cn\\csrasc.chm::/html/db_char)进行设置和统计。 | △ | 是 |
| 提供HTTP交易分析，可以通过图形化界面对HTTP进行[自动识别交易](mk:@MSITStore:C:\\Program%20Files%20(x86)\\Colasoft%20CSRAS%20Console%205.3\\mui\\zh_cn\\csrasc.chm::/html/db_auto)、[响应时间](mk:@MSITStore:C:\\Program%20Files%20(x86)\\Colasoft%20CSRAS%20Console%205.3\\mui\\zh_cn\\csrasc.chm::/html/db_response)、[交易时间](mk:@MSITStore:C:\\Program%20Files%20(x86)\\Colasoft%20CSRAS%20Console%205.3\\mui\\zh_cn\\csrasc.chm::/html/db_db_transtime)、[自定义交易](mk:@MSITStore:C:\\Program%20Files%20(x86)\\Colasoft%20CSRAS%20Console%205.3\\mui\\zh_cn\\csrasc.chm::/html/db_define)和[字段配置](mk:@MSITStore:C:\\Program%20Files%20(x86)\\Colasoft%20CSRAS%20Console%205.3\\mui\\zh_cn\\csrasc.chm::/html/db_char)进行设置和统计。 | △ | 是 |
| 提供SSL交易分析，可以通过图形化界面对SSL连接和SSL认证的响应时间、交易时间进行设置和统计。 | △ | 是 |
| 能够分类统计指定应用的通讯对象的应用交易处理状况，统计分类应当包括：客户端、服务器、网段统计、交易统计、应用交易日志等。 | △ | 是 |
| 11 | 流量监控警报 | 流量监控警报 | 支持异常访问警报，可按IP、端口、应用及协议元素定义访问规则，支持设置默认为允许或拒绝动作，支持设置规则优先级别。警报触发精度至少包括1秒、10秒、60秒、5分钟、1小时。（提供产品功能截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | △ | 是 |
| 能够实现对链路关键参数的基线报警。可自动计算链路的流量基线，通过设定流量和基线的偏移量产生警报。警报触发精度至少包括1秒、10秒、60秒、5分钟、1小时。（提供产品功能截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | △ | 是 |
| 支持突发警报，突发警报类型至少包括：链路突发警报、应用突发警报、网段突发警报、应用服务器突发警报、应用交易突发警报、交易突发警报、子链路突发警报。能够根据比特率、比特率峰值、比特率谷值、新增会话数、IP广播流量、IP组播流量、总利用率、交易总数等指标进行条件设置，支持自定义持续时间内与第一个时间点前N个历史数据对比，支持自定义突增百分比和基线数据偏差比。（提供产品功能截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | △ | 是 |
| 能够对TCP/UDP数据流进行监测，通过定义特征值，监测异常的TCP/UDP通讯并产生警报，特征值可以包括十六进制和ASCII的特征定义。警报触发精度至少包括1秒、60秒。 | △ | 是 |
| 12 | 报表功能 | 报表功能 | 系统具有报表功能，能够生成所见即所得的报表。支持自定义报表功能，能够根据需要组合各个报表组件按需生成报表。 | △ | 是 |
| 支持数据巡检能力，周期性巡检数据中的隐患事件，可基于业务、线路等制定不同的监测场景和监测阈值，实现对互联网链路、广域网链路、外联链路、网络区域、TCP应用、DNS应用、HTTP应用、HTTPS应用等对象的定期巡检并生成巡检报告（提供产品功能管理界面截图并加盖供应商公章）。 | # | 是 |
| 支持报表计划管理，能够按计划自动生成指定的报表，报表生成频率包括：每小时、每天、每周、每月。支持计划报表自动发送到指定电子邮件接收者。 | △ | 是 |
| 支持生成比对报表，可将报表周期内的数据与历史同期或指定的其他时段数据进行比对，并在同一报表内容中展现。例如：日报表可与前一日或上周同天数据比对。 | △ | 是 |
| 报告支持筛选数据时间段，例如：08:00-18:00（提供产品功能管理界面截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | △ | 是 |
| 表格类组件支持差异分析，可同比/环比对比历史数据（提供产品功能管理界面截图并加盖供应商公章，功能截图必须清晰标明参数中要求的功能点）。 | △ | 是 |
| 13 | 异常安全威胁流量分析 | 异常安全威胁流量分析 | 提供ARP攻击分析视图，通过流量特征主动过滤疑似感染ARP病毒的主机列表，并在单独的分析视图中展现。 | △ | 否 |
| 支持自动判断存在DOS攻击或被攻击现象的主机的网络行为特征并在单独的分析视图中展现。 | △ | 否 |
| 支持自动判断存在TCP端口扫描的主机的网络行为特征并在单独的分析视图中展现。 | △ | 否 |
| 支持自动判断存在TCP端口扫描的主机的网络行为特征并在单独的分析视图中展现。 | △ | 否 |
| 14 | 第三方接口 | 第三方接口 | 能够提供数据访问接口，可以将服务器捕获到的数据提供给第三方系统进行二次开发，数据访问接口采用HTTP和HTTPS协议。 | △ | 否 |
| 15 | 产品资质要求 | 产品资质要求 | 产品必须有公安部安全与警用电子产品质量检测中心颁发的《网络安全专用产品安全检测证书》。 | # | 是 |
| 16 | 售后服务要求 | 售后服务要求 | 要求原厂提供五年内免费硬件设备质保、五年内免费软件升级。 | ★ | 是 |
| 17 | 其他要求 | 其他要求 | 在中标公示后，中标方必须在5个工作日内提供设备现场对招标的详细技术要求验证测试，若发现虚假应标，直接取消中标资格。 | ★ | 否 |

