第三章　采购需求

一、项目概况（实质性响应）

巨灾防范工程包括观测系统、数据平台、运行环境建设，以及地震灾害防御体系技术系统、信息系统建设，该工程的建设能够全面提升应对灾害的响应能力，确保在灾害发生时能够快速产出科学、准确资料，为抗震救灾决策提供坚实科技支撑。

本项目为巨灾防范工程数据平台分项，整体要求包括：（1）完成海南省巨灾防范工程数据平台建设，包括但不限于：信息化硬件系统（通信网络和网络安全）、研发部署海南地震产品平台、系统集成等的基础建设；（2）完成各系统内部功能以及跨系统之间的业务化网络和网络安全集成；（3）完成与海南省巨灾防范工程其他分项目的联调联试及海南省巨灾防范工程整体联调联试及验收。

1.数据平台-通信网络系统：

购置省级中心路由器、交换机等网络设备 26 台套。在现有地震行业通信网络（10 网）基础上，对核心路由器、核心交换机、接入交换机等老旧通信网络设备进行更新，为全省地震实时观测数据、地球物理台网数据、地震视频会商等地震业务提供运行基础网络运行保障，实现地震业务数据与信息服务的快速、稳定、安全、可靠、连续传输；实现和现有地震网络的平滑过渡和升级，有效保障现有全省地震行业网络所承担业务系统正常运行；与国家地震行业网络通信网络系统无缝连接，实现我省与邻省地震业务数据共享等服务；同时，新建与国家中心 DNS 系统上下联动的省级中心 DNS 系统，负责全省地震业务域名权威应答与智能解析，实现全省地震业务内网业务调度、容灾切换；新建一套基于北斗卫星的省级中心 NTP 服务系统，实现全省地震行业网设备统一网络授时服务。

根据招标方要求，完成相关采购设备的安装与配置，实现全省地震行业网全部观测站点、省级中心、国家中心、省政务云之间的线路接入及通信线路的冗余和数据传输、汇聚、交换、处理及信息发布等全链条的联调联试，以及上述要求的各项功能。同时，所有采购设备调试和集成需联合省级中心、全省中心站及全部观测站现有的软硬件设备和已部署业务系统，包括但不限于地震行业网、预警网、互联网和省电子政务外网的核心路由器、台站接入路由器、VPN 路由器、数

据中心核心交换机、网络安全设备、服务器和相关各类软件与系统等，实现全省地震网络互联互通和业务连续。

2.数据平台-网络安全能力提升：

根据国家等级保护 2.0 系统等级保护要求、国家安全可靠测评要求，以及地震行业通信网络安全建设相应等级保护要求，更新和建设网络安全系统，包括边界防火墙、互联网防火墙、安全及日志审计、主机防护、安全访问等安全设备及系统。通过网络安全系统建设强化安全防护，增强系统安全管控能力，从安全管理体系、安全技术体系、运维体系和服务体系等方面开展建设工作，实现网络安全、主机安全、应用安全、数据安全，保证全省地震行业网络的安全稳定运行。

项目采购与集成包括安全软硬件设备，为全省地震行业业务系统正常稳定运行和数据资源保护等提供网络安全保障。同时，设备调试和集成需联合全省地震行业网、预警网、互联网和省电子政务外网等的软硬件设备，包括但不限于全省地震行业网、预警网、互联网和省电子政务外网的核心路由器、台站接入路由器、VPN 路由器、数据中心核心交换机、服务器等，和已有网络安全设备、以及业务部门目前在用和本次新建系统等，实现实现全省地震网络互联互通、业务连续，以及全省地震网络的整体安全。

（1）省中心安全部署：省中心共配置安全设备 31 台套，包括防火墙 8 台，安全管理平台 1 套，数据库审计 1 台，网络安全审计 1 台，上网行为管理 2 台，主机安全（包含防病毒功能）（包含 600 点授权）1 台，省中心堡垒机 2 台，日志审计 1 台，web 应用防火墙 4 台，负载均衡 2 台，网络安全准入 4 台，抗 DDOS 2 台，策略可视化 1 台，全流量分析 1 台。

（2）中心站（海口、琼中、三亚 3 个）安全部署：省地震局共 3 个中心站，共配置安全设备 12 台，每个中心站配置 4 台，包括防火墙 2 台，入侵检测 1 台，堡垒机 1 台。

3.数据平台-研发部署海南地震产品平台：

第一时间自动对接国家地震产品平台产出的各类地震产品，同时结合海南业务特点，新增研发定制化功能，实现海南及相邻区域台网规模与运行可视化、震后应急产品自动产出、常规地球物理场类产品定时汇集，从而服务一线地震应急决策、监测预报和科学研究等领域，提升海南地震业务信息化水平。

4.项目采购清单：

数据通讯设备					产地
序号	货物名称	是否为核心产品	数量	单位	产地
1	核心路由器	否	2	台	国产
2	核心交换机	否	2	台	国产
3	万兆流量复制器	否	2	台	国产
4	业务接入交换机	否	8	台	国产
5	带外汇聚交换机	否	2	台	国产
6	带外管理交换机	否	6	台	国产
7	DNS 服务器（系统）	否	1	套	国产
8	NTP 服务器（系统）	否	2	台	国产
9	网管软件	**是**	1	套	国产
总　　数			26	台/套	
省中心网络安全设备					
1	安全管理平台	否	1	台	国产
2	核心防火墙	否	2	台	国产
3	互联网防火墙	否	2	台	国产
4	边界防火墙	否	4	台	国产
5	数据库审计	否	1	台	国产
6	网络安全审计	否	1	台	国产
7	上网行为管理	否	2	台	国产
8	主机安全（包含防病毒功能）	否	1	套	国产
9	省中心堡垒机	否	2	台	国产
10	日志审计	否	1	台	国产
11	Web 应用防火墙	否	4	台	国产
12	负载均衡	否	2	台	国产

13	网络安全准入	否	4	台	国产
14	抗 DDOS	否	2	台	国产
15	策略可视化	否	1	台	国产
16	全流量分析	否	1	台	国产
总　　数			31	台/套	
中心站（海口、琼中、三亚 3 个）网络安全设备					
1	防火墙（中心站）	否	6	台	国产
2	入侵检测（中心站）	否	3	台	国产
3	堡垒机（中心站）	否	3	台	国产
总　　数			12	台/套	
海南地震产品平台					
1	海南本地化平台建设与基础管理	否	1	套	国产
2	地震应急决策专题	否	1	套	国产
3	台网概况与质量监控专题	否	1	套	国产
4	地震监测能力专题	否	1	套	国产
5	地球物理异常图件专题	否	1	套	国产
总　　数			5	套	

5.集成需求

5.1 业务需求：由于本项目涉及软/硬件数量较多，项目实施范围广且工作难度大，技术门槛高。因此，在项目执行过程中引入集成概念，投标人要对项目全生命周期负责，并需通过项目管理和技术管控两个方面，切实把握时间进度的管理、项目风险的管控、核心技术的选择、关键技术路线的设定等。 本项目建设主要是为实现安全、自主、可控的应用系统提供信息化硬件环境基础，是基于全局数据中心资源整合共享的基础上进行改建和扩建，项目总体包括如下几个部分：1、通信网络系统建设 2、网络安全系统建设。 本项目设备集成主要是提供业务应用系统运行的网络和安全系统。

5.2 技术需求：为保障业务系统不间断运转，系统集成技术需求需要投标方全面配合建设方提供集成技术方案，集成内容主要是以下几个方面： 1、通信网

络集成：按照大二层网络进行设计，采用万兆端口上下行的组网模式，承担核心路由与国家中心对接联调。因此需要网络设备支持大量端口，并支持 VxLAN 和 M-lag 等技术。 2、网络安全集成：1）所采购的防火墙均 2 台为 1 组（设备冗余）。省中心 4 组防火墙（即 2 台核心防火墙、2 台互联网防火墙、4 台边界防火墙）不能为同一品牌产品。2）安全管理平台对接并收集安全管理平台对接并收集网络设备、安全设备、操作系统、数据库等等设备的安全原始日志，进行统一分析和攻击链还原，以完成深度告警聚合。3）实现省中心对入侵防御、入侵检测统一可视化展示与集中管控，包括查看每个节点设备运行状态与威胁状态信息，能够统一更新威胁情报与防护规则、设置防护策略、专项威胁运维操作。基于等保 2.0 三级防护标准，建设合规的网络安全防护体系，形成满足要求的安全区域边界、安全计算环境等。

5.2.2 省中心网络与安全 **对所有采购设备进行集成，包括并不限于以下内容：**

（1）新设备上架调试并与原系统及本次项目中其他采购内容的集成。（含原系统设备所需要完成的配置调整）。

（2）新采购软件的部署实施及部署实施过程中涉及到的设备配置调整等。

（3）机柜位置优化调整：因机柜位置有限，新采购设备需与原机柜设备统筹考虑，将涉及机柜优化调整设计、老设备迁移配置、线缆重布。

（4）网络结构优化调整：依据网络现状，并根据业务需求，开展网络结构优化设计并予以实施。

（5）新增及调整设备在机房中的布线规划与铺设。

（6）全网新增安全设备策略的规划配置、原有安全设备策略规划、梳理与更新及与台站安全设备间的策略规划调整。

（7）项目在整个实施流程中，投标人团队成员须全权承担并负责项目所采购设备及与所采购设备相关联的海南省地震局地震网络中的原有设备的集成、设计、配置、调试等全部相关联工作，包括但不限于配合网管系统的实施开展全网拓扑连接梳理、配合综合业务展示系统实施开展监控系统展示优化设计、配合 NTP/DNS 设备实施完成全网联网设备 NTP/DNS 同步配置、DNS 与国家局之间的对接、配合安全平台实施完成全网安全设备对接、配合流量交换/监控等

设备开展全网流量镜像获取优化与配置、配合策略可视化软件开展全网安全设备策略梳理与网络设备路由梳理、配合设备实施及与各类业务系统的对接与整网融合。

5.2.3 中心站网络与安全

(1) 所有新采购网络与安全设备按照各中心站网络实际情况配置，均要与原有网络进行集成部署，保证业务稳定运行。

(2) 中心站承担地震行业网网络汇聚业务功能，每个中心站部署实施前要进行施工进度计划的规划。本次新购设备安装搭建并测试完毕后，再进行网络设备的切换，减少汇聚节点网络中断时间。

(3) 对现有机房的网络设备线缆进行重新梳理、统一标识。

系统需求 通过网络系统、网络安全系统建设，实现各业务系统基于高速网络的数据交换，并且能够满足等保 2.0 三级要求。

二、采购清单

说明：

①指标按重要性分为“★”、“#”和“△”。★代表实质性指标，不满足该指标项将导致投标被拒绝，#代表重要指标，△则表示一般指标项。

②“证明材料要求”项可填“是”和“否”。填“是”的，投标人/响应人须提供包含相关指标项的证明材料，证明材料可以使用生产厂家官方网站截图或生产厂家产品白皮书或具有检测资质的第三方检测机构的检验报告或其他相关证明材料，未提供有效证明材料或证明材料中内容与所填报指标不一致的，该指标按不满足处理。

③除需求中明确要求投标人承诺的事项外，其他要求提供证明材料的指标中，提供投标人承诺作为应答的不予认定。

④使用综合评分法的采购项目，提供相同品牌产品且通过初步审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按

