**上海市静安区政务外网升级改造项目招标采购需求**

目录

[1. 项目背景 1](#_Toc69967312)

[2. 建设目标及内容 1](#_Toc69967313)

[3. 系统现状 3](#_Toc69967314)

[4. 项目需求 4](#_Toc69967315)

[4.1. 设备清单 4](#_Toc69967318)

[4.2. 业务网络建设 5](#_Toc69967319)

[4.3. 光传输网络建设 5](#_Toc69967320)

[4.4. 运维管理系统建设 6](#_Toc69967321)

[4.4.1. 运维管理平台 6](#_Toc69967322)

[4.4.2. SDN及网络管理系统 6](#_Toc69967323)

[4.5. 网络安全建设 7](#_Toc69967324)

[4.5.1. 网络安全设备 7](#_Toc69967325)

[4.5.2. 安全管理平台 7](#_Toc69967326)

[4.6. 光缆及机柜资源建设 7](#_Toc69967327)

[4.7. 其他配套资源 7](#_Toc69967328)

[5. 项目实施要求 7](#_Toc69967329)

[5.1. 网络割接要求 7](#_Toc69967330)

[5.2. IP地址规划及实施要求 8](#_Toc69967331)

[5.3. 运维管理系统建设要求 8](#_Toc69967332)

[5.4. 网络安全建设要求 8](#_Toc69967333)

[5.5. 光缆及机柜资源建设要求 8](#_Toc69967334)

[5.6. 项目建设周期 9](#_Toc69967335)

[6. 售后及技术服务要求 9](#_Toc69967336)

[6.1. 技术支持要求 9](#_Toc69967337)

[6.2. 售后服务要求 9](#_Toc69967338)

[6.3. 人员要求 10](#_Toc69967339)

[6.4. 培训要求 11](#_Toc69967340)

[6.5. 重要活动保障服务要求 11](#_Toc69967341)

[6.6. 其他服务要求 11](#_Toc69967342)

[7. 附件-设备技术要求 12](#_Toc69967343)

[7.1. 路由器A（4台） 12](#_Toc69967344)

[7.2. 入侵检测A（1台） 15](#_Toc69967345)

[7.3. 探针A（4台） 17](#_Toc69967346)

[7.4. 路由器B（10台） 19](#_Toc69967347)

[7.5. 汇聚防火墙A（8台） 23](#_Toc69967348)

[7.6. 交换机A（8台） 25](#_Toc69967349)

[7.7. 接入交换机A型（10台） 27](#_Toc69967350)

[7.8. 接入交换机B型（10台） 28](#_Toc69967351)

[7.9. 接入交换机C型（26台） 29](#_Toc69967352)

[7.10. 路由器C（6台） 30](#_Toc69967353)

[7.11. 防火墙B（2台） 34](#_Toc69967354)

[7.12. 防火墙C（2台） 36](#_Toc69967355)

[7.13. 入侵防御（2台） 38](#_Toc69967356)

[7.14. 交换机B型（2台） 40](#_Toc69967357)

[7.15. 防火墙D（2台） 42](#_Toc69967358)

[7.16. 入侵检测B（1台） 44](#_Toc69967359)

[7.17. 交换机C型（2台） 50](#_Toc69967360)

[7.18. 防火墙E（2台） 53](#_Toc69967361)

[7.19. 沙箱 54](#_Toc69967362)

[7.20. 探针B（1台） 57](#_Toc69967363)

[7.21. 抗DDoS检测 59](#_Toc69967364)

[7.22. VPN网关 62](#_Toc69967365)

[7.23. 安全管理平台 64](#_Toc69967366)

[7.23.1. 安全管理中心平台 64](#_Toc69967367)

[7.23.2. 态势感知模块 65](#_Toc69967368)

[7.23.3. 预报预警模块 68](#_Toc69967369)

[7.23.4. 威胁情报共享模块 68](#_Toc69967370)

[7.23.5. 漏洞扫描模块 69](#_Toc69967371)

[7.23.6. 日志审计模块 70](#_Toc69967372)

[7.23.7. 安全管理控制模块 71](#_Toc69967373)

[7.24. 堡垒机 72](#_Toc69967374)

[7.25. 运维管理系统 77](#_Toc69967375)

[7.26. SDN及网管系统 79](#_Toc69967376)

[7.27. 日志存储服务器 83](#_Toc69967377)

[8. 投标投标方资质要求 84](#_Toc69967378)

[9. 评分细则 85](#_Toc69967379)

# 项目背景

为深入贯彻网络强国战略思想，支撑上海政务服务“一网通办”、城市运行“一网统管”现代化治理体系建设，进一步提升城市治理现代化水平，推进网络互通、数据共享、应用协同，发挥信息化对经济社会发展的引领作用，高水平适应信息时代对政务网络基础设施的新要求，做强电子政务外网“全市一张网”。上海市大数据中心结合我市实际，编制了《关于全面加强上海市电子政务外网建设的工作方案》，明确提出“2021年年底，完成市、区两级电子政务外网升级改造工作，建成市级100G、区级40G～100G带宽能力，市、区两网间‘千兆对接、万兆扩展’的光传输网络通道和业务网络，实现全网数据流量、视频流量‘一网双平面’架构，逻辑隔离、独立运行、互为备份运行，完成安全系统优化部署并迁移原政务外网业务”。同时，上海市大数据中心依据《国家电子政务外网建设总体规划》和《上海市公共数据和一网通办管理办法》等文件要求，组织编制《上海市电子政务外网建设和运行管理指南》，作为上海市电子政务外网的技术规范建议和指导手册，为上海市市、区两级政务外网的建设及日常运行维护和管理工作提供依据。

# 建设目标及内容

本项目主要建设目标：对标《上海市电子政务外网建设和运行管理指南》的技术标准，升级健全静安区政务外网，进一步提升区政务外网的综合应用承载能力，打造“统一监控、分级管理、流程闭环、智能分析、可视决策”的一体化维护管理能力，形成“物理安全、环境安全、信息安全、自主可控、协同联动”的政务外网综合安全防护能力，形成政务外网用户“一网接入”、政务外网业务“一网承载”的集约化建设模式。

本项目建设内容主要包括：

1. 业务网络建设

根据上海市大数据中心在《上海市电子政务外网建设和运行管理指南》要求，结合静安区业务特点，将静安区政务外网建设整体架构严格分区分层规划，实现核心、汇聚、接入三层架构的构建，主要包括核心平面、汇聚平面、接入平面等建设。

1. 光传输网络建设（租赁模式）

根据上海市大数据中心在《上海市电子政务外网建设和运行管理指南》中的要求，采用OTN技术，搭建一套光传输核心网络。

1. 运维管理系统建设

包括安全管理平台及运行支撑系统建设。

1. 网络安全建设

将区政务外网划分为5类区域，划定安全边界，并部署符合等保2.0三级规范要求的安全设备。

1. 光缆及机柜资源建设建设

在现有接入层至汇聚层、汇聚层至核心层光缆资源及机柜资源的基础上，租赁楼内光纤及机柜。

1. 其他配套资源

包括IP地址调整及配套工作。

# 系统现状

目前静安区政务外网有二个核心机房，分布在静安区的北区和南区，核心层上行连接至市电子政务外网，下行连接各委办局、街道、居委会。其中，南区的各委办局、街道、居委会就近连接到南区核心机房, 北区的各委办局、街道、居委会就近连接到北区核心机房。

# 项目需求

1.
2.

## 设备清单

本次设备采购如下表所示：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 建设规模 | 单位 | 备注 |
|  |
| 1 | 路由器A | 4 | 台 |  详见附件-设备技术要求 |  |
| 2 | 入侵检测A | 1 | 台 | 　详见附件-设备技术要求 |  |
| 3 | 探针A | 4 | 台 | 　详见附件-设备技术要求 |  |
| 4 | 路由器B | 10 | 台 | 　详见附件-设备技术要求 |  |
| 5 | 防火墙A | 8 | 台 | 　详见附件-设备技术要求 |  |
| 6 | 交换机A | 8 | 台 | 　详见附件-设备技术要求 |  |
| 7 | 接入交换机A型 | 10 | 台 | 　详见附件-设备技术要求 |  |
| 8 | 接入交换机B型 | 10 | 台 | 　详见附件-设备技术要求 |  |
| 9 | 接入交换机C型 | 26 | 台 | 　详见附件-设备技术要求 |  |
| 10 | 路由器C | 6 | 台 | 　详见附件-设备技术要求 |  |
| 11 | 防火墙B | 2 | 台 | 　详见附件-设备技术要求 |  |
| 12 | 防火墙C（信创目录内） | 2 | 台 | 　详见附件-设备技术要求 |  |
| 13 | 入侵防御（信创目录内） | 2 | 台 | 　详见附件-设备技术要求 |  |
| 14 | 交换机B | 2 | 台 | 　详见附件-设备技术要求 |  |
| 15 | 防火墙D | 2 | 台 | 　详见附件-设备技术要求 |  |
| 16 | 入侵检测B | 1 | 台 | 　详见附件-设备技术要求 |  |
| 17 | 交换机C | 2 | 台 | 　详见附件-设备技术要求 |  |
| 18 | 防火墙E | 2 | 台 | 　详见附件-设备技术要求 |  |
| 19 | 安全沙箱 | 1 | 台 | 　详见附件-设备技术要求 |  |
| 20 | 探针B | 1 | 台 | 　详见附件-设备技术要求 |  |
| 21 | 抗DDoS检测设备 | 1 | 台 | 　详见附件-设备技术要求 |  |
| 22 | VPN网关 | 1 | 台 | 　详见附件-设备技术要求 |  |
| 23 | 安全管理平台 | 1 | 套 | 　详见附件-设备技术要求 |  |
| 24 | 堡垒机 | 1 | 台 | 　详见附件-设备技术要求 |  |
| 25 | 运维管理系统 | 1 | 套 | 　详见附件-设备技术要求 |  |
| 26 | SDN及网管系统 | 1 | 套 | 　详见附件-设备技术要求 |  |
| 27 | 日志存储服务器 | 1 | 台 | 　详见附件-设备技术要求 |  |

本次项目所采购的设备需要配备必要的光模块，以满足组网需求。

## 业务网络建设

根据上海市大数据中心在《上海市电子政务外网建设和运行管理指南》要求，结合静安区业务特点，将静安区政务外网建设整体架构严格分区分层规划，实现核心、汇聚、接入三层架构的构建。

业务网络采用 “一网双平面”的架构设计，数据平面承载网络数据流量，视频平面承载网络视频流量，两个平面在政务外网骨干网上逻辑隔离、独立运行，且互为冗余备份。

## 光传输网络建设

根据上海市大数据中心在《上海市电子政务外网建设和运行管理指南》中的要求，采用OTN技术，搭建一套光传输核心网络。本项目中采取租赁模式（其中包含OTN设备及OTN设备之间联接的光纤资源租用一年）。选取5个节点建设OTN设备。其中两个核心节点、三个汇聚节点进行光传输网络租用。技术需求如下：

1. 采用单波速率100G及以上的OTN技术；
2. 支持带宽平滑扩容，网络具备向200G及以上带宽平滑扩容的能力；
3. 采用高可用的组网架构，具备网络自愈能力，能为各类政务应用提供安全可靠的传输网络支撑；
4. 采用保护路径和工作路径物理光纤分离的保护策略，端到端保护倒换时间小于50ms；
5. 具有SDH、分组、OTN等多种业务统一承载的能力，能提供多种业务类型接口的接入能力，具备与已建网络互联互通的能力；
6. 支持光纤线路诊断功能，能快速定位光纤线路故障；
7. 宜采用SDN技术，实现对业务和链路的快速下发和调整；
8. 应使用G.652或G.655规格的光缆，光缆的每公里线路衰耗在0.3dB以下。

设备要求：

|  |  |
| --- | --- |
| 特性 | 详细描述 |
| 交叉功能  | 具备OTN、分组、SDH交叉功能  |
| 业务类型  | FE/GE/10GE/40GE/100GE、STM-N(1/4/16/64)业务接入；单波10G/100G速率传输； |
| 光模块  | eSFP、SFP+、SFP28、CFP、CFP2、QSFP+、QSFP28  |
| 可靠性  | 电源冗余、风扇冗余、交叉冗余、通信控制与时钟单元冗余；支持OTN、分组、SDH网络级保护；  |

## 运维管理系统建设

### 运维管理平台

根据上海市大数据中心在《上海市电子政务外网建设和运行管理指南》要求以及静安区政务外网运维管理现状，本次项目运维管理平台的主要功能包括：配置管理、网络管理系统、运行管理组织、运行信息化支撑系统、网络资源管理、告警管理、性能管理、运行服务门户、数据仓库、运维项目跟踪、项目生命周期管理、运维团队管理、可视化、接口开发等。

### SDN及网络管理系统

通过基于SDN软件定义网络技术的网络管理系统，实现网络资源的灵活管理，保障应用高效部署、稳定运行。网络管理系统需要提供整网综合管理能力，实现网络资源、用户和业务的融合管理，提供基本的网络资源管理、拓扑管理、故障管理、性能管理、用户管理，采用SDN技术，实现业务快速部署，流量工程和智能流量调整能力；应基于智能检测技术，对网络中不同业务的运行状态、服务质量，做到实时监控、主动运维。