4.日志审计

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **指标种类** | **指标名称** | **指标内容** | **重要性** | **是否需要证明材料** |
| 1 | 核心指标 | 设备参数 | ≥标准2U设备，8个千兆电口，4个万兆光口，1个IPMI远程管理口，1个console口，6个USB接口，冗余电源，64G内存，480GSSD系统盘，数据盘4T\*4，Raid5，日志采集处理速度20000EPS，包含500个日志源授权。  硬件5年维保 | ★ | 否 |
| 2 | 重要指标 | 系统性能 | 数据存储能力：压缩加密存储，压缩比不低10:1；日志存储不低于10000条/M ；  支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于10s； | # | 否 |
| 3 | 重要指标 | 采集方式 | 支持Syslog、SNMP Trap、Netflow、JDBC、WMI、FTP、SFTP、SCP、kafka、文件等方式进行数据采集；支持通过Agent采集日志数据 | # | 否 |
| 4 | 重要指标 | 数据存储 | 对所管理设备的日志原始数据完整存储，支持数据本地集中存储； | △ | 否 |
| 5 | 一般指标 | 报表管理 | 基于时间轴展示数据分布，能够通过时间轴进行查询分析。智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应。 | △ | 否 |
| 6 | 重要指标 | 数据采集 | 1：支持对日志流量非常大但是日志重要程度低的syslog类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集； 2：支持实时自动刷新每个日志源的实时日志列表，支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志； 3：对于尚未支持的设备类型日志进行新增采集支持，在页面上传升级文件或增加配置文件即可；  支持主动、被动相结合的数据采集方式； 4：支持独立展示每个被采集源最近24小时的日志数量趋势，便于掌握设备的安全事件情况，支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态； | △ | 是 |
| 7 | 重要指标 | 数据存储 | 1：支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为1个月、3个月、6个月和永久保存等参数； 2：支持对所管理设备的日志原始数据完整存储，支持数据本地集中存储。 | △ | 是 |
| 8 | 一般指标 | 数据查询 | 1：支持为不同类型日志设置不同的查询条件和显示条件； 2：支持首页以全国地图、全球地图展示最近24小时日志访问源和访问目的的分布，能根据颜色区分访问来源和访问目的数据量大小，能够通过首页地图快速下钻查询指定区域的日志详细信息； 3：支持展示日志查询情况，包括查询条件命中数、日志总量、查询耗时等信息； 4：查询结果支持分页显示；  支持查询结果格式化日志、原始日志导出； 5：支持在日志查询结果上针对源IP、目的IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源IP和目的IP（公网地址）还支持以中国地图、世界地图方式展示，在统计图上能够进行点击下钻查询对应条件的日志结果； 6：支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析； | △ | 是 |
| 9 | 重要指标 | 告警管理 | 支持根据告警级别、告警规则类型、规则名称、时间范围、事件名称、设备IP、源IP、目的IP等方式快速检索安全事件告警，检索结果支持Excel等格式导出； 支持基于时间轴展示告警数据分布，能够通过时间轴进行查询分析； | # | 是 |
| 10 | 重要指标 | 日志源管理 | 1：支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息； 2：支持按照日志源名称、IP地址、日志源类型、接受时间及状态等维度对日志源列表进行排序；  支持为日志源指定类型、名称、IP地址、收集节点、收集方式、以及日志源启停状态等属性信息； 3：支持日志源在线状态监测告警，实时监测日志源的可用性，可显示每个日志源采集日志的最近时间，实时展示每个日志源最近一天日志趋势变化； 4：支持基于拓扑图的日志源相关数据信息快速查看；支持通过拓扑下钻查看对应日志源的日志、报表、告警数据。 5：支持以业务角度将日志源进行分组，支持在日志查询时以业务组进行查询，支持在首页拓扑展示时以业务组进行展示； | # | 是 |
| 11 | 一般指标 | 系统管理 | 2:系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。  1:支持将常用IP地址或IP地址网段标记为自定义名称，在日志查询界面可以在IP列中对应悬浮显示自定义名称； | △ | 是 |
| 12 | 一般指标 | 告警响应方式 | 支持邮件、Snmp Trap、声音、声光、短信、一信通响应、数据库响应等多种告警方式，支持报警内容引用字段变量参数。 | △ | 否 |
| 13 | 一般指标 | 统计报表管理 | 1:系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应； 2:支持自定义统计日志数据形成报表，支持统计分析报表以PDF、word、execl、html等方式导出；支持实时报表、计划报表。 | △ | 是 |
| 14 | 重要指标 | 产品资质 | 1:产品获得中国信息安全测评中心颁发的《信息技术产品安全测评证书》，需符合GB/T 18336-2015《信息技术 安全技术 信息技术安全评估准则》，并提供完整的评估技术报告复印件； 2:产品获得中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》，需符合GB/T 20945-2013《信息安全技术 信息系统安全审计产品技术要求和测试评价方法》（增强级），并提供完整的检测报告复印件； 3:产品获得中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》，需符合GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》，并提供完整的检测报告复印件； | # | 是 |

