

# 西华大学项目需求论证表

采购单位	西华大学	专业人员/专家组论证意见
项目名称	信息系统安全防护设备购置	
采购预算金额及资金来源	82.5 万元	财政资金
是否属于政府采购政策扶持范围	否	不属于政府采购政策扶持范围
项目类别	货物、工程、服务	货物
技术需求	见附件	采购数量、采购标的的功能标准、性能标准、材质标准、安全标准、服务标准满足项目需求，所涉及标准符合相关发了财法规规定，无倾向性、歧视性、排他性条款
拟采用的采购方式	公开招标、竞争性磋商、竞争性谈判、询价、单一来源采购	拟采用的采购方式为公开招标，符合相关规定
拟定的供应商资格要求	1. 须具备政府采购法第二十二条第一款规定的条件； 2. 具有良好的商业信誉和健全的财务制度； 3. 具有履行合同所必需的设备和专业技术能力； 4. 有依法纳税和社会保障资金的良好记录； 5. 参加政府采购活动前三年内，在经营活动中没有重大违法记录(若供应商存在违法经营行为而受到较大数额罚款的，数额以四川省人民政府规定的行政处罚罚款听证标准金额为准)；	供应商资格要求符合政府采购法第二十二条相关规定，无歧视性、倾向性、排他性条款。

项目实质性条款	履约时间（交货期）、履约方式（付款方式）、验收方法和标准	项目实质性条款满足项目需求，履约时间和地点，验收标准和方法符合政府采购法和合同法相关规定，未尽事宜按川财采（2015）第32号文执行。
专业人员/专家组 签字	马洪亮	
项目负责人签字：	李永通	
采购单位负责人 签字	王红	
经费主管部门负责人签字	王红	

注：

1. 项目预算大于 50 万元（含 50 万元）需提供采购单位设备需求论证的部（处）会议纪要或学院党政联席会议纪要。
2. 项目预算小于 300 万需至少 1 位专业人员论证。
3. 项目预算大于 300 万小于 1000 万需 3 人以上单数专家组论证。
4. 项目预算大于 1000 万需 5 人以上单数专家组论证，并在四川政府采购网向社会公示 3 个工作日内，征求潜在供应商和社会公众的意见。公示内容主要包括采购项目名称、预算金额、采购需求论证事项、专家组论证意见、采购人或者其委托的采购代理机构名称及联系人。

# 专家组需求论证名单

姓名	性别	专家证编号 (如有)	职务/职称	工作单位	联系电话
马法亮	男		副教授	西华药公司	13881997297

附件：

## 西华大学信息系统安全防护设备购置项目

### 一、项目概述

西华大学现有物理服务器 50 多台，使用 12 台物理机构建了基于 vmware 云平台，运行 200 多个虚拟机，其中约 100 个支撑了学校各类信息系统正常运行。按照我国网络安全法和网络安全等级保护测评的要求，需要增加数据库审计系统、日志管理审计系统、数据库审计系统，同时为了满足第六教学楼中小学教师资格考试、研究生考试等的要求，需要建立自安全网络系统。清单和参数如下，预算为 82.5 万元。

### 二、项目清单：

序号	名称	数量	单位
1	运维审计系统	1	套
2	日志管理审计系统	1	套
3	自安全核心交换机	1	台
4	自安全接入交换机	9	台
5	自安全运维日志平台	1	套
6	数据库审计系统	1	套
7	vsan 服务器	1	台

