# 技术、商务及其他要求

1.

## 采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **单位** | **数量** | **备注** |
| 1 | 流控设备 | 台 | 1 | 　 |
| 2 | VPN设备 | 台 | 1 | 　 |
| 3 | 磁盘管理组件(数据中心运维系统扩展) | 套 | 1 | 　 |
| 4 | AD域管理组件(数据中心运维系统扩展) | 套 | 1 | 　 |

## 技术参数及要求

重要性分为“\*”、“#”和一般无标示指标。\*代表最关键指标，不满足该指标项将导致投标被**拒绝**，#代表重要指标，无标识则表示一般指标项。

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **详细技术指标及功能需求** |
| **1** | **流控设备** | \*1、整机吞吐量≥22Gbps，七层吞吐量≥14Gbps，并发连接数≥3,800,000，在开启防火墙、IPS、WAF、流量控制、僵尸网络检测功能后，支持单向带宽不低于4Gbps。\*2、标准机架设备,冗余电源，配置4个千兆电口，8个千兆光口，4个万兆光口，所有端口需配置相应模块，同时设备包含2个高速USB2.0接口，1个RJ45串口，另外需提供用于Cisco N7009系列交换机千兆电口模块8块、千兆(多模)SPF光模块8块、10Gb万兆(单模)光模块4块。3、为保障设备的高可用性，要求设备支持链路聚合功能，当上行/下行端口链路出现故障时，对应的另一端下行/上行端口自动切断链路。#4、设备支持流量管理功能，并且具备多纬度的流量管理，支持根据应用、IP、时间和用户对带宽进行相应的保障和限制，并且能够根据应用类型设置带宽以保证应用类型的带宽优先级。#5、可视化流量控制：基于应用、网站、文件、时间、目标IP以及用户的多种流量控制，采用多线路技术、虚拟多线路技术、智能选路技术对多线路分别实现流控，保障核心业务、限制合法业务、阻断非法业务。6、应用识别能力：可识别各类互联网应用，不少于1000种应用规则策略，提供基于应用识别类型、用户名、接口、安全域、IP地址、端口、时间进行应用访问控制列表的制定。\*7、为满足多种流控场景，要求设备支持同时对总带宽进行不同纬度的流量划分，支持不同类别应用维度、单IP维度。#8、支持在链路聚合环境下使用流量控制，支持对不同链路（包括聚合链路）采用不同的流量控制策略。9、要求设备支持URL过滤和文件过滤功能，URL过滤支持不同的过滤类型，包括GET、POST请求过滤和HTTPS网站过滤等，通过支持根据文件的传递类型支持文件上传和下载过滤。10、能够有效监测并阻止DDOS攻击，可防护网络层和应用层的攻击，如SYN-Flood, Smurf, SSL-Flood,CC攻击,HTTP慢速攻击等。11、支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护、支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测。12、特征库检测：基于漏洞以及攻击行为的特征库，提供自动或手动升级方式。防御包括蠕虫、木马、后门、应用层DOS/DDOS、扫描、间谍软件、漏洞攻击、缓冲区溢出、协议异常、IPS逃逸攻击等。#13、支持内网访问控制，配置内网区域只允许指定的IP地址或IP范围对外进行访问，防止内部伪造源IP对外DoS攻击的情况。14、支持对信任区域主机外发的异常流量进行检测，如ICMP，UPD，SYN，DNS Flood等DDoS攻击行为。15、支持CC攻击防护。16、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。17、具备防护常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能。#18、可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则（提供产品界面截图并加盖厂商公章）。#19、支持针对网站的漏洞扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测。#20、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（提供产品界面截图并加盖厂商公章）。