照招标文件规定的方式确定一个投标人获得中标人推荐资格，采购文件未规定的采取随机抽取方式确定，其他同品牌投标人不作为成交候选人。

⑤指标按重要性分为“★”、“#”和“△”。

5．1 带“★”代表实质性指标，不满足该指标项不能通过符合性审查（无效投标认定条件）。

5.2 带“#” 技术指标（共 50 项）：每有 1 条不符合参数要求的扣 0.673 分，总共 33.65 分。

5.3 带“△” 技术指标（共 214 项）：每有 1 条不符合参数要求的扣 0.025 分，共计 5.35 分。

5.4 核心产品：网管软件

1.核心路由器

序号	重要性	指标项	指标要求	证明材料要求
1	★	性能要求	包转发率≥14400Mpps，交换网板整机交换容量≥110T bps，实配交换网板转发性能≥400Gbps; 整机转发容量单向≥480Gbps	是
2	△	主机配置	主机内存≥8G 实配冗余主控板卡、交换网板，包转发芯片采用可编程的 NP 芯片，实现灵活的新功能扩展及演进能力。	否
3	△	业务槽位	可用业务板槽位数≥4 个(不含主控槽)。	否
4	★	接口配置	配置的业务板卡实配 NetStream 或 Netflow、实配≥12 个 10G SFP+光接口并实配 12 个万兆 SFP+ 多模光模块、≥8 个 GE 口。	是
5	△	高可靠性	实配冗余电源和风扇	否
6	△	接口扩展	支持 GE、10GE、25GE、50GE、100GE 等接口	否
7	△	设备高度	考虑机房空间及部署方便，设备高度≤6U	否
8	△	热补丁升级	各组件均支持热插拔功能；支持热补丁功能，可在线进行补丁升级；实现全业务在线升级	否
9	△	端口功能	每端口支持 8 个优先级队列，3 个丢弃优先级，支持 PQ、WRR、PQ+WRR 等队列调度方式或 SP、WRR、SP+WRR 三种队列调度算	否

			法；支持精细化的流量监管，支持流量整形 Shapping，支持 WRED 拥塞避免，支持 802.1p、DSCP 优先级映射。	
10	△	路由协议	支持静态路由、RIP、RIPng、OSPF、IS-IS、BGP、PIM、MSDP、MBGP、SRv6 等路由协议；支持 BFD 快速检测，配合 FRR（快速重路由），实现故障链路的 50ms 级快速切换；	否
11	#	SRv6	支持 SRv6 分段路由,支持 SRv6 业务承载在 FlexE 网络硬切片上（提供权威机构出具的测试报告并加盖厂商公章）	是
12	#	FlexE	支持 FlexE 网络切片，支持硬切片在线带宽弹性扩容且业务不丢包，支持根据不同的网络服务要求如时延、带宽、安全性和可靠性等来划分切片网络，灵活的应对不同的网络应用场景（提供权威机构出具的测试报告并加盖厂商公章）	是
13	#	IFIT	支持 IFIT 随流检测。支持基于 IFIT 的逐会场逐跳的流量统计；支持对自定义应用的数据流进行压缩以节约带宽（提供权威机构出具的测试报告并加盖厂商公章）	是
14	#	自主可控	CPU（处理器）、LSW（转发芯片）均为国产自研芯片或采用飞腾、海思、鲲鹏、盛科、海光、兆芯等国产芯片（提供权威机构出具的测试报告并加盖厂商公章）	是

2.核心交换机

序号	重要性	指标项	指标要求	证明材料要求
1	#	性能指标	交换容量≥380Tbps,转发率≥115000Mpps。	否
2	★	槽位配置	实配双主控，实配≥4 个独立交换网板，≥4 个独立业务板卡槽位。单槽位支持 36 口 40G 单板线速，≥8 个独立交换网板槽位	是
3	△	可靠性	实配电源模块≥4 个，冗余风扇	否
4	★	接口配置	实配的业务板卡合计具备≥36 个 40G 端口,≥48 个 10G 端口。配置 36 个 40G 多模光模块，配置 48 个 10G 多模光模块。	是
5	△	设备高	考虑机房空间及部署方便，设备高度≤11U	否

		度		
6	△	热补丁升级	各组件均支持热插拔功能;支持热补丁功能，可在线进行补丁升级;实现全业务在线升级。	否
7	△	流量可视化	实配 NetStream 或 Netflow 或 sflow 流量统计功能。	否
8	△	路由协议	支持 IPv4 与 IPv6 双栈: 文持 IPv4 静态路由、RIP、OSPF、IS-IS、BGP4 等 IPv4 协议;支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+等 IPv6 协议;支持 MPLS L3 VPN，支持 MPLS L2 VPN，支持 MPLSVPLS，支持 MPLS TE，支持 MCE。	否
9	△	功能要求 1	实配信元交换，多个相同五元组的跨板流量基于信元交换在网板间负载分担，流量无丢包。（提供权威机构出具的测试报告并加盖厂商公章）	是
10	#	功能要求 2	集群或堆叠支持带外管理方式，主控板直连方式，管理链路和转发链路分离。（提供权威机构出具的测试报告并加盖厂商公章）	是
11	#	自主可控	CPU（处理器）、LSW（转发芯片）均为国产自研芯片或采用飞腾、海思、鲲鹏、盛科、海光、兆芯等国产芯片（提供权威机构出具的测试报告并加盖厂商公章）	否

3.业务接入交换机

序号	重要性	指标项	指标要求	证明材料要求
1	#	交换性能	交换容量≥4.8 Tbps，包转发率≥2000 Mpps，整机缓存≥32MB。	否
2	△	接口配置	实配≥48 个 10 GE SFP+光端口，满配 10G 光模块;实配≥6 个 100G 光端口（兼容 40GE），≥4 个 40GE 或 100GE 光模块;	否
3	△	可靠性	实配热拔插电源≥2，模块化风扇≥2 个	否
4	△	路由协议	支持 IPv4 与 IPv6 双栈。支持 IPv4 静态路由、RIP、OSPF、IS-IS、BGP4 等 IPv4 协议;支持 IPv6 静态路由、RIPng、OSPFV3、IS-ISv6、BGP4+等 IPv6 协议。	否
5	△	链路聚合	支持热补丁，跨设备端口聚合等功能。支持 M-LAG 或堆叠功能;	否
6	△	售后运维	为保障网络设备统一纳管和运维的要求，	否

			与核心交换机采用同一品牌。	
7	△	自主可控	CPU（处理器）、LSW（转发芯片）均为国产自研芯片或采用飞腾、海思、鲲鹏、盛科、海光、兆芯等国产芯片（提供权威机构出具的测试报告并加盖厂商公章）	是

4.带外汇聚交换机

序号	重要性	指标项	指标要求	证明材料要求
1	#	交换性能	交换容量≥4.8 Tbps，包转发率≥2000 Mpps，整机缓存≥32MB。	否
2	△	接口配置	实配≥48 个 10 GE SFP+光端口，满配 10G 光模块;实配≥6 个 100G 光端口（兼容 40GE），≥4 个 40GE 或 100GE 光模块;	否
3	△	可靠性	实配热拔插电源≥2，模块化风扇≥2 个	否
4	△	路由协议	支持 IPv4 与 IPv6 双栈。支持 Py4 静态路由、RIP、OSPF、IS-IS、BGP4 等 IPv4 协议;支持 IPv6 静态路由、RIPng、OSPFV3、IS-ISv6、BGP4+等 IPv6 协议。	否
5	△	链路聚合	支持热补丁，跨设备端口聚合等功能。支持 M-LAG 或堆叠功能;	否
6	△	售后运维	为保障网络设备统一纳管和运维的要求，与核心交换机采用同一品牌。	否
7	△	自主可控	CPU（处理器）、LSW（转发芯片）均为国产自研芯片或采用飞腾、海思、鲲鹏、盛科、海光、兆芯等国产芯片（提供权威机构出具的测试报告并加盖厂商公章）	是

5.带外管理交换机

序号	重要性	指标项	指标要求	证明材料要求
1	△	交换性能	交换容量≥670 Gbps，包转发率≥200 Mpps。	否
2	△	接口配置	配置千兆电口≥48，≥4 个万兆 SFP+光口及满配光模块,冗余可插拔电源。	否
3	△	专用口要求	支持专用堆叠口，不占用业务口带宽，最大堆叠带宽（双向）≥48Gbps	否
4	△	路由协议	支持 IPv4 与 IPv6 双栈。支持 IPv4 静态路由、RIP、OSPF、IS-IS、BGP4 等 IPv4	否

			协议;支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+等 IPv6 协议。	
5	△	售后运维	为保障网络设备统一纳管和运维的要求，与核心交换机采用同一品牌。	否
6	△	自主可控	CPU（处理器）、LSW（转发芯片）均为国产自研芯片或采用飞腾、海思、鲲鹏、盛科、海光、兆芯等国产芯片（提供权威机构出具的测试报告并加盖厂商公章）	是

6.网管软件

序号	重要性	指标项	指标要求	证明材料要求
1	△	管理范围要求	系统应支持多种设备和应用的管理，包括网络设备、安全设备、服务器、存储、操作系统、数据库、中间件等。	是
2	△	系统架构要求	系统使用 B/S 架构，支持使用 WEB 浏览器进行界面展示，支持 HTTPS。	否
3	△	系统安全性要求	系统提供分权分域功能，为不同的用户、角色分配不同的设备管理范围和操作权限	否
4	△	南向接口要求	系统应支持多种南向接口类型，包括SNMP、SNMP Trap、WMI、STelnet、FTP(服务端)、SFTP(客户端/服务端)、IPMI、HTTP(客户端)/HTTPS(REST/Redfish客户端、服务端)等，方便管理多种设备类型。	否
5	△	资源管理要求	支持资源的自动发现和分类识别。 支持将添加后的资源(如服务器、网络设备、存储设备等)进行分类和分组管理，用户通过配置不同的分组类型和分组将资源划分为不同类型以及不同分组；支持拓扑视图自动生成并具备编辑功能；一套软件可实现多个区域的统一监控。	否
6	△	故障管理要求	系统应提供多领域、多厂商数据采集能力，包括从下层第三方系统采集的告警信息，并将告警集中显示在告警面板中。 提供了多样化的告警过滤方式，帮助运维人员快速筛选所关注的告警，提高监控效率。系统应支持灵活的告警规则配	否

			置，将海量的告警进行关联和压缩，减少告警噪声，实现精准监控。	
7	△	性能管理要求	系统支持对设备的关键性能指标进行监控，并对采集到的性能数据进行统计，方便用户对设备性能进行管理。 支持通过设置不同的性能阈值，生成 4 级不同级别的告警:紧急、重要、次要、提示支持监控设备的实时性能数据，了解设备的运行状态，以便确认设备是否存在异常。	否
8	△	报表管理要求	支持用户拖拽式自定义报表内容，运用钻取、旋转、切片等操作，实现业务数据的灵活展现和统计汇总，提供自助式数据同比、环比、TOPN 等分析功能。 支持根据用户设定的周期自动生成报表,可以通过 Email 发送,也可以手动导出 Excel、PDFWord、Html 格式的报表。 系统应支持网络设备类型、设备 CPU 利用率、内存使用率统计、接口流量、链路流量、端口使用率等统计报表。	否
9	△	配置文件管理要求	系统提供全网设备的配置文件管理，可以提供即时和周期的配置文件备份，支持对已备份的配置文件进行基线化、恢复。	否
10	△	IP 地址管理	系统应支持支持 IP 地址状态的概览展示，IP 分组的管理和正子网的规划。支持管理员对 IP 地址进行分配，修改，回收，以及导入导出，可以根据配置参数和实际使用状态检测空闲 IP 地址。	否
11	△	授权数量	100 个设备节点（支持虚机、操作系统、服务器、数据库等）、100 个网络节点（支持交换机、安全设备等）	否
12	△	告警信息	可将告警信息分级分类通过短信或邮箱或电话等方式自动实时发送告警信息形式推送到不同的运维人员。	否
13	△	自主可控	支持麒麟、统信等操作系统	否