## 网络安全建设

### 网络安全设备

将区政务外网划分安全区域，划定安全边界，部署符合等保2.0三级规范要求的安全设备。

### 安全管理平台

安全管理中心包含态势感知、通报预警、威胁情报共享、漏洞扫描、安全管理控制、日志审计系统等设备及功能模块，实现区政务外网的全网威胁可视化、通报预警和统一安全运营能力。其中，态势感知、通报预警、威胁情报共享、漏洞扫描作为安全监测系统的关键部件，需要实现与市级安全监测系统的对接，实现市、区两级安全管理中心的信息交互和协同联动。

## 光缆及机柜资源建设

在现有接入层至汇聚层、汇聚层至核心层光缆资源及机柜资源的基础上，租赁楼内光纤及机柜。

## 其他配套资源

包括IP地址调整、配套工作。

# 项目实施要求

## 网络割接要求

本次项目网络割接需提供详细的实施方案，要求如下：

1. 提供各节点的网络割接和调整步骤以及具体工程实施计划；
2. 网络割接调整时需要考虑对在线业务的中断性影响，将影响控制在最小，确保平滑过渡，不影响静安区政务外网业务连续性。

## IP地址规划及实施要求

静安区政务外网业务网络应遵循《推进互联网协议第六版（IPv6）规模部署行动计划》的标准和要求，投标方需提供详细的全网IPv4/IPv6地址规划，所提供设备应均支持IPv4/IPv6双栈技术及IPv6线速转发。全网部署端到端双栈技术实现互通，并启用基于IPv6的路由协议。具体内容如下：

1. 根据网络结构和设备配置，给出本项目IP地址规划方案，满足区各单位使用需求。
2. 完成全区各单位IP地址调整及配套工作。

## 运维管理系统建设要求

按照国家电子政务外网“统筹建设、分级负责、属地管理”的制度要求，以及上海市大数据中心在《上海市电子政务外网建设和运行管理指南》中的要求，区政务外网运行和安全监测支撑系统应与上海市电子政务外网运行和安全监测支撑系统进行运维管理功能的对接。

## 网络安全建设要求

针对本项目的实际情况，提供网络边界划分规划及网络安全设计方案，并按照等级保护2.0要求进行实施部署，同时提供配套的安全服务，包括（不限于）：风险评估、漏洞扫描、安全加固、安全分析、安全咨询规划、应急响应、安全培训、重大活动期间安全保障服务。

配合用户完成静安区政务外网骨干网的等级保护定级、备案及测评工作。

## 光缆及机柜资源建设要求

根据静安原有情况，对光缆及机柜资源进行租赁。包括：光缆敷设（提供不少于36芯）及割接、机柜租赁（提供不少于2个机柜，满足实际设备部署需求）。

## 项目建设周期

投标人合同签订后1个月内完成区政务外网与市政务外网出口对接；4个月内完成业务网络建设、光传输网络及网络安全建设；7个月内完成运维管理系统建设；9个月内完成所有建设内容；12个月内完成试运行及整体项目验收工作。付款方式为：1、合同签订后十个工作日内，支付30%；2、项目组成立，项目人员到位，支付20%；3、项目工程完成后，经甲方和监理确认后，十个工作日内，支付30%；4、项目整体验收后，支付20%。具体以合同签订为准。

# 售后及技术服务要求

## 技术支持要求

1. 投标方提供详细的维护服务和技术支持计划。
2. 投标方需确保项目建设及运营期内所有设备设施的正常运行，以及原厂商和其它外联单位的协调工作。

## 售后服务要求

投标方必须提供完整的项目售后实施方案，服务范围包括本次项目建设的软硬件等设备，具体要求如下：

1. **服务机构**：投标方应设有专门的服务机构。
2. **服务响应体系**：提供7x24小时故障响应服务，安排专人进行维修。接到报修通知后，维修人员应在10分钟内响应，两个核心机房故障要求10分钟内到达现场，接入点故障半小时到达现场，排除故障要求3人以上（包括项目经理1人、核心机房1人和接入点1人），提供现场服务，并在故障解决后出具相应的故障分析报告。
3. 服务期内，投标方对所有新购设备应提供3年原厂质保服务及相关特征规则库3年升级服务，提供备品备件服务，并在需要替换时负责实施工作。
4. 项目整体验收合格后，投标方在免费维护服务期（3年）内，从项目正式验收通过之日起计算，免费维护期内的售后服务具体要求如下：
* 受理各网络使用单位和部门提出的服务请求，在10分钟内响应，两个核心机房故障要求10分钟内到达现场，接入点故障半小时到达现场，受理人员要求3人以上（包括项目经理1人、核心机房1人和接入点1人）。
* 每天两次对相关软硬件设备进行状态进行检查，确认系统运行状态。
* 每季度对安全、网络等设备进行巡检，检查系统日志错误记录、分析设备运行状态，排除潜在隐患，确保系统正常稳定运行，提交设备运行情况和预警报告。
* 5\*8小时的网络设备维护、安全设备维护及机房运维服务。
* 需每月进行一次深度威胁分析与响应服务及相关报告。
* 提供7\*24热线服务。
* 提供相关技术咨询服务。
1. **无推诿承诺：**无论由于哪一方产生的问题而使整体系统发生不正常情况时，并在得到招标人通知后，须立即派工程师到场，全力协助招标人和其他投标方，使系统尽快恢复正常。针对本项目所涉及的场所及相关设施，除不可抗力之外，投标方自身原因或投标方与其他投标方之间的纠纷问题，不能影响到本项目的日常运行管理；
2. **原厂备件：**投标方承诺提供原厂备品备件服务，原厂备件4小时到现场，原厂技术人员2小时到现场，提供原厂售后服务承诺。

## 人员要求

投标方应为本项目单独建立管理组织，配置实施团队，项目中所投入的人员需提供社保缴纳证明。

1. 项目经理

 对项目过程实行全面管理，执行检查控制协调项目的各项工作。

 项目经理必须具备高级工程师职称证书。

 从事项目经理或项目负责人至少5年以上类似项目管理实际经验。

1. 实施工程师

在项目实施过程中，投标人在项目实施期间，技术团队至少包含10人进行项目实施。

1. 服务工程师

项目实施完成后，每年至少四次进行巡检维护。维护期间提供专家级的咨询服务，能对系统设备的运行、系统升级优化等提出合理化建议。

服务工程师包含现场驻点运维工程师和二线支持团队，二线支持团队对一线运维进行远程技术与指导，紧急情况下处理应急事件、疑难问题和个案调查处理。并根据需要到现场进行响应、值守。

 服务工程师需提供相关证书（或者类似证书）：

 服务工程师中至少2名需具备网络认证相关证书。

 服务工程师中至少1名需具备信息安全认证工程师资格。

 从事网络、机房维护等相关工作至少3年以上实际经验。

## 培训要求

投标方应根据本项目的特点制定培训方案并提供培训，使静安区政务外网相关人员在培训后能够独立维护及使用。培训课程涵盖区政务外网所有设备的使用和管理培训，投标方负责安排专业培训讲师授课，并提供全套培训教材和培训课程计划表。

1)总体要求

投标方为所有被培训人员提供培训用文字资料和讲义等相关用品。所有的资料是中文书写。培训工作应在合同生效后安排。

2)培训内容与课程要求

投标方应对项目中所有产品的基本知识、系统或参数配置、管理维护等提供相应的培训。投标方详细列明相应的培训课程内容、人数和时间安排。

3)培训费用

投标方应将所有培训费用（含培训教材费）及各项支出计入资源服务费用中，不单独报价。

## 重要活动保障服务要求

投标方应根据静安区政务外网的实际需求，在春节、国庆、护网、两会、党代会、进博会等重保期间，安排相应的技术力量，为静安区政务外网做好风险评估、安全防护和现场保障工作。

## 其他服务要求

投标方应无条件提供与静安区政务外网的运行维护、安全保障、监测管理、应急处置、技术支持等方面的其他服务。

# 附件-设备技术要求

说明： △为关键技术参数,

## 路由器A（4台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 体系架构 | 提供设备面板图并指出对应的主控板、交换网板和业务板槽位 |
| 为保证设备可靠性，设备的转发全部有交换网板完成，主控板不集成转发芯片 |
| 为保证可靠性，设备需支持板卡（含主控，线卡，交换网板等）直接热插拔，同时不需要插拔电源风扇等其他关键部件 |
| 支持独立的交换网板≥4个，需提供官方网站截图 |
| 交换容量 | △交换容量≥150Tbps，以官网最小值为准，需提供官方网站截图，原厂盖章 |
| 包转发率 | △包转发率≥24000Mpps，以官网最小值为准，需提供官方网站截图，原厂盖章 |
| 业务槽位 | △为保障性能平滑升级，设备采用子母卡架构设计，子卡插在母板上，子卡母板均支持热拔插，单块母板支持嵌套安装2-4块业务子卡，提供产品图片证明并加盖原厂公章 |
| 单槽位转发性能 | △设备单槽位最大转发能力≥2Tbps  |
| 电源系统 | 支持内置交流电源，不能配置外置交流电源，也不额外占用业务槽位 |
| 支持电源个数≥6个，电源系统支持N+M冗余，支持一体化供电方式，当前实配情况下任意拔掉两个电源，设备能够正常运行 |
| 通风方式 | 支持前后通风 |
| 基本功能 | 支持PPP、MP、HDLC、ETHERNET等链路层协议 |
| 支持链路聚合（Link aggregation），支持动态聚合、手工聚合、跨板聚合 |
| 支持不同带宽的链路捆绑功能 |
| 支持多路径负责分担功能（UCMP），支持非等速链路的负载分担，实现不同路径按带宽比例负载分担 |
| 支持IPV4静态路由、RIPv1/v2、OSPFv2、BGP、IS-IS、路由策略，支持4M IPv4 FIB |
| 支持IPv6静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+，支持2M IPv6 FIB |
| 支持L2VPN、L3VPN、OptionA、B、C类跨域，支持16K VPN，支持4M VPN路由 |
| 接口类型 | 支持FE、GE、10Ge（LAN/WAN）、40Ge、100Ge、155M POS、622M POS、2.5G POS、10G POS、CPOS接口、155M ATM、622M ATM、E1等接口 |
| 支持ATM/POS端口灵活切换 |
| GRE | 支持分布式GRE功能，为保证性能，本次要求实配GRE功能板卡或license  |
| Netstream | 支持分布式Netstream功能，本次要求实配支持NetStream功能板卡或license |
| NAT | 支持分布式NAT功能，本次要求实配NAT功能板卡或license |
| 组播VPN（MVPN） | 支持分布式MVPN功能 |
| 虚拟化 | 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，需提供官方网站截图 |
| IPv6 | 具备IPv6能力，所投设备需提供IPv6 Ready II证书 |
| SRv6 | △支持SRv6功能，并提供权威检测机构颁发的SRv6 Ready检测证书，检测机构需要通过CNAS能力认可 |
| QOS | 支持优先级Mark/Remark、CAR（Committed Access Rate）、GTS等功能 |
| 为简化ACL配置，设备需支持全局ACL功能 |
| 支持FIFO、PQ、WFQ、LLQ等各种队列调度机制，支持拥塞避免算法：Tail-Drop、RED、WRED，支持层次化Qos（H-Qos） |
| SDN | 设备支持通过Netconf（RFC 6241）协议下发配置 |
| 设备支持YANG功能（RFC 6020） |
| 为实现设备间链路状态等信息共享，设备需支持BGP Link-State功能（RFC 7752) |
| 为实现单节点上安全策略同步功能，设备需支持BGP FlowSpec功能（RFC 5575) |
| 为实现报文最优路径转发，设备需支持Segment Routing（RFC7855）协议 |
| 为实现按业务优先级选择隧道路径，设备需支持CBTS功能（YD/T 1391.1） |
| 设备支持Openflow协议，报文可依据流表进行转发 |
| 为保证业务调度的精细化控制，设备需要支持13层标签 |
| 设备支持EVPN/VxLAN（RFC 7348）功能，能够完成MAC地址远端学习，实现基于VxLAN的二三层VPN  |
| 可靠性 | 实配双主控 |
| 支持VRRP/VRRPv3、MPLS TE FRR、IP FRR（静态路由/策略路由/RIP/IS-IS/OSPF等） |
| 为减小设备或线路故障对业务的影响、提高网络的可用性，需支持BFD for BGP/IS-IS/OSPF/LDP/VRRP/Static Route |
| 支持热补丁功能，可在线进行补丁升级 |
| 为提高设备软件稳定性及可靠性，主备倒换时业务不中断，需要支持NSR功能 |
| 为提高设备硬件稳定性及可靠性，交换网板、板卡、子卡支持热插拔功能 |
| 为检测设备之间的可达性、时延、丢包率、抖动等信息，设备需支持NQA检测网络网络质量 |
| 网络安全 | 设备支持防攻击能力，包括：ARP攻击、IPv6报文攻击、超大Trace报文攻击、TCP SYN flood、Ping flood、DHCP DDOS、PADI DDOS的防御等 |
| 支持OSPF、OSPFv3、ISIS、ISISv6、BGP、BGP4+的MD5认证功能，支持Keychain功能，可以支持基于时间段的生效的秘钥 |
| 维护特性 | 为方便设备运维管理，设备需内置TCL语言功能，能够解析执行TCL语言脚本 |
| 为方便设备运维管理，设备需内置Python语言功能，能够解析执行Python语言脚本 |
| 为实现设备精细化管理，实现不同进程动态部署到不同的CPU上，设备需支持进程分布式优化功能 |
| 为实现基于角色的权限灵活授权，并且和AAA联动，设备需支持RBAC功能 |
| 为方便设备配置文件管理，设备需支持配置回滚功能 |
| 工信部入网许可证 | 提供工信部入网许可证复印件 |
| 其它配置要求 | △实配双主控，四块电源模块，满配交换网板，100G光口≥12块，10G光口≥10块，100G模块≥6块，40G光模块≥2块，10G光模块≥10块，满足设备100G互连条件 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 入侵检测A（1台）