#21、支持对网站黑链进行检测（提供产品界面截图并加盖厂商公章）。#22、病毒检测：基于流引擎查毒技术，可以针对HTTP、FTP、SMTP、POP3等协议进行查杀；可实时查杀大量文件型、网络型和混合型等各类病毒；并采用新一代虚拟脱壳和行为判断技术，准确查杀各种变种病毒、未知病毒。23、支持叠加云端安全服务实现对设备的托管，由云端安全专家对设备进行日志分析和策略配置调整，并按月输出运营月报。#24、支持对终端已被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（提供产品界面截图并加盖厂商公章）。#25、对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告（提供具备相关云端查杀能力的证明） 。#26、支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址（提供具备相关云端大数据分析能力的证明）。#27、支持对经过设备的流量（部署方式：桥接、直通、虚拟链路、旁路流量、镜像流量等）进行分析，发现被保护对象存在的漏洞（非主动扫描），并根据被保护对象发现漏洞数量进行TOP 10排名，支持生成和导出威胁报告，报告内容包含对整体发现的漏洞情况进行分析（提供威胁报告并加盖厂商公章）。#28、提供安全报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，可以查看到有效攻击行为次数和攻击趋势（提供安全报表并加盖厂商公章）。29、针对数据中心优化，提供统计报表、趋势报表、汇总报表、汇总对比报表、指定对比报表危险行为报表、流速趋势报表等多种报表功能；提供详细的IPS/服务器防护统计、病毒信息统计分析功能；提供根据管理者自定义的风险行为特征自动挖掘并输出风险行为智能报表。\*30、产品应具备计算机信息系统安全专用产品销售许可证。#31、Web应用防护能力经过国际知名实验室NSS Labs测试，提供NSS Labs相关测试报告。32、提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》。33、生产厂家具备国家计算机网络应急技术处理协调中心《网络安全应急服务支撑单位CNCERT证书》。34、要求提供不低于5年的免费硬件质保、5年系统版本、相关数据库、资源库的升级。 |
| **2** | **VPN设备** | \*1、须为独立VPN设备，采用标准SSL、TLS 协议，同时支持IPSec VPN、SSLVPN两种VPN，非插卡或防火墙自带VPN模块设备。SSL VPN加密速度不小于100Mbps，SSL VPN最大并发用户数不小于300，SSL VPN每秒新建用户数不小于60，不少于4个千兆电口。\*2、本次采购需要配备150个SSL VPN并发接入授权以及50个移动应用发布并发接入授权，提供10个用于认证的USB key。3、支持网关模式、单臂模式部署两种方式。4、支持对基于HTTP、HTTPS、FileShare、DNS、H.323、SMTP、POP3、Telnet、SSH等的所有B/S、C/S应用系统，支持基于TCP、UDP、ICMP等IP层以上的协议的应用，例如即时通讯、视频、语音、Ping等服务。5、支持PC终端使用包括Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux等主流操作系统来登录SSLVPN系统。#6、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Windows EDGE，Google Chrome，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。（提供截图证明，加盖厂商公章）#7、支持IOS、Android等操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的SSL VPN接入。8、产品可扩展支持中国国家标准的商用密码算法（简称“国密”），包括：SM1（含SCB2），SM2、SM3、SM4。9、支持单点登录功能（SSO）,支持移动用户登录VPN后再登录内部B/S、C/S应用系统时不需要二次重复认证。支持针对B/S单点登录用户名密码加密传输，保证安全；支持针对不同的访问资源设定不同的SSO用户名和密码，支持用户自行修改SSO账号。