7.万兆流量复制器

序号	重要性	指标项	指标要求	证明材料

				要求
1	#	基本要求	标准机架式设备，支持≥48 个 SFP+的万兆接口(兼容千兆)，配置≥20 个万兆多模光模块。 L2-L7 性能:系统应支持 7*24 小时的稳定运行，处理性能不低于 480Gbps。	否
2	△	界面要求	系统应支持全中文化 WEB 操作界面，简化操作复杂度。系统应支持以面板图形方式展现所有接口的 LinkUP/LinkDOWN 状态、接口字符串描述、接口当前速率、SFP 模块插入/拔出状态，接口当前发送/接收报文计数等信息。	否
3	△	流量分发	应支持基本流量复制汇聚功能:可将采集的一路或多路网络流量进行复制并分发给不同的工具处理;可将通过不同网络端口采集的网络流量进行汇聚，并分发给单台工具处理;可将采集的多路网络流量进行汇聚之后同时复制成多份输出给不同的工具处理。	否
4	△	流量清洗	系统应支持数据去重功能:将来源于不同接口的流量进行分组之后执行数据去除重复。 系统应支持流量截短功能:支持基于不同的五元组规则下的流量截短功能，对不同的类型的流量能够输出不同截短后长度的数据包。	否
5	△	集中管控	支持 CLI、SNMP、WEB 管理配置界面具有友好型易用性，WEB 界面支持 HTTPS 且可完成所有配置管理，支持远程升级，支持远程 SYSLOG 服务，可将系统登入、操作日志、接口异常等信息上报。	否
6	△	其它功能	支持不低于 2 层 VLAN、四层 MPLS、IPinIP、GTP-U、GRE、ERSPAN 隧道报文的识别和外层头部去封装	否

8.DNS 系统

序号	重要性	指标项	指标要求	证明材料要求
1	#	性能指标	开启解析日志情况下，单 DNS 系统节点每秒查询次数 QPS≥80,000。	否

2	△	解析功能	系统须支持标准的 DNS 服务，支持正向解、反向解功能;支持常用的记录类型，包括但不限于 A,AAAA,CNAME,MX,NS,PTR,TXT,SRV,SPF 等，对配置的记录支持设置有效期限; 支持 URL, 解析跳转服务，即对指定域名的 HTTP 访问重定向到相应 URL;支持对权威记录自定义添加属性，其中属性名称和内容合法性可由用户自定义添加(如姓名、部门等)	是
3	△	访问调度	系统支持智能化的访问调度，支持 DNS 多种负载均衡动态就近性、CPU/内存负荷算法，来源就近算法、优先可用算法、返回备用 IP 算法、加权比率算法等。	是
4	△	健康检测	支持 4-7 层网络到应用的健康检测，支持多种协议类型的应用健康检测模板定制。支持对业务系统服务器设置多个探测条件,并支持对部分任务设置必须项，部分任务设置可选项两种判断可以同时存在;支持对单个业务系统服务单独配置探测协议，也可以通过资源池对引用的服务器指定公共的探测协议;应用状态探测变更、多个探测模板中任一探测状态变更、节点间信息同步时连接状态变更均支持告警。	是
5	△	高可用	支持探测节点间有冗余机制，当主用探测节点异常时可以由其他探测节点或者备份探测节点自动接替服务;支持域名级设置动态兜底的失败应答策略，减少人工重复配置。	是
6	△	安全防护	支持 Servfail 攻击、DNS 隧道攻击、缓存窥探、反射/放大等攻击防护	是
7	△	平台适配	所投产品部署的硬件要求支持鲲鹏、飞腾、龙芯、海光、兆芯等 CPU，软件系统要求支持麒麟统信等操作系统。	是
8	△	部署架构	所投产品为支持 ANYCAST 集群部署架构，全国 DNS 服务器同时对外提供相同的一个或多个 IP 地址。常态下，本省 DNS 服务节点接收本省 DNS 请求后做应答,当本省 DNS 服务节点发生异常时，由其他正常的 DNS 系统继续提供解析服务。	否
9	△	数据对	各省 DNS 系统应与台网中心 DNS 系	否

		接	统对接，实现数据实时同步与备份。支持通过标准 API 和 syslog 接口的方式与第三方平台进行数据对接，实现日志上传、系统状态监控等功能。	
10	△	资质要求	所投产品厂商具备国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位证书（省级）。	是

9.NTP 系统

序号	重要性	指标项	指标要求	证明材料要求
1	#	性能指标	客户端同步精度≤ 35μs;NTP 请求量≥20000 次/秒;服务器同步精度≤1μs。	是
2	△	硬件配置	冗余电源;网口配置≥6 个千兆电口(每个端口具备授时和管理功能)，支持万兆光口扩展;时钟服务器仅支持处理 B1I 、B1C、 B2I 、B2a、B2b、B3I 频段数据解算，同时软硬件层面均不可具备其他频段的数据处理功能。	是
3	△	授时功能	网络协议:支持 NTP v1/2/3/4(单播/多播/广播/Autokey)、SNTP、IPV4、IPV6、IPv4/IPv6 Hybrid。授时模式:支持 NTP Peer Client/Server Broadcast Multicast。系统支持用户身份鉴别、访问权限控制能力;支持心跳检测功能，两台设备网卡可设为同一 IP，互为冗余备份:支持 Bonding 功能，同一设备多网卡可设为同一 IP，可实现单机网卡故障备份。	是
4	△	监控功能	提供全网时间统一监控功能，可监视卫星信息、服务器信息、客户端信息。卫星信息包括卫星时间、锁定状态、锁定颗数、经纬度、高度等信息:服务器信息包括 NTP 授时状态、同步状态、服务器时间、网络配置等信息:监控告警信息支持本地日志存储; 支持不少于 10000 台客户端监视，可根据需要设置告警类型、告警级别等进行选择上报。	是
5	△	其它功能	具备日志存储功能:日志存储时间大于 6 个月,具有标准化接口可以导出日志，	是

			可扩展硬盘存储; 配置方法:支持 Console、Telnet 和 SSH 进行远程管理、配置和升级; 3、提供配套 NTP 授时软件，能够适配 Windows 操作系统。	
6	△	数据对接	可通过 API 或 SNMMP 远程查看设备时间、状态及锁定等信息。	否
7	△	资质证明	所投产品提供检测报告。	是
8	△	配件要求	实配卫星天线、避雷器、安装支架、时间同步软件、监控软件等	否
9	#	产品证书	产品 3C 证书	是

10.中心站防火墙

序号	重要性	指标项	指标要求	证明材料要求
1	#	硬件要求	≤2U 机架式硬件设备:冗余电源，冗余风扇;≥6 个万兆光口、≥12 个千兆光口、≥4 个千兆电口，满配相应光模块。提供≥5 年产品质保服务。 配置硬件 Bypass 模块，≥2 对万兆光口，增强设备直路部署时的可靠性;（提供官网链接，官网产品文档并加盖厂商公章）	是
2	#	设备可靠性	当电源模块、风扇模块出现故障时，可以在防火墙不断电的情况下，对电源模块、风扇模块进行更换（提供官网链接，官网产品文档及操作步骤说明，并加盖厂商公章）	是
3	★	性能要求	配置防火墙吞吐量≥10GB。最大并发连接数≥1000 万，每秒新建连接数≥25 万。防火墙配置多种安全业务的虚拟化功能，包括防火墙、入侵防御、防病毒等。不同用户可在同一台物理设备上进行隔离的个性化管理，实配虚拟系统功能。	是
4	△	特征库	防火墙实配防病毒、入侵防御等功能，明确病毒库、特征库等库表需更新授权。 提供 5 年病毒库、特征库等库表更新授	是

			权。	
5	△	防病毒	能够对 HTTP/FTP/POP3/SMTP/IMAP 协议进行病毒查杀。	否
6	△	入侵防御	支持漏洞防护功能，支持独立的入侵防护规则特征库，能对常见漏洞进行安全防护。规则库支持根据攻击类型、风险等级等进行分类，支持阻断、放行。	否
7	△	访问控制	支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制。支持基于单个对象、局域网络和地理区域维度设置安全访问控制策略。	否
8	#	Ipv6	支持一条安全策略中同时配置 ipv4 和 ipv6 地址。（提供功能截图及框选该功能，并加盖厂商公章）	是
9	△	IPv6 支持	支持 IPv4/Pv6 网络双栈、6to4 隧道;访问控制、攻击防护、应用识别、URL,过滤、防病毒、流量控制、入侵防御等功能支持 IPv6 业务场景。	否
10	△	部署方式	支持二层模式(透明模式)、三层模式(路由和 NAT 模式)和混合模式。	否
11	△	管理方式	支持 Web 和 ssh 方式管理设备和策略配置，支持多种用户认证，支持记录流量日志，包括源地址、目的地址、源端口、目的端口、策略允许/阻断情况。	否
12	△	系统接口	支持通过标准 API 和 syslog 接口的方式与第三方平台进行数据对接。	否
13	△	集成要求	支持将日志数据报送给安管平台。	否
14	△	自主可控	CPU（处理器）、LSW（转发芯片）均为国产自研芯片或采用飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否

11.中心站入侵检测

序号	重要性	指标项	指标要求	证明材料要求
1	#	硬件要求	≤2U 机架式硬件设备;冗余电源，≥1 个 Console 口，≥1 个 10/100/1000M 自适应带外管理口，≥4 个	否

			10/100/1000M 自适应千兆电口，≥4 个千兆光口。	
2	△	性能要求	整机吞吐量≥10Gbps，TCP 并发连接数≥300 万，TCP 每秒新建≥8 万；日志存储大于 6 个月。	否
3	△	入侵检测功能	支持检测 WEB 攻击、远程控制、WEB 后门访问、SMB 远程溢出攻击、隧道通信、扫描行为、暴力破解、挖矿、恶意工具利用、漏洞利用等风险;支持域名白名单、IP 白名单的配置。	否
4	△	IPv6 等协议支持	支持 IPv4 和 IPv6 网络环境下的部署，可同时对 IPv4 和 IPv6 网络流量分析检测;支持 SNMP V1-V3 和 syslog 接口，可接受第三方管理平台的集中时间管理。支持解析 HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、MSSOL、Oracle、SRV6.HTTP2。	否
5	△	部署方式	设备支持旁路部署、网桥部署、虚拟网线部署、混合部署多种部署方式。	否
6	△	集成要求	支持将日志数据报送给安管平台。	否
7	△	自主可控	支持飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否

12.中心站堡垒机

序号	重要性	指标项	指标要求	证明材料要求
1	△	硬件规格	≤2U 标准机架设备，≥4 个千兆电口，≥2 个万兆光口,满配相应多模光模块，冗余电源，硬盘容量≥4T，实配国密，支持基于 SM3/SM4 等国密算法的动态令牌进行双因子认证，数量≥20 个。	否
2	△	设备性能	可管理设备数量≥500 个，运维用户无限制;单台堡垒机字符类并发会话≥500、图形类并发会话≥150，实配对 IPv4、IPv6 资产的运维管理。实配应用 发布服务器软件，支持 C/S 架构软件的应用发布功能，允许发布≥30 个应用；可支持≥30 人使用。日志存储大于 6 个月。	否
3	△	支持协	字符协议支持 SSH、TELNET;图形协议	否