5.防火墙

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **指标种类** | **指标名称** | **指标内容** | **重要性** | **是否需要证明材料** |
| 1 | 核心指标 | 设备参数 | 1：≥标准2U设备,内存32G，机械硬盘4T，1个MGMT口，1个HA口，冗余电源，支持扩展槽位；  2：防火墙吞吐≥50G，并发连接≥1200万，每秒新建连接≥36万；应用层吞吐量40G，FW+IPS吞吐量8G，FW+AV吞吐量10G，FW+WAF吞吐量4G，全威胁吞吐量6G，IPSEC VPN吞吐3G，IPSEC VPN隧道数2000，SSL VPN吞吐2.5G，SSL VPN并发用户数5000 。  3：≥四个千兆电口，≥四个千兆光口，≥四个万兆光口；  4：≥四个千兆多模光模块，≥四个万兆多模光模块；  5：产品硬件保修≥5年；提供原厂出具的售后服务承诺函并加盖原厂公章。 | ★ | 是 |
| 2 | 重要指标 | 工作模式 | 支持路由、交换、虚拟线、Listening、混合工作模式； | # | 是 |
| 3 | 重要指标 | 路由交换 | 支持根据入接口、源/目的IP地址、协议、用户、应用、探测等多种条件设置策略路由；支持多种地址转换，支持源/目的NAT、双向NAT、NoNAT转换方式；支持源IP转换同一性；支持端口块地址转换和EIM地址转换 | # | 是 |
| 4 | 重要指标 | 链路聚合 | 支持链路聚合，可根据源/目的mac、源/目的IP、源/目的端口、五元组（指源IP地址，源端口，目的IP地址，目的端口和传输层协议）、端口轮询等条件提供不少于6种链路负载算法； | △ | 否 |
| 5 | 重要指标 | 访问控制 | 支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、高级威胁防护、WAF、邮件安全、数据过滤、文件过滤、僵木蠕防御、审计、数据库防护、防代理、APT等功能配置,简化用户管理；应逐项提供截图证明。 | # | 是 |
| 6 | 重要指标 | 访问控制 | 访问控制策略执行动作支持放行、阻断、认证、收集，对需要认证的流量进行Web认证，策略中可设置用户 Web 认证的门户地址或收集策略流量访问记录，生成更细粒的策略；应逐项提供截图证明，提供具备CNAS标识的关于“策略自学习”的产品功能检测报告 | # | 否 |
| 7 | 核心指标 | IPV6 | 具备IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；具备IPv6域名控制，具备对多级域名进行控制，域名对象具备通配符（需提供IPv6 Enabled Security Logo认证证书） | ★ | 是 |
| 8 | 一般指标 | 内容过滤 | 支持基于http、ftp、telnet、smtp、pop3协议的内容过滤策略，可对FTP上传/下载的文件名进行过滤，同时支持过滤FTP信令 | △ | 否 |
| 9 | 一般指标 | 高级威胁防护 | 内置高级威胁防护，可对DGA、隐蔽信道、恶意加密流量进行检测，支持监控高级威胁检测数据，并进行可视化展示； | △ | 否 |
| 10 | 一般指标 | 内容过滤 | 内置内容过滤功能，可对FTP上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等信令以及邮件发件人、收件人、主题、内容、附件等进行过滤； | △ | 否 |
| 11 | 一般指标 | 黑名单 | 支持将五元组、源MAC、地址范围、应用、用户等加入静态黑名单，可与URL过滤、病毒过滤、防代理功能进行联动实现动态黑名单封锁，支持静态和动态黑名单命中统计和监控； | △ | 否 |
| 12 | 一般指标 | 连接控制 | 支持连接控制和监控，可对源/目的地理对象、应用制定连接限制策略，可展示被拦截的IP、地址对象、应用的限制条件、被拒次数、最近被拒时间等信息； | △ | 是 |
