**采购需求**

**一、为落实政府采购政策需满足的要求：**

|  |  |  |
| --- | --- | --- |
| 序号 | 政策名称 | 内容 |
| 1 | 政府采购促进中小企业发展 | 提供材料详见招标文件第六章“报价文件” |
| 2 | 政府采购支持监狱企业发展 | 提供材料详见招标文件第六章“报价文件” |
| 3 | 政府采购促进残疾人就业 | 提供材料详见招标文件第六章“报价文件” |
| 4 | 政府采购鼓励节能产品 | 优先采购节能产品：提供材料详见招标文件第六章“商务和技术文件” |
| 5 | 政府采购鼓励环保产品 | 优先采购环保产品：提供材料详见招标文件第六章“商务和技术文件” |
| 6 | 政府采购进口产品 | 不允许采购进口产品 |

**二、采购资金的支付方式、时间、条件：**

1.合同货物全部到货后30天内支付合同总价的50%，安装、验收合格后30天内支付剩余50%，中标人应在采购人第二次付款前15天内向采购人提交与合同总价等额的增值税专用发票。

2.合同签订后10天内中标人向采购人支付合同总价的5%作为履约保证金，合同货物验收合格后履约保证金转为质量保证金，质保期满无质量及服务等问题后一周内无息退还。

**三、服务要求（技术要求里另有注明的以技术要求为准）：**

|  |  |
| --- | --- |
| 质保期 | 3年（项目验收合格后开始计算） |
| 服务标准 | 质保期内因不能及时排除的故障（相同故障发生超过2次或者维修超48小时才排除故障的视为不能及时排除的故障）而影响工作的情况每发生一次，其质保期相应延长60天，质保期内因货物本身缺陷造成各种故障或不能及时排除故障的应由中标人免费予以更换，否则将扣除质量保证金作为对采购人的补偿。质保期满后，仅收取零配件市场成本价费用，免人工费、差旅费，所涉及软件终身免费升级。 |
| 服务效率 | 提供7\*24小时电话响应，需上门服务的应在20分钟内响应，并在1小时内赶到现场，2小时内解决问题，如不能解决的，中标人需提供备用方案，确保采购人正常运行。 |
| 交付时间和地点 | 交付时间：中标通知书发出之日起30天内交货并安装调试完毕。  交货地点：采购人指定地点。 |
| 验收标准 | 1.中标人应提供合同货物的有效检验文件，经采购人认可后，与合同的性能指标一起作为合同货物验收标准。采购人对样品（如有）验收合格后，双方共同签署验收样品合格证书，在合同期限内采购人将对中标人提供的货物进行抽检验收，验收中发现合同货物达不到样品验收标准或合同规定的性能指标，中标人必须更换合同货物，并负担由此给采购人造成的损失，直到验收合格为止。  2.投标人应于投标文件中提供合同货物的验收标准和检测办法，并在验收中提供采购人认可的相应检测手段，验收标准应符合中国有关的国家、地方、行业的标准，如若中标，经采购人确认后作为验收的依据。  3.如中标人委托国内代理（或其他机构）负责安装或配合安装，应在签约时指明，但中标人仍要对合同货物及其安装质量负全部责任。  4.验收费用由中标人承担。 |
| 其他技术、服务要求 | 1.培训：  1.1 中标人应对采购人的操作人员、维修人员免费进行培训。  1.2 中标人应提供相应的培训计划，包括但不限于提供CISP、CISP-BDSA、CISP-CSE三种认证工程师的培训及考试。  1.3 投标人应对上述内容的实现方式、地点、人数、时间在投标文件中详细说明。  2.技术支持：  中标人应及时免费提供合同货物软件的升级，免费提供合同货物新功能和应用的资料。  3.安装调试（若需要安装调试）：  3.1 安装地点：采购人指定地点。  3.2 安装完成时间：中标通知书发出之日起30天内交货并安装调试完毕，如在规定的时间内由于中标人的原因不能完成安装和调试，视为中标人逾期交货，中标人应承担违约责任及由此给采购人造成的损失。  3.3 安装标准：符合我国国家有关技术规范要求和技术标准，所有的软件和硬件必须保证同时安装到位。  3.4 中标人免费提供合同货物的安装服务。  3.5 投标人在投标文件中应提供安装调试计划、对安装场地和环境的要求。 |

**四、技术要求：**

1.需实现的功能或者目标：支撑之江实验室行政、科研应用有效运行；

2.需执行的国家相关标准、行业标准、地方标准或者其他标准、规范：有强制性标准的执行国家强制性标准，无强制性标准的统一执行最新相关标准、规范，且能在本合同约定的项目中正常运行和使用；

3.需满足的质量、安全、技术规格、物理特性等要求：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 名称 | 数量 | 备注 |
| 1 | 管理服务器 | 2 | 国产品牌，具有自主知识产权 |
| 2 | 计算虚拟化节点  **(核心产品)** | 12 |
| 3 | GPU计算节点1 | 3 |
| 4 | GPU计算节点2 | 2 |
| 5 | GPU计算节点3 | 3 |
| 6 | 认证服务器 | 1 |
| 7 | 认证软件 | 1 |
| 8 | 核心交换机 | 2 |
| 9 | 10Gb交换机 | 2 |
| 10 | 25Gb交换机 | 2 |
| 11 | BMC管理交换机 | 2 |
| 12 | 10G光模块 | 1 |
| 13 | 25G光模块 | 2 |
| 14 | 100G光模块 | 1 |
| 15 | 下一代防火墙 | 2 |
| 16 | 核心存储 | 1 |
| 17 | 光纤交换机 | 2 | 无 |
| 18 | 一体化运维管理平台 | 1 | 国产品牌，具有自主知识产权 |
| 19 | FC光模块 | 2 | 无 |
| 20 | 千兆光模块 | 10 | 国产品牌，具有自主知识产权 |
| 21 | 入侵防御系统1 | 1 |
| 22 | 入侵防御系统2 | 1 |
| 23 | WEB应用防火墙 | 1 |
| 24 | APT攻击预警系统 | 1 |
| 25 | 数据库审计系统 | 1 |
| 26 | 运维审计系统 | 1 |
| 27 | 综合日志审计系统 | 1 |
| 28 | 远程安全评估系统 | 1 |
| 29 | 全流量深度威胁检测平台 | 1 |
| 30 | 网站卫士（网页防篡改） | 10 |
| 31 | 网站安全监测服务 | 1 |
| 32 | 安全评估服务 | 1 |
| 33 | 应急演练服务 | 1 |
| 34 | 应急响应服务 | 1 |
| 35 | 网站云防护服务 | 1 |
| 36 | 智能排查软件系统 | 1 | 无 |