		议	支持 RDP、VNC、X11;文件传输协议支持 FTP、SFTP，SCP;支持通过浏览器页面 H5 方式发起运维操作。	
4	△	支持主机类型	支持 Windows 主机、Unix 主机、Linux 主机，支持麒麟、统信、方德等操作系统和网络设备、安全设备;	否
5	△	支持数据库类型	支持 Oracle、SQL Server、MySQL、达梦、kingbase、海量、瀚高等主流数据库及开源数据库;	否
6	△	运维访问管理	支持 SSH、RDP 协议的文件上传、下载操作，支持 SSH、TELNET、RDP、VNC、X11 协议的运维，支持基于用户、资产、资产账号、协议配置访问控制策略，SFTP/FTP 协议支持控制上传文件、下载文件、删除文件、重命名文件、创建文件目录、删除文件目录等。	否
7	△	用户管理	支持用户角色划分功能，如审计管理员、系统管理员、运维管理员等，支持角色自定义功能;支持用户密码策略，包括:最小、最大密码长度、密码复杂度、密码有效期、历史密码不能重复的次数设置、锁定策略:支持提醒用户 7 天内密码过期，7 天后登录修改密码;	否
8	△	资产管理	支持针对 IP 地址段内的目标设备自动发现和导入功能:应支持资产权限视图功能，可直观展示能够访问此资产的用户账号、授权关系等信息;具备应用发布功能，实现 C/S 和 B/S 架构应用的资产管理。	否
9	△	认证管理	支持本地密码认证、动态口令认证;Radius 认证、LDAP 认证、AD 域认证、短信认证、指纹认证:支持 x5.09 证书;支持用户忘记登录密码时，在登录首页申请密码重置:支持重置密码:	否
10	△	审计管理	具备在线会话和历史会话审计，文持以字符会话回放、图形会话回放、数据库会话回放等方式实现会话操作审计; 具备文件传输审计功能，支持传输文件查看及下载，支持文件传输留痕配置;	否
11	△	授权管理	设备登录、命令操作审批策略，审批人可针对登录行为或命令操作进行同意或者驳回审批;支持动态规则的运维授权，特定用户组，资产组授权模式，用户加入用户组，资产加入资产组直接可	否

			白动授权支持访问策略的批量导入、导出及批量编辑功能;	
12	△	系统管理	支持实时监控系统 CPU、内存、磁盘空间、在线用户、资产并发的实时信息;支持分权分域管理功能，针对多部门实现权限精细划分，各个部门的管理员分别管理本部门的用户、资产及子部门，从而实现各部门之间的权限相互独立:	否
13	△	集成要求	支持将日志数据报送给安管平台。	否

13.安管平台

序号	重要性	指标项	指标要求	证明材料要求
1	★	平台要求	冗余电源和风扇，接口:千兆电口≥4个、万兆光口≥4个;配置≥1台采集探针。具有数据采集、威胁情报、资产管理、数据分析、日志检索、联动处置、通报预警、安全态势、报表管理、数据对接等相关功能，实时汇聚报送安全事件和相关安全数据。	是
2	#	探针要求	冗余电源，网络层吞吐量≥2Gbps;内存大小≥8G，硬盘容量≥128GSSD;接口:千兆口≥6个、10G光口≥2个。	否
3	△	部署模式	支持单机、级联、集群等部署模式。采用国产化操作系统、国产数据库部署。	否
4	△	支持协议	能够识别常见协议并还原网络流量,用于取证分析、威胁发现。实现识别包括但不限于 http、dns、smtp、pop3、imap、webmail、DB2、Oracle、SOL Server、MySQL、 PostgreSQL、 Sybase、SMB、FTP、SNMP、telnet、nfs 等协议，实现对 VNC、SSH、RDP 等协议的漏洞利用攻击检测。实现解析 IPv6 地址、转换数据格式、解压缩。	否
5	△	监控大屏	支持多种网络安全态势监控大屏。支持整体安全态势的评估展示;包括资产态势、脆性态势、网络攻击态势、安全事件态势、外连态势、横向威胁态势;实现页面跳转到对应态势大屏，并具备大	否

			屏告警能力。	
6	△	威胁展示	支持主机视角展示某主机下所有威胁事件，展示内容包括不限于:严重级别、IP 及资产属性、主机威胁状态或安全事件、检出威胁标签或来源、最近告警时间及处置状态或操作;支持对所有的主机进行威胁状态判定，如“被外部攻击成功”或入侵、“发起内网渗透或横向扩散、“已失陷””、“APT”“建立远控链接”或命令控制、“Webshell”’、“挖矿”“对外攻击”或攻击利用等。	否
7	△	流量检测	基于双向全流量做检测，能够从多个维度捕获攻击，并且自动化完成对后续攻击成功失败的判定和严重级别的调整，在外部攻击/内网渗透检测场景自动判定攻击成功/失败结果，在内网失陷检测中自动判断受害者主机是否和远控端建立连接，并记录完整连接内容;	否
8	#	加密流量检测	针对加密流量，在无需对流量解密的前提下，通过检测模型实现对加密流量的异常检测，并呈现被感染主机及访问的 C&C 服务器信息,恶意加密 C&C 流对网络的危害信息，取证详情及处理建议。（提供权威机构出具的测试报告并加盖厂商公章）	是
9	△	攻击链分析	支持以攻击者或攻击团伙视角通过时间线的方式将零散的告警聚合成完整的威胁事件，将攻击者从第一次攻击到最后一次攻击按照时间线展示出来; 支持通过攻击团伙的手法类型、时间分布等元素，结合威胁情报识别针对性攻击，并还原攻击过程。对于攻击卫，支持通过威胁情报、历史攻击访问行为、云端共享数据等，综合分析攻击者特征，提供给企业安全运营团队在日常安全运营和重保防御过程中进行调查。	否
10	△	资产检测	联动漏洞扫描，支持对社会面所有重要漏洞进行检测，支持通过准确发现失陷主机与被控端的连接，精准定位失陷主机，点击查看详情后可以看到告警明细及针对告警的分析与处置建议;支持资产全生命周期自动管理，包括资产白动发现、资产审核、资产离线风险识别、	否

			资产退库、资产数据更新，责任人管理机制等。	
11	△	处置流程	支持自动化编排的自定义处置流程策略的设置，融入事件自动处置流程，节省运维处置时间，可根据实际生产环境需要对接所需安全设备。	否
12	△	系统集成	平台支持各类安全告警信息通过短信、电话、邮箱等形式进行发布。支持通过标准 API 和 syslog 接口的方式与第三方平台进行数据对接，确保与中国地震台网中心的安全管理平台对接，并与省本级的安全设备对接，收集省中心及中心站的防火墙、网络安全审计、上网行为管理、入侵检测、入侵防御、日志审计等设备的安全原始日志，进行统一分析和攻击链还原，实现深度告警聚合（提供承诺函并加盖厂商公章）	是
13	△	自主可控	所投产品 CPU 支持飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否

14.核心防火墙

序号	重要性	指标项	指标要求	证明材料要求
1	#	硬件要求	≤2U 机架式硬件设备。冗余电源;冗余风扇，1 个 console 口，1 个 MGT 口;≥6 个万兆光口、≥8 个千兆光口、≥8 个千兆电口，并满配相应的光模块;提供≥5 年产品质保服务。 配置硬件 Bypass 模块，≥2 对万兆光口,增强设备直路部署时的可靠性;(提供官网链接,官网产品文档并加盖厂商公章）	否
2	#	设备可靠性	当电源模块、风扇模块出现故障时，可以在防火墙不断电的情况下,对电源模块、风扇模块进行更换(提供官网链接，官网产品文档及操作步骤说明并加盖厂商公章）	是
3	★	性能要求	配置防火墙吞吐量≥30GB。应用层吞吐量≥15Gbps，最大并发连接数≥1000 万，每秒新建连接数≥25 万。防火墙配置多种安全业务的虚拟化功能,包括防火墙、入侵防御、防病毒等。不同用	是

			户可在同一台物理设备上进行隔离的个性化管理，实配虚拟系统功能。	
4	△	特征库	防火墙实配防病毒、入侵防御等功能。提供 5 年病毒库、IPS、特征库等库表更新授权。	是
5	△	品牌异构需求	为降低同一品牌导致系统风险，要求与互联网防火墙、边界防火墙两类区域边界安全能力异构，采用不同生产厂家产品。	否
6	△	防病毒	能够对 HTTP/FTP/POP3/SMTP/IMAP 等协议进行病毒查杀。	否
7	#	URL	支持 URL 识别能力和 URL 地址识别库，云端 URL 识别库≥5 亿。（提供功能截图并框选，加盖厂商公章）	是
8	△	入侵防御	支持漏洞防护功能，支持独立的入侵防护规则特征库，能对常见漏洞进行安全防护。规则库支持根据攻击类型、风险等级等进行分类，支持阻断、放行。	否
9	△	访问控制	支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制。支持基于单个对象、局域网络和地理区域维度设置安全访问控制策略。	否
10	△	IPv6 支持	支持 IPv4/IPv6 网络双栈、6to4 隧道;访问控制、攻击防护、应用识别、URL 过滤、防病毒、流量控制、入侵防御等功能支持 IPV6 业务场景。	否
11	△	部署模式	支持路由模式、透明(网桥)模式、混合模式。	否
12	△	管理方式	支持 Web 和 ssh 方式管理设备和策略配置，支持多种用户认证，支持记录流量日志，包括源地址、目的地址、源端口、目的端口、策略允许/阻断情况。	否
13	△	系统接口	支持通过标准 API 和 syslog 接口的方式与第三方平台进行数据对接。	否
14	△	集成要求	支持将日志数据报送给安管平台。	否
15	△	自主可控	CPU（处理器）均为国产自研芯片或采用飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否

15.互联网防火墙

序号	重要性	指标项	指标要求	证明材料要求
1	#	硬件要求	≤2U 机架式硬件设备。冗余电源;冗余风扇，1 个 console 口，1 个 MGT 口;≥6 个万兆光口、≥8 个千兆光口、≥8 个千兆电口，并满配相应的光模块;配置硬件 Bypass 模块，≥2 对万兆 Bypass 光口，增强设备直路部署时的可靠性；提供≥5 年产品质保服务。	否
2	★	性能要求	配置防火墙吞吐量≥20GB。应用层吞吐量≥10Gbps，最大并发连接数≥1000 万,每秒新建连接数≥25 万支持路由、交换、混合工作模式,支持策略略路由,支持根据入接口、源/目的 IP 地址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、NoPAT 转换方式。	是
3	△	特征库	防火墙实配防病毒、入侵防御等功能。实配≥5 年 IPS 授权、AV 防病毒授权、应用识别特征库等全功能模块授权。	是
4	△	品牌异构需求	为降低同一品牌导致系统风险,要求与核心防火墙、边界防火墙两类区域边界安全能力异构，采用不同生产厂家产品。	否
5	△	防病毒	能够对 HTTP/FTP/POP3/SMTP/IMAP 协议进行病毒查杀;支持 URL 识别能力和 URL 地址识别库，云端 URL 识别库≥5 亿。	否
6	△	入侵防御	支持漏洞防护功能,支持独立的入侵防护规则特征库,能对常见漏洞进行安全防护。规则库支持根据攻击类型、风险等级等进行分类，支持阻断、放行。	否
7	△	访问控制	支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制。支持基于单个对象、局域网络和地理区域维度设置安全访问控制策略。	否
8	△	工作模式	支持路由、交换、透明、旁路、混合工作模式。支持 IPv4/IPv6 双栈工作模	否