### 二、技术指标要求

序号	设备	技术要求	数量	单位
----	----	------	----	----

1	运维审计系统	<p>1、硬件要求：设备高度≤2U, 硬盘≥2*2T SATA, 内存≥8G；至少2个电源，至少可以管理300个目标设备对象；</p> <p>2、用户管理：★支持自定义用户角色，并可依据角色灵活配置相应系统模块的管理权限；★支持短信验证码、X.509 数字证书、USB Key 认证；★支持 AD 账号的自动化同步，当 AD 域中的账号有变更时，会被自动同步的系统中</p> <p>3、资产管理：★支持对 IPV6 资产的管理（截图）；★支持动态全景视图管理，管理员在配置好资产的层级属性后，系统可自动生成动态全景视图；★支持将 Windows Server 2016 作为应用发布服务器；</p> <p>4、权限管控：★支持基于 ABAC 模式的动态权限管控，管理员可基于用户属性、资产属性、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、资产、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、资产、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；</p> <p>5、资产访问：★支持资产收藏功能，用户可以对经常需要访问的目标资产做一键收藏，以便于下次可以直接在收藏夹中找到；★针对基于云盘模式的文件传输操作：用户将文件暂存在运维安全管理平台上，再经由平台一键上传到目标资产或者一键下载到用户本地，此过程无需依赖第三方工具；</p> <p>6、行为审计：★具备命令识别方面的先进性技术，可实现对命令行操作行为的 100%记录；需提供国家知识产权局颁布的技术先进性证明文件扫描件；★具备数据库审计方面的先进性技术，可实现对 oracle、sqlserver、mysql 数据库客户端操作行为的 100%的 SQL 语句还原；★支持以 2M 会话流量或者 15 分钟操作时长为标准的会话缩略图切片展示功能，管理员点击任意切片，即可直接定位到对应操作片段；</p> <p>7、账号安全管理：★支持目标资产的自动化改密功能，可基于资</p>	1套
---	--------	---	----

		<p>产属性和账号属性创建弹性动态改密规则，只要满足相关属性的资产和账号即会被自动纳入改密计划；★支持账号生命周期管理，可通过运维安全管理平台以工单流的方式对目标资产系统账号进行变更操作，包括创建、删除、修改、锁定等操作，需提供加盖原厂鲜章的全屏功能界面截图证明；</p> <p>8、系统管理：★支持等价资产功能，以便让 HA/ 集群等部署方式下的资产实现归一化管理，当其中一个资产的属性发生变更时，等价资产的属性随之自动调整；★支持等价账号功能，以便让不同资产下的系统账号实现归一化管理，当其中一个账号信息发生变更时，等价账号信息随之自动调整；</p> <p>9、API：★支持登陆认证、访问权限、 用户账号、目标资产、操作审计、定期改密、命令复核、等 API 接口；支持与第三方系统集成。需提供加盖原厂鲜章的全屏功能界面截图证明；</p>		
2	日志管理审计系统	<p>1、支持与学校大数据平台进行无缝对接，提供解析后的结构化数据或计算处理后的结果数据，并需要具备数据源直接对接和 API 对接等方式，根据具体场景进行确定。</p> <p>2、离线日志数据计算任务分钟级延迟，实时流式计算秒级延迟。</p> <p>3、百 GB 级数据的关联检索延迟在秒级。</p> <p>4、架构上需要支持学校现存所有日志数据的接入，例如 H3C 无线 AP 日志、深澜认证计费日志、深信服 VPN 日志、juniper 防火墙日志等，并在架构上具有灵活拓展性，支持未来硬件设备或应用与操作系统日志的接入处理。</p> <p>5、支持日志数据结构化处理时对于无用信息的过滤，节省存储空间。</p> <p>6、提供数据压缩功能，压缩比不低于 5:1。</p> <p>7、提供日志分析工具的数据库访问方式及数据字典。</p> <p>8、自主产权，非 OEM 产品，提供日志分析软件类的软件著作权登记证书，并加盖公章</p>	1	套