| **指标项** | **参数要求** |
| --- | --- |
| 硬件平台 | 产品采用多核并行处理架构，并采用国产处理器和国产操作系统。 |
| 硬件规格 | 产品不少于4千兆光口，5个千兆电口，冗余电源，2 U机箱。 |
| 性能要求 | 网络层吞吐量：50Gbps，并发连接数：7000000，新建连接数：250000 |
| 部署方式 | 产品支持旁路镜像部署方式  |
| 攻击检测能力 | 系统需要支持如下常见协议的解析：ETHER、ARP、RARP、IP、ICMP、IGMP、PPPoE、Vlan Tag、MPLS、TCP、UDP、NetBIOS、CIFS、SMB、FTP、TELNET、POP3、SMTP、IMAP、SNMP、MSRPC、SUNRPC、TNS、TDS、HTTP、QQ、MSN、BT、Thunder、CHARGEN、ECHO、AUTH、DNS、FINGER、IRC、MSPROXY、NFS、NNTP、NTALK、PCT、WHOIS等，协议覆盖面广，与之对应的事件库完备； |
| 能够对缓冲区溢出、网络蠕虫、网络数据库攻击、木马软件、间谍软件等各种攻击行为进行检测； |
| 系统需具备对针对Web系统（包括浏览器、服务器）的攻击具备检测能力：SQL注入（包括各种变形）、XSS（包括存储式XSS、反射式XSS）及其各种语法变形、Webshell、网页挂马、语义变形、编码等环境下的精确检测能力； |
| 用户可自定义添加入侵检测规则，并定义入侵响应时间 |
| 多级分布和全局预警 | 系统支持多级部署，集中管理能力，可以添加组件（包括子控、引擎）提供各个组件（子控、引擎）的拓扑图，并在图中动态显示组件之间的实时连接状态； |
| 级联环境中，上级针对下发策略的锁定，锁定子控的一些策略，锁定的事件是不允许进行配置、编辑、删除等操作的； |
| 威胁响应能力 | 支持如下报警响应方式：计入日志、页面报警、发送邮件、发送SNMP Trap信息、发送SYSLOG信息、发送RST阻断报文、防火墙联动、全局预警、提取原始报文； |
| 报表功能 | 系统需提供完善的报表系统，支持面向安全结论的分析报表；报表需支持如下格式：HTML、PDF、EXCEL、WORD，所生成的报表可以自动发送到多个邮箱，能辅助用户查阅； |
| 规则库升级 | 安全规则库支持在线自动升级、手动升级升级等多种方式 |
| 资质要求 | 产品要求取得中国人民共和国公安部的《计算机信息系统安全专用产品销售许可证》,提供有效证书的复印件 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 探针A（4台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 性能要求 | 吞吐性能，≥10Gbps。 |
| 接口数量 | 不少于4个万兆光口，8个千兆光口，8个千兆电口； |
| 部署模式 | 旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响。 |
| 资产发现 | 具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。 |
| 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等, 具备多种的入侵攻击模式或恶意URL监测模式,可完成模式匹配并生成事件,可提取URL记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP对)进行原始报文的录制。 |
| 监测识别规则库 | 能够识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。漏洞利用规则特征库数量在4000条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号。 |
| 异常流量检测 | 支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等。 |
| 深度监测能力 | 可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描，端口扫描，ARP欺骗，IP协议异常报文检测和TCP协议异常报文等常见网络异常流量事件类型。 |
| 高级检测 | 支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。 |
| 日志审计 | 支持DNS审计日志，主要用于平台dns flow分析引擎进行安全分析；HTTP审计日志，主要用于平台http flow分析引擎进行安全分析；SMB审计日志，主要用于平台SMB flow分析引擎进行安全分析；同步SMTP、POP3、IMAP审计日志，主要用于平台Mail flow分析引擎进行安全分析，同步AD域协议审计日志，主要用于平台AD域分析引擎进行安全分析。 |
| 违规访问检测 | 能够针对IP，IP组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式。 |
| 流量记录 | 能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP会话记录、Web访问记录、SQL访问记录、DNS解析记录、文件传输行为、LDAP登录行为。 |
| 抓包分析 | 支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式。 |
| 集中管控 | 支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级。 |
| 部署 | 可以多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台。 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 路由器B（10台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 体系架构 | 支持主控板、交换网板、业务板完全物理分离，主控板、交换网板、业务板分布在不同的物理槽位，需提供设备面板图并指出对应的主控板、交换网板和业务板槽位 |
| 为保证设备可靠性，设备的转发全部有交换网板完成，主控板不集成转发芯片 |
| 为保证可靠性，设备需支持板卡（含主控，线卡，交换网板等）直接热插拔，同时不需要插拔电源风扇等其他关键部件 |
| 交换容量 | △交换容量≥130Tbps，以官网最小值为准，需提供官方网站截图，原厂盖章 |
| 包转发率 | △包转发率≥18000Mpps，以官网最小值为准，需提供官方网站截图，原厂盖章 |
| 业务槽位 | △为保障性能平滑升级，设备采用子母卡架构设计，子卡插在母板上，子卡母板均支持热拔插，单块母板支持嵌套安装2-4块业务子卡，提供产品图片证明并加盖原厂公章 |
| 电源系统 | 支持电源个数≥4个，电源系统支持N+M冗余 |
| 基本功能 | 支持PPP、MP、HDLC、ETHERNET等链路层协议 |
| 支持链路聚合（Link aggregation），支持动态聚合、手工聚合、跨板聚合 |
| 支持不同带宽的链路捆绑功能，提供第三方测试报告 |
| 支持多路径负责分担功能（UCMP），支持非等速链路的负载分担，实现不同路径按带宽比例负载分担，提供第三方测试报告 |
| 支持IPV4静态路由、RIPv1/v2、OSPFv2、BGP、IS-IS、路由策略，支持4M IPv4 FIB |
| 支持IPv6静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+，支持2M IPv6 FIB |
| 支持L2VPN、L3VPN、OptionA、B、C类跨域，支持16K VPN，支持4M VPN路由 |
| 接口类型 | 支持FE、GE、10Ge（LAN/WAN）、40Ge、100Ge、155M POS、622M POS、2.5G POS、10G POS、CPOS接口、155M ATM、622M ATM、E1等接口 |
| 支持ATM/POS端口灵活切换 |
| GRE | 支持分布式GRE功能，为保证性能，本次要求实配GRE功能板卡或license  |
| Netstream | 支持分布式Netstream功能，本次要求实配支持NetStream功能板卡或license |
| NAT | 支持分布式NAT功能，本次要求实配NAT功能板卡或license |
| 组播VPN（MVPN） | 支持分布式MVPN功能 |
| 虚拟化 | 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，需提供官方网站截图 |
| IPv6 | 具备IPv6能力，所投设备需提供IPv6 Ready II证书 |
| SRv6 | △支持SRv6功能，并提供权威检测机构颁发的SRv6 Ready检测证书，检测机构需要通过CNAS能力认可 |
| QOS | 支持优先级Mark/Remark、CAR（Committed Access Rate）、GTS等功能 |
| QOSSDN | 为简化ACL配置，设备需支持全局ACL功能，提供第三方测试报告 |
| 支持FIFO、PQ、WFQ、LLQ等各种队列调度机制，支持拥塞避免算法：Tail-Drop、RED、WRED，支持层次化Qos（H-Qos） |
| 设备支持通过Netconf（RFC 6241）协议下发配置 |
| SDN可靠性 | 设备支持YANG功能（RFC 6020） |
| 为实现设备间链路状态等信息共享，设备需支持BGP Link-State功能（RFC 7752) |
| 为实现单节点上安全策略同步功能，设备需支持BGP FlowSpec功能（RFC 5575) |
| 为实现报文最优路径转发，设备需支持Segment Routing（RFC7855）协议 |
| 为实现按业务优先级选择隧道路径，设备需支持CBTS功能（YD/T 1391.1） |
| 设备支持Openflow协议，报文可依据流表进行转发 |
| 为保证业务调度的精细化控制，设备需要支持13层标签 |
| 设备支持EVPN/VxLAN（RFC 7348）功能，能够完成MAC地址远端学习，实现基于VxLAN的二三层VPN |
| 实配双主控 |
| 可靠性网络安全 | 支持VRRP/VRRPv3、MPLS TE FRR、IP FRR（静态路由/策略路由/RIP/IS-IS/OSPF等） |
| 为减小设备或线路故障对业务的影响、提高网络的可用性，需支持BFD for BGP/IS-IS/OSPF/LDP/VRRP/Static Route |
| 支持热补丁功能，可在线进行补丁升级 |
| 为提高设备软件稳定性及可靠性，主备倒换时业务不中断，需要支持NSR功能 |
| 为提高设备硬件稳定性及可靠性，交换网板、板卡、子卡支持热插拔功能 |
| 为检测设备之间的可达性、时延、丢包率、抖动等信息，设备需支持NQA检测网络网络质量 |
| 设备支持防攻击能力，包括：ARP攻击、IPv6报文攻击、超大Trace报文攻击、TCP SYN flood、Ping flood、DHCP DDOS、PADI DDOS的防御等 |
| 网络安全维护特性 | 支持OSPF、OSPFv3、ISIS、ISISv6、BGP、BGP4+的MD5认证功能，支持Keychain功能，可以支持基于时间段的生效的秘钥，提供第三方测试报告 |
| 为方便设备运维管理，设备需内置TCL语言功能，能够解析执行TCL语言脚本 |
| 维护特性工信部入网许可证 | 为方便设备运维管理，设备需内置Python语言功能，能够解析执行Python语言脚本 |
| 为实现设备精细化管理，实现不同进程动态部署到不同的CPU上，设备需支持进程分布式优化功能，提供第三方测试报告 |
| 为实现基于角色的权限灵活授权，并且和AAA联动，设备需支持RBAC功能 |
| 为方便设备配置文件管理，设备需支持配置回滚功能，提供第三方测试报告 |
| 提供工信部入网许可证复印件 |
| △单台实配 | 4台配置：实配双主控，双电源模块，100G光口≥6块，10G光口≥10块，100G光模≥3块，10G光模块≥4块，满足设备100G互连条件，支持SRv6功能； |
| 6台配置：实配双主控，双电源模块，100G光口≥4块，40G光口≥2块，10G光口≥6块，100G光模块≥2块，40G光模块≥2块，10G光模块≥4块，满足设备100G互连条件； |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 防火墙A（8台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 硬件架构 | 采用多核路由器架构，双主控，双电源 |
| 接口板和业务板分离，电源、主控板、接口板、业务板支持热插拔； |
| 当风扇模块出现故障时，可以在防火墙不断电的情况下，对风扇模块进行更换； |
| 采用多核路由器架构，双主控，双电源；除两个主控板外，整机扩展插槽≥6（提供设备照片）； |
| 性能要求 | △吞吐量实配≥100G；每秒新建连接数≥60万，最大并发数≥2500万 |
| 路由特性 | IPv4：静态路由、策略路由、路由策略、RIP、OSPFv1/v2、BGP、IS-IS；IPv6：RIPng、OSPFv3、BGP4+、IPv6 IS-IS、IPv6RD、ACL6 |
| 策略路由支持的匹配条件：源IP/目的IP，服务类型，应用类型，用户(组)，入接口，DSCP优先级。 |
| 应用识别&控制 | 可识别应用层协议数量≥5000种 |
| 支持URL识别能力和URL地址识别库，URL识别库≥8000万 |
| 支持在本地部署URL服务器实现URL过滤。 |
| 支持DNS过滤，提高WEB网页过滤的性能。 |
| 策略管理 | 支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维。 |
| 支持将基于端口的安全策略转换为基于应用的安全策略，对安全策略进行命中分析，冗余分析。 |
| 数据安全 | 支持DNS过滤，提高WEB网页过滤的性能； |
| 入侵防御及病毒防护 | 基于特征检测，支持超过5000种特征的攻击检测和防御 |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能。 |
| 产品资质 | 产品要求取得中国人民共和国公安部的《计算机信息系统安全专用产品销售许可证》,提供有效证书的复印件 |
| 实配 | △万兆光口≥6块，100GE接口≥4个，并配置相应模块；配置URL、入侵防御、防病毒功能和3年规则库更新授权 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 交换机A（8台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 交换容量 | 交换容量≥250Tbps |
| 包转发率 | 包转发率≥14000Mpps |
| 单板槽位 | 主控引擎与交换网板物理分离；主控引擎≥2；独立交换网板≥2；整机业务板槽位数≥4主控槽位与业务线卡槽位宽度相同，为全宽槽位 |
| 槽位带宽 | 支持每槽位转发能力≥2.4Tbps |
| MAC | 支持整机MAC地址≥512K |
| 二层功能 | 支持IEEE 802.1d(STP)、 802.1w(RSTP)、 802.1s(MSTP)，支持1:1、 N:1、1:N端口镜像，支持流镜像，支持远程端口镜像（RSPAN），支持ERSPAN |
| IPv6 | 支持IPv6过渡技术，IPv4/IPv6双栈、6over4隧道、4 over6隧道支持IPv6 DHCP SERVER、IPv6 DHCP Relay、DHCP Snooping |
| MPLS | 支持MPLS L3VPN、MPLS L2VPN(VPLS，VLL)、MPLS-TE、MPLS QoS |
| 安全性 | 支持DHCP snooping binding table (DAI, IP source guard)，防止ARP攻击、DDOS攻击、中间人攻击支持自动隔离攻击源技术 |
| 可靠性 | 支持真实业务流的实时检测技术，实现对IP网络的精确丢包监控和快速故障定界能力 |
| 支持硬件BFD/OAM，3.3ms稳定均匀发包检测，提高设备的可靠性 |
| 管理特性 | 支持SNMP V1/V2/V3、Telnet、RMON、SSHV2支持通过命令行、中文图形化配置软件等方式进行配置和管理 |
| 实配 | 配置双主控，双电源；≥48个千兆电口，≥48个万兆光接口，≥6个100G接口；并配置相应模块，≥2个电源；含原厂3年现场维保服务 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 接入交换机A型（10台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 交换容量 | 交换容量≥19Tbps |
| 包转发率 | 包转发率≥1400Mpps |
| 机柜要求 | 适用600mm深度机柜 |
| 设备高度≤4U |
| 硬件 | 主控引擎≥2；整机业务板槽位数≥3 |
| 支持颗粒化电源，整机电源槽位数≥3 |
| 颗粒化电源模块上支持电源开关，可控制单电源模块的供电状态，便于安装、维护及更换； |
| 为适应机柜并排部署，设备机箱（包括业务板卡区）采用后出风风道设计 |
| 用户管理 | 支持802.1X、MAC、Portal等认证方式 |
| 支持基于流量、DAA目的地址和时长计费方式 |
| VLAN | 支持4K VLAN支持1：1，N：1 VLAN mapping |
| 二层功能 | 支持IEEE 802.1d(STP)、 802.w(RSTP)、 802.1s(MSTP)支持ERSPAN, 通过GRE隧道实现跨域远程镜像； |
| IP路由 | 支持IPv4路由转发FIB表项≥128K，提供权威第三方测试报告 |
| 支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6支持路由协议多实例 |
| IPV6 | 支持IPv6过渡技术，IPv4/IPv6双栈、6over4隧道、4 over6隧道支持IPv6 DHCP SERVER, IPv6 DHCP Relay, DHCP Snooping，支持IPv6 Souce Guard |
| MPLS | 支持MPLS L3VPN、MPLS L2VPN(VPLS，VLL)、MPLS-TE、MPLS QoS |
| 访问控制 | 支持整机ACL表项≥256K |
| 安全性 | 支持DHCP Snooping trust, 防止私设DHCP服务器；支持DHCP snooping binding table (DAI, IP source guard), 防止ARP攻击、DDOS攻击、中间人攻击； |
| 可靠性 | 支持真实业务流的实时检测技术，秒级快速故障定位 |
| 管理特性 | 支持SNMP V1/V2/V3、Telnet、RMON、SSHV2 |
| 支持通过命令行、中文图形化配置软件等方式进行配置和管理 |
| 支持WEB网管 |
| 实配 | 配置双主控，双电源，≥6个40G/100GE接口，≥48个万兆光接口，并配置相应模块含原厂3年现场维保服务 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 接入交换机B型（10台）

