# 技术、商务及其他要求

## 采购清单

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备名称 | 单位 | 数量 |
| 1 | WEB应用防火墙 | 台 | 2 |
| 2 | 漏洞扫描系统 | 台 | 1 |
| 3 | 抗拒绝服务系统 | 台 | 1 |
| 4 | 网页防篡改 | 套 | 2 |

## 技术参数及要求

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **详细技术指标及功能需求** |
| **1** | **WEB应用防火墙** | 1、★要求为国产自主研发，非OEM产品，具备自主知识产权，具备《计算机软件著作权》，请提供加盖厂商鲜章的证书复印件；2、★支持基于单域名的反向代理部署模式（每个设备端口支持反向代理域名不低于255个）。提供配置界面截图证明；3、★设备支持的反向代理域名总数不受限制。4、支持针对虚拟站点的细粒度防护。5、★支持双机热备。6、★应支持设备到货后逐一功能测试。7、★网络吞吐量16G，应用层吞吐量≥8G，每秒新建能力≥60000，并发能力：≥100万，2个USB接口，1个串口，2个管理口，4个接口扩展槽位（至少支持扩展8个万兆接口或16个10/100/1000M自适应光/电接口），2U机架式设备，冗余电源。配置2个万兆接口和4个千兆光接口。配置5年硬件质保服务8、★支持对注入（包括SQL注入、LDAP注入、XPATH注入及命令行注入）、XSS、SSI指令、路径穿越、远程文件包含、WebShell防护。提供配置界面截图证明；9、支持非法下载防护，可以根据文件大小、MIME类型、及文件扩展名，灵活定义下载限制策略，限制用户非法获取网站的关键数据（比如数据库文件，配置文件等），提供配置界面截图。10、支持扫描防护，可实现自动判定扫描行为（可设置扫描防护阈值，并实现阻断）。支持以统计算法分析扫描行为的扫描防护。提供设备截图及权威材料证明。#11、支持与WEB漏洞扫描设备联动性。通过上传扫描文件到WEB应用防火墙，WAF可转化为针对性的WEB安全防护策略。提供设备截图及权威材料证明。12、提供盗链防护，应采用Referer和Cookie算法13、支持CSRF（跨站请求伪造）防护，提供配置界面截图；14、支持敏感信息过滤，对用户的个人隐私信息（信用卡卡号、手机号、身份证号码）泄露进行检测、阻断或替换。#15、支持对安全策略的一键式例外配置。提供配置界面截图证明。16、支持在安全日志中带有客户端真实IP地址，便于IP溯源。17、支持紧急模式，当并发连接数超过阀值时，WAF自动进入紧急模式，已经代理的连接正常代理，对新增的请求不进行代理，直接转发，防止WAF成为访问瓶颈。当连接数恢复正常时，自动退出紧急模式。提供配置界面截图证明18、产品是经过市场考验的成熟产品，产品上市时间不少于10年。提供上市第一年销售许可证或软件著作权证书等有效证明材料并加盖原厂鲜章；19、支持HTTP访问控制功能，可以提供针对HTTP元素和客户端的组合访问控制策略。支持对多种HTTP方法执行访问控制，包括：GET、POST、HEAD、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS、PROPFIND、PROPPATCH、LOCK、UNLOCK TRACE、SEARCH、CONNECT。20、支持Cookie安全机制，包括加密和签名的防护方法，支持Cookie自学习，提供配置界面截图；21、支持TCP Flood防护；支持基于信誉机制及用户行为识别的HTTP Flood防护。提供配置界面截图证明**#**22、产品支持与抗拒绝服务系统产品联动，实现基于单个IP的流量牵引，提供配置界面截图。