| 13 | 一般指标 | 入侵防御 | 支持独立的入侵防护规则特征库，规则库支持根据攻击类型、风险等级、流行程度、操作系统等进行分类，特征总数在5000条以上（提供证明材料）；能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；  入侵防护动作包括告警、阻断、记录攻击报文，支持针对地址、应用设置入侵防御白名单，支持攻击规则搜索以及自定义，可对自定义规则导入导出；  厂商需具备强大的漏洞和攻防研究能力，为CNNVD二级及以上支撑单位（提供官网证明材料） | △ | 是 |
| 14 | 一般指标 | 病毒防御 | 支持对HTTP/SMTP/POP3/FTP/IM等协议进行病毒防御；病毒特征库规模超过300万（提供证明材料） | △ | 是 |
| 15 | 一般指标 | 防火墙虚拟化 | 防火墙支持将一台物理设备扩展为多个虚拟防火墙系统（要求提供功能截图并加盖原厂公章）； | △ | 是 |
| 16 | 一般指标 | 未知威胁 | 支持行为分析，及时发现异常行为并告警，同时能够与APT进行联动，实现协同防御； | △ | 否 |
| 17 | 一般指标 | DDOS防御 | 支持针对IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、SIP、NTP等协议进行DDOS防护；  支持NTP DDOS防护，采用阀值检查、源/目的限流、源认证等方式综合进行NTP REQUEST FLOOD、NTP REPLY FLOOD攻击防护；支持SIP DDOS防护，采用阀值检查、源/目的限流、源认证方式进行SIP FLOOD攻击防护； | △ | 否 |
| 18 | 一般指标 | 邮件安全 | 内置邮件安全防护功能，支持邮件过滤、邮箱防暴力破解、邮件泛洪攻击防护、邮件黑、白名单检测； | △ | 是 |
| 19 | 一般指标 | IPSEC VPN | 支持IPSec VPN功能，支持国密算法VPN加密、认证算法，支持对隧道内网络流量进行监控展示； | △ | 否 |
| 20 | 一般指标 | SSL VPN | 支持SSL VPN功能，满足远程用户安全接入内网，支持windows、Android、iOS等远程客户端接入； | △ | 否 |
| 21 | 一般指标 | 配置维护 | 支持多个配置文件并存，支持对访问控制策略、NAT策略等关键配置进行单独及加密备份和恢复；支持对配置命令及配置文件的操作行为进行审计； | △ | 否 |
| 22 | 一般指标 | 审计 | 支持独立审计策略，可对URL地址、网页标题、网页内容、邮件行为、邮件内容、FTP上传/下载行为及文件内容进行审计；  提供完善的审计数据查询功能，方便管理员对用户的上网行为进行审查和分析。支持对用户上网行为进行完整的审计数据查询，包括访问网站、邮件收发、FTP；（提供截图）同时支持对用户上网流量时长进行完整的审计数据查询，包括服务端IP、用户名、协议、上行流量、下行流量、总流量、时间等； | △ | 否 |
| 23 | 一般指标 | 日志 | 支持日志本地存储，可对不同类型日志设置存储空间，支持日志外发至多个服务器，可设置日志传输协议、时间类型、日志语言、是否合并及加密传输等参数； | △ | 否 |
| 24 | 一般指标 | 设备状态 | 支持系统温度、CPU温度、CPU利用率、内存利用率、电源故障等告警，支持CPU利用率、内存利用率、磁盘利用率等硬件资源实时利用率及其历史使用情况追踪；； | △ | 否 |
| 25 | 一般指标 | 流量统计 | 支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数； | △ | 是 |
| 26 | 重要指标 | 产品要求 | 提供产品计算机信息系统安全专用产品销售许可证或网络安全专用产品安全检测证书。  提供国家认证机构颁发的EAL4+证书。  提供生产厂商针对该项目的正式授权。 | # | 是 |
| 27 | 重要指标 | 厂商安全要求 | 设备厂商提供CCRC信息安全服务资质认证证书二级 | # | 是 |