| **指标项** | **参数要求** |
| --- | --- |
| 交换容量 | 交换容量≥650Gbps |
| 包转发率 | 包转发率≥144Mpps |
| 电源数量 | 为了提高设备可靠性，支持模块化可插拔双电源 |
| 硬件 | 支持48个10/100/1000Base-T以太网端口，4个万兆SFP+，并配置相应光模块 |
| 二层 | 支持MAC地址规格≥32K |
| 支持Super VLAN、支持Voice VLAN、支持组播VLAN |
| 支持4K VLAN，支持QinQ，灵活QinQ、支持端口VLAN、协议VLAN、IP子网VLAN |
| 三层 | 支支持RIP、RIPng、OSPF、OSPFv3、ISIS、BGP等路由协议 |
| 支持Ipv4路由FIB表≥16K，Ipv6路由FIB表≥8K |
| QOS | 支持DRR、SP、DRR+SP调度方式 |
| 支持双向端口限速，广播风暴抑制功能 |
| 可靠性 | 支持真实业务流实时检测技术，实时检测网络故障 |
| 管理维护 | 支持SNMP v1/v2/v3、Telnet、RMON、SSHv2；支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理； |
| 实配 | 配置相应模块，实配双电源 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 接入交换机C型（26台）

| **指标项** | **参数要求** |
| --- | --- |
| 交换容量 | 交换容量≥650Gbps |
| 包转发率 | 包转发率≥105Mpps |
| 电源 | 为了提高设备可靠性，支持并实配模块化可插拔双电源 |
| 端口类型 | 支持24个10/100/1000Base-T以太网端口，4个万兆SFP+，配置相应光模块 |
| 二层功能 | 支持MAC地址规格≥32K |
| 支持ARP表项规格≥8K |
| 支持4K VLAN，支持QinQ，灵活QinQ、支持端口VLAN、协议VLAN、IP子网VLAN |
| 三层功能 | 支持静态路由、RIP v1/v2、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+ |
| 支持IPv4 路由表≥16K |
| 支持IPv6 路由表≥8K |
| 镜像功能 | 支持多个物理端口的流量镜像到一个端口支持流镜像、远程端口镜像（RSPAN） |
| QoS | 支持DRR、SP、DRR+SP调度方式支持双向端口限速，广播风暴抑制功能 |
| 可靠性 | 支持真实业务流实时检测技术，实时检测网络故障 |
| 管理维护 | 支持SNMP v1/v2/v3、Telnet、RMON、SSHv2；支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理；  |
| 实配 | 并配置相应模块，实配双电源 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 路由器C（6台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 体系架构 | 支持主控板、交换网板、业务板完全物理分离，主控板、交换网板、业务板分布在不同的物理槽位，需提供设备面板图并指出对应的主控板、交换网板和业务板槽位 |
| 为保证设备可靠性，设备的转发全部有交换网板完成，主控板不集成转发芯片 |
| 为保证可靠性，设备需支持板卡（含主控，线卡，交换网板等）直接热插拔，同时不需要插拔电源风扇等其他关键部件 |
| 交换容量 | △交换容量≥115Tbps，以官网最小值为准，需提供官方网站截图，原厂盖章 |
| 包转发率 | △包转发率≥9000Mpps，以官网最小值为准，需提供官方网站截图，原厂盖章 |
| 业务槽位 | △为保障性能平滑升级，设备采用子母卡架构设计，子卡插在母板上，子卡母板均支持热拔插，单块母板支持嵌套安装2-4块业务子卡，提供产品图片证明并加盖原厂公章 |
| 电源系统 | 支持电源个数≥4个，电源系统支持N+M冗余 |
| 基本功能 | 支持PPP、MP、HDLC、ETHERNET等链路层协议 |
| 支持链路聚合（Link aggregation），支持动态聚合、手工聚合、跨板聚合 |
| 支持不同带宽的链路捆绑功能，提供第三方测试报告 |
| 支持多路径负责分担功能（UCMP），支持非等速链路的负载分担，实现不同路径按带宽比例负载分担，提供第三方测试报告 |
| 支持IPV4静态路由、RIPv1/v2、OSPFv2、BGP、IS-IS、路由策略，支持4M IPv4 FIB |
| 支持IPv6静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+，支持2M IPv6 FIB |
| 支持L2VPN、L3VPN、OptionA、B、C类跨域，支持16K VPN，支持4M VPN路由 |
| 接口类型 | 支持FE、GE、10Ge（LAN/WAN）、40Ge、100Ge、155M POS、622M POS、2.5G POS、10G POS、CPOS接口、155M ATM、622M ATM、E1等接口 |
| 支持ATM/POS端口灵活切换 |
| GRE | 支持分布式GRE功能，为保证性能，本次要求实配GRE功能板卡或license  |
| Netstream | 支持分布式Netstream功能，本次要求实配支持NetStream功能板卡或license |
| NAT | 支持分布式NAT功能，本次要求实配NAT功能板卡或license |
| 组播VPN（MVPN） | 支持分布式MVPN功能 |
| 虚拟化 | 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，需提供官方网站截图 |
| IPv6 | 具备IPv6能力，所投设备需提供IPv6 Ready II证书 |
| SRv6 | △支持SRv6功能，并提供权威检测机构颁发的SRv6 Ready检测证书，检测机构需要通过CNAS能力认可 |
| QOS | 支持优先级Mark/Remark、CAR（Committed Access Rate）、GTS等功能 |
| 为简化ACL配置，设备需支持全局ACL功能 |
| 支持FIFO、PQ、WFQ、LLQ等各种队列调度机制，支持拥塞避免算法：Tail-Drop、RED、WRED，支持层次化Qos（H-Qos） |
| SDN | 设备支持通过Netconf（RFC 6241）协议下发配置 |
| 设备支持YANG功能（RFC 6020） |
| 为实现设备间链路状态等信息共享，设备需支持BGP Link-State功能（RFC 7752) |
| 为实现单节点上安全策略同步功能，设备需支持BGP FlowSpec功能（RFC 5575) |
| 为实现报文最优路径转发，设备需支持Segment Routing（RFC7855）协议 |
| 为实现按业务优先级选择隧道路径，设备需支持CBTS功能（YD/T 1391.1） |
| 设备支持Openflow协议，报文可依据流表进行转发 |
| 为保证业务调度的精细化控制，设备需要支持13层标签 |
| 设备支持EVPN/VxLAN（RFC 7348）功能，能够完成MAC地址远端学习，实现基于VxLAN的二三层VPN |
| 可靠性 | 实配双主控 |
| 支持VRRP/VRRPv3、MPLS TE FRR、IP FRR（静态路由/策略路由/RIP/IS-IS/OSPF等） |
| 为减小设备或线路故障对业务的影响、提高网络的可用性，需支持BFD for BGP/IS-IS/OSPF/LDP/VRRP/Static Route |
| 支持热补丁功能，可在线进行补丁升级 |
| 为提高设备软件稳定性及可靠性，主备倒换时业务不中断，需要支持NSR功能 |
| 为提高设备硬件稳定性及可靠性，交换网板、板卡、子卡支持热插拔功能 |
| 为检测设备之间的可达性、时延、丢包率、抖动等信息，设备需支持NQA检测网络网络质量 |
| 网络安全 | 设备支持防攻击能力，包括：ARP攻击、IPv6报文攻击、超大Trace报文攻击、TCP SYN flood、Ping flood、DHCP DDOS、PADI DDOS的防御等，提供第三方测试报告 |
| 支持OSPF、OSPFv3、ISIS、ISISv6、BGP、BGP4+的MD5认证功能，支持Keychain功能，可以支持基于时间段的生效的秘钥 |
| 维护特性 | 为方便设备运维管理，设备需内置TCL语言功能，能够解析执行TCL语言脚本 |
| 为方便设备运维管理，设备需内置Python语言功能，能够解析执行Python语言脚本 |
| 为实现设备精细化管理，实现不同进程动态部署到不同的CPU上，设备需支持进程分布式优化功能，提供第三方测试报告 |
| 为实现基于角色的权限灵活授权，并且和AAA联动，设备需支持RBAC功能 |
| 为方便设备配置文件管理，设备需支持配置回滚功能 |
| 资质证书 | 提供工信部入网许可证复印件 |
| 提供工信部BNAS入网许可证复印件 |
| 统一纳管技术适配 | △设备厂家须提供承诺（加盖公章）：投标设备能够被市级政务外网通过SDN控制器进行统一纳管、控制。 |
| △单台实配 | 2台配置：实配双主控，双电源模块，不少于3个40G光口，10个10G光口， 2块40G多模光模块，4块10G多模光模块，每两台配置1根100G电缆，支持SRv6功能； |
| 2台配置：实配双主控，双电源模块，不少于5个10G兆光口，4个1G光电复用口，3块10G多模光模块，每两台配置1根100G电缆，支持SRv6功能； |
| 2台配置：实配双主控，双电源模块，不少于2个100G光口，1个40G光口，2块100G多模光模块，1块40G多模光模块，每两台配置1根100G电缆，支持SRv6功能； |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 防火墙B（2台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| **硬件规格** | 产品不少于4个40G光口，12个万兆光口，4个千兆光口，4个千兆电口 |
| **性能要求** | 网络层吞吐量≥60Gbps，应用层吞吐量≥35Gbps |
| **部署方式** | 具备路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。 |
| **路由功能** | 支持静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议。 |
| **地址转换** | 支持IPv4／IPv6下NAT地址转换，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持NAT64、NAT46 地址转换。 |
| **IPv6** | 支持IPv4/IPv6双栈工作模式，支持IPv6环境的应用控制策略设置，能针对IPv6的IP地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。 |
| **VPN** | IPSec VPN支持智能选路功能，保障业务的高可靠性。 |
| **地域访问控制** | 支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。 |
| **流量控制** | 具备基于国家/地区的流量管理功能，对数据流量和访问来源进行辨识和分类，保障精细化管理和控制。 |
| **双机部署** | 支持主主、主备两种双机模式部署。 |
| **安全报表** | 产品内置安全报表模板，可定义报表内容，包括网络整体安全状况、服务器安全风险分析、终端主机安全风险分析等。 |
| **用户管理权限** | 支持三权分立功能，根据用户权限分为安全管理员、审计员、系统管理员三种角色； |
| **集中管理** | 产品支持接入集中管理平台实现多设备的统一管理，通过集中管理平台统一配置产品的安全策略，包括但不限于访问控制、入侵防御、防病毒、Web应用防护等安全策略。 |
| **产品资质** | 产品要求取得中国人民共和国公安部的《计算机信息系统安全专用产品销售许可证》,提供有效证书的复印件 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 防火墙C（2台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| **硬件要求** | 系统应为2U标准式机架硬件设备， CPU采用国产处理器，操作系统采用国产操作系统； |
| 千兆光口≥2个, 千兆电口≥2个； |
| 硬盘存储空间≥1T； |
| **性能要求** | 网络层吞吐量≥10G； |
| 新建连接数≥14万； |
| 最大并发连接数≥500万； |
| **防火墙** | 支持虚拟线、二层透明、路由、混合，适应各种网络环境需求。 |
| 支持IPMAC绑定，支持手动和自动探测绑定 |
| 能够在一条策略里配置源/目的IP地址、安全区、应用/应用组、协议/端口、时间、用户、安全模板/模板组， |
| 支持策略优化（冗余，冲突） |
| 支持基于策略的双向NAT、动态/静态NAT。 |
| 支持基于源/目的地址、接口的、基于服务、应用类型、用户的策略路由； |
| 支持链路探测，能够在每接口上以ICMP/TCP/UDP协议探测目标主机可达性，探测链路是否有效 |
| 支持基于源、目地IP、应用类型、时间段实行带宽限制、带宽保证等策略； |
| 支持泛洪类攻击防护：UDP/DNS/SYN/PING 泛洪；支持ARP欺骗类攻击； |
| **识别能力** | 支持对2000+种应用平台及2200+种的应用进行识别和控制，至少支持5大类，比如：商业系统、协作应用、一般网络应用、媒体等及28子类，比如：认证服务、数据库、ERP-CRM、软件更新、电子邮件、VOIP视频、游戏等；支持自定义应用；  |
| 支持应用过滤器，至少支持4个维度进行过滤，比如：应用类别、实现技术、风险等级、标签， |
| 能够将通过应用过滤器筛选出来的应用直接生成模板供用户统一管理使用， |
| 可以识别和控制文件传输途径，如允许/禁止QQ/MSN、FTP、飞信等传文件，支持达梦和神州通用的内容识别 |
| 支持达梦，人大金仓，神州通用等国产数据库的识别 |
| 支持设置应用超时时间， |
| **入侵防护** | 支持4400+种入侵规则过滤，  |
| 支持远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL注入、跨站脚本等等检测和防护， |
| 支持对入侵规则库的分类组织和管理，包括：攻击手段/技术/流行度/危险度/服务类型 |
| 支持自定义规则/规则组 |
| **URL过滤** | 提供64+种精细分类（广告及弹出窗口、烟酒、匿名网站、艺术、聊天、盗用网站、犯罪活动等） |
| **内容过滤** | HTTP、FTP、邮件等，支持对文件类型过滤 |
| HTTP支持协议命令过滤，如GET、POST |
| 支持网页浏览、论坛发帖、电子邮件、即时通讯、文件传输、服务器操作等信息关键字的实时检测和过滤， |
| 支持自定义内容过滤关键字 |
| **防病毒** | 支持病毒检测与防护功能 |
| **HA** | 支持主备、主主两种模式 |
| 支持会话同步、状态同步，配置同步， 支持链路状态的监测  |
| **系统管理** | 在界面上除了支持完全备份，还需支持单独项备份  |
| 支持实时显示Top10应用、Top10用户、各接口流量走势； |
| 支持防火墙、入侵防护、URL过滤、防病毒、内容过滤的日志记录； |
| 能够呈现历史应用流量、应用会话走势图，并可按时、日、周显示； |
| **产品资质** | 产品需为信创目录内产品 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 入侵防御（2台）