23、支持使HTTP头域中的Cookie、Referer、User-Agent，Except字段过防护策略，提供配置界面截图；24、可生成PCI-DSS合规性报表。提供设备截图及权威材料证明。22、支持针对主流Web服务器及插件的已知漏洞防护。Web服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS等插件应覆盖:dedecms、phpmuadmin、PHPWind、shopex、discuz、echsop、vbulletin、wordpress等23、支持对攻击源地址的智能阻断，可以自定义IP封禁时间，并且可以手工解除解禁。提供配置界面截图证明。24、支持客户在手机客户端的自助远程运维功能，并且自助系统要求能实现客户自主免费对设备健康状态（CPU、内存）、版本、历史告警信息的实时查看，可以实时调整策略以应对网络突发攻击。请提供手机页面截图证明。**★**25、为实现安全设备的统一管理和日志收集，要求免费配置安全管理中心。并提供至少五年的软件升级和更新服务。26、WEB应用防火墙具有《国家信息安全测评信息技术产品安全测评证书》级别：EAL3+，提供加盖厂商鲜章的证书复印件证明。27、WEB应用防火墙具有互联网安全研究中心颁发的WEB应用防火墙认证证书，提供加盖厂商鲜章的证书复印件证明； |
| **2** | **漏洞扫描系统** | ★1、域名或IP地址授权许可≥512个，2个USB接口，1个RJ45 Console口，1个管理口，6个10/100/1000M自适应电口。1个接口扩展插槽（可扩展8个千兆电口或8个千兆光口或4个千兆电口及4个千兆光口）。★2、支持数据接口模块，提供HTTP RPC接口支持，方便与第三方产品联动。★3、配置5年硬件质保服务4、支持SQL注入、Cookie安全问题、支持跨站脚本攻击、伪造跨站点请求、支持网页挂马、隐藏字段、Web服务（如IIS、Tomcat、Apache等）漏洞等的检测。5、支持基于basic、NTLM、Cookie等认证方式的Web应用系统安全扫描，预设Cookie和登录预录制检测，HTTP和SOCKS代理扫描；6、提供支持深度优先及广度优先爬行顺序的能力、通过解析flash来获得Web应用的链接；7、产品支持直接部署于虚拟化环境中，无需安装第三方操作系统；8、可在界面中列出被检测网站的目录结构，点击相应的结构可以直接呈现当前页面的扫描结果；9、产品提供漏洞验证功能，直观展示漏洞验证过程信息，验证漏洞真实存在；10、提供标准的Web Service接口支持，方便与第三方安全产品或管理平台进行数据采集和调用；#11、支持与WEB应用防火墙产品联动，生成报表可供WAF生成安全防护策略，通过漏洞检测和威胁防护的循环式管理，无缝保护站点安全；提供配置界面截图证明。12、系统自动生成的WEB漏洞扫描报告具有详细的漏洞描述和对应的解决方案描述；13、提供漏洞知识库中包含的主流操作系统、数据库、网络设备的列表信息。为保证能够提供了实时可靠的主机探测信息，要求提供主机探测系统和方法的证明，要求提供权威材料证明。14、厂商漏洞知识库大于33000条，提供加盖厂商公章的互联网安全威胁报告。15、产品内置漏洞知识库漏洞信息大于17000条，提供详细的漏洞描述和对应的解决方案描述；漏洞知识库与CVE、CNCVE、CNNVD、CNVD标准同时兼容，并提供截图证明及CVE Compatible证书。**#**16、产品要求为国内开发，具备自主知识产权，并经过十年以上应用检验。提供上市第一年销售许可证或软件著作权证书等有效证明材料并加盖原厂鲜章。