3	自安全 核心交换机	<p>★1. 配置千兆电口<math>\geq 20</math>个，千兆光口（复用）<math>\geq 8</math>个；万兆光口<math>\geq 4</math>个（含相应的光模块）；交换容量<math>\geq 5\text{Tbps}</math>、包转发率<math>\geq 340\text{Mpps}</math>，扩展插槽<math>\geq 1</math>个，以官网指标为准；（提供官网截图和官网链接并加盖原厂鲜章）</p> <p>2. 可扩展 40G 光接口模块（QSFP）、万兆光接口模块（SFP+）；</p> <p>3. 支持 RIPv1/v2、OSPF、IS-IS、BGP、VRRP、RIPng、OSPFv3、BGP4+ for IPv6、VRRPv3 等路由协议</p> <p>4. 支持 OpenFlow、Netconf 等 VxLAN 特性；</p> <p>★5. 为保障设备稳定性，要求设备采用无风扇设计；为保障设备环境适应能力，要求设备支持 <math>0^{\circ}\text{C}</math>-<math>70^{\circ}\text{C}</math> 宽温工作，6KV 端口防雷能力；（提供第三方权威机构出具的测试报告证明并加盖原厂商鲜章）</p> <p>6. 支持虚拟化部署；（提供第官网截图证明并加盖原厂商鲜章）</p>	1	台
4	自安全 接入交换机	<p>★1. 配置千兆电口<math>\geq 24</math>个，千兆光口（非复用）<math>\geq 4</math>个（含相应的光模块）；交换容量<math>\geq 5\text{Tbps}</math>、包转发率<math>\geq 210\text{Mpps}</math>，以官网指标为准；（提供官网截图和官网链接并加盖原厂鲜章）</p> <p>2. 支持静态路由、RIPv1/v2、OSPF；（提供官网截图和官网链接并加盖原厂鲜章）</p> <p>3. 要求设备单端口支持的 MAC 地址用户数<math>\geq 4\text{k}</math>；</p> <p>★4. 为保障设备稳定性，要求设备采用无风扇设计；为保障设备环境适应能力，要求设备支持 <math>0^{\circ}\text{C}</math>-<math>70^{\circ}\text{C}</math> 宽温工作；（提供第三方权威机构出具的测试报告证明并加盖原厂商鲜章）</p> <p>5. 为节能环保考虑，降低 UPS 电源的功率，要求设备最大功耗<math>\leq 22\text{W}</math>；（提供官网截图和官网链接并加盖原厂鲜章）</p> <p>★6. 支持对病毒的网络层传播行为进行溯源及阻断，防止内网病毒扩散；（提供第三方权威机构出具的测试报告证明并加盖原厂商鲜章）</p> <p>7. 支持防 IP 扫描、防 UDP 端口扫描、防 TCP 端口扫描等异常行为；（提供第三方权威机构出具的测试报告证明并加盖原厂商鲜章）</p> <p>★1. 配置千兆电口<math>\geq 20</math>个，千兆光口（复用）<math>\geq 8</math>个；万兆光口<math>\geq 4</math>个（含相应的光模块）；交换容量<math>\geq 5\text{Tbps}</math>、包转发率<math>\geq 340\text{Mpps}</math>，扩展插槽<math>\geq 1</math>个，以官网指标为准；（提供官网截图和官网链接并加盖原厂鲜章）</p> <p>2. 可扩展 40G 光接口模块（QSFP）、万兆光接口模块（SFP+）；</p> <p>3. 支持 RIPv1/v2、OSPF、IS-IS、BGP、VRRP、RIPng、OSPFv3、BGP4+ for IPv6、VRRPv3 等路由协议</p> <p>4. 支持 OpenFlow、Netconf 等 VxLAN 特性；</p> <p>★5. 为保障设备稳定性，要求设备采用无风扇设计；为保障设备环境适应能力，要求设备支持 <math>0^{\circ}\text{C}</math>-<math>70^{\circ}\text{C}</math> 宽温工作，6KV 端口防雷能力；（提供第三方权威机构出具的测试报告证明并加盖原厂商鲜章）</p> <p>6. 支持虚拟化部署；（提供第官网截图证明并加盖原厂商鲜章）</p> <p>7. 资质证书：</p>	9	台