			式。	
9	△	部署模式	支持路由模式、透明(网桥)模式、混合式。	否
10	△	管理方式	支持 Web 和 ssh 方式管理设备和策略配置，支持多种用户认证，支持记录流量日志，包括源地址、目的地址、源端口、目的端口、策略允许/阻断情况。	否
11	#	系统接口	支持通过标准 API 和 syslog 接口的方式与第三方平台进行数据对接。 支持基于安全策略设定会话长连接	否
12	△	集成要求	支持将日志数据报送给安管平台。	否
13	△	自主可控	采用自主研发的关键芯片（CPU）或采用飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否

16.边界防火墙

序号	重要性	指标项	指标要求	证明材料要求
1	#	硬件要求	≤2U 机架式硬件设备。冗余电源;冗余风扇，1 个 console 口，1 个 MGT 口;≥6 个万兆光口(≥2 对硬件 Bypass 模块）、≥8 个千兆光口、≥8 个千兆电口，并满配相应的光模块；提供≥5 年产品质保服务。	否
2	★	性能要求	配置防火墙吞吐量≥20GB。应用层吞吐量≥10Gbps，最大并发连接数≥1000 万，每秒新建连接数≥25 万。防火墙配置多种安全业务的虚拟化功能，包括防火墙、入侵防御、防病毒等。不同用户可在同一台物理设备上进行隔离的个性化管理，实配虚拟系统功能。	是
3	△	特征库	防火墙实配≥5 年防病毒、入侵防御等功能，明确病毒库、特征库等库表需更新授权。	是
4	△	品牌异构需求	为降低同一品牌导致系统风险，要求与核心防火墙、互联网防火墙两类区域边界安全能力异构，采用不同生产厂家产品。	否
5	△	防病毒	能够对 HTTP/FTP/POP3/SMTP/IMAP 协议进行病毒查杀；支持 URL 识别能力和	否

			URL 地址识别库。	
6	#	入侵防御	支持漏洞防护功能，支持独立的入侵防护规则特征库，能对常见漏洞进行安全防护。规则库支持根据攻击类型、风险等级等进行分类，支持阻断、放行。 支持 DDOS 防护功能，支持 DNS DDOS 防护，可对 DNS 投毒攻击、DNS NX 异常比率检测等；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攻击防护；支持根据 DOS/DDOS 攻击行为自动添加动态黑名单功能；（要求提供功能截图页面并框画该功能重点标记同时加盖产品厂商公章））	是
7	#	访问控制	支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN 等多种方式进行访问控制。支持基于单个对象、局域网络和地理区域维度设置安全访问控制策略。 支持文件过滤，可对即时通讯、社交网络、网络硬盘、网页邮箱、IM 文件传输等应用类型以及 HTTP/FTP/SMTP/POP3 等标准协议进行检测。支持邮件安全防护，可对邮件过滤、邮箱防暴力破解、邮件泛洪攻击防护、邮件黑、白名单检测；（要求提供功能截图页面并框画该功能重点标记同时加盖产品厂商公章）	是
8	△	IPv6 支持	支持 IPv4/Pv6 网络双栈、6to4 隧道;访问控制、攻击防护、应用识别、URL,过滤、防病毒、流量控制、入侵防御等功能支持 IPv6 业务场景。	否
9	△	部署模式	支持路由模式、交换模式、旁路模式、虚拟网线工作模式;部署模式切换无需重启设备。	否
10	△	管理方式	支持 Web 和 ssh 方式管理设备和策略配置，支持多种用户认证，支持记录流量日志，包括源地址、目的地址、源端口、目的端口、策略允许/阻断情况。	否
11	△	系统接口	支持通过标准 API 和 syslog 接口的方式与第三方平台进行数据对接。	否
12	△	集成要求	支持将日志数据报送给安管平台。	否
13	△	自主可控	采用自主研发的关键芯片（CPU ）或采	否

			用飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	

17.数据库审计系统

序号	重要性	指标项	指标要求	证明材料要求
1	△	性能要求	业务流量处理能力≥2Gbps，数据库实例个数≥20 个，SQL 处理性能≥15000 条 SQL/s，默认含应用规则库。	否
2	△	硬件规格	机架式≤2U，硬盘≥2T，1 个 console 口，1 个 MGT 口；实配≥4 个千兆电口，≥4 个万兆光口(≥4 个万兆多模模块)；冗余电源，冗余风扇；存储日志在 6 个月以上。	否
3	△	兼容性要求	支持细粒度解析多种数据库协议，包括关系型数据库、NoSQL 等，兼容 Oracle、SQL Server、DB2、MySQL(TDSQL)、Informix、Sybase、Caché、PostgreSQL、达梦、人大金仓、海量、翰高等数据库。	否
4	△	部署方式要求	支持旁路镜像部署，可利用 agent 或镜像数据直接进行审计，满足在虚拟化以及物理环境中对数据库的审计要求。	否
5	△	系统功能	支持数据库请求和返回的双向审计，特别是 SQL,返回结果集、SQL,语句响应时间、连接时长、表影响的字段、影响行数等内容。 支持依据数据库实例监控各个数据的数据库类型、活跃会话数、总会话数、负载等信息。 支持频次统计，在一定时间内操作达到闽值进行单独记录和展示，时间与次数可按需配置支持自定义日志查询。	否
6	△	系统加固	支持双因子认证，密码策略，用户分权等，满足等保要求的措施。	否
7	△	集成要求	支持将日志数据报送给安管平台。	否
8	△	自主可控	支持飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否

18.网络安全审计

序号	重要性	指标项	指标要求	证明材料要求
1	#	性能要求	吞吐量≥2Gbps，最大并发连接数≥120万，最大新建连接数≥40000 个/秒，默认含应用识别功能。	否
2	△	硬件规格	机架式≤2 U，硬盘≥4T，1 个 console 口，1 个 MGT 口；实配≥6 个千兆电口，≥6 个万兆光口(满配万兆多模模块)，冗余电源，冗余风扇，≥2 个扩展槽位。存储日志在 6 个月以上。	否
3	#	系统功能	内容审计:支持协议内容审计，支持 HTTP、FTP、Telnet、Radius、文件共享等协议。可以把应用协议分组进行审计，用户可以根据需求自行选择审计内容。行为审计:支持应用协议行为识别及自定义规则库。 支持审计查询，支持标准查询、经典查询和专家查询多种查询方式。支持界面展示查询条件、事件数、应用协议及任务运行时间。支持自定义查询事件数，支持千万级数据秒级查询，支持 csv 格式导出审计日志。（要求提供功能截图页面并框画该功能重点标记同时加盖产品厂商公章）	是
4	#	应用识别	内置应用识别规则库，支持应用协议自动识别与审计记录。 支持异常流量检测，支持 flood 攻击检测、接口流量监测。支持配置异常连接检测周期、接口流量上限及总流量上线。（要求提供功能截图页面并框画该功能重点标记同时加盖产品厂商公章）	是
5	△	系统加固	支持双因子认证，密码策略，用户分权等，满足等保要求的措施。	否
6	#	集成要求	支持将日志数据报送给安管平台。支持日志外发，支持 Syslog、snmptrap、Kafka、邮箱、短信等方式向外发送审计日志。支持抓包工具，可配置抓包个数、源和目的 IP、协议类型等。（要求提供功能截图页面并框画该功能重点标记同时加盖产品厂商公章）	是
7	△	自主可控	支持飞腾、海思、鲲鹏、盛科、海光、	否

			兆芯等芯片	

19.上网行为管理

序号	重要性	指标项	指标要求	证明材料要求
1	#	硬件规格	≤2U 标准机架设备;≥6 千兆电口;≥4 万兆光口（配置硬件 Bypass 模块），满配相应多模光模块，冗余电源；冗余风扇。	否
2	△	设备性能	网络层吞吐量≥10G，应用层吞吐量≥1.5Gb，带宽性能≥1Gb，支持用户数≥5000，每秒新建连接数≥14000，最大并发连接数≥600000。	否
3	△	核心功能	具备所有核心功能:上网认证、应用控制、流量控制、内容审计、日志报表、准入控制等;所有核心功能(上网认证、应用控制、流量控制、内容审计、日志报表等)都支持 IPv6，设备接口及部署模式均支持 ipv6 配置。	否
4	△	授权要求	提供≥5 年 URL 库、应用特征库升级，授权到期后不影响现有功能。	否
5	△	部署模式	支持路由模式(NAT、路由转发、DHCP、GRE、OSPF)、网桥模式(多路桥接模式)、旁路模式;	否
6	△	应用管控	内置应用识别规则库，支持根据标签选择应用，并支持给每个应用自定义标签;支持根据标签选择一类应用做控制;	否
7	△	异常流量分析	支持 PPS 异常、丢包异常、ARP 异常、内网 DOS 攻击等异常情况实时监测，显示每日异常事件个数及情况;	否
8	△	文件审计	支持 WEB/FTP/SMB 类型业务的行为和内容审计，对上传/下载文件可选择只审计文件名或同时审计文件内容。	否
9	△	系统接口	支持通过标准 API 和 syslog,接口的方式与第三方平台进行数据对接。	否
10	△	集成要求	支持将日志数据报送给安管平台。	否
11	△	自主可控	支持飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否

20.主机安全

序号	重要性	指标项	指标要求	证明材料要求
1	★	基础参数	产品实配不少于 600 个 License 授权，其中服务器端不少于 240 个授权，电脑端不少于 360 个授权；整体提供不少于 5 年原厂维保和特征库升级服务。	是
2	△	核心功能	资产清点：需支持识别并采集主机的主机层、系统层等各层资产信息。 风险发现：支持检测主机操作系统和软件应用的漏洞、弱密码、危险配置等内部风险。 入侵检测：支持暴力破解、异常登录、操作系统文件篡改、等主机入侵事件实时检测，支持按照不同时间段，发现失陷主机，并提供对入侵事件的响应手段。 合规基线：根据安全标准对主机操作系统、展示基线检查结果，给出基线整改建议。 病毒查杀：具备多引擎病毒查杀能力，可对文件进行扫描查杀，同时可实时监控运行进程，发现病毒时立即上报告警并进行处置。 访问控制：配置黑、白名单网络策略，控制主机的网络访问行为。 隔离失陷主机：一键隔离失陷主机的网络，阻断出入主机的网络访问。	否
3	△	大屏展示	需支持大屏展示功能，从不同维度汇总并可视化的呈现主机的总体安全状况。	否
4	△	部署模式	支持分级部署、分级管理模式。支持分级部署、分级管理模式。	是
5	△	信创环境支持	支持部署于主流国产化环境。	是
6	△	其它功能	对文件、进程、注册表等进行实时监测，并对异常行为做出响应，及时阻止病毒入侵。	否
7	△	系统接口	能够通过标准的 API 接口和 syslog 等方式与第三方平台进行数据对接。	否