17、可以通过资产仪表盘直观展示资产的风险值、主机风险等级分布、资产风险趋势、资产风险分布等内容；可提供资产树功能，通过资产树直观呈现网络资产的安全风险。提供截图证明；18、产品应支持通过多种维度对漏洞进行检索，包括：CVE ID、BUGTRAQ ID、CNCVE ID、 CNVD ID、CNNVD ID、MS 编号、风险等级、漏洞描述、是否为危险插件、漏洞发布日期等信息；提供截图证明；**#**19、支持扫描国产操作系统、应用及软件的安全漏洞，如红旗、麒麟、起点操作系统，请提供功能截图。20、产品支持在同一任务中同时对目标系统进行漏洞扫描和安全配置核查，支持利用配置核查时获得的系统信息对目标系统进行登录扫描。21、产品支持新建配置检测等级模板，同时详细配置控制点分类、等保级别系。并根据等保级别对目标设备进行配置核查。请提供功能截图。**#**22、产品支持对系统漏洞扫描、WEB漏洞扫描、安全配置合规检查和结果综合分析、综合评分，并可输出同时包含漏洞扫描、配置核查、弱口令检查结果的报表，请提供功能截图。23、具备单独口令猜测扫描任务，支持多种口令猜测方式，包括利用SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP等协议进行口令猜测，允许外挂用户提供的用户名字典、密码字典和用户名密码组合字典。请提供功能截图。24、支持和微软WSUS补丁系统的联动，能够在发给主机管理员的邮件中附带自动配置WSUS的注册表文件，方便进行自动化的补丁修补，请提供功能截图。25、具备对外接口，支持安全运营平台或其它安全产品通过该接口下发扫描任务以及获取检查结果。请提供功能截图。**#**26、支持专门针对DNS服务的安全漏洞检测，包括DNS投毒和中毒等漏洞检测能力；支持“幽灵木马”检测；请提供功能截图。27、支持针对大数据组件框架的漏洞检测，请提供功能截图。28、支持分布式网络扫描任务，请提供权威材料证明；29、具备应急漏洞响应能力，可在紧急漏洞爆发后第一时间提供检测插件，2016年上半年发布的紧急漏洞检测插件不少于7个。请提供功能截图和链接。**#**30、厂商需在信息安全领域有丰富的经验与先进的技术，须有对系统漏洞进行发现、验证、以及提供应急服务的技术能力。如满足上述条件，需提供自主发现的安全漏洞列表，需超过34包含CVE编号、CVE网站的网址、漏洞名称。31、产品具有中国信息安全测评中心《信息技术产品安全测评证书--EAL3+》，请提供有效证书复印件并加盖生产厂家鲜章。32、产品具有中国信息安全认证中心《中国国家信息安全产品认证证书-增强级》，请提供有效证书复印件并加盖生产厂家鲜章。 |
| **3** | **网页防篡改系统** | 1、网页防篡改系统提供第三方接口可以与WEB应用防火墙联动。**★**2、产品为软件形态，支持Windows、Linux、HP-Unix、IBM AIX等；3、能够根据防护的网站、被篡改内容、篡改内容的类型、试图进行的篡改、成功的篡改、发现的日期、事件发生的日期等条件进行详细信息的查询；4、攻击检测、防护功能：利用WEB Shell等进行的文件篡改、SQL注入、跨站攻击、非法上传。请提供设备界面截图；6、文件防护规则支持顺序匹配；7、具有木马、病毒攻击的防御能力，请提供权威机构的检验报告；8、支持网络内容篡改防护，请提供权威材料证明；9、能检测防护利用WEB Shell等进行的文件篡改、SQL注入、跨站攻击、非法上传等。同时对网页请求/响应内容中的非法关键字进行检测、过滤；10、网页挂马/后门扫描：应用爬虫技术和网页挂马检测技术，提供挂马扫描功能，提供后门扫描功能。请提供设备界面截图；11、兼容不同的网站发布系统，请提供权威机构的检验报告。12、告警类型包括：试图进行网页篡改的各种攻击行为；对可视内容的非法增加、删除、修改的行为；对关键资源的访问行为；非法上传文件等行为。