成都中医药大学附属医院

信息安全等级保护相关系统调研及询价的公告

我院拟购买信息安全等级保护相关系统，正式采购前需进行市场调研和询价，诚邀有意向的厂家或供应商按照本公告的要求前来报名。

一、报名须具备的条件：

1、具有独立法人资格，有固定的办公和工作场地，能独立承担法律责任；

2、具有良好的商业信誉和健全的财务会计制度；

3、具有履行合同所必须的设备和专业技术能力；

4、具有依法缴纳税收和社会保障资金的良好记录；

5、此前在经营中无违法记录；

6、企业是生产商或重要代理商。

二、报名须提供的书面材料：

1、有效的营业执照副本（年检合格）；

2、组织机构代码证副本（年检合格）；

3、国税、地税的税务登记证（年检合格）；

（已实行三证合一的只需提供营业执照复印件）

5、报名公司法人对销售代表的签名授权书（原件）；

6、授权代表身份证复印件；

7、设备报价单（见附件）；

9、提供推荐产品、技术参数、配置清单、售后服务承诺；

10、参选公司需提供承诺书，承诺交来的所有资质，皆为原件复印件且 真实有效。提供虚假资料者取消报名资格，5 年内禁入医院并追究相关法律责任。

注：上述所有证明材料，需加盖公司公章。

三、报名截止时间：2019 年 8 月 9 日下午 5 点前交至采供部（行政楼 1 楼采供部 117 室）。过期不予受理。

五、联系方式：

1、联系电话：028-87762327

2、联系人：梁老师

3、地址：成都市金牛区十二桥路 39 号

附件：报价清单。

附件

核心产品、技术（服务）及商务需求：

本项目技术（服务）及商务需求：

外网：

区域	产品名称	数量
外网	下一代防火墙（含 IPS 模块及杀毒）	1
	网闸	1
	态势感知平台	1
	安全探针	1

设备名称	关键功能性能指标	数量
下一代防火墙（含 IPS 模块及杀毒）	1.性能参数：三层吞吐量≥10G，应用层吞吐量≥3G，最大并发连接数≥220W，千兆电口≥10 个，千兆电口≥4 个，SSL VPN 加密流量≥300M，IPsec 加密流量≥450M，支持 BYPASS 功能；提供传统防火墙、IPS、WAF、AV 网关杀毒、僵尸网络检测、漏洞识别等功能；包含三年规则库更新和硬件质保软件升级； 2.为保证产品处理性能，产品应采用自研高性能多核并行安全操作系统，并有相关软件著作权 3.设备具备完整的 WAF 功能，支持 Web 漏洞扫描功能，可扫描检测网站是否存在 SQL 注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞； 4.采用无特征 AI 检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测，给出基于 AI 技术的病毒检测报告，并具有未知威胁防护与杀毒能力相关软件著作权证书；（提供著作权证书） 5.要求防火墙产品经过国际知名实验室 NSS Labs 测试，并获得 recommended 推荐级别；（提供测试报告） 6.要求防火墙产品在近两年有入围 Gartner 企业级防火墙魔力象限（提供证明材料） 7.厂商应具备软件开发成熟度 CMMI5 证书；（提供证书证明）	1 台
安全探针	1.性能参数：吞吐量≥1.5Gbps，千兆电口≥4，千兆光口≥4；配置 SATA 盘≥1T，内存≥4G，标准 2U 设备；包含三年规则库更新和硬件质保软件升级； 2.采集网络安全攻击日志及流量元数据，传输到态势感知平台做统一分析，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	1 台