**1.管理服务器**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ★基础架构 | 配置≥2颗Intel Xeon E5-2650 v4处理器 |
| 配置64G内存，要求单根≥16GB，最大支持24根DDR4内存插槽，速率最高支持2400MT/s，支持RDIMM或LRDIMM，最大容量1.5TB**（投标文件中提供官网截图及链接）。** |
| 单RAID卡支持2GB缓存，配置2端口SAS 1G缓存riad卡，支持RAID0/1/5/10。 |
| 支持≥8个2.5寸热插拔硬盘槽位，可扩展至≥24个2.5寸硬盘槽位，全部硬盘可在不打开主机箱盖的情况下热插拔维护，配置≥2块600G 10K SAS硬盘，≥4块4T 7.2K SAS盘。 |
| 支持高达256GB SATA M.2选件 |
| 支持10个PCIe 3.0可用插槽，支持3块双宽GPU卡**（投标文件中提供官网截图及链接）。** |
| 高度2U，双电源550W。 |
| 接口要求 | 5个USB3.0接口 |
| 配置≥1块2端口万兆光网卡(含两个原厂万兆多模光模块) |
| 品牌要求 | 与核心交换机同品牌 |

**2.计算虚拟化节点**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ★基础架构 | 支持Intel Xeon SCALABLE处理器 |
| 最大支持24根DDR4内存插槽，速率最高支持2666MT/s，支持RDIMM或LRDIMM，最大容量3.0TB**（投标文件中提供官网截图及链接）。** |
| 单RAID卡支持2GB缓存，本次配置2端口SAS riad卡，支持RAID0/1/5/10。 |
| 配置≥8个2.5寸热插拔硬盘槽位，全部硬盘可在不打开主机箱盖的情况下热插拔维护。 |
| 支持NVMe硬盘，最高支持32块前置NVMe硬盘**（投标文件中提供官网截图、链接及产品彩页）。** |
| 单节点最大支持40块盘**（投标文件中提供官网截图、链接及产品彩页）** |
| 支持高达256GB SATA M.2选件 |
| 支持10个PCIe 3.0可用插槽，支持3块双宽GPU卡**（投标文件中提供官网截图及链接）。** |
| 高度2U，双电源800W。 |
| 接口要求 | 5个USB3.0接口，最高可扩展至6个USB接口。 |
| 标配1个VGA，可选配支持最高2个VGA接口。 |
| 支持后部独立的管理端口 |
| 可管理性 | 配置≥1Gb独立的远程管理控制端口 |
| 配置虚拟KVM功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，支持3D图形化的机箱内部温度拓扑图显示，可支持动态功率封顶。 |
| 认证要求 | CCC、CECP、SEPA**（投标文件中提供证明材料）** |
| 中标麒麟操作系统认证证书**（投标文件中提供复印件）** |
| 品牌要求 | 与核心交换机同品牌 |
| ▲配置要求 | 配置≥2颗Intel Xeon Gold 6140处理器；  配置≥256G内存，要求单根≥32GB；  配置≥2块480G S4500 SSD硬盘；  配置≥1块2端口万兆光网卡(含两个原厂万兆多模光模块)，≥1块2端口25Gb网卡(含两个原厂25G多模光模块)，≥2块1端口16Gb FC HBA卡(含两个原厂16G多模光模块)。 |

**3.GPU计算节点1**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ★基础架构 | 支持Intel Xeon SCALABLE处理器 |
| 最大支持24根DDR4内存插槽，速率最高支持2666MT/s，支持RDIMM或LRDIMM，最大容量3.0TB**（投标文件中提供官网截图及链接）。** |
| 配置2端口SAS riad卡，支持RAID0/1/5/10。 |
| 配置≥8个2.5寸热插拔硬盘槽位，全部硬盘可在不打开主机箱盖的情况下热插拔维护。 |
| 支持NVMe硬盘，最高支持32块前置NVMe硬盘**（投标文件中提供官网截图、链接及产品彩页）。** |
| 单节点最大支持40块盘**（投标文件中提供官网截图、链接及产品彩页）** |
| 支持高达256GB SATA M.2选件 |
| 支持10个PCIe 3.0可用插槽，支持3块双宽GPU卡**（投标文件中提供官网截图及链接）。** |
| 高度2U，双电源1600W。 |
| 接口要求 | 5个USB3.0接口，最高可扩展至6个USB接口。 |
| 标配1个VGA，可选配支持最高2个VGA接口。 |
| 支持后部独立的管理端口 |
| 可管理性 | 配置≥1Gb独立的远程管理控制端口 |
| 配置虚拟KVM功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，支持3D图形化的机箱内部温度拓扑图显示，可支持动态功率封顶。 |
| 认证要求 | CCC、CECP、SEPA**（投标文件中提供证明材料）** |
| 中标麒麟操作系统认证证书**（投标文件中提供复印件）** |
| 品牌要求 | 与核心交换机同品牌 |
| ▲配置要求 | 配置≥2颗Intel Xeon Gold 6140处理器；  配置≥256G内存，要求单根≥32GB；  配置≥2块480G S4500 SSD硬盘；  配置≥1块2端口万兆光网卡(含两个原厂万兆多模光模块)，≥1块2端口25Gb网卡(含两个原厂25G多模光模块)，≥2块1端口16Gb FC HBA卡(含两个原厂16G多模光模块)；  配置≥1块NVIDIA Tesla V100 16GB GPU。 |

**4.GPU计算节点2**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ★基础架构 | 支持Intel Xeon SCALABLE处理器 |
| 最大支持24根DDR4内存插槽，速率最高支持2666MT/s，支持RDIMM或LRDIMM。 |
| 配置2端口SAS riad卡带2G缓存，支持RAID0/1/5/10。 |
| 支持NVMe硬盘 |
| 高度4U |
| 电源 | ≥4个1600W电源 |
| PCIE扩展 | ≥10×PCIe3.0 ×16 slots或20×PCIe3.0 ×8 slots**（投标文件中提供官网截图及链接）** |
| 显卡要求 | 支持多达10颗双宽GPU或20颗单宽GPU**（投标文件中提供官网截图及链接）** |
| 接口要求 | 4×USB3.0(前置、后置各2个)，1×串口(前置)，1×VGA(前置)。 |
| 支持100Gb/56Gb/40Gb/25Gb/10Gb多种高速网卡扩展，实现多GPU服务器间高效数据交换**（投标文件中提供官网截图及链接）。** |
| 可管理性 | CPU、内存条、供电电压监测 |
| CPU、内存条及系统温度监测 |
| 风扇、电源在位指示灯显示 |
| 过温报警 |
| 品牌要求 | 与核心交换机同品牌 |
| ▲配置要求 | 配置≥2颗Intel Xeon Gold 6148处理器；  配置≥256G内存，要求单根≥32GB；  配置≥2块480G S4500 SSD硬盘，≥10块2T SATA硬盘；  配置≥1块2端口万兆光网卡(含两个原厂万兆多模光模块)，≥1块2端口25Gb网卡(含两个原厂25G多模光模块)；  配置≥2块NVIDIA Tesla V100 16GB GPU。 |