21.省中心堡垒机

序号	重要性	指标项	指标要求	证明材料要求
1	△	硬件规格	≤2U 标准机架设备，≥4 个千兆电口，≥2 个万兆光口,满配相应多模光模块，冗余电源，硬盘容量≥4T，实配国密加密，支持基于 SM3/SM4 等国密算法的动态令牌进行双因子认证，数量≥20 个。	否
2	△	设备性能	可管理设备数量≥500 个，运维用户无限制;单台堡垒机字符类并发会话≥500、图形类并发会话≥150，实配对 IPv4、IPv6 资产的运维管理。实配应用发布服务器软件，支持 C/S 架构软件的应用发布功能，允许发布≥30 个应用；可支持≥30 人使用。日志存储大于 6 个月。	否
3	△	支持协议	字符协议支持 SSH、TELNET;图形协议支持 RDP、VNC、X11;文件传输协议支持 FTP、SFTP，SCP;支持通过浏览器页面 H5 方式发起运维操作。	否
4	△	支持主机类型	支持 Windows 主机、Unix 主机、Linux 主机，支持麒麟、统信、方德等操作系统和网络设备、安全设备;	否
5	△	支持数据库类型	支持 Oracle、SQL Server、MySQL、达梦、kingbase、海量、瀚高等主流数据库及开源数据库;	否
6	△	运维访问管理	支持 SSH、RDP 协议的文件上传、下载操作，支持 SSH、TELNET、RDP、VNC、X11 协议的运维，支持基于用户、资产、资产账号、协议配置访问控制策略，SFTP/FTP 协议支持控制上传文件、下载文件、删除文件、重命名文件、创建文件目录、删除文件目录等。	否
7	△	用户管理	支持用户角色划分功能，如审计管理员、系统管理员、运维管理员等，支持角色自定义功能;支持用户密码策略，包括:最小、最大密码长度、密码复杂度、密码有效期、历史密码不能重复的次数设置、锁定策略:支持提醒用户 7 天内密码过期，7 天后登录修改密码;	否
8	△	资产管理	支持针对 IP 地址段内的目标设备自动发现和导入功能:应支持资产权限视图	否

			功能，可直观展示能够访问此资产的用户账号、授权关系等信息;具备应用发布功能，实现 C/S 和 B/S 架构应用的资产管理。	
9	△	认证管理	支持本地密码认证、动态口令认证;Radius 认证、LDAP 认证、AD 域认证、短信认证、指纹认证:支持 x5.09 证书;支持用户忘记登录密码时，在登录首页申请密码重置:支持重置密码:	否
10	△	审计管理	具备在线会话和历史会话审计，文持以字符会话回放、图形会话回放、数据库会话回放等方式实现会话操作审计; 具备文件传输审计功能，支持传输文件查看及下载，支持文件传输留痕配置;	否
11	△	授权管理	设备登录、命令操作审批策略，审批人可针对登录行为或命令操作进行同意或者驳回审批;支持动态规则的运维授权，特定用户组，资产组授权模式，用户加入用户组，资产加入资产组直接可白动授权支持访问策略的批量导入、导出及批量编辑功能;	否
12	△	系统管理	支持实时监控系统 CPU、内存、磁盘空间、在线用户、资产并发的实时信息; 支持分权分域管理功能，针对多部门实现权限精细划分，各个部门的管理员分别管理本部门的用户、资产及子部门，从而实现各部门之间的权限相互独立:	否
13	△	集成要求	支持将日志数据报送给安管平台。	否

22.日志审计系统

序号	重要性	指标项	指标要求	证明材料要求
1	△	硬件要求	≤2U 设备，冗余电源，冗余风扇;1 个 console 口，1 个 MGT 口；≥4 个千兆电口，≥2 个万兆光口(含 2 个万兆光模块);≥1 个扩展插槽;内存≥64G，硬盘≥4*2T，支持扩容，支持 RAID、SM2/SM3/SM4 等国密算法。	否
2	△	性能要求	日志处理性能≥15000EPS;支持≥200 个日志源; 支持数据加密存储，加密算法支持国密	否

			算法; 支持数据交互式多条件查询，查询响应时间小于 10s; 实配符合等保三级要求的日志存储加密功能。日志存储大于 6 个月。	
3	△	系统架构	系统基于 B/S 架构，可通过 Web 方式直接对系统管理;支持内/外置采集器，进行日志采集;支持传输加密;	否
4	△	系统功能	日志采集:描述采集范围，支持的设备类型、支持的协议类型等; 日志解析:描述支持的解析设备类型、解析规则等，内置 5000 种以上设备类型的解析规则; 日志存储:描述日志存储的备份策略、存储方式等; 日志检索:描述支持的检索方式、检索规则等; 日志分析:支持将不同设备上采集的日志进行关联分析，可扩展关联分析规则。	否
5	△	日志告警	支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件;	否
6	△	告警转发	支持把告警通过 API 的方式发送至第三方接口，告警内容支持自定义。	否
7	△	自主可控	支持飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否

23.Web 应用防火墙

序号	重要性	指标项	指标要求	证明材料要求
1	#	硬件要求	≤2U 设备，冗余电源，冗余风扇;配置 1 个 console 口；千兆电口≥4 个;万兆光口≥4 个(配置 2 对硬件 Bypass 模块);光模块满配。	是
2	★	性能要求	整机吞吐≥10Gbps，最大并发连接数≥500 万，每秒新建连接数≥5 万;产品必须为专业性 WEB 应用防火墙硬件设备，而非下一代防火墙\UTM 类设备集成的 WEB 防护功能。	是
3	△	品牌异构	为降低同一品牌导致系统风险，要求与	否

		需求	互联网防火墙、抗 DDOS 异构，采用不同生产厂家产品。	
4	△	部署模式	支持透明部署，旁路部署，反向代理模式、镜像部署等部署模式。	否
5	#	分析能力	支持对 SSL(HTTPS)加密会话进行分析，支持对客户端 HTTP 请求的 SSL,加载，及对服务器侧的 SSL 卸载:支持设定前置参数名、正则表达式、参数范围等匹配特定的 Host、URL 进行限定。（提供权威机构出具的测试报告并加盖厂商公章）	是
6	△	防护能力	支持基础防护、专项防护、扩展防护能力等:	否
7	#	注册防护	支持通过设置 Cookie 校验、注册地址、注册校验地址、标识、告警阀值、阻断阀值、作用时间等参数实现注册防护。（提供产品配置截图证明）	是
8	△	集成要求	支持将日志数据报送给安管平台。	否
9	△	自主可控	支持飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否

24.负载均衡系统

序号	重要性	指标项	指标要求	证明材料要求
1	#	配置要求	≤2U 设备；≥1 个管理口、≥1 个 HA 口、≥6 个千兆电口、≥2 个千兆光口、≥4 个万兆光口 SFP+;并满配相应光模块。冗余电源。	否
2	#	性能要求	四层吞吐≥20Gbps，最大并发连接≥1000 Wcps，四层最大新建连接 CPS≥18Wcps，七层最大新建连接 RPS≥35Wcps。	否
3	△	功能要求	支持链路负载均衡、服务器负载均衡和全局负载均衡的多功能合一,无需额外购买相应授权。	否
4	#	配置信息	支持配置导入/导出功能，可以 Excel 表格的形式，导入/导出服务器负载均衡、链路负载均衡等业务的多种配置信息。（提供产品配置截图证明 并加盖厂商公章）	是
5	△	链路算法	支持轮询、比率、最小连接数、最小往	否

			返延时等算法。	
6	#	健康检查	支持主动健康检查和被动健康检查相结合的方式。 支持自动和非自动一致性检查，支持显示检查结果是否一致。可展示不一致详情信息，包括地址池、NAT 策略、包过滤、真实服务、真实服务组、虚拟服务、健康监测、会话保持、HTTP 内容调度、SSL 策略等差异化对比。（提供产品配置截图并框选该功能，加盖厂商公章）	是
7	△	自主可控	支持飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否

25.网络安全准入

序号	重要性	指标项	指标要求	证明材料要求
1	#	配置要求	标准机架式，≥6 个千兆电口，≥2 个千兆光口(满配千兆多模模块)，冗余电源，冗余风扇。终端管控许可≥2000 个;管理 VLAN、子网≥120 个;最大并发连接数≥100/每秒	否
2	△	部署要求	支持纯旁路部署。	否
3	△	集成要求	支持将日志数据报送给安管平台,支持管理员自定义每个入网事件的处理动作,支持发送 SYSLOG/邮件/短信等。	否
4	#	准入控制	准入未放行前支持 web 重定向、邮件重定向方式引导；支持准入控制阻断和提醒模式，提醒并帮助用户自助安装；支持有客户端与无客户端的端口级准入效果（提供产品功能界面截图并标注该功能，加盖厂商公章）	是
5	△	终端发现	支持自动发现在网终端设备，10 秒内发现新接入终端。支持自动发现网中网行为，如小路由、随身 WiFi、免费 WIFI、代理上网等行为。	否
6	△	入网策略	可基于子网配置是否开启新终端入网注册策略。支持采用浏览器 Portal 页面方式进行终端注册。 支持自定义准入策略，可基于终端隶属部门/终端类型/终端操作系统/自定义	否

			标签组合方式进行区分配置并可基于 VLAN 定义不同的准入策略。 支持通过多种认证方式入网。至少包括用户名密码认证、MAC 地址认证、手机验证码登录或图形密码认证登录，支持与外部认证平台联动，如:企业微信、ADLDAP、Radius 服务器等。支持基于上级准入系统作为认证源，承载下级准入系统范围内的入网终端认证。支持对哑终端进行仿冒检查，在不安装客户端或插件的情况下，进行 MAC 地址仿冒检查。 支持策略路由、端口镜像、802.1X、Portal 等准入技术，支持准入技术自由组合使用。	
7	#	其它功能	支持智能应急逃生方式，系统检测到运行中出现的异常和故障需要能够自动应急，一定时间内连续出现的多台终端准入失败自动临时放行且阈值可自定义（分钟级别）确保企业网络的可用性（提供产品功能界面截图并加盖厂商公章）	是
8	△	集成要求	支持将日志数据报送给安管平台。	否
9	△	自主可控	支持飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否

26.抗 DDOS 系统

序号	重要性	指标项	指标要求	证明材料要求
1	#	配置要求	≤2U 设备，内存≥8 G，硬盘≥1TB;≥1 个管理口，≥1 个 HA 口; ≥6 个千兆电口;≥4 个万兆光口(满配多模光模块)，≥4 个千兆光口(满配光模块);冗余电源，冗余风扇。配置硬件 Bypass 模块，≥2 对万兆光口，增强设备直路部署时的可靠性。（提供官网链接，官网产品文档并加盖厂商公章）	否
2	#	设备可靠	当电源模块、风扇模块出现故障时，可	是

		性	以在防火墙不断电的情况下，对电源模块、风扇模块进行更换（提供官网链接，官网产品文档及操作步骤说明并加盖厂商公章）	
3	△	性能要求	清洗性能≥10Gbps，最大并发连接数≥1000W，最大新建连接数≥10W/s	否
4	△	品牌异构需求	为降低同一品牌导致系统风险，要求与互联网防火墙、Web 应用防火墙异构，采用不同生产厂家产品。	否
5	△	数据对接要求	支持通过标准 API 和 syslog,接口的方式与第三方平台进行数据对接。	否
6	△	部署模式	支持 IPv4/IPv6 双协议栈;支持串联、旁路部署方式。	否
7	△	网络层清洗	支持包括但不限于:IP Fragment Flood、ICMP FLOOD、land attack、tcp misuse、udp misuse、tcpsscan attack、targa3 attack、smurf ack、fraggle attack、rr attack、sr attack、ip option attack、tracert attack、ping of death attack、redirect attack、unreach attack、icmp large attack、protocolnull attack 等网络层攻击的清洗。	否
8	△	传输层清洗	支持对 TCP flood、TCP FRAG flood、syn flood、ack flood、synack flood、fin flood、rst flood、TCP ABNORMAL FLAG FLOOD、新建 SESSION FLOOD、SESSION FLOOD、UDP FLOOD、UDP FRAG FLOOD、UDP 反射 flood 等传输层协议的清洗。	否
9	△	过滤器	支持基于 IP、TCP、UDP、ICMP、ICMPv6、HTTP、HTTPS、DNS、SIP 、NTP、OTHER 等协议的自定义报文特征过滤;支持基于应用协议的关键字段的过滤;支持基于源地理 PP 流量的过滤，要求国内精准到省级、直辖市，国外精准到具体国家。	否
10	△	集成要求	支持将日志数据报送给安管平台。	否
11	△	自主可控	支持飞腾、海思、鲲鹏、盛科、海光、兆芯等芯片	否
12	#	智能防御	DDoS 支持攻击智能化自动防御,防御全程自动化，无需人工干预。（提供权威机构出具的测试报告，并加盖厂商公章）	是