	式， 3.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；（提供截图证明） 4.产品与态势感知平台同一品牌且能统一升级更新 5.厂商是微软安全响应中心的 MAPP 计划成员（提供证明材料） 6.产品厂商具备 CSA-CMMI5 云安全证书（提供证书）	
态势感知平台	1.专业的安全管理平台，对内网安全情况进行全方位分析展示，实现内网安全的统一管理，设备硬盘容量≥13TB，内存容量≥32G，存储容量≥16T，设备接口配置千兆电口≥6，单电源，1U 设备；包含三年规则库更新和硬件质保软件升级； 2.支持全网资产自动梳理、资产风险监测、安全威胁监测、攻击事件监测、横向攻击监测、流量及日志的联动分析处置、漏洞分析等； 3.平台支持采用无特征 AI 检测技术对恶意攻击进行检测，并具有未知威胁防护与杀毒能力相关软件著作权证书；（提供软件著作权证书） 4.安全管理中心需要接入现有的第三方安全设备，具备第三方设备接入授权相关软件的著作权证书（提供软件著作权证书） 5.厂商需要是国家级应急响应支撑单位，同时是国家国家信息安全漏洞库 CNNVD 技术支撑单位（提供证明材料） 6.产品厂商具备 CSA-CMMI5 云安全证书（提供证书证明）	1 台
网闸	1、专业网闸设备，吞吐量≥1G，最大可扩展吞吐量不低于 9G，千兆电口≥6 个，千兆光口≥4 个，采用 2+1 系统架构即内网单元+外网单元+FPGA 专用隔离硬件。不采用网线等形式直通，即可为内外网提供安全数据隔离交换。包含三年规则库更新和硬件质保软件升级； 2、外网端不允许配置任何形式的管理接口，所有管理配置操作均通过专用的网闸内网可信端管理接口进行配置。 3、产品内置各类应用支持模块包含：邮件模块、安全浏览模块、视频交换模块、数据库访问模块、数据库同步模块、文件交换模块、OPC 模块、MODBUS 模块、WINCC 模块、组播代理模块、用户自定义应用模块等各类应用模块,并可控制相应应用协议的的动作、参数、内容。 4、支持 MODBUS 协议传输代理模块，西门子的 WINCC 控制协议传输代理模块可按照用户需求控制具体功能代码，比如只允许读取，不能控制等（提供截图证明） 5.厂商需是中国反网络病毒联盟 ANVA 成员单位；（提供证明材料）	1 台

内网：

区域	产品名称	数量
内网	下一代防火墙	1
	服务器防病毒软件授权	1
	态势感知平台	1
	安全探针	1
	日志审计系统	1
	漏洞扫描系统	1
	数据交换平台	1

设备名称	关键功能性能指标	数量
下一代防火墙	1. 产品架构：标准机架式设备。 2. 采用专业的安全操作系统，具备高性能一体化智能安全处理引擎（提供原厂证明函复印件及国家版权局颁发的计算机软件著作权登记证书复印件）； 3. 硬件接口：配置≥6 个千兆电口、≥4 个 SFP 插槽，≥2 个接口扩展槽，≥2 个 USB 接口，1 个 console 口；配置液晶屏（提供原厂证明函复印件及面板截图证明材料）； 4. 性能要求：吞吐量≥10G，并发连接≥260 万，每秒新建连接数≥18 万； 5. 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式； 6. 所投产品应支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能； 7. 所投产品支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮	1 台

	询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于 12 种路由负载均衡方式，支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP 等方式的链路探测； 8. 所投产品支持 ISP 路由负载均衡，最大可支持 8 条链路负载，支持自定义负载权重，支持基于优先级的 ISP 路由链路备份；支持基于 IPv4 或 IPv6 的 TCP、HTTP、DNS、ICMP 等方式的链路探测； 9. 所投产品应支持针对 IPv6 流量通过 HTTP、HTTPS 实现 Web 认证，用户身份信息可存储在本地或 Active Directory\Radius\TACACS+\POP3 等第三方服务器；通过 HTTPS 实现 Web 认证支持使用本地 CA 颁发的证书同时使用证书验证客户端身份； 10. 所投产品应支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计；（提供原厂证明函复印件及提供能够体现上述功能及配置选项的截图证明材料）； 11. 具有高性能 IPv6 防火墙系统，确保高性能 IPv4 到 IPv6 的平稳过渡，保障网络顺畅，具有自主知识产权（提供原厂证明函复印件及国家版权局颁发的计算机软件著作权登记证书复印件）； 12. 所投产品支持基于不同安全区域防御 DNS Flood、HTTP Flood 攻击，并支持警告、阻断、首包丢弃、TC 反弹技术、NS 重定向、自动重定向、手工确认等多种防护措施； 13. 所投产品应支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机 IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断（提供原厂证明函复印件及提供能够体现被入侵、攻破的主机的状态的截图证明材料）； 14. 所投设备应提供关联的威胁事件日志，系统可自动将产生	