**5.GPU计算节点3**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ★基础架构 | 支持Intel Xeon SCALABLE处理器 |
| 最大支持24根DDR4内存插槽，速率最高支持2666MT/s，支持RDIMM或LRDIMM，最大容量3.0TB**（投标文件中提供官网截图及链接）。** |
| 配置2端口SAS riad卡，支持RAID0/1/5/10。 |
| 配置≥8个2.5寸热插拔硬盘槽位，全部硬盘可在不打开主机箱盖的情况下热插拔维护。 |
| 支持NVMe硬盘，最高支持32块前置NVMe硬盘**（投标文件中提供官网截图、链接及产品彩页）。** |
| 单节点最大支持40块盘**（投标文件中提供官网截图、链接及产品彩页）** |
| 支持高达256GB SATA M.2选件 |
| 支持10个PCIe 3.0可用插槽，支持3块双宽GPU卡**（投标文件中提供官网截图及链接）。** |
| 单台配置2块480G S4500 SSD盘 |
| 高度2U，双电源1600W。 |
| 接口要求 | 5个USB3.0接口，最高可扩展至6个USB接口。 |
| 标配1个VGA，可选配支持最高2个VGA接口。 |
| 支持后部独立的管理端口 |
| 可管理性 | 配置≥1Gb独立的远程管理控制端口 |
| 配置虚拟KVM功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，支持3D图形化的机箱内部温度拓扑图显示，可支持动态功率封顶。 |
| 认证要求 | CCC、CECP、SEPA**（投标文件中提供证明材料）** |
| 中标麒麟操作系统认证证书**（投标文件中提供复印件）** |
| 品牌要求 | 与核心交换机同品牌 |
| ▲配置要求 | 配置≥2颗Intel Xeon Gold 6140处理器；  配置≥256G内存，要求单根≥32GB；  配置≥1块2端口万兆光网卡(含两个原厂万兆多模光模块)，≥1块2端口25Gb网卡(含两个原厂25G多模光模块)，≥2块1端口16Gb FC HBA卡(含两个原厂16G多模光模块)；  配置≥2块NVIDIA M60 GPU。 |

**6.认证服务器**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ★基础架构 | 支持Intel Xeon SCALABLE处理器 |
| 最大支持24根DDR4内存插槽，速率最高支持2666MT/s，支持RDIMM或LRDIMM，最大容量3.0TB**（投标文件中提供官网截图及链接）。** |
| 配置2端口SAS riad卡带1Gb缓存，支持RAID0/1/5/10。 |
| 配置≥8个2.5寸热插拔硬盘槽位，可扩展至≥24个2.5寸硬盘槽位，全部硬盘可在不打开主机箱盖的情况下热插拔维护。 |
| 支持NVMe硬盘，最高支持32块前置NVMe硬盘**（投标文件中提供官网截图、链接及产品彩页）。** |
| 单节点最大支持40块盘**（投标文件中提供官网截图、链接及产品彩页）** |
| 支持10个PCIe 3.0可用插槽，支持3块双宽GPU卡**（投标文件中提供官网截图及链接）。** |
| 高度2U，双电源800W。 |
| 接口要求 | 5个USB3.0接口，最高可扩展至6个USB接口。 |
| 标配1个VGA，可选配支持最高2个VGA接口。 |
| 支持后部独立的管理端口 |
| 可管理性 | 配置≥1Gb独立的远程管理控制端口 |
| 配置虚拟KVM功能，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，支持3D图形化的机箱内部温度拓扑图显示，可支持动态功率封顶。 |
| 认证要求 | CCC、CECP、SEPA**（投标文件中提供证明材料）** |
| 中标麒麟操作系统认证证书**（投标文件中提供复印件）** |
| 品牌要求 | 与核心交换机同品牌 |
| ▲配置要求 | 配置≥2颗Intel Xeon Gold 5118处理器；配置≥64G内存，要求单根≥32GB；配置≥6块600G 10K SAS硬盘，≥4块1T SATA硬盘；配置≥1块2端口万兆光网卡。 |

**7.认证软件**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ★总体要求 | 提供认证系统服务管理：能够支持Portal、802.1x等多种认证模式，提供vpn接入认证服务，提供Eduroam认证服务，提供ipv4及ipv6服务。 |
| 提供认证系统的日常维护服务工作 |
| 提供每月一次的巡检，协助实验室管理员进行终端用户的使用排查。 |
| 系统管理 | 系统管理采用B/S架构，管理员可以在任何地方，任何机器，在授权允许的情况下，无需安装任何客户端采用浏览器即可管理认证系统。 |
| 认证系统架构必须满足安全、稳定、易扩展，安装的数据库系统必须确保无任何版权争议，为Linux平台部署，能够部署在云平台上。 |
| 支持单机系统逃生技术，服务出现故障后能切换到逃生工具上。 |
| 支持扁平化的接入认证功能，支持华为、H3C、中兴、Juniper、CISCO全系列Bras和无线AC设备，支持阿里云AC设备。 |
| 用户管理 | 支持本地账号密码认证，支持AD域服务器、LDAP服务器、第三方RADIUS服务器作为身份认证源进行联动认证。 |
| 支持从外部服务器上同步账户信息，支持自动、手工和按需同步。 |
| 灵活的带宽控制，同时支持个人带宽与组带宽、起控时间段、HTTP带宽保证率、起控阀值。 |
| 能够支持多元素绑定功能，这些数据包括：IP地址、MAC地址、VLAN号、用户账号等多元素的绑定，能够支持自动绑定数据功能。 |
| 支持用户数据本地备份，异地备份，确保数据安全性。 |
| 用户首次认证成功接入后，以后接入网络认证时不需要再次输入用户名密码，系统会自动记录用户信息并且与设备绑定。 |
| 认证系统可以自动识别手持终端和pc，并在web认证的时候分别推出相应的portal页面，保障手持终端用户和pc用户认证页面不相同，便于用户的使用。 |
| 对于账号采用多维度控制策略，要求同一个账号可以隶属于多个策略组，每个策略组可以绑定多个控制策略，实现一个账户有多种控制和控制策略，达到基于条件的控制。 |
| 访客管理 | 预置普通访客、团体访客、长期访客、Eduroam漫游访客、新生访客等常用访客角色，方便管理者快速配置。 |
| 支持访客申请、审批、授权、分发、审计、下线、冷却、销户的全生命周期管理 |
| 灵活的实名审核模式：访客扫二维码获取短信验证码、员工扫访客二维码，团体访客扫描会议二维码、后台预约审核等。 |
| 多样化账号审核通知方式：短信、email、微信推送、Web方式通知 |
| 访客认证方式：二维码、短信、微信、无感知认证、Eduroam等 |
| 支持可配置细致的访客审核权限，提供给不同访客场景独立的访客审核管理权限，角色权限包括：访客申请审核页面、审批访客类型、是否允许审核、最大审核期限、最大审核人数、批量导入权限、访客组控制策略配置、指定访客组。 |
| 支持多维度可视化分析，包括：访客在线实时监控、各访客类别/访客组用量分布、资费、上线次数、人数统计、访客充值统计、访客无感知统计、访客外部认证统计等。 |
| ★接口管理 | 基于http restful协议的开发相应接口，可用于各类型接口开放对接，能够提供用户上网日志信息等进行大数据分析。 |
| 实现与实验室审计系统的对接，通过联动形成用户上网信息（包含：账号、ip、mac等必要字段）的完整数据链条，实现更精细化的上网行为管理。 |
| ★Eduroam接入管理 | 提供eduroam智能接入服务、eduroam用户管理服务、eduroam智能策略控制服务、eduroam智能分析服务、eduroam认证系统安全管控及服务等相关功能 |
| 实现对不同学校eduroam用户下发不同控制策略 |
| 提供对eduroam直观的图形化管理：漫游区域控制、访客并发数控制、使用时间/使用流量控制、访客实时在线情况、访客历史、访客使用明细、学校访客使用统计区域分布、来访问学校使用量 |
| ★IPv6管理 | 提供IPv6用户认证管理、实现Portal服务和认证服务对IPv4/v6单栈、双栈支持，认证服务日志记录能记录单栈或双栈下IPv6信息。 |
| 统一身份认证 | 支持802.1x认证、MAC认证、Portal认证、安全网关认证、VPN认证等多种认证方式以实现有线无线的统一认证 |
| HTTPS证书 | 协助实验室申请和部署https证书功能，证书为通配符DV SSL证书，GeoTrust品牌证书，证书服务期限为2年。 |
| 短信平台 | 提供短信平台服务，在服务期内能够满足用户使用的短信功能，短信平台服务期限为2年。 |
| ★实际配置 | 500个用户授权，不限制注册用户数授权，服务期限为2年 |
| ★质保要求 | 原厂免费3年质保服务（自货物交采购人验收合格之日起起算），中标后签订合同前，提供原厂售后服务承诺函原件和授权书原件。 |
| 提供原厂浙江省杭州市办事机构证明。 |