| **指标项** | **参数要求** |
| --- | --- |
| 硬件规格 | 系统应为2U标准式机架硬件设备，全内置封闭式结构，具有国产化的操作系统、内存≥16G；硬盘存储空间≥4T；支持冗余电源； |
| 千兆电口≥8个,千兆光口≥4个,扩展槽位≥1； |
| 产品性能 | 网络层吞吐量≥9.5Gbps,应用层吞吐量≥3Gbps；最大并发TCP会话数≥500万； |
| 产品功能 | 系统须提供对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破解等恶意流量的检测。 |
| 系统应提供覆盖广泛的攻击特征库，能够针对攻击行为、异常事件，以及网络资源滥用流量进行检测。 |
| 系统应提供入侵行为和应用软件特征的自定义接口，可根据用户需求定制对其它流量的检测规则。 |
| 系统应支持多种抗逃避检测技术 |
| 系统应能够有效抵御SQL注入等多种常见的应用层安全威胁 |
| DoS/DDoS检测 | 系统应提供DoS/DDoS攻击检测能力，支持TCP/UDP/ICMP/ACK Flooding，以及UDP/ICMP Smurfing等常见的DoS/DDoS的攻击 |
| 支持设置阈值 |
| 应用识别 | 系统应能识别主流的应用程序，识别不少于2500个应用 |
| 流量分析 | 系统应支持全面的流量分析功能，可察看网络实时流量，包括：流量协议分布、流量IP分布、常见流量TOP10等。 |
| 攻击响应 | 系统应提供攻击响应功能，包括会话阻断功能，满足用户响应需求 |
| 攻击取证 | 系统应具备攻击快照功能，详细记录触发告警的数据特征，以便做进一步的事件分析 |
| 日志归并 | 系统应具备实时的日志归并功能，可以根据用户需要，按照告警事件的源/目的IP、事件类型等信息，对告警日志执行归并，有效抵御告警风暴 |
| 用户认证 | 系统应具备用户身份识别能力，支持基于用户身份进行策略配置、日志记录与查询；支持自动与手动获取用户信息列表并生成组织结构图 |
| IPv6协议 | 系统须支持IPv6/IPv4双协议栈功能，能同时辨识IPv4和IPv6通讯流量。支持IPv6环境下攻击检测技术和基于IPv6地址格式的安全控制策略，为IPv6环境提供入侵检测 |
| 设备管理 | 系统应支持私有升级中心功能，部署在局域网的设备也能够实现自动升级 |
| 系统应提供标准snmp 、syslog接口，可接受第三方管理平台的集中事件管理 |
| 产品资质 | 产品需为信创目录内产品 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 交换机B型（2台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 交换机性能 | 24口款型：交换容量≥336Gbps，包转发能力≥108Mpps |
| 端口要求 | 24口款型：千兆电口≥24，不复用的万兆光口≥4 |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN；最大VLAN数(不是VLAN ID)≥4094 |
| MAC表 | ≥16K |
| 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN，要求提供CNAS认证权威检测机构颁发的测试报告证明 |
| 链路聚合 | 支持最多8个GE口E端口聚合，支持最多14个聚合组；支持LACP |
| 三层路由功能 | 支持Ipv4和Ipv6三层路由功能，包括静态路由、RIP、RIPng、OSPF等 |
| QoS | 支持802.1P，DSCP/TOS优先级和重新标记能力，支持基于时间段的流分类和QoS控制能力；提供广播风暴抑制功能 |
| 组播协议 | 支持IGMP v1/v2/v3，MLD v1/v2，IGMP Snooping v1/v2/v3，MLD Snooping v1/v2，要求提供CNAS认证权威检测机构颁发的测试报告证明；支持组播VLAN |
| 生成树 | 支持STP/RSTP/MSTP协议；支持PVST协议, 要求提供CNAS认证权威检测机构颁发的测试报告证明 |
| 访问控制策略 | 支持基于第二层、第三层和第四层的ACL；支持IPv6的ACL策略 |
| 安全特性 | 支持IP+MAC+PORT的绑定；支持DHCP Snooping，防止欺骗的DHCP服务器；支持ARP检测来抵御ARP欺骗攻击；支持IP Source Check；支持IPv6安全特性包括IPv6环境下的IP＋MAC＋PORT绑定，NP detection，ND Snooping等；支持802.1x认证，支持集中式MAC地址认证； |
| 堆叠 | 支持多台设备虚拟化为一台，实现单一IP管理，跨设备链路聚合；支持通过标准以太网接口进行堆叠；支持本地堆叠和远程堆叠 |
| 管理特性 | 支持SNMP V1/V2/V3、RMON、SSHV2；支持虚电缆检测功能，快速准确定位网络中故障电缆的短路或断路点；支持单向链路检测,有效的防止网络中单通故障的发生；支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理 |
| 资质认证 | 提供工信部入网证 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 防火墙D（2台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| **硬件规格** | 产品不少于4个40G光口，12个万兆光口，4个千兆光口，4个千兆电口 |
| **性能要求** | 网络层吞吐量≥60Gbps，应用层吞吐量≥35Gbps |
| **部署方式** | 具备路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。 |
| **路由功能** | 支持静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议。 |
| **地址转换** | 支持IPv4／IPv6下NAT地址转换，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持NAT64、NAT46 地址转换。 |
| **IPv6** | 支持IPv4/IPv6双栈工作模式，支持IPv6环境的应用控制策略设置，能针对IPv6的IP地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。 |
| **VPN** | IPSec VPN支持智能选路功能，保障业务的高可靠性。 |
| **地域访问控制** | 支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。 |
| **流量控制** | 具备基于国家/地区的流量管理功能，对数据流量和访问来源进行辨识和分类，保障精细化管理和控制。 |
| **入侵防御** | 支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则。 |
| 支持僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。 |
| **双机部署** | 支持主主、主备两种双机模式部署。 |
| **安全报表** | 产品内置安全报表模板，可定义报表内容，包括网络整体安全状况、服务器安全风险分析、终端主机安全风险分析等。 |
| **用户管理权限** | 支持三权分立功能，根据用户权限分为安全管理员、审计员、系统管理员三种角色； |
| **集中管理** | 产品支持接入集中管理平台实现多设备的统一管理，通过集中管理平台统一配置产品的安全策略，包括但不限于访问控制、入侵防御、防病毒、Web应用防护等安全策略。 |
| **产品资质** | 产品要求取得中国人民共和国公安部的《计算机信息系统安全专用产品销售许可证》,提供有效证书的复印件 |
| **服务及质保要求** | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 入侵检测B（1台）