6.交换机

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **指标种类** | **指标名称** | **指标内容** | **重要性** | **是否需要证明材料** |
|  | 核心指标 | 硬件规格 | 48个GE电口、4个SFP+光口；  1个Console配置接口；  冗余电源；  产品硬件保修≥5年；  PoE交流电源模块； | ★ | 是 |
|  | 核心指标 | 实配 | 48个GE电口，4个SFP+光口，满配万兆多模光模块、电源、风扇、PoE交流电源模块。 | ★ | 是 |
|  | 核心指标 | 设备性能 | 交换容量≥670Gbps；包转发率≥140Mpps，如有双重指标，以官网最小值为准。 | ★ | 是 |
|  | 重要指标 | MAC容量 | ≥64K | # | 是 |
|  | 核心指标 | 产品资质 | 提供工信部入网证 | ★ | 是 |
|  | 一般指标 | 二层 | 支持4K个VLAN，支持基于端口、Mac、IP地址、协议端口号的Vlan, 支持VLAN Mapping；  支持端口聚合、支持IEEE 802.3ad（链路聚合），每个链路聚合组支持32个端口、端口隔离，  支持多对一的端口镜像，远程端口镜像RSPAN，流镜像，支持静态MAC配置。 | △ | 否 |
|  | 重要指标 | Vxlan | 支持Vxlan协议，并支持BGP EVPN 协议 | △ | 是 |
|  | 重要指标 | 可靠性 | 支持硬件BFD，3.3ms发包检测，故障倒换时间小于50ms | △ | 是 |
|  | 一般指标 | 安全功能 | 支持标准、扩展ACL，基于MAC的ACL、基于时间ACL等；  支持Local认证，Radius，Tacacs+，802.1x认证。 | △ | 否 |
|  | 一般指标 | 管理维护 | 支持Telemetry；  支持Telnet、Console、SNMP等管理方式。 | △ | 否 |
|  | 一般指标 | 流量控制 | 支持基于端口、MAC地址、IP地址、IP优先级、DSCP优先级、TCP/UDP端口号、协议类型等流分类，支持CAR、SP、WDRR、SP+WDRR、PQ+WDRR、WRED；  支持基于端口的广播流量抑制，基于端口的未知组播流量抑制，基于端口的未知单播流量抑制。 | △ | 否 |

## 3.4服务要求

**3.4.1系统集成服务**

中标供应商须提供集成服务，提供所有硬件设备的到货、安装、配置、调试、综合布线等全部系统集成服务。

**3.4.2售后服务要求**

中标供应商必须向采购人承诺技术后援支持。为用户设备提供5年原厂免费技术支持，并提供5年原厂服务承诺。中标供应商在应答时应详细阐述免费技术支持的内容与范围。

1.设备质保

（1）设备质保期为5年，质保期自项目终验合格之日起之日起计算。

（2）质保期内，设备原厂负责对其提供的设备与软件进行维修维护，不收取额外费用。

（3）质保期内，设备原厂提供设备固件与软件的免费升级。

（4）质保期内，设备原厂技术人员，在采购人进行网络架构调整更换部分设备时，须全程提供现场技术支持。

（5）投标供应商必须在24小时内对招标方所提出的维修要求做出实质性反应。

（6）设备运行过程中如果出现技术故障，投标供应商应保证48小时内解决问题。

（7）设备运行过程中如果发生硬件故障，投标供应商必须保证用户在三个工作日内得到无故障设备。

（8）投标供应商须认真理解上述质保要求，详细列出质保方案。

2.系统维护服务保证

投标供应商必须向项目单位说明并承诺下列系统维护服务内容：

（1）5年内免费维修、维护及维修、维护的范围（产品、技术、模块、部件）。

（2）5年内免费系统故障处理。诊断、解决系统故障，对其错误及缺陷进行排错。接到采购人请求后，0.5小时内给出实质性响应，需要现场维护的，2小时内到达现场，并提供7×24小时的电话技术支持。

（3）技术咨询。解答采购人使用中的常见问题。

（4）5年后收费维修、维护及维修、维护的范围（产品、技术、模块、部件）。

（5）中标供应商书面承诺在接到采购人保修电话后2个小时内维修人员到达现场提供售后服务。

3.备品与备件

投标供应商应保证招标方5年的备件和消耗品的需求。这些备件及消耗品内容包括:满足投标需求的备件和消耗品；投标供应商依据IT业界的标准、惯例以及以往的经验,增加采购人未曾指定的备件或消耗品。

## 3.5其他要求

无。

# 4人员要求

### 4.1团队要求

### 4.1.1基本要求

无。

### 4.1.2优选资质/优选指标

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **人员类别** | **人员岗位** | **人员要求** | **是否作为加分项** |
| 1 | 无 | 无 | 无 | 无 |

# 5管理实施要求

1.供应商负责项目所有设备的上架，系统的安装、许可激活；所有设备的网络连接，调试；补充所需的综合布线，包括但不限于列头柜至网络汇聚区线缆、配线架、桥架等。在项目实施中需要的各类配件、线缆由供应商提供。