**8.核心交换机**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 品牌与成熟度 | 与10Gb交换机、25Gb交换机同一品牌 |
| 具有工信部颁发的电信设备进网许可证**（投标文件中提供复印件并提供链接备查）** |
| ★产品架构 | 支持多级交换架构，能够配置独立的交换网板与独立的主控板，交换网板与主控板硬件槽位分离。 |
| 采用CLOS+多级多平面正交交换构架，无中板设计，提供持续的带宽升级能力**（提供工信部测试报告）。** |
| 基于信元交换转发，可实现严格无阻塞交换，提高转发性能**（投标文件中提供官网截图及链接）。** |
| 业务插槽数≥4 |
| ▲设备性能 | 交换容量≥110Tbps，包转发率≥115000Mpps（若存在双指标，以较小值为准，**投标文件中提供官网截图及链接）。** |
| ★主控引擎 | 主控引擎模块≥2，满足1+1冗余，主控槽位与业务线卡槽位宽度相同的全宽槽位，提供更好的扩展性和可靠性。 |
| 支持X86构架云主控**（投标文件中提供X86构架主控板照片）** |
| 云主控板支持运行SDN控制器**（投标文件中提供官网截图及链接）** |
| 云主控板支持SSD硬盘 |
| 交换网冗余 | 支持独立交换网模块≥6**（投标文件中提供官网截图及链接）** |
| 电源冗余 | 电源模块支持N+M冗余，在线更换单板对转发无影响， |
| 关键部件热插拔 | 主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔 |
| ★接口要求 | 以太网支持千兆电口，千兆光口，万兆光口，万兆电口，40G端口，100G端口，25GE口。 |
| 单槽位万兆端口密度≥48**（投标文件中提供官网截图及链接）** |
| 单槽位40G端口密度≥48**（投标文件中提供官网截图及链接）** |
| 单槽位100G端口密度≥48**（投标文件中提供官网截图及链接）** |
| 支持FCoE**（投标文件中提供第三方权威机构测试报告）** |
| ★网络安全一体化 | 支持安全业务插卡FW、IPS、ACG、LB安全插卡**（投标文件中提供官网选配信息截图及链接）** |
| ACL | 为满足本次之江实验室数据中心访问控制需求，支持双向ACL，ACL≥1M**（投标文件中提供第三方权威机构测试报告）。** |
| 支持端口ACL |
| 支持VLAN ACL |
| QOS | 每端口支持8个优先级队列，3个丢弃优先级，支持SP、WRR、SP+WRR三种队列调度算法。 |
| 支持精细化的流量监管，粒度可达8K。 |
| 支持流量整形Shapping |
| 支持WRED拥塞避免 |
| 支持802.1p、TOS、DSCP、EXP优先级映射 |
| ★可靠性 | 双引擎快速倒换，主备切换时候板内转发无丢包。 |
| 支持NSF/GR for OSFP/BGP/IS-IS |
| 支持热补丁功能，可在线进行补丁升级**（投标文件中提供第三方权威机构测试报告）** |
| 支持不间断转发技术NSR，双引擎快速倒换，实现50ms的引擎故障主备切换时间**（投标文件中提供第三方权威机构测试报告）。** |
| 支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由，同时支持MPLS VPN、SR-TE**（投标文件中提供官网截图及链接）**。 |
| MAC | 为满足本次之江实验室数据中心接入设备二层转发需求，MAC表≥750K**（投标文件中提供第三方权威机构测试报告）** |
| 路由表 | 为满足本次之江实验室数据中心接入设备三层转发需求，IPv4 路由表项≥4194K**（投标文件中提供第三方权威机构测试报告）。** |
| ARP | 为满足本次之江实验室数据中心接入设备三层转发需求，ARP表项≥1048K**（投标文件中提供第三方权威机构测试报告）。** |
| ★虚拟化 | 多虚一技术(N:1)，支持4框虚拟化技术**（投标文件中提供第三方权威机构测试报告及官网截图和链接）。** |
| 一虚多技术（1:N）**（投标文件中提供第三方权威机构测试报告及官网截图和链接）** |
| ★VxLAN | 支持VxLAN 网关**（投标文件中提供第三方权威机构测试报告）** |
| ★产品资质 | 工信部入网证及检测报告**（投标文件中提供复印件）** |
| 阿里专有云硬件认证，阿里云官网可查**（投标文件中提供阿里云使用合同）** |
| ★厂商资质 | 具有知识产权管理体系认证证书**（投标文件中提供复印件）** |
| 具有有害物质过程管理体系认证证书**（投标文件中提供复印件）** |
| 具有国家企业信用信息公示系统无行政处罚记录证明**（投标文件中提供截图）** |
| ▲配置要求 | 双主控，2+1冗余电源模块，冗余风扇模块，实配3+1冗余交换网板，实配100G光口≥18个，实配40G光口≥4个，实配10G光口≥48个，配置万兆多模光模块≥2个，配置40G光模块≥2个，配置100G多模光模块≥2个。 |