		<p>设备支持工信部入网许可证；</p> <p>设备厂商具备 ISO9001、ISO14001、QC080000、TL9000 证书</p> <p>以上证书提供证书复印件并加盖厂商鲜章</p> <p>8. 支持“肉鸡”源主机的溯源及阻断；支持 IP 仿冒、MAC 仿冒溯源与阻断，支持识别 IPC 等哑终端设备类型，并支持开启终端安全功能，只允许特定类型的设备接入网络；（提供第三方权威机构出具的测试报告证明并加盖原厂鲜章）</p>		
5	自安全运维日志平台	<p>1. B/S 架构，安装在服务器或 PC 上；</p> <p>2. 支持通过图形界面方式规划网络拓扑，并展示设备自动上线过程（提供功能页面截图）；</p> <p>3. 要求支持基于用户以及用户组进行网络资源编排，实现用户以及用户组和网络属性 VLAN、IP 网段、IP 地址的绑定。简化底层网络规划；（提供功能页面截图）；</p> <p>4. 可自动发现网络中的 IP 摄像头、打印机、一体机等设备终端并提供保护，可识别 IP、MAC、接入位置、接入端口等信息</p> <p>要求可根据事先导入系统的设备网各类哑终端 MAC 地址列表，实现哑终端的自动化上线，自动完成对接入层设备、汇聚层设备的配置下发，实现专网隔离、配置随行效果；</p> <p>5. 提供一次接入，多次使用的无感知认证，只需要输入一次用户名/密码，后续接入无需再输入用户名/密码；</p> <p>6. 支持对用户的业务异常行为、连接数异常行为等进行实时阻断及告警；（提供功能页面截图）；提供强大的“黑名单”管理，可以将恶意猜测密码的访客加入黑名单，并可按 MAC、IP 地址跟踪非法行为的来源；</p> <p>★7. 支持识别终端类型、IP、MAC、接入端口等信息，防路由器和 HUB 私接，并限制单端口下接入终端数量；具备对病毒感染主机的网络隔离功能，可对其内网病毒传播行为进行检测及阻断与告警功能；支持基于用户设定新建速率阈值并进行监控，支持对 TCP、UDP、ICMP 等协议下报文速率的阈值设置，并可根据网络需求自定义防护级别，支持对 SYN Flood、UDP Flood、ICMP Flood 等攻击设置防护策略，支持防 ARP 欺骗、防 ARP 广播攻击；以上安全特性功能要求在接入层实现；（提供第三方权威机构出具的测试报告证明并加盖原厂鲜章）</p> <p>8. 支持安全日志基于时间、事件、攻击源 IP、目的 IP 进行查询和报表导出功能，支持安全日志多维度分析功能，基于端口、源 IP、目的 IP、TOP 频率等（提供软件界面截图）；</p> <p>9. 为保证产品软件安全稳定可靠，要求厂商软件开发能力通过 CMMI5 认证，并提供《计算机系统安全专用产品销售许可证》；</p>	1	套
6	数据库审计系统	<p>1、国产品牌，标准 1U 机架一体化设备（审计引擎和数据引擎一体化设备），产品形态≤1U；</p> <p>2、. 硬件要求：≥4 个千兆以太网电口，支持≥2 路审计监听功能，独立管理端口（RJ45）≥1 个，独立 HA 端口（RJ45）≥1 个，USB 接口≥2 个，硬盘≥1T；采用多核多平台并行操作系</p>	1	套



		<p>统，SQL 处理能力≥15000 条/秒，采用海量日志存储及高速检索技术，日志存储能力≥50 亿条（1T 本地存储），提供原设备生产厂商出具满足上述性能要求的承诺函或提供产品彩页并加盖原厂商鲜章；</p> <p>3、支持代理部署模式、旁路部署方式，支持系统危险链路旁路阻断功能。</p> <p>4、★单一设备即可同时支持包括数据库审计、风险扫描、状态监控、运维审计等功能，可按需扩展。（需提供设备配置截图证明）；</p> <p>5、★支持 Oracle、MSSQL、DB2、Sybase、Informix、MYSQL、南大通用、人大金仓、神通、达梦、湖南上容、浪潮 KDB、PostgreSQL、TeraData、Access 等主流数据库防护和审计；</p> <p>6、数据库访问记录应至少包括发生时间、业务用户名、操作终端主机名及 IP 地址、终端工具名称、服务器端主机名及 IP 地址、数据库名、表名、SQL 语句、响应时间、返回结果等关键信息；</p> <p>7、支持对 SQL 语句执行结果（成功/失败）、SQL 语句执行时间、SQL 语句执行异常等数据库操作响应信息的审计；</p> <p>8、能够自动记录和分析 SQL 语句并快速制定安全策略，包括：将 SQL 语句归纳为不同的集群；支持定义所有 SQL 的相应威胁程度，至少包括高、中、低、提醒等告警级别</p> <p>9、能够定义所有 SQL 的相应记录方法可以将同类型的多条安全事件进行汇聚，并可以限定同类型安全事件的记录条数；</p> <p>10、系统提供白名单规则策略，系统提供黑名单规则策略，系统提供正则表达式规则策略，系统提供关键字表达式规则策略，系统提供例外规则策略；</p> <p>11、可对日志进行细粒度解析，支持审计数据库操作 (DM)、对象管理 (DD)、控制 (DC) 等操作语句的审计，解析后的日志记录至少包括访问发生时间、客户端 IP 地址、客户端 MAC、终端程序、访问账号、访问数据库名、操作表名、SQL 语句、数据库响应时间以及返回结果等关键信息；</p> <p>12、设备必须自带默认审计策略，支持用户自定义策略和规则，系统必须支持配置操作行为的黑名单、白名单，方便用户灵活配置审计规则；审计规则设置支持以服务器 IP、数据库类型、数据库表、操作类型设定的各种组合审计规则，还支持以关键字设定规则；</p> <p>13、支持以操作类型、时间、IP 地址、用户名、主机名、终端名、数据库操作类型、数据库表、影响的行、字符串、认证结果、响应时间、敏感数据、等作为事件识别规则</p> <p>14、内置自动告警设置，允许用户设定威胁自动告警，告警必须提供级别设定，至少提供致命、高风险、中风险、低风险 4 种告警级别，支持 SYSLOG、SNMP TRAP、邮件、FTP 等多种事件告警和提示方式；</p>	
--	--	--	--