2.供应商负责项目文档资料管理，对于项目施工过程中的施工方案、验收报告等所有资料进行归类整理并装订成册，提交用户留存。

3.货物清单中未列出但项目中必须的设备材料，以及系统运行和验收需要的所有费用都须包含在投标报价中。供应商在投标报价中的错算或漏算，由供应商承担全部损失。供应商应能保证系统使用运行所需的备件和具备相关技术保障机制，如出现设备故障，需更换设备或配件，供应商应在4小时内提供并更换设备或备件，备件要保证为原厂新品，不能因为设备停产而拒绝提供设备、备品备件。供应商派专业技术人员对采购人方的技术人员免费进行使用操作、维护等技术的现场培训，直至采购人方的技术人员能独立工作；供应商免费指导所投产品所有部分的使用和维护。供应商能够根据客户的需求，对设备进行安装、迁移、配置、优化，对系统打补丁、升级，保证采购人的扩展需求。

4.供应商在项目实施过程中，如出现以下情形须承担相应的违约责任。

（1）中标人逾期交付货物的，中标人应按合同全款每日6‰向招标人支付违约金，由招标人从待付货款中扣除。逾期超过约定日期五个工作日不能交货的，招标人可解除本合同。中标人因逾期交货或因其他违约行为导致招标方解除合同的，中标人应向招标人支付合同全款5%的违约金，如造成招标人损失超过违约金的，超出部分由中标人继续承担赔偿责任。

（2）中标人所交的货物品种、型号、规格、技术参数、质量不符合合同规定及招标文件规定标准的，招标人有权拒收该货物，中标人愿意更换货物但逾期交货的，按中标人逾期交货处理。中标人拒绝更换货物的，招标人可单方面解除合同。

（3）中标人未在规定时间内完成故障处理、更换配件等后续维保服务的，对供应商造成的损失应由中标人承担，每次扣除履约保证金20%。

# 6风险管控要求

无。

# 7履约验收要求

## 7.1总体要求

|  |  |
| --- | --- |
| **验收名称** | **验收要求** |
| 第1次验收 | 到货验收 |
| 第2次验收 | 最终验收 |

### 7.2具体要求

（一）到货验收

在合同硬件产品到达采购人指定的地点后，供应商与采购人共同开箱验货，依标书要求对全部产品的型号、规格、数量、外形、包装及资料、文件进行验收。当出现损坏、数量不全或产品不符等问题时，由供应商负责解决；同时按标书技术部分要求对其产品的性能和配置进行测试检查，确保设备正常运行，并达到标书要求的性能和产品指标中规定的性能。

供应商保证所提供设备必须是原厂全新产品。

（二）最终验收

完成全部硬件安装、网络配置调试及系统稳定运行1个月后，供应商提供验收测试计划，按采购人要求对设备进行现场验收测试，对硬件技术指标和网络联通总体性能进行验收。

系统验收后，签署系统终验文件。

# 8其他要求

## 8.1必备要求

## 8.1.1通用必备要求

1.本项目中如涉及商品包装和快递包装的，其包装需求标准应不低于《关于印发<商品包装政府采购需求标准（试行）>、<快递包装政府采购需求标准（试行）>的通知》（财办库〔2020〕123 号）规定的包装要求，如有其他包装需求，详见采购文件技术部分相关章节。

2.本项目中如涉及网络关键设备或网络安全专用产品的，应严格执行国家互联网信息办公室、工业和信息化部、公安部、财政部和国家认证认可监督管理委员会 2023年第 1 号《关于调整网络安全专用产品安全管理有关事项的公告》及国家互联网信息办公室、工业和信息化部、公安部和国家认证认可监督管理委员会 2023 年第 2号《关于调整<网络关键设备和网络安全专用产品目录>的公告》等相关文件要求，所投标（响应）设备或产品至少符合以下条件之一：一是已由具备资格的机构安全认证合格或安全检测符合要求；二是已获得《计算机信息系统安全专用产品销售许可证》，且在有效期内。

3.本项目中如涉及国家强制性产品认证证书（CCC 认证证书）、电信设备进网许可证、无线电发射设备核准证等市场准入类资质的，应严格执行国家相关法律法规的要求。

以上相关要求，由供应商在响应时应答，在履约验收中，采购人将按照采购文件、中标/成交供应商响应文件、采购合同等对中标/成交供应商提供的货物和服务进行验收，必要时依法依规开展相应检测、认证。

## 8.2付款安排建议

如因上级部门政策变化、重大技术变化等导致服务内容需要调整的，根据实际发生额支付费用。根据付款进度安排，供应商及时向采购人提供发票及相关资料，交采购人审核后10个工作日内支付服务费（节假日顺延）。

|  |  |  |
| --- | --- | --- |
| **付款名称** | **付款要求** | **付款比例(%)** |
| 第1次付款 | 到货验收合格 | 60 |
| 第2次付款 | 终验合格 | 40 |