**9.10Gb交换机**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ★品牌与成熟度 | 与核心交换机、25Gb交换机同一品牌 |
| 具有工信部颁发的电信设备进网许可证**（投标文件中提供复印件并提供链接备查）** |
| ▲设备性能 | 交换容量≥2.5Tbps，转发性能≥1000Mpps（若存在双指标，以较小指标为准，**投标文件中提供官网截图及链接**）。 |
| ★电源 | 支持模块化双电源 |
| ★风扇 | 冗余热插拔风扇，风扇数量≥3**（投标文件中提供官网截图及链接）** |
| ★性能指标 | 支持智能表项技术，整机资源可调。 |
| MAC地址表≥280K（大MAC模式） |
| ARP地址表≥200K（大ARP模式） |
| 路由表容量≥250K（大路由模式） |
| 整机BUFFER≥16M |
| ★接口类型 | 整机最大万兆光端口≥48，40GE端口≥6 |
| 支持USB接口及带外管理接口 |
| 支持MINI USB接口 |
| QOS | 支持对端口接收报文的速率和发送报文的速率进行限制，限速粒度<=8Kbit/s。 |
| 支持报文的802.1p和DSCP优先级重新标记 |
| 每端口支持的输出队列数>=8 |
| 支持灵活的队列调度算法，可以同时基于端口和队列进行设置，支持SP（Strict Priority）、WDRR（Weighted deficit Round Robin）、WFQ（Weighted Fair Queuing）、SP+WDRR、SP+WFQ等模式。 |
| ★堆叠 | 最大堆叠台数≥9台**（投标文件中提供第三方权威机构测试报告）** |
| 支持跨设备链路聚合，单一IP管理，统一的路由表项。 |
| 支持通过标准以太端口进行堆叠，可实现链式堆叠和环形堆叠等多种连接方式。 |
| 堆叠带宽(单向)>=160G，双向>=320G。 |
| 支持远距离堆叠，最大堆叠距离>=10KM。 |
| 路由协议 | 支持静态路由、RIP v1/2、OSPF、BGP等动态路由协议，支持RIPng、OSPF V3、IS-IS V6、BGP+ FOR IPV6、IPV6策略路由，支持VRRP，支持等价路由。 |
| 组播协议 | 支持PIM-DM、PIM-SM、IGMP、IGMP Snooping等组播协议 |
| 支持MLD，MLD Snooping、IPV6 PIM-DM、IPV6 PIM-SM 等IPv6组播协议 |
| 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN |
| 同时支持4组多对一的端口镜像 |
| ★MPLS VPN | 支持MCE，MPLS L3VPN、MPLS L2VPN、VPLS |
| 数据中心特性 | 支持VXLAN GW |
| 支持OpenFlow+Netconf的VXLAN集中式控制平面 |
| 支持大二层网络，支持多链接半透明互联（TRILL）。 |
| 管理和维护 | 支持SNMP V1/V2/V3，SSHv2。 |
| 支持WEB网管，支持电源的告警功能。 |
| 支持风扇、温度告警 |
| 支持sFlow和Netstream流量管理 |
| 支持基于端口速率百分比的风暴抑制，支持基于PPS的风暴抑制，支持基于bps的风暴抑制。 |
| 支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理 |
| ★认证和证书 | 产品具有工信部入网证及检测报告**（投标文件中提供复印件）** |
| 产品通过阿里专有云硬件认证，阿里云官网可查**（投标文件中提供阿里云使用合同）。** |
| 厂商具有知识产权管理体系认证证书**（投标文件中提供复印件）** |
| 厂商具有有害物质过程管理体系认证证书**（投标文件中提供复印件）** |
| 厂商具有国家企业信用信息公示系统无行政处罚记录证明**（投标文件中提供截图）** |
| ▲配置要求 | 万兆光端口≥48，40GE端口≥6，冗余电源、2+1冗余风扇，配置万兆多模光模块≥23个，40G光模块≥2个。 |

**10.25Gb交换机**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ★品牌与成熟度 | 与核心交换机、10Gb交换机同一品牌 |
| 具有工信部颁发的电信设备进网许可证**（投标文件中提供复印件并提供链接备查）** |
| ▲设备性能 | 交换容量≥4Tbps，转发性能≥2000Mpps（若存在双指标，以较小指标为准，**投标文件中提供官网截图及链接**）。 |
| 电源 | 支持模块化双电源 |
| 风扇 | 支持模块化风扇，风扇数量≥5，风扇支持热插拔。 |
| ★性能指标 | MAC地址表≥280K |
| 路由表容量≥320K |
| 整机Buffer≥32M，且支持所有端口共享。 |
| ★接口类型 | 整机最大25GE端口≥48，100GE端口≥8，千兆光口≥2。 |
| 支持USB接口及带外管理接口 |
| 支持MINI USB接口 |
| QOS | 支持对端口接收报文的速率和发送报文的速率进行限制，限速粒度<=8Kbit/s。 |
| 支持报文的802.1p和DSCP优先级重新标记 |
| 每端口支持的输出队列数>=8 |
| 支持灵活的队列调度算法，可以同时基于端口和队列进行设置，支持SP（Strict Priority）、WDRR（Weighted deficit Round Robin）、WFQ（Weighted Fair Queuing）、SP+WDRR、SP+WFQ等模式。 |
| 横向虚拟化 | 支持跨设备链路聚合，单一IP管理，统一的路由表项。 |
| 支持通过标准以太端口进行堆叠，可实现链式堆叠和环形堆叠等多种连接方式。 |
| 单堆叠组堆叠台数>=10台 |
| 堆叠带宽(单向)>=800G，双向>=1.6T。 |
| 支持远距离堆叠，最大堆叠距离>=10KM。 |
| 路由协议 | 支持静态路由、RIP v1/2、OSPF、BGP等动态路由协议，支持RIPng、OSPF V3、IS-IS V6、BGP+ FOR IPV6、IPV6策略路由，支持VRRP，支持等价路由。 |
| 组播协议 | 支持PIM-DM、PIM-SM、IGMP、IGMP Snooping等组播协议；支持MLD，MLD Snooping、IPV6 PIM-DM、IPV6 PIM-SM 等IPv6组播协议 |
| 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN |
| 同时支持4组多对一的端口镜像 |
| MPLS VPN | 支持MCE，MPLS L3VPN、MPLS L2VPN、VPLS |
| ★数据中心特性 | 支持VXLAN GW**（投标文件中提供官网截图及链接）** |
| 支持OpenFlow+Netconf的VXLAN集中式控制平面**（投标文件中提供官网截图及链接）** |
| 支持EVPN分布式网关**（投标文件中提供官网截图及链接）** |
| 支持RDMA和RoCE**（投标文件中提供官网截图及链接）** |
| 支持Service chain**（投标文件中提供官网截图及链接）** |
| 管理和维护 | 支持SNMP V1/V2/V3，SSHv2。 |
| 支持WEB网管，支持电源的告警功能。 |
| 支持风扇、温度告警 |
| 支持sFlow和Netstream流量管理 |
| 支持基于端口速率百分比的风暴抑制，支持基于PPS的风暴抑制，支持基于bps的风暴抑制。 |
| 支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理 |
| ★认证和证书 | 产品具有工信部入网证及检测报告**（投标文件中提供复印件）** |
| 投标产品阿里云使用合同**（投标文件中提供复印件）** |
| 厂商具有知识产权管理体系认证证书**（投标文件中提供复印件）** |
| 厂商具有国家企业信用信息公示系统无行政处罚记录证明**（投标文件中提供截图）** |
| ▲配置要求 | 25GE端口≥48，100GE端口≥8，千兆光口≥2，冗余电源，4+1冗余风扇，配置25G多模光模块≥20个，100G多模光模块≥2个。 |