		<p>15、支持通过 IP 地址、用户名、操作类型、关键词、时间等基本条件查询审计事件</p> <p>16、★支持将审计日志的敏感字段进行模糊化处理，防止敏感数据泄露（需提供设备配置截图证明）</p> <p>17、10 亿条日志的任意关键字组合（包括通配符）检索时间 &lt;10 分钟</p> <p>18、提供对风险和危害访问的分析，包括：高危操作分析和追踪、大规模数据泄露分析和追踪、批量数据篡改分析和追踪、SQL 注入行为分析和追踪</p> <p>19、支持按日志属性、日志类型、时间范围进行数据备份，自动与手动两种备份归档方式；支持 FTP 将数据备份到其他存储上，以备本机硬盘空间不够的情况下，数据能够依然保存</p> <p>20、系统界面可以显示数据库状态、缓冲区击中率、库缓存大小等变化趋势图；系统界面可以显示数据库的会话明细、查询缓冲击中率等信息；支持对 SQL 语句操作类型统计、事件类型统计、风险级别统计、流量统计，同时按在线用户、客户端 IP、会话、模板数等支持在线信息统计</p> <p>21、具备强大的报表模板以及可定制的客户化报表，满足不同层次用户需求。可提供 DPA、SOX、等保、医疗防统方等行业模板；支持自定义报表模板</p> <p>22、提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能</p>		
7、	vsan 服务器	<p>1、非 OEM 产品，具有自主知识产权，外观≤2U 机架式，可放入 42U 标准机柜；</p> <p>2、★配置 2 颗 Intel 12 核处理器 Xeon E5-2650 v4；</p> <p>3、★配置内存≥256GB 2133MHz DDR4 内存，内存插槽数量≥24，最大内存可扩展至 1.5TB；内存板支持热插拔，可支持内存备用，内存镜像功能；具备重构内存管理、降低内存功耗方法及功能（投标时须提供国家机关或权威第三方评测机构出具的相关技术证明材料复印件，原件备查）；</p> <p>4、★配置 10 块 4000GB 7200 RPM 3.5 寸 NL SAS 硬盘；</p> <p>5、★支持多种槽位的机架，最大硬盘数支持≥28 块（提供彩页证明）。</p> <p>6、★支持双 SD 卡，支持硬件 RAID1，可安装启动系统，hypervisor，虚拟化软件等（提供白皮书复印件证明）。</p> <p>7、★标配集成显卡，显存≥32M，分辨率最大支持 1920*1200（提供白皮书复印件证明）。</p> <p>8、★具备自主开发的中文版管理软件，提高设备的可管理性，提供软件著作权证书复印件。</p> <p>9、★支持 BIOS 中文界面，并提供截图证明。</p> <p>10、★支持触摸式液晶屏 LCD，提高设备的可管理性（提供白皮书复印件证明）。</p>		

		<p>11、配置专用 RAID 卡提供 RAID 0/1/10；具备热备盘数据迁移、数据重组及对 RAID 进行控制的方法功能，同时，具备闪存控制方法和固态硬盘的均衡方法功能（投标时须提供国家机关或权威第三方评测机构出具的相关技术证明材料复印件，原件备查）；</p> <p>12、★PCIe 扩展插槽最大支持≥9；</p> <p>13、板载集成 2 个千兆网口；具备对服务器及其访问卷的方法和存储设备的输入输出处理装置功能（投标时须提供国家机关或权威第三方评测机构出具的相关技术证明材料复印件，原件备查）；</p> <p>14、配置 2 个 750W 交流电源模块，支持 1+1 冗余；</p> <p>15、★通过中国环境标志认证，提供认证证书复印件；</p> <p>16、★通过 Energy Star 认证，提供认证证书复印件。</p> <p>17、★投标时应提供设备生产厂家针对此项目的授权书（厂家盖章）和售后服务承诺书的原件（厂家盖章）。</p> <p>18、提供设备安装服务和 3 年维保服务。</p>		
--	--	--	--	--