10、支持断线重连自动技术，防止用户误操作关闭浏览器导致VPN隧道断开；防止用户在无线网络环境下网络正常切换时VPN隧道断开。11、支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式。12、支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。#13、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。（可提供证明材料，加盖厂商公章）#14、支持针对移动APP的VPN安全代码的自动封装，实现App应用的安全加固。（提供界面配置截图，加盖厂商公章）#15、产品必须在Windows和MAC操作系统下支持远程应用发布功能。（提供界面截图证明，加盖厂商公章）16、远程应用发布数据传输过程中使用SSLVPN协议加密，加密算法支持中国家标准的商用密码算法，保证了数据传输的合法性和安全性。\*17、支持改写WindowsRDP协议，经改写的协议必须独立于OS运行环境，避免跨平台兼容性，针对图像数据，服务端必须支持有损压缩算法。服务端必须能够支持过滤动态内容（gif/flash/video）以减少传输流量，且根据需要配置。（提供界面截图证明，加盖厂商公章）18、支持系统实时监控，图形化显示一段时间内的运行状况，可查看CPU占用率、各条线路网络吞吐量、各条线路的IP地址及发送接收流速、并发会话数、SSL并发用户数；可查看历史最高并发用户数并显示时间记录；可实时查看SSL接入用户的用户名、发送流速、接收流速、发送流量、接收流量、接入时间、并发会话数、接入IP、虚拟IP、认证方式等信息，并可在线中断指定用户。19、支持独立日志中心进行SSLVPN实时日志记录，可详细记录用户访问资源记录（用户、主机IP、资源、时间）、管理员日志（管理员、主机IP、时间、管理行为、对象）、系统日志、告警日志。20、支持Syslog（系统日志）服务器，可将管理员日志，系统日志、用户日志输出到syslog服务器中。#21、支持整体网关配置的本地及远程备份、恢复功能；支持SSLVPN配置的单独备份、恢复功能。22、提供公安部信息安全产品检测中心颁发的《GA/T 686-2007信息安全技术 虚拟专用网安全技术要求》三级或三级以上检测报告（三级以上为四级、五级）。23、提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》。24、要求提供不低于5年免费硬件质保、5年系统版本的升级。 |
| **3** | **磁盘管理组件(数据中心运维系统扩展)** | \*1、配置规模要求：存储设备数量≥8个，不限制磁盘数，完全基于B/S架构（监视及管理），中文界面，风格友好，操作简便。2、采用JAVA架构开发，可运行在Windows、Linux平台上。\*3、可管理SAN交换机,包括Brocade，McDAta，EMC，Cisco，HP，IBM等厂商。\*4、可管理RAID，包括Hitachi，NetApp，LSI，StorageTek，Accordance等厂商。5、可管理磁带库，包括ADIC，StorageTek，Quantum，Tandberg，Sun StorEdge等厂商。\*6、可管理HBA,包括Qlogix,Emulex等厂商。7、可管理主机,包括Windows,Linux,IBM-AIX8、能够自动发现网络中的存储设备。#9、通过拓扑图显示了整个存储网络，设备及其相互关系；通过不同的颜色显示设备和链接的状态；深入分析视图能呈现子图和设备明细。（提供截图加盖原厂鲜章）#10、能随时更新包含所有设备属性的资产清单；用户还可以输入一些诸如支持消息的附加字段。#11、提供设备可用性和性能的实时报表。\*12、提供包含告警、厂商、故障单等信息。\*13、通过报表识别那些使用过度或利用不足的设备元素。#14、报表可以保存为PDF格式或者打印出来用于参考。#15、捕捉传感器故障，涉及电源、温度、风扇、电池等。\*16、捕捉状态变化通知。#17、对于故障可以指派所有者、添加注释、清除故障、或者删除某个故障。#18、基于自定义规则通过Email或SMS向管理员报告警报。#19、能够与现有监控运维平台进行无缝对接。1. 要求提供不低于1年的免费原厂服务，提供软件模块、系统、相关文件、数据库、资源库的升级。