27.策略可视化

序号	重要性	指标项	指标要求	证明材料要求
1	△	授权要求	配置设备的管理节点授权≥80 个	否
2	#	功能要求	1、实现异构网络及安全设备的策略集中管理，包括各类安全策略、NAT 策略的可视化展示、清理优化、分析开通、开通校验等，提供访问控制策略的一体化全周期管理能力。 2、基于网络和安全设备的实际配置，依托可视化技术，实现面向业务视角的安全域拓扑架构可视，使业务域及核心资产的位置分布、风险暴露面、互访关系、访问路径清晰可见。 3、实现从业务开通请求、开通分析、开通建议、策略风险、策略下发到开通验证的全流程策略自动化开通，确保业务变更准确。 4、支持设备配置最后更新时间的信息展示；支持设备位置信息的显示。 5、统计网络对象、服务对象未被引用的占比；支持策略分析的总览展示；支持对防火墙安全策略、网络对象、服务对象、区域的分析结果导出和查询。 6、支持展示检测规则的描述、风险、建议、影响资产信息；支持检测规则可以设置白名单；支持对设备检查分析统计汇总；支持导出检查结果报告，提供修复的建议。（要求提供产品功能界面截图并在截图上标注对应功能参数，加盖产品厂商公章）	是
3	#	报表管理	针对策略、对象以及合规分析的结果，可输出图形化报表，同时支持周期或定时以邮件形式发送。 支持配置变更总览信息展示，包含配置变更设备、配置变更次数、配置变更项、最近一份配置等管理，方便快速运维。（要求提供产品功能界面截图并在截图上标注对应功能参数，加盖厂商公	是

			章）	
4	△	路径分析	支持路径的自动分析，防火墙对象自动分析并自动生成相应的策略脚本编排。支持针对即将下发策略进行隐藏、冗余、可合并、合规检查的关联分析及优化建议，可选择在锚点下发、在指定位置下发、及接受优化建议	否
5	△	展示要求	安全域和策略的可视化展示，安全域间支持分析下挖，支持安全域的一键收缩；支持鼠标放大、拖动安全域。（要求提供产品功能界面截图并在截图上标注对应功能参数，加盖产品厂商公章）	是
6	△	对防火墙性能监测	对防火墙的重传、分段丢失、服务端无响应、服务端重置等性能故障进行监测，并主动告警；	否
7	△	资产梳理	能够发现未知资产，统计资产的最近在线时间，能够发现离线资产。	否
8	#	访问关系梳理	能够以图形化形式展现网络内资产间的访问关系，并详细记录访问明细，包括访问是否成功。要求提供产品功能界面截图并在截图上标注对应功能参数，加盖厂商公章）	是
9	△	集成要求	支持将日志数据报送给安管平台。	否

28.全流量分析系统

序号	重要性	指标项	指标要求	证明材料要求
分析平台				
1	#	业务配置与功能	实现对关键业务系统中的网络异常、应用性能异常和网络行为异常的秒级发现，以及区分异常原因的智能回溯分析，提升了对关键业务系统的运行保障能力和问题处置效率。	否
2	#	业务性能监控与分析	全面监控业务系统各环节服务质量、快速发现并定位影响关键业务性能及稳定性问题。最大提升业务网络的运维效率和故障处置能力，围绕业务网络提供以业务为核心的支撑网络环境梳理、实时性能监控和快速故障定位等分析功能。集中收集分布部署在网络各个节点的网	否

			络回溯分析系统的实时分析数据，以图形化、图表化的方式为运维人员直观呈现业务系统各个环节的工作状况。	
网络回溯分析系统				
1	△	性能指标与功能	支持处理流量≥10G/S，流量采集口不少于 2 个 10G，所含光口满配多模光模块。集成大容量存储的高性能数据包采集和智能分析软硬件一体化平台，冗余电源；冗余风扇。可以分布式部署在网络的关键节点，支持对物理网络和网络流量的采集分析。实现对关键业务系统中的网络异常、应用性能异常和网络行为异常的秒级发现，以及区分异常原因的智能回溯分析，提升对关键业务系统的运行保障能力和问题处置效率。	否
2	△	应用性能分析	系统以关键应用为中心，实现对应用的网络访问性能、系统服务性能、应用响应性能等关键性能指标的智能分析，服务性能关键指标应当包括:总字节数、上行字节数、下行字节数，传输效率、上行传输效率、下行传输效率，TCP 重复确认包、最大响应时间、平均响应时间、最大首次响应时延、平均用户响应时间、最大用户响应时间，客户端平均窗口大小、服务器平均窗口大小，重传率、分段丢失率，TCP 交易总数、TCP 交易无响应次数、TCP 交易无响应率，客户端平均重传时延、服务器平均重传时延等,所有指标需支持 1 秒精度刷新。	是
3	△	回溯分析	可以实时捕获并保存网络通讯流量，具备对长期网络通讯数据进行快速数据挖掘和回溯分析能力。 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、进/出字节数、会话结束时间、会话持续时间、会话创建时间、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 重传包、TCP 分段丢失率、TCP 分段丢失包、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	是

			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、客户端请求平均/最大传输时间、服务器响应平均/最大传输时间等;最高分析精度至少支持秒级。	

29.海南地震产品平台

序号	设备名称	技术参数	单位	数量
1	海南本地化平台建设与基础管理	完成平台的软硬件环境搭建与部署，基于分布式集群架构，高效地存储结构化和半结构化数据,具备软硬件的运行情况展示与告警。具备平台整体数据资源情况概览统计功能；具备提供各类产品的上线、下架、离线、订阅和检索等管理功能；具备对产品的达到等情况的运维监控与告警;设计开发标准接口，适配数据处理和展示需求，提供统一数据接口服务，服务二次开发等需求。	套	1
2	地震应急决策专题	（1）地震速报信息 实现中国地震台网中心海南速报信息（自动报、正式报）实时对接并本地存储，为后续分析与应用服务。 （2）震情概况 获取震后海南地震震情概况，包括地震构造背景、最近断裂带、震源机制解类型、历史地震序列类型等信息，表述出该地震概貌。 （3）快速评估 震后快速给出本次地震产生的预估灾损情况，包括烈度区参数、人口和经济损失、周边学校、医院和铁路等公共设施。 （4）余震统计 实时获取一手余震信息，并提供余震分级别统计结果，同时联动提供历史上周边 5 级大震信息。开发海南余震分布动态 GIF 时序打点图。 （5）历史地震 基于电子地图，建设按空间范围、发震时间、震级大小、历史震害等信息的历史地震矢量化展示与交互功能。 （6）周边台站 基于电子地图，建设按测震、预警、地球物理、中心站等分类的台站基础信息矢量化展示与交互功能。 （7）图件产品 实时对接获取国家地震产品平台产出的各类	套	1

		应急图件，包括不限于：震源机制解、推测地震烈度分布图、快速评估影响范围图、前兆异常梳理图、不明事件分布图、震区地壳运动背景场图、人口人力图等，支撑地震应急决策。 （8）地震波形 对接获取并存储海南地震事件波形，提供miniseed格式的波形文件查询、打包与下载。 （9）电子地图 平台电子地图至少提供天地图、百度地图、台网中心矢量地图三种形式,同时具备测距、标记等功能。接入震防中心断层等矢量化图层，为本地展示、分析和图件生成服务。 （10）报告生成 提供围绕某个地震的相关文件和图件产品的一键式打包生成与下载，其中内容选项可以根据需求选择配置。		
3	台网概况与质量监控专题	建设台网概况专题，实时展现预警、测震、地球物理等台站数、仪器数，并提供分布图和标注基础信息，具备学科、地震关联等属性的查询与展示。对接国家地震产品平台测震和地球物理数据质量指标，联动地图进行多维度展示，可根据指标算法，给与声光电、微信等形式告警。	套	1
4	地震监测能力专题	结合海南与台网中心监测能力数据和基础信息，震后自动产出海南监测能力专报，并自动发送微信群等，实现第一时间常规和移动应急办公服务。专报内容包括：震区台站分布情况及图件、震区监测地震监测能力结果及图件和加密台站结论。具备手动触发和演练功能，满足应急演练和系统测试等需求。	套	1
5	地球物理异常图件专题	结合海南与台网中心预报部门产出的前兆异常站点或仪器信息，震后自动制作并推送相关仪器历史曲线图和周边各学科背景场图件，以服务趋势走向的分析研究等工作。进一步,基于海南局认可的同震或干扰等算法，定制开发自动推送相关仪器曲线图和学科场类图件。	套	1

三、商务要求

说明：所有商务要求均属于本项目的实质性要求，不接受任何负偏离，投标人须完全满足或优于所有商务要求，否则将被认定为无效投标。

1、交货地点和交货时间（交付期）

交货地点：省中心设备到货地址海南省海口市美兰区美苑路 13 号海南省地震局；中心站设备交付地址分别为海口、琼中、三亚中心站。

交货时间（交付期）：签订合同后 45 天内，完成软硬件设备到货及到货验收确认;设备到货后 45 天内,完成软硬件设备安装部署及调试等全部建设内容。

2、付款条件

2.1 合同签订之日起 7 个工作日内，中标人向采购人支付合同金额的 5%作为合同履约保证金；

2.2 采购人收到中标人合同履约保证金后支付合同金额的 50%,中标人提供等额发票；

2.3 全部货物到场验收，支付合同金额的 30%，中标人提供等额发票；

2.4 项目通过验收后支付合同金额的 20%，中标人提供等额发票。经中标人书面申请，采购人在 20 个工作日内向中标人无息退还合同履约保证金。

注：1、乙方每次申请付款应提供付款申请书、符合甲方要求的等额发票及甲方报账所必须的相关材料。乙方申请付款时，如乙方提供的材料不完整、不真实，或者因政府相关资金未能及时到位的，甲方有权暂缓付款而不视为违约。2、履约保证的有效期从验收合格之日起至项目通过验收止,若无质量问题,甲方将保证金退回乙方。如因产品、安装等引起的质量问题，乙方需按照售后要求及时解决，由此发生的费用由乙方承担。若乙方不能按时解决，甲方有权委托其他单位处理质量问题，并向乙方索赔。（具体以签订的合同条款为准）

3、服务要求

3.1、原厂售后服务承诺函：投标人应承诺通信网络与网络安全采购软硬件设备提供自合同终验之日起不少于 3 年（应答附加维保服务期限的，按照应答年限时间）原厂免费保修、备品备件、软件升级服务，（技术参数中已实际要求 5 年的设备，按要求算。网络安全设备质保期应内提供设备规则库、策略库、特征库、病毒库等库表升级服务，且许可到期后不影响设备现有功能。），以及提