	威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL 过滤、文件过滤等安全模块检查的日志集中显示（提供原厂证明函复印件及关联威胁事件日志的设备截图证明材料）； 15. 所投产品应支持与云端联动，至少实现病毒云查杀、URL 云识别、应用云识别、云沙箱、威胁情报云检测等功能（提供原厂证明函复印件及体现上述功能及配置选项截图证明材料）。	
服务器防病毒软件授权	1、要求提供≥5 个 Linux 服务器授权，≥15 个 Windows 服务器授权。 2、控制中心：采用 B/S 架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、终端软件管理、硬件资产管理以及各种报表和查询等功能。 3、防病毒模块：支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS 病毒等进行查杀，支持主动防御系统防护等功能。 4、生产厂商采用语境关联分析技术实现准确的威胁识别，具有自主知识产权（提供国家版权局颁发的计算机软件著作权登记证书复印件，并加盖厂商公章）。 5、生产厂商获得国家互联网应急中心应急服务支撑单位（国家级）称号（提供证书复印件，并加盖原厂公章）。 6、生产厂商具备强大的漏洞挖掘与发现能力，入选中国国家信息安全漏洞库 CNNVD 一级技术支撑单位（提供证明材料，并加盖原厂公章）。 7、提供三年软件与特征库升级服务（加盖厂商公章）。	1 套
安全探针	1.性能参数：吞吐量≥1.5Gbps，千兆电口≥4，千兆光口≥4；配置 SATA 盘≥1T，内存≥4G，标准 2U 设备；包含三年规则库更新和硬件质保软件升级； 2.采集网络安全攻击日志及流量元数据，传输到态势感知平台做统一分析，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， 3.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；（提供截图证明） 4.产品与态势感知平台同一品牌且能统一升级更新 5.厂商是微软安全响应中心的 MAPP 计划成员（提供证明材料） 6.产品厂商具备 CSA-CMMI5 云安全证书（提供证书）	1 台
态势感知平台	1.专业的安全管理平台，对内网安全情况进行全方位分析展示，实现内网安全的统一管理，设备硬盘容量≥13TB，内存容量≥32G，存储容量≥16T，设备接口配置千兆电口≥6，单电源，1U 设备；包含	1 台

	三年规则库更新和硬件质保软件升级； 2.支持全网资产自动梳理、资产风险监测、安全威胁监测、攻击事件监测、横向攻击监测、流量及日志的联动分析处置、漏洞分析等； 3.平台支持采用无特征 AI 检测技术对恶意攻击进行检测，并具有未知威胁防护与杀毒能力相关软件著作权证书；（提供软件著作权证书） 4.安全管理中心需要接入现有的第三方安全设备，具备第三方设备接入授权相关软件的著作权证书（提供软件著作权证书） 5.厂商需要是国家级应急响应支撑单位，同时是国家国家信息安全漏洞库 CNNVD 技术支撑单位（提供证明材料） 6.产品厂商具备 CSA-CMMI5 云安全证书（提供证书证明）	
日志审计系统	1.专业日志审计系统软件，接入内网各类数通、安全、服务器设备所产生的安全日志，进行统一存储并关联分析，发现安全事件，≥150 个日志接入授权，千兆电口≥6 个，硬盘容量≥MSATA 64GB SSD + SATA 1TB 企业盘* 2，系统可从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段；包含三年规则库更新和硬件质保软件升级； 2.支持内置归并策略，对HTTP数据进行自动归并处理； 3.厂商具备软件开发成熟度 CMMI 5 级认证（提供证书） 4.厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位；国家信息安全漏洞共享平台(CNVD)技术组成员；（提供证明材料）	1 套
漏洞扫描系统	1、接口：业务千兆电口≥6 个，业务千兆光口≥2 个，接口扩展槽≥1 个，内存：内存≥8GB;性能：整机最大任务并发数量≥50 个，扫描进程并发数量≥150，支持最大可扩展到无限个 IP 地址或域名电源：单电源，硬盘容量：设备配置硬盘 SATA 盘≥1TB，能对全网的信息资产、安全设备、网络设备进行深度的风险扫描，包括配置基线检查、漏洞扫描等； 包含三年规则库更新和硬件质保软件升级； 2.支持一次性任务、立即任务、周期任务等多种调度方式；支持漏洞扫描、WEB 扫描、弱口令、安全基线检查、变更检查的五合一任务，五者也可任意组合执行任务（提供截图证明） 3.系统需要具备检索能力，提供包括对象的全文检索功能，且搜索栏不固定，出现于每个页面。 4.提供详细查看功能，针对违反安全基线中的事件能够查看违规的信息。 5.厂商具有中国信息安全测评中心颁发的信息安全服务资质（安全工程类一级）（提供证明材料）	1 套
数据交换平台	1．交换容量≥336Gbps，包转发率≥132Mpps，提供原厂证明函复印件及官网链接、截图证明材料。 2． MAC 地址表≥16K，路由表容量≥512（支持 OSPF），ACL	1 台