#21、要求厂商具有经济和信息化委员会颁发的软件企业认定证书；#22、投标产品具有国家版权局颁发的软件著作权登记证书。 |
| **4** | **AD域管理组件(数据中心运维系统扩展)** | 1. 简化重复性、繁琐复杂的AD域管理工作，满足SOX、HIPAA等合规性审计需求。

\*2、要求与存储管理必须为同一厂商产品。\*3、本次授权支持域数量不少于4个域帐号控制服务器。4、采用JAVA架构开发,完全基于B/S架构（监视及管理），能通过HTTP和HTTPS进行访问。、批量编辑终端服务主文件夹、路径、启动程序、会话时间和远程设置，可运行在Windows平台上（含32/64位）。#5、通过批量创建和编辑用户帐户，指派管理权限等，简化Windows AD域的管理。（提供截图加盖原厂鲜章）#6、重置多个用户帐户的密码、配置密码策略、启用/禁用密码过期的用户。（提供截图加盖原厂鲜章）\*7、支持技术员指派基于角色的访问权限，单个或批量创建、管理和删除用户帐户和AD对象。8、丰富的报表，满足合规性审计的需求。#9、可作为Windows服务运行。#10、要求可以通过手机App管理AD域用户。\*11、按照不同的需求为用户定制专有的模板，减少创建用户时的麻烦，节省管理时间。12、可通过CSV文件导入方式创建修改用户。13、对用户的命名、组、联系属性自定义设置。14、支持自定义用户属性。15、支持自定义标题、部门、公司等信息。16、支持设置用户的dial-in和VPN以及允许登录的终端。17、支持修改用户组的Exchange属性。18、支持设置终端服务，为用户编辑终端服务主文件夹和配置文件路径，从终端服务登录的用户编辑启动程序，修改会话持续时间、活动会话限制、空闲会话限制等，启用/禁用远程控制属性。19、在组中批量添加/移除计算机。20、批量设置计算机的属性，如：描述、位置等。21、批量启用禁用计算机。22、在组织单元间批量移动计算机。23、管理员可以通过从CSV文件导入，批量创建联系人。从而无需使用命令工具逐个创建联系人，更加简单灵活地管理联系人。24、用户报表：有以下特征：基于web的用户界面，完全可定制，及时更新/编辑选项，计划报表，直观的图表格式，对指定OU生成报表，报表可导出CSV, Excel, PDF, HTML, CSVDE多种格式。\*25、密码报表：密码报表提供有关无效登录的用户、密码过期的用户、密码即将过期的用户、密码过期时间、无法更改密码的用户、不应该更改密码的用户等信息。#26、用户登录报表：提供活动目录用户帐户的登录信息，即用户登录的Windows网络的日期和时间。27、NTFS报表：文件夹和文件和其属性的访问权限，生成直观的报表，帮助管理员清楚了解环境中文件级安全设置。28、组报表：管理员可以查看安全组、分发组、对象数量最多的组等。\*29、计算机报表：自动执行AD域管理任务和生成报表，为管理员提供有关域中计算机的全面信息，如：不活动的计算机、禁用的计算机、域控制器、工作站、允许委派的计算机、基于操作系统的报表、最近更改的计算机。30、不活动/禁用帐户报表：不活动用户的报表提供一段时间内未登录的用户列表，禁用用户报表提供所有被AD管理员禁用的用户帐户。#31、能够与现有监控运维平台进行无缝对接。1. 要求提供不低于1年的免费原厂服务，提供软件模块、系统、相关文件、数据库、资源库的升级。

#33、要求厂商具有经济和信息化委员会颁发的软件企业认定证书；#34、投标产品具有国家版权局颁发的软件著作权登记证书。 |

## ★项目履约时间、地点：

履约时间：合同签订后30天交货；

履约地点：西南交通大学犀浦校区信息化与网络管理处。

## ★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.成交人需提供增值税专用发票。

## 服务要求

重要性分为“★”和一般无标示指标。★代表最关键指标，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。

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务要求项目 | 重要性 | 服务要求标准 |
| 1 | 服务承诺函 | ★ | 一、中标软件、硬件产品的原厂服务要求1、硬件设备提供不低于3年的原厂质保服务、系统升级服务、资源库升级服务；2、软件产品提供不低于1年的原厂质保服务、系统升级服务、资源库升级服务；3、对于特别约定的原厂质保服务年限的软件、硬件产品，需满足其详细技术指标中的要求。二、中标者需要提供的服务响应速度、服务网络及服务人员素质要求1、中标方应确保本次招标项目的各设备安全稳定的运行，并承诺提供不少于三年的免费维保服务。中标方应提供报修电话及相关联系人的移动电话，维保期内，在接到学校方售后服务申请后，中标方须在2小时内响应，4小时内免费上门现场维护，并在24小时内解决问题。2、中标产品质保期起始日期按验收合格日期计算，产品质保期内，在接到学校方售后服务申请后，中标方会同原厂商须在2小时内响应，4小时内免费上门现场维修，并在24小时内解决问题。3、中标产品保修期的第一年，所提供的产品在三个月内连续两次以上出现同一故障，中标方会同原厂商必须无偿更换同一档次产品。4、在中标产品的设计使用寿命周期内，中标方对所提供的产品需承诺终身维护，保证学校方更换到原厂原装的零部件，确保产品的正常使用。三、中标软件、硬件产品的培训要求软件、硬件产品均应该提供原厂培训，包括 实际现场培训、培训文档、培训案例等资料；并提供7×24咨询。 |
| 2 | 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。 |
| 3 | 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。 |

## 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. 成交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. 成交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。
9. 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。

## 其他要求

1. 供应商应保证在本项目使用的任何产品和服务（包括部分使用）时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由供应商承担所有相关责任。
2. 采购人享有本项目实施过程中产生的知识成果及知识产权。
3. 供应商如欲在项目实施过程中采用自有知识成果，需在响应文件中声明，并提供相关知识产权证明文件。使用该知识成果后，供应商需提供开发接口和开发手册等技术文档，并承诺提供无限期技术支持，采购人享有永久使用权。
4. 如采用供应商所不拥有的知识产权的产品，则在报价中必须包括合法获取该知识产权的相关费用。