**11.BMC管理交换机**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ★交换容量 | ≥336Gbps**（投标文件中提供官网截图及链接）**（若存在双指标，以较小为准） |
| ★转发性能 | ≥132Mpps**（投标文件中提供官网截图及链接）**（若存在双指标，以较小为准） |
| 性能指标 | MAC地址表≥32K |
| ★接口类型 | ≥48个GE端口，≥4个万兆SFP+口。 |
| 堆叠 | 最大堆叠台数≥9台 |
| 最大堆叠带宽≥40G |
| 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 |
| 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 |
| **以上投标文件中提供第三方权威机构测试报告** |
| VLAN特性 | 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 |
| ERPS | 实现ERPS功能，能够快速阻断环路。 |
| CPU防护 | 实现CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作**（投标文件中提供第三方权威机构测试报告）。** |
| 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 |
| ★路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF**（投标文件中提供第三方权威机构测试报告）** |
| 支持IPv6静态路由、RIPng**（投标文件中提供第三方权威机构测试报告）** |
| ★可靠性 | 支持RRPP（快速环网保护协议） |
| 支持Smartlink |
| 支持RSTP功能 |
| 支持MSTP功能 |
| 支持PVST功能 |
| 访问控制策略 | 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。 |
| SDN/OPENFLOW | 支持OPENFLOW 1.3标准支持普通模式和Openflow模式切换**（投标文件中提供证明材料）**，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 |
| 管理和维护 | 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 |
| 绿色节能 | 符合IEEE 802.3az（EEE）节能标准**（投标文件中提供第三方权威机构测试报告）** |
| 端口定时down功能（Schedule job） |
| 支持端口休眠，关闭没有应用的端口，节省能源。 |
| 支持智能风扇调速 |
| ★成熟度 | 产品具有工信部入网证**（投标文件中提供复印件）** |
| 厂商具有知识产权管理体系认证证书**（投标文件中提供复印件）** |
| 厂商具有CMMI 5资质**（投标文件中提供证明材料）** |
| ★兼容性 | 与核心交换机同一品牌 |

**12.10G光模块**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 硬件指标 | SFP+万兆模块(850nm，300m，LC) |
| 与核心交换机同一品牌 |

**13.25G光模块**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 硬件指标 | 25G SFP28光模块(850nm，100m，SR，MM，LC) |
| 与核心交换机同一品牌 |

**14.100G光模块**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 硬件指标 | 100G QSFP28光模块(850nm，100m，OM4，SR4，MPO) |
| 与核心交换机同一品牌 |

**15.下一代防火墙**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| ★配置要求 | 千兆电口≥8，千兆combo接口≥4，万兆光口≥8**（投标文件中提供官网截图及链接）**，配置≥2个万兆多模光模块。 |
| ★硬件架构 | 非X86多核架构，支持（双）交/直流电源。 |
| 硬件采用双主控，前后通风，具备可插拔冗余电源模块，可插拔风扇模块，接口扩展插槽≥1个**（投标文件中提供产品架构白皮书）。** |
| ★性能要求 | 吞吐量≥40Gbps，最大并发连接数≥2000万，每秒新建连接数≥40万。 |
| 部署模式 | 实现路由模式、透明（网桥）模式、混合模式 |
| 路由实现 | 实现静态路由、策略路由、RIP、OSPF、BGP等路由协议 |
| NAT功能 | 实现一对一、多对一、多对多等多种形式的NAT，实现DNS、FTP、H.323等多种NAT ALG功能。 |
| VPN | 实现高性能IPSec、L2TP、GRE VPN、SSL VPN等功能 |
| 支持IPsec VPN隧道自动建立，无需流量触发。 |
| 支持IPsec VPN智能选路，根据应用和隧道质量调度流量。 |
| 攻击防护 | 实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC和IP绑定功能，基于MAC的访问控制列表，802.1q VLAN透传等功能。 |
| 安全策略 | 支持一体化安全策略，能够基于时间、用户/用户组、应用层协议、地理位置、五元组、内容安全统一界面进行安全策略配置**（投标文件中提供功能截图)。** |
| 支持策略冗余分析，冲突策略分析以及命中率统计**（投标文件中提供功能截图)。** |
| 支持策略风险调优，定期分析用户策略，结合应用状况和流量情况，给出优化建议。 |
| 应用识别 | 可识别应用层协议数量≥3000种，针对微信、QQ等应用可精细化识别文字、语音、文件传输等内容**（投标文件中提供功能截图)。** |
| URL过滤 | 设备提供海量预分类的URL地址库（本地+云端方式），支持根据URL类别实现URL过滤。 |
| 设备支持管理者自定义新的URL地址和URL分类 |
| ★用户行为画像 | 提供基于用户名（或用户IP地址）实现对用户行为统一分析界面，采用饼状图对访问应用流量、网站访问集中分析展示，包含基于时间轴的访问行为轨迹(应用账号、行为内容等)，关联账号（微信、QQ）等相关用户行为审计内容**（投标文件中提供功能截图)。** |
| 行为审计 | 基于应用协议识别对各类聊天软件进行详细审计，可审计应用类型（如QQ、微信），应用识别账号，应用行为（如登录、发送消息、接收消息），操作时间，终端类型（Android、IOS）等。 |
| ★入侵防御 | 实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL注入、IDS/IPS逃逸等攻击的防御，实现攻击特征库的分类。 |
| 支持超过7000种特征的攻击检测和防御**（投标文件中提供功能截图)** |
| 防病毒 | 可基于病毒特征进行检测，实现病毒库手动和自动升级，报文流处理模式，实现病毒日志和报表。 |
| 支持超过37000条病毒规则**（投标文件中提供功能截图）** |
| 数据安全 | 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配。 |
| ★流量控制 | 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等，支持带宽通道独占以及共享管理模式**（投标文件中提供功能截图）。** |
| 加密流量检测 | 支持HTTPS，POP3S，SMTPS，IMAPS加密流量的安全检测。 |
| APT攻击防御 | 支持与云沙箱联动，实现对APT攻击的防御功能。 |
| 流量地图 | 支持基于地理位置的流量和威胁分析 |
| IPv6 | 实现IPV6动态路由协议、IPV6对象及策略、IPV6状态防火墙、IPV6攻击防范、IPV6 GRE/IPSEC VPN、IPV6日志审计、IPV6会话热备等功能 |
| 支持IPV6下的访问控制、IPSec VPN、DDoS防护等安全功能 |
| ★负载均衡 | 支持链路负载均衡功能，支持智能DNS，支持加权轮转、随机、加权最小连接、源IP地址hash、源IP地址和端口hash、目的地址hash、带宽算法、最大带宽算法、ACL、动态就近性、基于优先级的调度算法、主备实服务器组12种调度算法**（投标文件中提供配置截图）。** |
| 支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率**（投标文件中提供功能界面截图）。** |
| DDoS防护 | 能够防范DOS/DDOS攻击：Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、SYN Flood、ICMP Flood、UDP Flood、HTTP Flood（cc）攻击、ARP欺骗、TCP报文标志位不合法、超大ICMP报文、地址扫描的防范、端口扫描的防范、DNS Flood、ACK Flood、FIN Flood、分片Flood、Tiny-Fragment |
| 支持流量自学习功能，可设置自学习时间，并自动生成DDoS防范策略**（投标文件中提供功能截图）。** |
| ★诊断中心 | 支持报文示踪功能，可对原始报文进行回放**（投标文件中提供功能截图）。** |
| 支持丢包统计，提供详细分析丢包原因。 |
| 国密算法 | 支持国密SM1/2/3/4算法**（投标文件中提供功能截图）** |
| ★安全服务链 | 支持基于SDN网络的部署模式，支持对数据流进行服务链VXLAN封装转发。 |
| 通过集中控制器对安全业务进行按需编排，实现安全能力的弹性扩展及多业务能力共享**（投标文件中提供功能截图）。** |
| ★虚拟化能力 | 支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能，可独立分配CPU/内存等计算资源，虚拟防火墙可独立管理，独立保存配置，虚拟防火墙具备独立会话管理、NAT、路由等功能**（投标文件中提供功能截图）。** |
| 支持高可靠性（包含主备/主主模式）部署 |
| 设备管理 | 支持SNMPv1、SNMPv2、SNMPv3、RMON等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。 |
| 提供开放API接口（RESTful，NetConf），可编程管理防火墙，不再仅依赖网管软件。 |
| ★厂商资质 | 具有CMMI 5资质**（投标文件中提供证明材料）** |
| 具有信息技术服务管理体系认证证书**（投标文件中提供复印件）** |
| 具有信息安全管理体系认证证书**（投标文件中提供复印件）** |
| 具有信息安全服务资质证书(安全工程类一级及以上)**（投标文件中提供复印件）** |
| 中国反网络病毒联盟（ANVA）成员单位**（投标文件中提供证明材料）** |
| CNNVD（中国国家信息安全漏洞库）一级支撑单位资质，CNVD（中国国家信息安全漏洞共享平台）技术组成员资质**（投标文件中提供证明材料）。** |
| 具有信息安全等级防护安全建设服务机构能力评估合格证书**（投标文件中提供复印件）** |
| 通过中国网络安全审查技术与认证中心信息安全风险评估一级**（投标文件中提供证明材料）** |
| ★产品资质 | 具有计算机信息系统安全专用产品销售许可证**（投标文件中提供复印件）** |
| 具有国家信息安全产品认证证书（ISCCC）**（投标文件中提供复印件）** |
| 具有信息技术产品安全测评证书（EAL3+）**（投标文件中提供复印件）** |