供 7*24 小时原厂工程师技术支持服务，电话报修后 3 小时上门服务、12 小时内排除故障；投标人承诺如设备软硬件出现故障且 8 小时内无法修复时，在 24 小时内提供备品、备件进行替换，确保系统能在最短时间恢复运行。质保期内，所有硬件设备维修及软件维护升级等均包含在本次报价中。所有设备质保到期后产品可终生使用，所有功能不受限制。

3.2 部分产品要求：

（1）为降低同一品牌带来的系统风险，对于采购的核心防火墙、互联网防火墙、边界防火墙要求品牌异构；互联网墙、抗 DDOS 与 web 防火墙异构。

（2）海南地震产品平台建设所需服务器，由招标人提供。

（3）投标人须承诺所投 DNS 产品根据上级国家业务中心相关对接要求无偿集成接入实现与国家业务中心 DNS 系统的整体联动建设;所投安全管理平台产品根据上级国家业务中心相关对接要求无偿集成接入实现与国家业务中心安全管理平台的整体联动建设。

3.3 产品质量要求：投标人需承诺投标设备须为全新设备，不得为返修，或被退回的设备，完整、技术成熟稳定、性能质量良好并未曾使用的产品，货物及相关许可证明文件、技术文件、软件、服务等均不存在瑕疵。到货后，由招标人、中标人及监理按照装箱单和合同设备清单共同实施开箱检验，并逐台登记核验设备的序列号和质保期限，软件产品进行安装环境功能验证，如有缺陷、缺损、功能缺失或与合同规定和招标文件要求不符的，招标人有权要求中标人进行更换或补充发货。对于存在质疑的技术指标，招标人有权要求中标人提供测试证明，如测试结果不能达到投标文件的响应的技术需求，招标人有权要求中标人免费更换成满足技术指标需求的货物，由此产生的一切费用由中标人承担。提供加盖投标人公章的承诺函。

3.4 其他集成要求 1：

（1）投标人应承诺合同执行期间，因投标人自身基础设施建设、业务迁移等原因，可能会对采购人数据通信传输造成影响或导致中断的，应至少提前 48 小时书面通知采购人，且承诺影响时长不超 2 小时，并经采购人同意后方可实施。提供加盖投标人公章的承诺函。

（2）投标人应承诺因项目建设需要，采购人认为需要保密的技术文档、施工或建设内容，涉及到本次项目的实施及服务人员必须按照采购人要求签订保密协议。提供加盖投标人公章的承诺函。

（3）关键隐蔽工程施工、主要设备安装部署、骨干通讯线路布设等需有采购人代表或监理人员在场，方可施工。

3.5 其他集成要求 2：

（1）项目实施过程中投标人需按照采购单位及监理单位的统一安排，合理安排工序工期，保障项目整体实施。需提供加盖投标人公章的承诺函。

（2）测评协助：投标人应按照等保测评申报要求，协同招标人完成部分业务系统的网络安全等保测评估工作。提供加盖投标人公章的承诺函。

3.6 其他集成要求 3：

（1）投标人承诺在招标人业务系统建设前完成设备到货、安装上架、综合布线、网络接入等调试工作；须按照招标人的相关要求完成软硬件设备的上架加电、配置参数调整，确保基础环境能够满足招标人业务系统的运行需要。需提供加盖投标人公章的承诺函。

（2）质保期内的重大配置调整、系统迁移等工作由设备生产厂商工程师完成。需提供加盖投标人公章的承诺函。

3.7 其他集成要求 4：

负责提供部署本项目所需的网线/光纤、设备所需光模块等辅助材料和工具等，所需费用包含在报价内，所需线材的长度需根据实际施工情况测定。 提供加盖投标人公章的承诺函。

4、实施要求

4.1 项目实施过程控制：投标人应制定严格的实施方案，至少包括人员组织、质量控制、时间控制等关键要素；投标人应根据本项目特点详细分析项目实施中存在的风险因素，制定切实可行的风险应对方案。**包括但并不限于以下内容**

（1）提供机房部署方案。内容包括：提供详细的机房内设备机柜安装布局图（含旧设备调整）、设备连接拓扑图。

（2）提供详细的设备割接实施方案。应按照设备涉及的断网区域进行割接分类，方案中应提供：全网割接分类，每类割接具体实施步骤、割接前后拓扑

变化，割接前后设备端口调整、路由调整、地址调整，割接预估中断时长，以及应急预案。

（3）提供设备连接规划。内容包括：新增设备与原有设备的端口连接规划表、设备命名规划、VLAN 规划、IP 地址规划。

4.2 项目实施过程文档管理：投标人应安排固定人员作为本项目的档案联络员，除提供所供货物所必备的使用说明、操作手册等外，投标人还应按照本项目档案管理机构的要求提供所需文档，并根据总体技术方案编制单项实施方案、设备验收方案、系统测试方案、培训方案等。

4.3 项目安装过程安排：投标人应制定详细的安装过程计划，说明关键步骤。设备安装前应备齐所需材料工具，熟悉作业环境；设备到达现场，具备安装条件后 5 个工作日内完成上架安装，并完成单项集成工作，包括但不限于到货验收；设备安装及调测，含设备安装所需配件、耗材等；系统联调及测试；需根据应用系统需求，进行配置调整及系统优化工作。关键隐蔽工程施工、主要设备安装部署、骨干通讯线路布设等需有采购人代表或监理人员在场，方可施工。合同执行期间，因采购人根据项目建设的功能目标或业务流程调整，进行的建设内容、施工地点等变更，投标人应提供及时的变更服务。

4.4 项目实施管理：在整个合同执行期间，需全过程接受监理单位监理和采购单位组织进行的评审和考核。建设质量不达标或不能满足项目的功能目标要求，采购单位有权不组织验收、延期付款，相关责任由投标单位承担，投标人应无条件接受。

4.5 保密要求：因项目建设需要，采购人认为需要保密的技术文档、施工或建设内容，涉及到本次项目的实施及服务人员必须按照采购人要求签订保密协议。

4.6 项目培训安排：投标方需提供项目的整体培训服务方案，分类制定培训方案和编制培训教材，提供培训场地和搭建操作训练环境。培训内容包括各系统及其软硬件的总体架构、系统集成、基本原理、安装配置、使用操作、运行维护等方面，以及相关基础软件、支撑软件等工具的培训。培训方式包括但不限于 PPT 授课、实际操作训练两种方式。

确保采购人的技术人员能够在最短的时间内熟悉货物的各项特性，具备初步的维护和使用能力。投标人应为本项目方提供至少 1 次培训。每次培训不少于 5 天(报到、疏散各 1 天，培训 3 天)不少于 10 人的数据中心建设相关的高级培

训课程。期间除来往交通费外，其他费用包括但不限于场地、食宿等与培训相关的费用均由投标人承担，培训标准按照财政部统一颁布的会议标准。如投标人不能按照本合同约定完成培训服务，采购人有权另行采购第三方提供的培训服务，因此产生的相关费用及损失可以直接从履约保证金中扣除相应数额，不足部分由投标人承担。

5、包装和运输

5.1 投标人应承诺中标的所有设备、主要材料等均需出厂原包装完好运达施工现场，经采购人代表或监理人员现场确认并签字后方可拆除包装。主要设备及原材料，需提供产地证明、装箱清单、技术说明书、质量保证书、保修卡等必备的相关资料。

5.2 交付货物的包装和运输的费用必须包含在投标报价中，且必须满足中国法律法规、相关部门的相应产业标准及采购文件、合同等要求。交付的货物在验收合格前，投标人应对货物的提供风险保障，所产生的保险费用由乙方承担。

6、项目实施相关保障及要求

6.1 质量保证措施

深入研究本项目建设内容与要求，能够针对本项目提出切实可行的质量保障措施，确保本项目建成后满足海南省地震巨灾防范工程数据平台信息化硬件集成项目的要求与规范。

6.2 实施要求

（1）各类方案与实施必须满足国家项目指南要求及业务使用需求，对需要断网割接断必须在采购人允许的时间范围内完成。

（2）梳理全网地址划分、vlan 划分等，所有设备按照机房现有标准进行命名、地址规划分配、制作设备标签、线缆标签，布线应符合机房规定。

（3）在项目建设过程中，投标人须根据采购人要求将替换的设备进行拆除，并按采购人要求迁移到指定位置。对不用的线缆按采购人要求进行拆除。

（4）项目整体接受监理公司管理，投标人必须配合监理公司完成监理要求的各项内容。

（5）项目实施过程实行每日日志记录模式，投标人项目团队应有至少一名固定人员在项目实施期间工作日内驻场，每天下午 17:00 提交当日工作进展和明日工作计划情况汇报。同时项目实施过程中相关报告、设备配置、跳线、标签等各类内容全部需要开展审核，审核人员与编制或实施人员不得为同一人。审核人员完成审核后，在当日工作日志中进行审核内容的描述与确认，审核人员对审核内容负全责，具体审核确认提交方式依据招标方要求完成。

6、知识产权

投标人必须保证，采购人在中华人民共和国境内使用投标货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，如有第三方向采购人提出侵犯其专利权、商标权或其它知识产权的主张，该责任应由投标人承担。

投标报价应包含所有应向所有权人支付的专利权、商标权或其它知识产权的一切相关费用；涉及相关专有技术的，在投标时应提供该技术专有人的使用授权正本附于投标书中，否则作无效投标处理。

本项目采购的所有设备以及实施过程中产生的知识成果及知识产权归采购人拥有。

投标人应承诺对开发过程中涉及的建设图纸、设计方案等资料进行严格保密。

7、验收要求

项目验收安排：投标人应制定详细项目验收方案，至少包括参与验收的人员、投标人投入的验收测试设备、验收测试的方法和步骤等，并配合第三方评测工作，同时根据合同要求完成验收工作。

投标人向项目建设单位和监理单位提出本项目验收申请。验收基本要求如下：

（1）设备无故障问题，各项指标符合要求，提供相应的技术支持与服务保障方案。设备运行期间稳定运行，整体运行正常；（2）产品满足采购人要求；（3）提供必要的技术培训；（4）提交实施过程中所产生的全部文档，如技术文档、实施文档、用户使用和操作手册等；（5）安装、布线、调试、测试和试运行时出现的问题均已被解决；（6）提供完备的重要保障方案和应急处置预案。（7）当验收不合格时，中标人应承诺无条件进行返工。

项目验收文档要求，收集齐全验收所需档案资料。投标人在本项目实施过程中，应提供完备的项目文档，包括但不限于：（1）实施类文档 包括项目实施方案、系统上线保障方案、设备到货验收及测试记录、网络拓扑图、机柜图、试

运行方案等。 （2）管理类文档 包括项目进度计划、项目工作周报、项目阶段报告、验收方案、问题处理及解决情况报告、运行报告、整改报告等。

附件：关于强制性政府采购政策的有关承诺

致：海南政通招投标有限公司

为响应贵公司组织的____（项目名称）____（招标编号：____）的招标采购活动，我公司（单位）承诺：

本项目采购的产品如属于列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品的，我方承诺所投的对应产品均符合《信息安全技术网络安全专用产品安全技术要求》等相关国家标准的强制性要求，并由具备资格的机构安全认证合格或者安全检测符合要求。

若我单位以上承诺不实，自愿承担提供虚假材料谋取中标、成交的法律责任。

承诺供应商（全称并加盖公章）：

日期： 年 月 日

本项目执行：财政部、国家发展改革委、生态环境部、国家市场监管总局《关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）文件、根据国家互联网信息办公室、工信部、公安部、财政部等联合发布《关于调整网络安全专用产品安全管理有关事项的公告》、海南省财政厅关于印发《海南省绿色产品政府采购实施意见（试行）》的通知（琼财采规〔2019〕3号）。