| **指标项** | **参数要求** |
| --- | --- |
| 硬件指标 | ≥1TB硬盘，≥2\*10GE，≥6\*GE |
| 性能指标 | TCP最大并发数：500万，满检速率：19739.901Mbps |
| 部署方式 | 产品支持旁路镜像部署方式  |
| 攻击检测能力 | 系统需要支持如下常见协议的解析：ETHER、ARP、RARP、IP、ICMP、IGMP、PPPoE、Vlan Tag、MPLS、TCP、UDP、NetBIOS、CIFS、SMB、FTP、TELNET、POP3、SMTP、IMAP、SNMP、MSRPC、SUNRPC、TNS、TDS、HTTP、QQ、MSN、BT、Thunder、CHARGEN、ECHO、AUTH、DNS、FINGER、IRC、MSPROXY、NFS、NNTP、NTALK、PCT、WHOIS等，协议； |
| 能够对缓冲区溢出、网络蠕虫、网络数据库攻击、木马软件、间谍软件等各种攻击行为进行检测； |
| 系统需具备对针对Web系统（包括浏览器、服务器）的攻击具备检测能力：SQL注入（包括各种变形）、XSS（包括存储式XSS、反射式XSS）及其各种语法变形、Webshell、网页挂马、语义变形、编码等环境下的精确检测能力； |
| 用户可自定义添加入侵检测规则，并定义入侵响应时间 |
| 多级分布和全局预警 | 系统支持多级部署，集中管理能力，可以添加组件（包括子控、引擎）提供各个组件（子控、引擎）的拓扑图，并在图中动态显示组件之间的实时连接状态； |
| 级联环境中，上级针对下发策略的锁定，锁定子控的一些策略，锁定的事件是不允许进行配置、编辑、删除等操作的； |
| 威胁响应能力 | 支持如下报警响应方式：计入日志、页面报警、发送邮件、发送SNMP Trap信息、发送SYSLOG信息、发送RST阻断报文、防火墙联动、全局预警、提取原始报文； |
| 报表功能 | 系统需提供完善的报表系统，支持面向安全结论的分析报表；报表需支持如下格式：HTML、PDF、EXCEL、WORD，所生成的报表可以自动发送到多个邮箱，能辅助用户查阅； |
| 规则库升级 | 安全规则库支持在线自动升级、手动升级升级等多种方式 |
| 产品资质 | 产品要求取得中国人民共和国公安部的《计算机信息系统安全专用产品销售许可证》,提供有效证书的复印件 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 交换机C型（2台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 业务槽位 | 槽位数≥3 |
| 交换容量 | 交换容量≥28.8Tbps，以官网最小值为准，需提供官方网站截图 |
| 转发能力 | 包转发率≥4320Mpps，以官网最小值为准，需提供官方网站截图 |
| 电源冗余 | 电源模块冗余配置 |
| 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 |
| 主控引擎 | 主控引擎模块≥2，实配1+1冗余 |
| 接口要求 | 以太网支持千兆电口，千兆光口，万兆光口、万兆电，25G端口、40G端口、100G端口 |
| 单槽位万兆线速端口密度≥48 |
| 单槽位40G端口密度≥ 24  |
| 2台实配端口不少于48个千兆电口，16个万兆光口，并配置相应光模块 |
| 支持GEPON OLT或10G EPON OLT接口，提供官网配置手册截图和链接 |
| 链路聚合 | 聚合组数≥1023组，每组成员≥32个 |
| 支持跨设备链路聚合 |
| ACL | 支持双向ACL，ACL≥4K |
| 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BFD，能够实现BFD与OSPF/VRRP联动。 |
| 支持sFlow、Netstream流量统计和分析功能 |
| IPv6 | 支持RIPng、OSPFv3、BGP4+、IS-ISv6协议 |
| 支持IPv6策略路由； |
| 支持DHCPv6功能、IPv6 portal功能、IPv6管理功能； |
| 支持基于IPv6的VXLAN二三层互通； |
| 支持基于IPv6的VRRP功能 |
| 虚拟化 | 支持多虚一技术(N:1)，支持4框虚拟化技术，需提供官方网站截图 |
| 支持一虚多技术（1:N） |
| 支持多虚一技术和一虚多技术的配合使用 |
| 支持二级PE端口扩展设备级联：CB（Controlling Bridge）控制设备能够支持二级PE（Port Extender）端口扩展设备级联，即一级PE端口扩展设备下挂二级PE端口扩展设备。 |
| 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； |
| 网络安全一体化 | 支持IPS、应用控制、LB、FW等安全业务插卡，需提供官方网站截图 |
| 可视化 | 支持Telemetry流量可视化功能 |
| 多业务融合化 | 支持多业务融合板卡，与设备紧耦合无需外部连线，支持部署Windows Server及SDN控制器，实现方案与设备一体化部署 |
| 终端管理及网络安全 | 支持融合多业务板卡，实现对摄像头等物联终端统一识别、认证和管理， |
| 支持PC终端、哑终端、网络设备等连接元素的准入控制和权限划分，确保网络的可信可控 |
| 支持设备识别、归类、类型定义，可以对全网资产进行梳理，识别异常终端链接，确保网络的安全性 |
| MPLS | 支持L3 VPN、VLL、支持VPLS、支持MCE |
| SDN/OPENFLOW | 支持OPENFLOW |
| 支持普通模式和Openflow 模式切换 |
| VxLAN | 支持VXLAN，能够实现VXLAN二三层互通 |
| 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MACsec加密技术 |
| 支持端口隔离 |
| 支持IP+MAC+VLAN+PORT的绑定 |
| 支持802.1x、mac认证、Portal认证 |
| 管理特性 | 支持Console/AUX/Telnet/SSH2.0 |
| 支持风扇管理、电源管理 |
| 支持SNMPv1/v2、SNMPv3 |
| 支持RMON(RFC2819) |
| 支持端口镜像、VLAN镜像、流镜像 |
| 支持RSPAN |
| 产品资质 | 提供工信部入网证 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 防火墙E（2台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 硬件规格 | 产品不少于4个千兆电口，4个千兆光口，6个万兆光口 |
| 性能要求 | 网络层吞吐量≥40Gbps，应用层吞吐量≥20Gbps |
| 部署方式 | 具备路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。 |
| 路由功能 | 支持静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议。 |
| 地址转换 | 支持IPv4／IPv6下NAT地址转换，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持NAT64、NAT46 地址转换。 |
| IPv6 | 支持IPv4/IPv6双栈工作模式，支持IPv6环境的应用控制策略设置，能针对IPv6的IP地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。 |
| VPN | IPSec VPN支持智能选路功能，保障业务的高可靠性。 |
| 地域访问控制 | 支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。 |
| 流量控制 | 具备基于国家/地区的流量管理功能，对数据流量和访问来源进行辨识和分类，保障精细化管理和控制。 |
| DDoS防御 | 支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 |
| 入侵防御 | 支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则。 |
| 支持僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。 |
| 双机部署 | 支持主主、主备两种双机模式部署。 |
| 安全报表 | 产品内置安全报表模板，可定义报表内容，包括网络整体安全状况、服务器安全风险分析、终端主机安全风险分析等。 |
| 用户管理权限 | 支持三权分立功能，根据用户权限分为安全管理员、审计员、系统管理员三种角色； |
| 集中管理 | 产品支持接入集中管理平台实现多设备的统一管理，通过集中管理平台统一配置产品的安全策略，包括但不限于访问控制、入侵防御、防病毒、Web应用防护等安全策略。 |
| 产品资质 | 产品要求取得中国人民共和国公安部的《计算机信息系统安全专用产品销售许可证》,提供有效证书的复印件 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 沙箱（1台）

| **指标项** | **参数要求** |
| --- | --- |
| 硬件指标 | 系统应为2U标准式机架硬件设备，含冗余电源，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 |
| 支持扩展插槽≥4，支持电口和光口扩展，RJ45串口≥1，USB接口≥2，硬盘≥1T。 |
| 文件处理数≥4万个/天，静态检测能力700万/天。 |
| 动态检测（虚拟执行） | 提供基于虚拟执行的动态检测技术，可以基于软件在虚拟环境的行为及通用漏洞利用特征（ROP等），发现各种高级恶意软件攻击，包括零日攻击及APT攻击 |
| 支持C&C检测，通过虚拟执行检测出的bot程序，获取的bot外连的C&C地址，检测到恶意行为会保存pcap数据 |
| 支持的应用类型：Adobe Reader应用、Office应用、Adobe Flash Player应用、IE应用等 |
| 支持的文件类型包括PDF类型文件、Office类型文件、可执行文件，支持对常见压缩格式内的文件的检测等 |
| 支持的协议类型包括HTTP、FTP、POP3、IMAP、SMTP等 |
| 支持WindowsXP、Windows7、Win10、安卓虚拟执行环境 |
| 安全情报 | 支持云端安全情报获取，包括且不限于文件、URL、C&C等安全情报内容 |
| 设备能够生成本地安全情报，包括不限于文件、URL、C&C恶意IP地址等 |
| 沙箱逃逸检测 | 支持常见的沙箱逃逸检测，当恶意文件进行逃逸尝试，应在文件分析报告中进行体现 |
| 白名单 | 支持白名单管理，文件、URL和域名可以增加至白名单，白名单内容不进行分析 |
| 静态检测和AV检测 | 支持无签名静态检测技术，主要有无差别的shellcode检测 |
| 支持YARA自定义规格检测，能够编辑YARA规则文件，导入YARA规则 |
| 支持的文件类型包括Office文档类型文件、flash类型文件、pdf类型文件、网页类型文件等 |
| 支持基于文件方式的病毒检测，系统内置不低于两个病毒检测引擎，用户可自主选择检测引擎并自定义检测策略规则（提供配置界面截图） |
| 部署方式 | 支持旁路检测模式；支持邮件部署模式 |
| 支持离线扫描模式，对指定的文件或目录进行检测 |
| 支持API方式进行文件提交，API方式获取分析结果 |
| Web管理 | 支持HTTPS管理方式，同时支持SSH和串口进行管理和配置 |
| 支持仪表盘展示，包括24小时威胁趋势、Top源地址、Top目的地址等；可以自定义仪表盘，仪表盘可以选择展示小组件 |
| 提供对设备状态的实时监控，包括检测引擎状态，证书状态，CPU、内存、存储产品的状态等； |
| 日志管理 | 实时的威胁事件监控和威胁趋势分析图 |
| 支持基于地理的威胁展示，包括可视化地图展示恶意URL活跃度的分布、可视化地图展示C&C服务器活跃度的分布 |
| 提供详细的威胁分析报告说明，包括，受感染的主机、触发的恶意行为、恶意软件的来源等关键信息 |
| 报表管理 | 提供基于威胁来源地理位置、基于主机、基于用户、基于应用协议及文件类型等多种统计报表； |
| 提供多维度的安全综合分析，直观的展示影响最大的受害主机、恶意软件及命令控制服务器 |
| 提供基于全球地图的实时统计监控，跟踪恶意软件来源及命令控制服务器地址的分布情况 |
| 关联分析 | 提供基于特定恶意软件关联的威胁分析说明，特定的恶意软件，网络中主机被感染次数、出现的回连次数等信息 |
| 提供基于主机的关联分析说明，特定的主机，受感染的恶意软件个数、出现的C&C回连次数信息 |
| 提供基于C&C回连的关联分析说明，特定的C&C回连地址，网络中回连的主机个数、恶意软件个数等信息； |
| 备份和恢复 | 支持配置文件的备份和恢复 |
| 升级 | 产品提供在线升级及本地升级多种升级方式； |
| 产品资质 | 产品应具备公安部颁发的“APT安全监测产品”销售许可 |
| 产品应具备全球IPv6测试中心颁发的“IPv6 Ready Logo认证” |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 探针B（1台）

| **指标项** | **参数要求** |
| --- | --- |
| 性能要求 | 吞吐性能，≥5Gbps。 |
| 接口数量 | 不少于6个千兆电口，4个千兆光口，2个万兆光口； |
| 部署模式 | 旁路部署，支持探针同时接入多个镜像口，每个口相互独立不影响。 |
| 资产发现 | 具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。 |
| 基础检测功能 | 具备报文检测引擎,可实现IP碎片重组、TCP流重组、应用层协议识别与解析等, 具备多种的入侵攻击模式或恶意URL监测模式,可完成模式匹配并生成事件,可提取URL记录和 域名记录,在特征事件触发时可以基于五元组和二元组(IP对)进行原始报文的录制。 |
| 监测识别规则库 | 能够识别应用类型超过1100种，应用识别规则总数超过3000条，具备亿万级别URL识别能力。漏洞利用规则特征库数量在4000条以上，漏洞利用特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号。 |
| 异常流量检测 | 支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括3389、53、80/8080、21、69、443、25、110、143、22等。 |
| 深度监测能力 | 可提供网络流量的会话级视图,根据网络流量的正常行为轮廓特征建立正常流量模型,判别流量是否出现异常,对原始流记录进行异常检测,可发现网络蠕虫、网络水平扫描、网络垂直扫描、IP地址扫描，端口扫描，ARP欺骗，IP协议异常报文检测和TCP协议异常报文等常见网络异常流量事件类型。 |
| 高级检测 | 支持5种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。 |
| 日志审计 | 支持DNS审计日志，主要用于平台dns flow分析引擎进行安全分析；HTTP审计日志，主要用于平台http flow分析引擎进行安全分析；SMB审计日志，主要用于平台SMB flow分析引擎进行安全分析；同步SMTP、POP3、IMAP审计日志，主要用于平台Mail flow分析引擎进行安全分析，同步AD域协议审计日志，主要用于平台AD域分析引擎进行安全分析。 |
| 僵尸网络检测 | 支持对终端种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为。具备独立的僵尸主机识别特征库，恶意软件识别特征总数在35万条以上。 |
| 违规访问检测 | 能够针对IP，IP组，服务，端口，访问时间等策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单（哪些访问逻辑是正常的）和黑名单（哪些访问逻辑肯定是异常的）两种方式。 |
| 流量记录 | 能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP会话记录、Web访问记录、SQL访问记录、DNS解析记录、文件传输行为、LDAP登录行为。 |
| 抓包分析 | 支持通过设备对流量进行抓包分析，可定义抓包数量、接口、IP地址、端口或自定义过滤表达式。 |
| 集中管控 | 支持安全感知平台对接入探针的统一升级，可展示当前所有接入探针的规则库日期、是否过期等，并支持禁用指定探针的升级。 |
| 部署 | 可以多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台。 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 抗DDoS检测（1台）

| **指标项** | **参数要求** |
| --- | --- |
| **设备要求** | 产品为标准机架式1U设备，≥2个USB接口，≥1个RJ45串口，≥2个GE管理口，≥8个千兆电口，≥8个千兆光口，≥16个千兆光口。 |
| 设备吞吐能力≥60G，设备清洗能力≥20G。 |
| **部署方式** | 流量清洗产品支持串联部署、支持旁路部署以及集群部署方式。 |
| **攻击防范功能** | 支持对欺骗与非欺骗的SYN Flood、ACK Flood、ICMP Flood、ICMP Fragment、UDP Flood、UDP Fragment、FIN/RST Flood、TCP Misuse、TCP Connection Flood、TCP Fragment、HTTP Flood、HTTP Slow Attack、HTTPS Flood、SIP Flood、DNS Query Flood、DNS Reply Flood、DNS Amplification、SSDP Amplification、NTP Amplification、Chargen Amplification、SNMP Amplification及混合类型攻击进行检测、告警并防护。 |
| 支持水印防护算法自定义校验特征，满足对CS架构业务的精准防护需求。具备针对缓存DNS服务器及授权DNS服务器专用的DNS防护手段 |
| 设备具备针对HTTP Get Flood攻击具备不少于9种专有防护手段，能够对HTTP进行解码。设备具备针对HTTP POST Flood攻击具备专有防护算法。支持导入SSL证书对HTTPS流量进行防护。 |
| 支持肉鸡防护，通过对源IP的URL访问比例进行统计防护肉鸡攻击。支持反射规则防护。 |
| 设备具备对不同类型的url请求合法性进行验证，实行不同的防护策略，可防御CC及变种的能力。设备具备对连接耗尽型攻击的防御能力。 |
| 设备支持使用智能攻击流量识别的技术进行防护，而不需要基于特定规则的方式，即当发生未知攻击，无需专门的撰写规则即可对这些攻击进行防护。 |
| 设备支持高级模版匹配的功能，过滤策略可定义内容至少包含：目标IP/掩码、目标端口、源IP/掩码、源端口、协议类型、接口范围、包长范围、TOS、TTL/HopLimit、UDP校验、ICMP类型、ICMPv6类型、TCP选项、TCP标志位、偏移量、深度、payload字符。并支持对每条策略添加描述。 |
| 设备提供过滤功能，支持白名单、黑名单、ACL、正则表达（同时支持TCP和UDP协议）、GeoIP功能。 |
| 支持URL访问控制规则等多种分组过滤方式。 |
| UDP防护支持多种检查和限速方式，包括最小包长、最大包长、源IP+源端口限速、源IP限速、目的IP+目的端口限速、目的IP+源端口限速、目的IP限速。 |
| 支持调用威胁情报库对流量进行防护，并支持IP信誉查询 |
| 支持自动识别APP访问来源，与PC源配置差异化防护策略进行精准过滤 |
| **牵引回注功能** | 支持静态和动态牵引方式，并且支持BGP路由协议和OSPF协议。 |
| 支持OSPF、ISIS、RIP、OSPF6、LDP、ripng等高级路由配置。 |
| **管理功能** | 管理界面要友好、易用性强，应支持集中管理、本地管理、远程管理等多种管理方式，并能实时显示攻击事件、流量、系统运行状况等信息。 |
| 系统具备统一管理平台，在集群部署时支持对多台设备的集中管理，日志收集，运行状态监控，策略下发。 |
| 系统支持用户分级分权管理，并具备合理的分级层次及权限划分粒度。 |
| 系统具备安全日志功能，可完整地记录用户对设备的重要操作、访问信息。 |
| 设备支持通过snmp、syslog、API等方式与第三方平台进行联动 |
| 支持配置文件导入导出，用于设备配置备份和紧急恢复 |
| 实现链路带宽监控，允许配置监控阈值，带宽超限后产生告警 |
| 支持设备自身登录安全认证，包括密码强度检查、登录IP访问控制、超时退出、密码生存周期检查、允许登录错误次数限制 |
| 支持TCPDUMP管理流量抓包，可筛选接口、目的/源IP、协议 |
| 提供界面手动及自动抓包功能，抓包参数定义范围至少包含如下几项：接口、协议、抓包数量、源IP、目标IP、源或目标IP、最大包长、流量方向、抓包时长、源端口、目的端口、源或目的端口。 |
| **产品资质** | 产品要求取得中国人民共和国公安部的《计算机信息系统安全专用产品销售许可证》,提供有效证书的复印件 |
| 中国信息安全认证中心颁发的《IT产品信息安全认证书》,提供有效证书的复印件 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## VPN网关（1台）