**16.核心存储**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 品牌要求 | 具备自主知识产权的国产存储品牌，非OEM产品，具有存储产品研发能力。 |
| 获得Vmware VAAI、SRM、VASA、VVOL兼容性认证**（投标文件中提供Vmware官方网站截图）** |
| 通过1.6.1版本的SNIA SMI-S CTP认证**（投标文件中提供SNIA网站截图）** |
| 2018年Q1的IDC高端存储市场全国排名前10位**（投标文件中提供IDC截图）** |
| 阵列控制器 | 多控制器架构设计，控制器支持横向扩展，本次实配2个Active-Active控制器。 |
| 对于单一LUN，多个控制器可以并行读写。 |
| ★多控制器架构，采用PCI-E协议实现控制器间互连，多控架构中控制器最大可扩展到≥16个SAN控制器（SAN控制器不包括外接虚拟化网关或者NAS控制器等）**（投标文件中提供相关证明材料）。** |
| ★支持在同一存储控制器上实现NAS、FC-SAN和IP-SAN多种访问方式（非SAN存储加NAS文件引擎的方式实现NAS功能），本项目同时配置FC-SAN和IP-SAN两种存储接口与访问服务。 |
| 完全的硬件冗余：处理器、缓存、电源、风扇、适配卡、总线等都提供冗余，并保证在某硬件出问题时，能够进行自动切换，不出现单点故障。 |
| 写缓存镜像，配置缓存降落技术，掉电后能够将缓存数据下刷到硬盘中进行永久保存。 |
| 当数据盘无法写入时，能够将缓存中的数据进行冻结，保证数据不丢失**（投标文件中提供相关证明材料）。** |
| 为满足本次项目性能要求，投标产品通过SPC-1 V3版本测试，并且在测试平均延迟不高于0.3ms，最大延迟不得高于0.5ms测试下，IOPS性能值超过40万**（投标文件中提供SPC-1官网截图和SPC-1官网链接）。** |
| ★配置要求 | 当前配置缓存≥256GB（不含任何性能加速模块或NAS缓存、FlashCache、PAM卡，SSD Cache等） |
| 二级缓存扩展能力≥6.4TB |
| 配置16个16Gb FC主机接口（包含全部SFP）、4个10G ISCSI接口（包含全部光模块）、6个1Gbps iSCSI。 |
| 配置后端磁盘通道≥8个，SAS3.0规范，总带宽≥384Gb。 |
| ★磁盘系统 | 配置一体化企业级1.92TB SSD硬盘≥30块，配置企业级8TB 7.2K SAS硬盘≥40块，配置企业级600GB 10K SAS硬盘≥4块。 |
| 每双控可扩展≥1000块硬盘**（投标文件中提供相关证明材料）** |
| SSD、SAS、NL-SAS、SATA等（支持不同类型硬盘混插）**（投标文件中提供官网截图及链接）** |
| 硬盘安全管理 | 支持硬盘缓上电技术，避免大量硬盘同时上电时，引起电流过载，跳闸风险。 |
| 支持多种RAID存储方式，包括RAID1，RAID0，RAID10，RAID5，RAID6，支持不同RAID级别并存。 |
| ★配置RAID快速重建功能，单块硬盘发生故障，重建时间不超过30分钟，单块硬盘发生故障，热备盘重建时间不超过30分钟**（投标文件中提供第三方评测机构测试报告）。** |
| 存储管理软件 | 配置图形化管理平台软件，采用开放存储管理软件，提供API接口，支持功能特性植入和二次开发**（投标文件中提供接口方案说明）。** |
| 支持软件下发功能，存储设备批量统一升级。 |
| 支持自动计算出系统中网络拓扑，展示网络的实际物理结构，支持对大规模应用环境进行分区块管理。 |
| 支持平台支持管理员帐户和普通帐户，实现分级管理，各接入单位可通过自助服务平台查询资源的使用情况以及各种数据业务的运行情况等。 |
| 支持提供多种业务监控手段，通过存储用户列表，存储设备列表和复制关系列表，分别从不同的维度展示业务的相关信息，了解目前业务的运行情况。 |
| 支持提供对存储系统所管理的各种设备性能参数的实时监视功能，随时了解IT系统的运行状态，预防潜在的系统故障，预测系统发展趋势，合理优化IT系统。 |
| 配置路径冗余和故障切换（含多路径软件支持）未来增加任意平台、任意主机不需要额外付费 |
| ★配置自动精简功能，结合业务应用，进行空间的预分配，增加业务空间分配的灵活性，保证后续业务平滑扩展。 |
| 配置QoS功能，能够提供图像化管理界面，能够按照IOPS、带宽等维度进行策略调整**（投标文件中提供相关证明材料）。** |
| ★支持IPv4、IPv6双协议栈，主机和存储之间可以通过IPv4/v6协议构建IP SAN存储网络，管理终端和存储之间可以通过IPv4/v6协议构建带外管理网络**（投标文件中提供相关证明材料）。** |
| 配置call-home管理功能，在配置告警服务器的前提下，设备的告警信息可以自动发给存储原厂售后管理中心。 |
| ★管理安全性 | 管理界面采用BS架构，能够抵抗一定程度的黑客攻击和数据拦截。 |
| BS界面采用HTTPS安全加密传输方式，保护用户的数据安全，针对登录接口的前端RSA加密传输和后台解密验证，保证用户的账户安全。 |