## 8.3其他要求

### 8.3.1保密要求

一、供应商派出的人员应严格遵守采购人的信息安全保密制度和日常办公规定。严禁擅自操作所负责系统以外的设备，内外网计算机严格隔离，严禁出现内网计算机违规外联情况，出现责任事故采购人有权追究供应商的责任。

二、采购人与供应商及现场服务人员签订保密协议，供应商及其现场服务人员未经允许不得擅自调整系统及相关系统的各类参数和后台数据，不得泄露系统及相关系统各类信息，不得擅自从数据库中提取各类税费数据提供给新疆税务系统内外的各类机构和人员。一旦发生上述情况，使系统及相关系统造成重大故障、税收数据发生泄漏，造成严重的社会影响和经济损失，采购人将追究供应商及相关人员的法律责任。供应商在投标时需提供《保密承诺书》并签字盖章，《保密承诺书》可参考以下内容：

**保密承诺书**  
 我司了解有关保密法规制度，知悉应当承担的保密义务和法律责任。

我司郑重承诺：

一、认真遵守国家保密法律、法规和规章制度，履行保密义务；

二、认真遵守我司与甲方签订的保密协议；

三、认真遵守其它各项安全保密的相关规定；

四、对参与的信息化项目和服务所涉及技术资料和数据信息履行保密义务，未经许可，不对外发表或使用。

承诺单位（盖章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

法定代表人或授权代表签字：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

日期：XX年XX月XX日

三、供应商所提供的工作人员的工作成果归采购人所有，供应商在未征得采购人书面同意的前提下，不得将技术资料泄露给其他人员及单位。如违反上述协议内容，采购人将保留追究供应商法律责任的权利。

### 8.3.2知识产权要求

无。

### 8.3.3★供应链安全管理要求

1、人员资格要求

（1）签订承诺书。供应商应严格落实国家税务总局网络安全和保密管理要求，承担技术支持人员的网络安全和保密管理责任，按采购人要求签订协议和承诺书。

（2）开展背景审查。供应商承担技术支持人员背景审查工作，提供其身份证明、履历、家庭成员及主要社会关系、无犯罪记录证明等材料，并提交采购人进行备案。

（3）设置网络安全负责人（由驻场运维人员兼任）。供应商为本项目配备一名网络安全负责人，该负责人具备独立决策能力并保持相对稳定，在项目实施的全过程负责网络安全工作，组织落实各项网络安全要求。

2、日常行为规范要求

（1）工作能力要求。供应商负责对技术支持人员进行资格条件、工作胜任力以及网络安全能力评估，对技术支持人员承担的工作进行安全保密风险分析，明确技术支持人员工作范围和边界，重点防范设备和资料失窃、误操作导致的软硬件故障、工作秘密和税费数据等信息泄露、信息系统越权访问和网络攻击等风险。

（2）教育培训要求。供应商负责对技术支持人员进行网络和数据安全法律法规、网络安全意识、网络安全管理、网络安全技能、保密意识以及网络安全警示教育等培训，上岗前对其进行考核。

3、违约惩戒措施

供应商对供应链安全管理责任落实不到位，造成安全事件或产生不良影响的，采购人按照《税务系统信息化服务商失信行为记录名单制度（试行）》（税总办征科发〔2022〕1号）要求，组织对供应商进行失信行为认定，并采取相应的处置措施。

4、其他要求

为切实落实《网络安全法》《数据安全法》《个人信息保护法》等法律法规和规范性文件要求，加强税务信息化供应链安全管理，供应商应遵守以下要求：  
 （1）供应商应定期对聘用离职税务人员情况进行排查，建立聘任税务离职人员姓名等基本情况信息、离职时间、入职时间、入职主要工作职责等相关档案资料。  
 （2）供应商及其派驻的开发或运维人员签订网络安全承诺书，相关个人提交无犯罪记录证明。  
 （3）供应商应建立网络安全负责人制度，并设置项目网络安全负责人，且该负责人保持相对稳定，如需更换应先向采购人报告，经同意后更换网络安全负责人。  
 （4）供应商应积极参加采购人组织的网络安全和数据安全意识和技能方面的教育培训、考核及警示教育培训等。  
 （5）未经批准严禁变更办公环境，严禁安装非必要的应用程序和组件，未经批准严禁擅自复制、使用和修改文档、数据以及其他开发测试资料。  
 （6）供应商发现的网络安全漏洞、缺陷、数据泄露或其他重大网络安全风险要及时向采购人报告。定期检查所使用产品及第三方组件情况， 对存在高危漏洞的应及时通过限制访问、更新补丁、版本升级、设备防护等措施进行加固处置情况。  
 （7）供应商不得利用提供产品和服务的便利条件非法获取数据、非法控制和操纵设备。  
 （8）供应商应当遵守落实采购人相关安全管理的相关规定。