| **指标项** | **参数要求** |
| --- | --- |
| 性能指标 | 理论加密流量不低于1260Mbps，最大理论并发用户数不低于20000，IPSec加密最大流量950（Mbps）；不少于6千兆电口、4千兆光口、2万兆光口。 |
| 基本特性 | 专业VPN设备，采用标准SSL、TLS协议，同时支持IPSecVPN、SSLVPN两种VPN，非插卡或防火墙带VPN模块设备。 |
| 支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如WindowsEDGE，GoogleChrome，Firefox，Safari，Opera最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用。 |
| 支持Mac系统主流浏览器，如Chrome、Firefox等最新版，免安装浏览器插件登陆SSLVPN。 |
| 产品应支持国家商用密码算法包括：SM1,SM2,SM3,SM4算法 |
| 终端安全 | 产品必须支持防中间人攻击，产品可在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。 |
| 支持用户终端登录前、登陆后的安全性检测，检测范围包括：用户接入IP、接入时间、接入线路IP、进程、文件、注册表、操作系统、使用终端，可以检测出客户端是否安装指定的防火墙或杀毒软件。 |
| 产品应提供HTTPS驱动病毒查杀工具，支持对Windows环境下的针对HTTPS拦截监听的驱动病毒进行扫描查杀，避免因为HTTPS驱动病毒导致无法正常接入和使用SSL VPN。 |
| 权限、服务器安全 | 产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的IP地址、端口、提供的服务、URL地址等进行权限控制；针对同一B/S资源，可对不同用户做到细致到URL级别的授权。 |
| 支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统。 |
| 身份认证 | 产品必须支持LocalDB、USBKEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USBKEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证 |
| 产品资质 | 产品要求取得中国人民共和国公安部的《计算机信息系统安全专用产品销售许可证》,提供有效证书的复印件 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 安全管理平台（1套）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 安全管理中心（产品软件） | 作为安全管理的第一入口，支撑政务外网综合安全运营中心，做到态势感知、通报预警、威胁情报、漏洞分析、日志分析、安全策略的统一管理 |
| 态势感知（软件产品（含硬件）） | 性能参数：存储容量：》=32T，在带宽性能1Gbps时存储时长：1800天/1Gbps。（服务器2台做集群）包括数据采集层、数据存储和挖掘层、态势展现层。数据釆集层 通过部署探针、接收安全设备H志、漏洞扫描设备扫描日志等方式获取原始数据；数据存储 挖掘层建立在大数据分析系统之上，对1P地址库、GIS地图库、恶意IP、恶意文件库、资产库等基础数据信息进行安全和威胁的深度挖掘；态势展现层对安全分析结果进行威胁态势可视化呈现、通报预警和威胁情报的共享和发布 |
| 通报预警（产品软件） | 通过二级子账号、工单创建和派发流程，可以设定规则由系统在一定条件下自动创建，然后由管理员选择派发工单；对于没有及时完成的工单进行提醒，提醒方式支持站内消息、邮件等。二级单位自行进行处理，监管单位定时查看与通报 |
| 威胁情报共享（产品软件） | 从安全数据中分析、提取出来，用于在实际应用中发现安全问题，应包含失陷检测情报、文件信誉情报、安全预警通告情报等类型； |
| 漏洞扫描（购买服务（每年）） | 性能参数：包含资产数：500。含安全配置核查、漏洞扫描、配置变更检查、WEB漏洞扫描、弱口令检测五大引擎。功能包括：任务管理、检测报告、结果对比，告警分析、综合报表 |
| 日志审计（软件产品（含硬件）） | 性能参数：包含主机审计许可证书数量：1000，单台可用存储量：16TB，平均每秒处理日志数（eps）最大性能：4000。基于B/S的安全管理平台，实现整网日志管理、安全业务分析和日志审计等功能（包含互联网出口、市区政务外网互联互通区域、政务云接入区、汇聚区审计） |
| 可视化模块软件定制开发 | 从业务视角、态势感知数据接入的质量情况、量化的业务体验情况、纵向承载重点业务的网络设备运行健康度情况、各业务在线用户、并发请求数、流量占用等维度进行业务的可视化呈现 |
| 通报预警模块软件定制开发 | 对接接口，数据类型定义 |
| 威胁情报共享模块软件定制开发 | 对接接口，事件处理系统 |
| 安全管理控制 | 设备管理，策略管理，策略合规性检查，策略仿真，协同联动（安全管理平台发现问题将安全策略下发给安全设备） |

## 堡垒机（1台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 硬件规格 | 硬件要求：1U高机架式硬件架构，单电源，8G内存，2T硬盘容量，配置6个以太网千兆电口，4个万兆接口，2个万兆多模光模块 |
| 性能要求 | 最大图形并发连接数不少于200，最大字符并发连接数不少于700。配置支持500个资产的管理能力，支持无限个资产管理的扩容能力。 |
| 兼容性 | 浏览器 | 支持Chrome、Firefox、IE、Safrai等主流浏览器，产品应用不依赖JAVA及Flash |
| 操作终端 | 操作终端支持Winddows及Mac OS操作系统 |
| 用户管理 | 角色管理 | 系统支持账号分权管理，包括超级管理员、配置管理员、操作员、审计员及自动化人员等多种角色，并可根据功能自定义用户角色 |
| 身份认证 | 支持与Ldap、AD域、Radius、短信网关（阿里云、腾讯云）等第三方认证平台对接，实现统一身份认证 |
| 支持基于动态令牌、国密动态令牌、USBKEY、手机软令牌的双因素认证功能 |
| 支持双因素组合认证，可以将两种认证方式自定义组合为全新的认证方式 |
| 账号安全 | 具备账号密码的防爆力破解功能，可在用户持续输错三次（可自定义）密码后自动锁定和自动解锁 |
| 支持基于用户来源IP及Mac地址限制用户的登录行为 |
| 账号维护 | 支持通过Excel批量导、导出用户信息 |
| 支持web页面批量修改用户信息 |
| 资源管理 | 协议类型 | 支持SSH、Telnet、RDP、SFTP、XDMCP、VNC等多种协议，支持通过应用发布方式实现对BS、CS应用的纳管 |
| 动态视图 | 支持按不同属性对资产进行多级分类并自动生成树状结构的资源视图 |
| IPv6资产管理与审计 | 支持对IPv6资产进行统一管理，同时可完整记录用户对IPv6资产的运维操作行为 |
| 跳转管理 | 支持不同资产之间的联动配置，彼此之间可实现自动跳转访问 |
| 支持目标设备系统账号切换登录 |
| 等价信息 | 支持将一个实际资产/账号在系统中配置成多个资产/账号，并自动同步属性和配置 |
| 资产维护 | 支持资源信息批量导入、导出、修改、删除管理 |
| 支持资源添加后的一键网络端口连通性测试及ping连通性测试 |
| 部门管理 | 资源分权 | 支持用户帐号和目标设备的部门分权，不同的用户和设备可以归属于不同的部门（子部门） |
| 权限分权 | 支持访问控制策略按部门分权，不同部门的配置管理员只能针对自己部门及自己直属子部门设备进行访问权限设置 |
| 审计分权 | 支持审计功能按部门分权，使得不同部门的审计管理员只能审计自己部门、自己直属子部门设备上的操作日志 |
| 权限管控 | 访问权限 | 支持以用户（用户组）、目标设备（设备组、程序）、系统账号、服务等维度灵活设置访问策略 |
| 支持动态权限管控，管理员可基于用户属性、设备属性、系统账号属性来创建弹性动态权限规则，只要满足相关属性的用户、设备、账号即会被自动赋予对应访问权限 |
| 支持变更单管理功能，管理员可以基于使用人、资源、系统账号、到期时间，来上传、创建值班表模式的权限变更单，变更单无需审批，但可以自动生成时效性的访问权限 |
| 支持资源访问工单：用户填写包含工单标题、工单描述、需要访问的设备、需要使用的系统账号、需要访问的时间段的电子工单，经审批通过后可自动生成时效性的访问权限 |
| 高危操作 | 可跟据用户（用户组）、目标设备（设备组）、系统帐号、命令集来设置详细的命令权限控制策略，支持命令黑白名单、命令批复、告警通知等多种模式 |
| 支持基于A/B角管理模式的双人复核，当用户登录到目标设备时，必须经过复核人的复核确认后才能正常操作当会话复核人发现操作存在风险，可实时暂停 |
| 密码工单 | 支持密码工单管理，可通过工单申请相应资源的明文密码，审批通过后可通过邮件方式向申请人发送相应提示信息，有效期后平台会自动回收相应账号密码，并自动触发密码变更操作 |
| RDP剪切板权限管控 | 支持对通过rdp协议登录到目标资源后的剪贴板控制，可限制剪贴板的文件上行、字符上行、文件下行、字符下行操作 |
| 权限克隆 | 支持动态权限一键克隆功能 |
| 权限查看 | 支持按用户、资源统计查看权限分配情况 |
| 密码管理 | 密码托管 | 支持以EXCEL方式批量导入资源系统账号及密码 |
| 支持资源账号密码托管，实现资源单点登录功能 |
| 支持系统账号密码触发式校验功能，对托管的口令进行验证 |
| 自动改密 | 支持自动改密功能，管理员可自定义密码策略、改密周期、密码备份方式，支持密码分段保管功能 |
| 资源访问 | 资源展示 | 支持通过web页面以树状结构方式展现用户可访问的设备资源信息 |
| 支持在非web页面模式下以菜单方式展示用户可访问的资源列表 |
| 访问管理 | 支持Web、Mstsc、SSH Client等多种访问模式 |
| 支持SSH、SFTP、MSTSC透传访问 |
| 支持批量启动功能，可一次性登录选择好的目标设备 |
| 支持设备收藏功能，用户可以对经常需要访问的目标设备做一键收藏，以便于下次可以直接在收藏夹中找到 |
| 文件传输 | 针对基于云盘模式的文件传输操作：用户将文件暂存在系统上，然后一键上传到目标系统或者一键下载到用户本地，同时可通过文件分享功能以URL链接的方式将文件分享给其他用户 |
| 　 | 图形操作审计 | 支持图形化操作智能审计，可在审计回放界面上，同步显示关键的键盘操作、标题栏操作、剪贴板操作等文字信息，并能在点击任意文字信息，可直接定位到相关画面 |
| 支持图形操作的关键事件切片，管理员点击任意切片，即可直接定位到对应操作片段 |
| 字符操作审计 | 支持以录像方式完整展示用户的指令操作，同时支持命令输入、输出分层管理 |
| 文件传输审计 | 支持文件传输审计，可以完整记录用户通过系统进行的文件传输操作，并可对传输的文件信息进行留存，以便于事后审计 |
| 数据库审计 | 支持sqlserver、mysql、oracle等数据库操作行为审计，可通过录像及sql语句方式查看用户相关操作 |
| 审计分析 | 支持以topN模型展示用户的操作热点，如高危指令热度、用户操作热度分析等 |
| 支持资源、用户、操作三个维度审计智能检索，其中在操作检索层面，支持多关键字检索，检索结果直接定位到相关操作片段，并能将多个会话的操作片段进行一键合并和基于时间的操作排序重组 |
| 事件审计 | 支持记录登录、配置及审计行为 |
| 报表管理 | 统计报表 | 支持用户、资产、系统账号、会话等信息的统计报表 |
| 自动报表 | 支持自动化报表，可依据报表模板自动生成日报、周报、月报等自动化报表 |
| 资质要求 | 产品资质 | 具备公安部《计算机信息系统安全专用产品 销售许可证》运维安全管理产品证书具备中国网络安全审查技术与认证中心《IT产品信息安全认证证书》 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 运维管理系统（1套）