请提供设备界面截图；**#**13、提供进程、注册表、文件及服务的自我保护。请提供设备界面截图；14、系统支持对一定时期（包括年、月、周）的网页篡改攻击进行统计并查询；15、系统须能够对遭受的网页篡改攻击按照攻击次数、防护的网站、遭受攻击的网页、攻击类型、攻击时间（或者发现攻击的时间）等进行统计并排名。请提供设备界面截图；**#**16、产品可对下列事件产生审计记录：1) 对保护内容进行增加、删除、修改和恢复等操作行为；2) 对保护内容进行访问等操作行为；审计信息包含事件发生时间、访问的源IP、事件类型、试图访问的资源、操作是否成功等信息。请提供设备界面截图；#17、支持对站群、邮件系统进行防护。18、网页防篡改系统具有中华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》，要求提供“网站恢复”（增强级）检测报告及有效证书的复印件，证书明确写有“网站恢复”字样。19、网页防篡改系统具有中国国家信息安全产品认证证书(CCC证书)，要求提供公安部信息安全产品检测中心的网站数据恢复产品（增强级）检测报告及有效证书的复印件，证书明确写有“网站数据恢复”字样。 |
| **4** | **抗拒绝服务系统** | **#**1、抗拒绝服务系统提供第三方接口，可以和WEB应用防火墙联动。**★**2、交流双电源，≥2个USB接口，≥1个RJ45串口，≥2个GE管理口，≥4个链路扩展卡插槽（可至少支持扩展16个万兆接口或32个10/100/1000M自适应电口/光口接口）。配置2万兆接口，4个千兆光口。配置5年硬件质保服务。攻击流量处理能力≥4Gbps，攻击包处理能力≥400万pps；3、产品具备针对UDP53、TCP53及3DNS提供专用的DNS Query Flood防护手段，要求提供配置界面截图证明。 4、产品能够有效防护CC攻击，并提供etag、http cookies、url验证、ascii图片验证、bmp图片验证、传奇游戏验证、FCS检查和模式匹配检查防护算法以抵御不同程度的攻击，要求提供配置界面截图证明。 5、产品支持流量自学习功能，可结合自学习流量生产防护策略集参数，要求提供配置界面截图证明。6、产品具备对连接耗尽型攻击的防御能力，要求提供配置界面截图证明。 7、产品支持对代理型攻击（代理服务器，wap网关，CDN环境）的针对性防护，要求提供配置界面截图证明。**★**8、产品支持CC反向探测页面自定义功能，要求提供配置界面截图证明。 9、提供基于七元组（源IP地址、目的IP地址、源端口、目的源口、协议类型、TOS及接口）以及对数据包的特征字符进行匹配的模式匹配规则，要求提供配置界面截图。10、产品支持信任限速功能，对加入信任列表的IP地址进行流量控制，要求提供配置界面截图证明。11、产品支持设HTTP慢速攻击防护，要求提供配置界面截图证明。 12、产品支持对欺骗与非欺骗的TCP (SYN, SYN-ACK, ACK, FIN, fragments) 、UDP (random port floods, fragments)、ICMP (unreachable, echo, fragments)、(M)Stream Flood及混合类型攻击的防护，要求提供配置界面截图证明，在透明模式下防止SYN Flood 攻击，提供截图与专利证明。**#**13、支持客户在手机客户端的自助远程运维功能，并且自助系统要求能实现客户自主免费对设备健康状态（CPU、内存）、版本等信息的实时查看，请提供手机页面截图证明。14、产品需要有中国国家信息安全测评认证中心颁发的《国家信息安全测评信息技术产品安全测评证书》（EAL3），提供有效证书的复印件； |