	≥1K； 3. 接口类型： 10/100/1000BASE-T 以太网端口≥48 个，10G BASE-X SFP+万兆端口≥4 个； 4. 实现 ERPS 功能，可与其他厂商设备混组网，能够快速阻断环路，链路收敛时间≤50ms。 5. 实现 CPU 保护功能，能限制非法报文对 CPU 的攻击，保护数据交换平台在各种环境下稳定工作。 6. 最大堆叠台数≥9 台，最大堆叠带宽≥80G（万兆上行主机），可要求堆叠带宽≥80G（万兆上行主机），并要求实配接口的基础上额外满配堆叠带宽所需的接口和互联模块，支持跨设备链路聚合，单一 IP 管理，分布式弹性路由，支持通过标准以太端口进行堆叠（万兆）；支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成 MAC 和 IP 地址的重配置，无需手动干预；支持远程堆叠；提供原厂证明函复印件及泰尔实验室（或其他权威机构）测试报告。 7. 支持 IRF3，可以做 PE 端； 8. 支持基于端口的 VLAN，支持基于协议的 VLAN；支持基于 MAC 的 VLAN；最大 VLAN 数(不是 VLAN ID) ≥4094； 9. 支持最多 8 个端口聚合；支持最多 128 个聚合组（IRF2）；支持 LACP； 10. 支持本地端口镜像和远程端口镜像 RSPAN；支持流镜像；同时支持 N：M 的端口镜像（M 大于 1）； 11. 组播协议：支持 IGMP v1/v2/v3，MLD v1/v2；支持 IGMP Snooping v1/v2/v3，MLD Snooping v1/v2；支持 PIM Snooping；支持 MLD Proxy；支持组播 VLAN；支持 PIM-DM，PIM-SM，PIM-SSM；支持 MSDP，MSDP for IPv6；支持 MBGP，MBGP for Ipv6。 12. 路由协议：支持 IPv4 静态路由、RIP V1/V2、OSPF；支持 IPv6 静态路由、RIPng；	

	13. 支持 RRPP（快速环网保护协议），环网故障恢复时间不超过 50ms；支持 Smartlink，收敛时间≤50ms；支持 RSTP 功能：收敛时间≤50ms；支持 MSTP 功能：收敛时间≤50ms；支持 PVST 功能：收敛时间≤50ms。 14. 支持基于第二层、第三层和第四层的 ACL；整机提供 ACl 条目数不小于 1K/512 条；支持基于端口和 VLAN 的 ACL；支持 IPv6 ACL；支持出方向 ACL，以便于灵活实现数据包过滤；支持 802.1x 认证，支持集中式 MAC 地址认证。 15. 支持 OPENFLOW 1.3 标准支持普通模式和 Openflow 模式切换，需提供官网网站命令手册佐证支持多控制器（EQUAL 模式、主备模式）；支持多表流水线；支持 Group table；支持 Meter；提供配套的 SDN controller。 16. 支持 SNMP V1/V2/V3、RMON、SSHV2；支持 OAM(802.1AG，802.3AH)以太网运行、维护和管理标准。	