|  |  |
| --- | --- |
| 指标项 | 参数要求 |
| 配置管理 | 业务自动化发放；设备信息查询及修改。通过实施配置管理过程，对网络系统中的资源进行系统的配置管理。并指导配置管理人员建立配置库，利用配置库管理所有配置项，从而提供配置项的存取和检索功能，有利于配置项的更改控制，保证配置项的完整性和可跟踪性 |
| 网络管理系统 | 统一运维管理；VPN业务开通和监控；网络质量监控；业务承载质量监控 |
| △运行管理组织 | 管理组织：支持受理服务、应答服务、服务处理、服务记录等功能；项目生命周期管理：针对运维及建设项目的通用文档:办会、招投标、合同；项目建设过程：立项审核-预算申报、需求设计、实施、试运行验收；运行维护：实施、验收；绩效：信息化绩效、财务绩效等重要节点管理等（要求提供界面截图） |
| 运行信息化支撑系统 | 支持系统交互接口、服务管理、监控、接入管理等功能 |
| 网络资源管理 | 基础资源管理、地址资源管理、设备资源管理、版本资源管理 |
| 告警管理 | 业务告警关联、告警转发、告警前转、告警分发、trap告警管理 |
| 性能管理 | 网络及安全设备性能采集、性能批量配置、性能综合展示等 |
| 运行服务门户 | 为政务外网运行和安全监测支撑系统提供统一鉴权的服务入口，包含业务信息门户和运维工作门户 |
| 数据仓库 | 将不同类型的运维数据进行价值管理。对有价值的运维数据按照不同类型进行定义和管理，对接入的元数据进行二次处理、计算生成的价值数据形成“资产”，并对相应的运维价值数据进行维护和管理。做到各种应用数据一目了然。 |
| 可视化 | 运行保障可视化，提供资源、资产、安全态势、安全告警、关键运行指标等信息的可视化展示，具备至少三层下钻能力；让业务人员掌握全网的运行情况、资源情况、骨干网络拓扑、业务拓扑、故障情况、运行趋势，及时全面掌握网络上各类设备的运行情况和服务质量 |
| 业务全景可视化，从业务视角、各委办接入的质量情况、量化的业务体验情况、纵向承载重点业务的网络设备运行健康度情况、性能等维度进行业务的可视化呈现 |
| 运营管理可视化，对值班排班信息、工单处理情况和服务效率、故障类型和数量、工单处理的服务满意度等进行统计及呈现。 |
| 接口开发（与大数据平台） | 开发北向上报接口，向市级平台上报数据。 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂售后服务承诺 |

## SDN及网管系统（1套）

1. **SDN软件**

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 控制器架构及特性 | 控制器采用ODL开放式架构，可以通过开发APP的方式灵活扩展新的功能 |
| 控制器提供GUI界面，可以完成网络配置的图形化配置、编辑和查看展示 |
| 控制器支持Restful API北向接口（要求接口免费开放并且提供接口说明文档） |
| 控制器支持OpenFlow 、NETCONF、SNMP、SSH、Telemetry、PCEP南向接口协议 |
| 基础能力 | 支持管理不少于2000台路由器 |
| 多场景融合 | 支持WAN、园区控制器统一部署在一套平台上，能够通过SDN技术对现有利旧汇聚交换机实现统一管理、控制。 |
| 拓扑收集 | 支持控制器通过BGP-LS协议自动收集实际的拓扑信息 |
| 支持由管理员手动在控制器添加设备、链路等拓扑信息，控制器对导入的网络拓扑和实际运行情况进行校对，最后形成整网的实际拓扑 |
| 拓扑管理 | 支持对网络设备进行管理，包括增加、删除、属性修改等操作 |
| 支持管理员手动定义网络中各设备地理位置等信息，并在地图上进行呈现 |
| 支持对物理链路进行管理，包括增加、删除、属性修改等操作 |
| 隧道管理 | 支持在IP与MPLS网络中，使用SR隧道来对所有需要调度的应用流量进行封装 |
| 支持控制器根据调度需要自动在设备间建立SR隧道，承载被调度的应用流量，支持OSPF、IS-IS的SR-TE隧道（要求提供第三方测试报告） |
| L3VPN业务部署 | 支持PE对接CE侧，自动化对L3VPN业务添加、修改、删除、回滚配置、查看操作（要求提供界面截图） |
| 支持L3VPN业务与应用组关联、修改关联、删除关联操作 |
| QoS业务部署 | 支持图形化配置LAN口业务自定义带宽值限速 |
| 支持图形化配置WAN口队列调度，按比例或带宽绝对值分配带宽，应用优先级进行业务保障 |
| 支持图形化配置WAN口限速（要求提供界面截图） |
| 拓扑可视 | 支持能将地图信息呈现出来，并和设备位置信息关联，实现网络中各设备的位置图形化，支持地图定制（要求提供界面截图） |
| 呈现完整拓扑Underlay拓扑 |
| 可按照区域自动进行拓扑折叠（要求提供界面截图） |
| 设备可视 | 支持呈现CPU、内存、温度 等基础资源的健康状态（要求提供界面截图） |
| 设备名称、序列号等静态信息呈现 |
| 对CPU、内存、温度等历史信息（包括过去1小时、过去1天、过去一周、过去一月）进行统计和呈现（要求提供界面截图） |
| 链路可视 | 支持链路名称、两端接口IP等静态信息呈现（要求提供界面截图） |
| 支持链路通断，拥塞，质量状况呈现（要求提供界面截图） |
| 链路质量（延时、抖动、丢包）详细信息的实时呈现，支持秒级呈现 |
| 对链路的历史质量信息（包括过去1小时、过去1天、过去一周、过去一月）进行统计和呈现（要求提供界面截图） |
| 支持呈现链路实时流量、全网链路实时流量TOPN、链路历史流量分布、链路承载应用历史流量分布，支持秒级呈现（要求提供界面截图） |
| 应用组粒度粒呈现实时带宽信息，应用组实例粒度呈现实时带宽信息（要求提供界面截图） |
| 时延、抖动、丢包、带宽利用率、应用组带宽/占比（要求提供界面截图） |
| 流量调度 | 支持自动计算、半自动计算、手工指定三种方式选路 |
| 支持严格选路、松散选路、排除选路方式选路（要求提供界面截图） |
| 支持为应用组选择等价路径（要求提供界面截图） |
| 支持永久、指定时间、周期性时生效等时间段策略 |
| 支持根据业务质量（时延、抖动、丢包）、带宽需求，为业务按需自动调整路径（要求提供第三方测试报告；要求提供界面截图） |
| 支持应用SLA不满足、链路带宽超过80%、设备故障、链路故障、主备路径重合、路径非最优情况下，自动调整路径（要求提供第三方测试报告；要求提供界面截图） |
| 支持路径预计算出来后，需管理员确认路径才会下发 |
| 支持对自动调度应用进行定时或周期性的全网路径优化（要求提供第三方测试报告；要求提供界面截图） |
| 支持应用主备路径、路径自动逃生（要求提供第三方测试报告；要求提供界面截图） |
| 故障自动诊断 | 支持自动诊断设备连接故障，设备CPU、内存、温度超过阈值（要求提供界面截图） |
| 支持自动诊断链路中断，链路质量低于阈值（要求提供界面截图） |
| 支持自动诊断应用质量是否满足需求（要求提供界面截图） |
| 设备隔离冻结 | 支持可单独将某设备隔离，不再参与路径计算（要求提供界面截图） |
| 告警管理 | 支持拓扑图中直接呈现故障信息（要求提供界面截图） |
| 支持E-mail推送告警信息 |
| 支持告警阈值设置（要求提供界面截图） |
| 设备管理 | 支持BGP-LS、Netconf、SNMP、Netstream、Telemetry、PCEP |
| 支持同一设备5个不同时间的配置比对，可显示配置不同点 |
| 日志管理 | 支持导出用户操作日志（要求提供界面截图） |
| 支持导出历次流量调度日志（要求提供界面截图） |
| 支持导出控制器自身日志（要求提供界面截图） |
| 报表导出 | 支持链路质量报表、链路带宽报表、应用组流量报表、应用组内实例流量报表等（要求提供界面截图） |
| 支持提供固定时长（如过去1小时、过去1天、过去一周、过去一月、过去一年）或自定义时间段内的报表信息（要求提供界面截图） |
| 控制器可靠性 | 支持控制器集群部署（控制器集群状态页面，要求提供界面截图） |
| 支持定期自动或手工异地备份数据库（要求提供界面截图） |
| 网络可靠性 | 支持节点设备堆叠部署 |
| 支持节点设备背靠背部署 |
| 支持一键取消控制器路径，切换传统转发模式 |
| 用户访问 | 支持多用户同过用户名、密码认证 |
| 支持对不同用户分配不同管理权限 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

1. **网管系统**

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 分布式部署 | 需资源拓扑、告警、性能等功能组件支持多服务器负载分担部署，保证各网管组件性能； |
| 多平台支持 | 支持Windows、Linux平台及SQL Server、Oracle数据库，需提供官网公开的安装手册、软件安装包的链接及截图； |
| 多厂商设备配置及软件管理 | 支持H3C/HUAWEI/3COM/CISCO/HP设备的批量配置和软件管理，包括的软件版本和软件库中最新可用的软件，更新设备的软件支持220+设备厂商，8000+设备款型； |
| 自定义用户主页 | 管理员可以首页中通过拖拽，自定义需要在首页展示页面，同时支持Widget扩展； |
| 自动发现拓扑 | 自动发现网络中的所有网络设备，并在拓扑中显示出来，可以自动将网络中的逻辑连接关系显示出来； |
| 用户分权管理 | 可以为不同的管理员设置不同的用户名、密码，并限制管理员的管理权限和管理范围，实现用户分权管理； |
| 配置需求 | 实配可管理有线网络设备节点数量≥500 |
| 设备与用户统一管理 | 支持网络管理平台实现设备管理与用户管理联动，如通过点击拓扑楼层接入交换机查看该楼层所有接入用户帐户信息，需提供界面截图； |
| 设备与流量分析统一管理 | 支持设备与流量分析统一管理：支持网络管理平台实现设备管理与流量分析联动，如通过点击拓扑某链路可查看该链路的关键应用流量分布、关键用户流量使用等，需提供界面截图； |
| 性能管理 | 支持基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警； |
| 故障管理 | 支持对全网设备告警的实时监控和统一浏览；支持多种提醒方式，如告警实时提醒（告警板）、告警音响提示；支持多种转发方式，比如转E-mail，转短信，转上级网管或其它网管等支持告警分析，可以屏蔽重复告警、闪断告警，支持告警自动确认功能； |
| 批量的设备配置备份和恢复 | 支持向导方式或者任务方式（周期性任务、一次性任务或立即任务）批量的备份、恢复完整的配置文件，也可以批量的下发配置片断； |
| 运维报表 | 需提供多种报表样式，包括普通的行列报表、主/子报表、图形摘要报表、交叉表、TopN和BottomN报表支持多种图形展示：包括条形图、饼图、曲线图、甘特图、面积图、圆环图、三维梯形图、三维曲面图、XY 散点图、雷达图、气泡图、股票图、漏斗图等； |
| 周期性报表机制 | 支持天报表、周报表、月报表、季度报表、半年报表、年报表可以设定周期性报表的开始时间、失效时间可以将自身的组织名称和Logo融入到发布的报表中，可以定时生成后Email到指定邮箱； |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

## 日志存储服务器（1台）

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 形态 | 2U机架式设备，标配原厂导轨 |
| 处理器 | 配置≥2颗2.3GHz/16核CPU |
| 内存 | 配置≥64GB DDR4内存，单根内存条容量32G，可扩展≥24个内存插槽 |
| 实配硬盘 | 实配硬盘配置≥2\*1.2TB 硬盘 |
| 硬盘槽位 | 配置≥8个热插拔硬盘槽位，且全部硬盘可在不打开主机箱盖的情况下热插拔维护 |
| 阵列控制器 | 配置独立Raid阵列卡，支持RAID0/1/10/5/6/50/60，≥2GB缓存以及掉电保护模块 |
| 网卡 | 配置,1个Intel 4端口千兆电网卡 |
| GPU | 可配置≥3块双宽或8块单宽GPU卡 |
| 风扇 | 最大需提供≥6个热插拔冗余风扇； |
| 电源 | 配置2个热插拔冗余电源 |
| 售后服务 | 三年7x24含硬盘不返回维保服务，以及首次基础安装服务 |
| 服务及质保要求 | 3年产品原厂标准维保服务，需提供原厂针对本项目3年原厂售后服务承诺函 |

# 投标要求

## 投标方资质要求

1. 具有《企业法人营业执照》；
2. 能提供良好的技术支持和快速的服务响应；
3. 要求项目成员具有高级项目经理资质证书、其他项目人员具有网络相关资质证书；
4. 须提供近3年以来行业类似项目业绩；
5. 本次招标不接受联合体方式投标。

## 述标要求

投标方在投标当日需进行现场讲标，限时5分钟。要求从对项目现状和需求的理解、方案设计、设计难点和优势、实施计划、售后服务等方面进行述标。

## 关键技术参数响应索引

投标方需对关键技术参数（设备技术要求△标记项）响应情况单独列出索引页。