说明：技术参数要求中的★号为关键指标，不满足该项指标投标将被**拒绝**；#号、无标识项，按照第4章中的“**表二：详细评审标准**”进行评分。

## 项目履约时间、地点

履约时间：合同签订后40天交货安装调试完成

履约地点：西南交通大学信息化与网络管理处信息化机房

## 付款方式

1.分期付款，第一期，合同签署后支付合同总额的60%；第二期，货到验收合格，在中标人支付招标人5%的质保金后十个工作日内，招标人支付合同总额的40%；第三期，正常运行一年后退还质保金；

2.中标人需提供增值税普通发票。

## 服务要求

|  |  |  |
| --- | --- | --- |
| **序号** | **服务要求项目** | **服务要求标准** |
| 1 | 服务要求 | 1、技术文件：应提供全套、完整的书面技术资料。2、设备安装、调试和验收：在合同生效后应向用户提供详细的安装要求并提供技术咨询。3、技术培训：投标人能够提供详细且完善的项目培训方案，能够提供专业的技术培训，能够有效保障用户技术人员掌握项目中涉及的相关系统运行维护的相关知识。到货安装调试完成后，有专业工程师现场提供系统的使用培训服务。培训课程，场地、交通等与培训相关的费用均由投标人承担。4、★软件升级：应免费向用户提供在硬件许可条件下的终生软件升级服务。 |
| 2 | 售后服务承诺 | 投标人提供完善的售后服务方案，对项目售后服务内容的合理性、全面性进行综合比较评分。 |
| 3 | 服务标准 | ★保修期：5年及以上免费保修。 |
| 4 | 备品备件 | 投标人提供的备品备件方案完善、合理且具有针对性 |
| 5 | 服务体系 | 技术支持与服务体系健全，组织机构、管理和服务人员针对工程实际配置且合理。  |
| 6 | 响应速度 | ★投标人故障现场服务时间要求：保修期内，在收到用户的维修服务要求后2小时内做出回应，4小时内到达现场，配件24小时内送达， 12小时内排除故障，48小时内提供备机服务并提供原厂工程师服务。 |
| 7 | 人员资格 | 本项目项目经理1名；注：投标文件中须提供上述人员在投标人单位的社保证明（以社保机构出具的投标截止日前三个月内任何一个月的社保证明为准）复印件加盖投标人公章。 |
| 8 | 培训 | ★投标人能够提供详细且完善的项目培训方案，能够提供专业的技术培训，能够有效保障用户技术人员掌握项目中涉及的相关系统运行维护的相关知识。到货安装调试完成后，有专业工程师现场提供系统的使用培训服务。培训课程，场地、交通等与培训相关的费用均由投标人承担。 |
| 9 | 集成实施服务 | 投标人要根据本项目特点，提供集成实施和安装施工调试方案，负责本次所有投标产品的安装调试集成等服务工作，费用包含在投标总价中。1. 设备安装调试：电脑桌椅安装、设备拆包装、设备连接、系统安装、网络联调，软件安装测试。
2. ★原厂工程师在现场负责系统的安装调试
3. 在保修期间，如有必要，工程师需要进驻学校进行安全监控服务。
 |

说明：服务要求中★号（若有）为关键要求项，不满足该指标项将导致投标被**拒绝**；无标识则表示一般指标项，按照**第4章中的“表二：详细评审标准”**进行评分。

##  验收标准

1. 货物到达现场后，供应商应在采购人在场情况下当面开包，共同清点、检查外观，作出验货记录，双方签字确认后开始安装调试。
2. 供应商应保证货物到达采购人所在地完好无损，如有缺漏、损坏，由供应商负责调换、补齐或赔偿。
3. 供应商应提供完备的技术资料、装箱单、授权文件和生产厂商提供的原厂正品出货证明材料（非装箱清单组成材料）等，并派遣专业技术人员进行现场部署调试。验收合格条件如下：
4. 产品技术参数与采购合同一致，性能指标达到规定的标准；
5. 产品技术资料、装箱单、授权文件等资料齐全；
6. 在产品（系统）试运行期间所出现的问题得到解决，并运行正常；
7. 在规定时间内完成交货并验收，并经采购人确认。
8. 产品在部署调试并试运行符合要求后，才作为最终验收。

5、采购人对供应商交付的产品（包括质量、技术参数等）进行确认，并出具书面验收意见。