### 8.3.4税务信息化服务商廉政相关要求

为进一步落实全面从严治党要求，构建亲清新型政商关系，加强税务信息化项目建设过程中的党风廉政建设和反腐败工作，确保项目建设规范、廉洁推进，中标人在参与税务部门信息化项目工作过程中，需严格遵守法律法规、规范履行合同，积极协助税务部门开展廉政风险防控工作。请严格遵守并落实如下要求：

1.积极发挥廉政风险防控正向作用。中标人有义务配合税务部门在信息化项目工作中加强廉政风险防控，执行有关措施。

2.健全廉政风险防控机制。中标人有责任在项目管理机制中健全内部廉政防控措施，包括但不限于：对参与本项目的员工提出廉洁行为规范；指定专人对项目实施各环节进行廉政监督；在项目验收过程中提交本项目廉政情况报告等。

3.杜绝违纪违法行为。中标人及相关项目人员必须严格遵守党纪国法，坚守职业道德，杜绝任何形式的利益输送、权力寻租等违纪违法行为，对甲方工作人员不得实施以下行为：

（1）以各种形式和名义提供礼品、礼金、电子红包、支付凭证、商业预付卡、名贵特产、有价证券、股权、其他金融产品等财物。

（2）以各种形式和名义提供宴请、旅游、健身、娱乐、私人会所等活动安排；代付加班餐费、打车费等。

（3）以讲课费、咨询费等名义，提供或变相提供报酬。

（4）借款、借房、借车，报销应由个人负担的费用。

（5）以无偿、象征性地收取费用等方式提供家政、司机等服务劳务。

（6）其他通过任何形式行贿或输送利益的行为。

4.信守承诺。中标人应承诺在项目实施过程中，严格遵守国家法律法规合法、诚信经营，杜绝商业贿赂、规范经营活动、公开透明合作、严格内部管理，并签订《税务信息化项目服务商廉洁承诺书》提交甲方负责项目实施的单位。《税务信息化项目服务商廉洁承诺书》可参考以下内容：

**税务信息化服务商廉洁承诺书**

为深入贯彻落实党中央关于全面从严治党的决策部署，进一步加强税务信息化项目合作中的廉政建设，防范廉政风险发生，确保项目公开、公平、公正推进，我司郑重承诺如下：

**一、合法合规经营。**严格遵守国家法律法规及税务部门的相关规定，坚持廉洁从业、诚信经营的原则。在合作过程中不以任何形式进行利益输送，维护良好的政商关系。

**二、杜绝商业贿赂。**加强内部管理，我司及我司员工均不对甲方工作人员实施以下行为：

（一）以各种形式和名义提供礼品、礼金、电子红包、支付凭证、商业预付卡、名贵特产、有价证券、股权、其他金融产品等财物。

（二）以各种形式和名义提供宴请、旅游、健身、娱乐、私人会所等活动安排；代付加班餐费、打车费等。

（三）以讲课费、咨询费等名义，提供或变相提供报酬。

（四）借款、借房、借车，报销应由个人负担的费用。

（五）以无偿、象征性地收取费用等方式提供家政、司机等服务劳务。

（六）其他通过任何形式行贿或输送利益的行为。

**三、规范经营活动。**严格按照合同约定履行义务，保证项目质量，按时完成建设任务；在合作过程中不以任何借口拖延工期、虚报成本或谋取私利。

**四、公开透明合作。**我司承诺在项目实施过程中保持公开透明，主动接受税务部门及纪检监察机构的全程监督，并积极配合任何有关廉洁从业的调查工作。

**五、严格内部管理。**加强企业内部廉洁教育，确保员工知晓并遵守相关法律法规及廉洁要求；加强项目实施全过程廉洁监督；对于违反廉洁承诺的员工，将严肃处理，并承担相应责任。

**六、积极参与监督。**在税务信息化项目实施过程中，如发现任何违纪违法行为，将如实反馈问题和意见。

承诺单位（盖章）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

法定代表人或授权代表签字：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

日期：XX年XX月XX日

5.自觉接受监管。中标人有义务配合税务机关的正常业务监管以及纪检监察、外部审计、督察内审等监督机构对税务信息化项目全过程的监督检查工作，如实提供相关资料和信息，不得隐瞒、篡改或销毁与项目建设有关的文件、数据等资料。

6.举报和反馈意见。项目执行过程中，中标人有权举报、反馈甲方索贿受贿、吃拿卡要、违反中央八项规定精神等违纪违法行为。项目验收前，应填写《税务信息化项目服务商廉政反馈书》，提交甲方税务机关网络安全和信息化领导小组办公室。

让我们在廉洁、诚信、公平、公正的基础上开展合作，共同为高水平建设效能税务、高质量推进中国式现代化税务实践贡献力量。