| 高级功能 | ★支持阵列级双活功能，不接受采用网关形式或软件形式实现方式：  1.阵列级双活架构，可实现两套核心存储数据双活（主机能够并发读写同一双活卷），任何一套设备宕机均不影响上层业务系统运行；  2.双活架构需要具备独立的第三方仲裁设备，仲裁设备故障时，不影响业务运行，同时双活卷仍能保持数据实时一致；  3.双活引擎数据传送采用专用同步通道，不可与业务数据网络复用，且带宽≥100G**（投标文件中提供原理说明和产品界面截图）。**  **以上内容投标文件中提供第三方评测机构测试报告** |
| 支持异构虚拟化技术：  1.支持异构虚拟化功能，能够提供异构存储虚拟化整合功能，能接管现网异构存储，无需破坏或者改变现有数据格式，构成异构资源池，进行统一的资源调配和管理；  2.异构虚拟化兼容业界主流存储（如EMC、HP、HDS、IBM、Huawei、NetApp等多个厂家的阵列）；  3.提供快速回退功能，即被接管的阵列可直接映射给业务主机使用，防止由于虚拟化失败或者虚拟化不能快速回退造成的数据丢失，导致业务系统不可恢复；  4.支持对异构存储创建FC和iSCSI链路，进行数据传输，并管理异构LUN；  5.异构虚拟化平台支持提供异构存储之间的数据镜像功能；  6.异构虚拟化平台支持提供异构存储之间的双活应用。 |
| 配置三重检验的RAID方式，允许同一个RAID组中任意三块硬盘发生整盘物理故障，数据不丢失**（投标文件中提供相关证明材料）。** |
| ★配置基于时间点的数据快照功能，有效预防各种软故障的发生，单卷支持快照数量≥2000个，可进行有效的数据回滚**（投标文件中提供相关证明材料）。** |
| ★配置智能数据分层功能，用于数据生命周期管理，支持分层透明移动数据，数据根据访问频度的不同，可以被自动分配到不同速率的介质**（投标文件中提供截图和技术说明）。** |
| 配置云盘功能 | 实现个人文件和企业文件的云端存储和备份，支持用户间的文件分享和协作，支持文件快速分发汇集，实现文件按权限按级别灵活访问控制，采取多种安全措施保障文档安全，本次配置50个用户配额。 |
| 系统需要支持一文一密，并在加密情况下实现去重，用户文档仅用户可见（用户文件数据对系统管理员不可见），系统需要支持三种加密，服务端不得保存密钥。 |
| 支持外链功能与外部协作，同一用户对同一个文件可生成多个外链方便同时分享给不同的人，外链需要进行统一管理，可以一键复制外链快速分享。 |
| 云盘系统的文档接口符合UOMl标准 |
| 云存储互联功能要求 | 为了保证未来的节点扩展能力，统一存储资源池最大可扩展至≥280个纯SAN节点（单节点实际配置SAN控制器数≥2），节点之间互联采用IB或IP网络，节点之间互联速率带宽≥80Gbs**（投标文件中提供官网截图及链接）**，在需要扩展配置≥4个存储节点互联时，互联架构需保证任意存储节点控制器可以访问其他存储节点控制器所属卷，同时配置≥4个节点的任意控制器之间的卷可以进行双活功能**（投标文件中提供经测试的证明材料）。** |
| 不需要借助存储设备之外的任何网关设备或主机软件，支持将上述多个纯SAN节点整合为统一存储资源池，实现存储资源在一个管理界面上的统一配置、管理和分配（非异构虚拟化方式），包括但不限于创建RAID、创建LUN、主机挂载、Qos策略配置、数据复制、快照管理、热点缓存分配、磁盘管理、故障告警等，存储资源池支持在线动态增加和减少存储节点，多控架构需保证主机通过一个控制器可以访问其他任意控制器所属卷，并实现所有控制器间的链路负载均衡访问。 |
| 存储系统支持集群式系统访问，服务器可以通过任意链接链路访问后端存储磁盘卷，并且只要存在链接链路，任意其他链路损坏，不会影响前端服务器对后端存储磁盘的访问**（投标文件中提供经测试的证明材料）。** |
| 云共享分布式存储软件 | 配置分布式存储软件系统，整个产品架构采用全对称模式，元数据需要分布在所有节点上，整体系统由共享数据容量节点、共享互联节点组成。 |
| 文件系统支持海量文件场景，单一文件系统支持100亿个文件，可在单个扁平目录管理超过2000万个文件，单一文件系统大小≥256PB，单一文件大小≥256TB，支持POSIX Mac OS 客户端。 |
| 提供分布式网络客户端功能，以替代传统的网络客户端通过CIFS、NFS协议实现网络数据共享服务，实现对共享文件系统中数据的高可靠性、高性能网络访问，消除了NFS和CIFS数据共享的一些弊端和隐患。 |
| 兼容性要求：  1.Windows XP/Win7 32位和64位；  2.Windows 2003/2008/2012 Server 32位和64位；  3.中标麒麟 6及以上32位和64位；  4.SUSE Linux enterprise 11及以上32位和64位  5.AIX客户端64位。 |
| 配置容量授权≥50TB。 |
| 国产数据库支持 | 支持国产数据库、支持国产操作系统**（投标文件中提供认证证书）** |
| Veritas支持 | 通过Veritas认证**（投标文件中提供Veritas官网截图）** |
| 自动运维管理软件 | 配置自动巡检功能，针对设备系统信息，硬件信息自动生成分析结果、日志、诊断信息和glist信息，并形成报告及建议优化信息，打开即可查看，并自动通过邮件发送报告。 |
| 服务要求 | 提供软件与硬件免费3年原厂服务（自货物交采购人验收合格之日起起算），合同签订前提供原厂针对本项目专项授权和服务承诺函，并可通过原厂800/400服务热线查询服务期限。 |

**17.光纤交换机**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| SAN交换机尺寸 | 能固定于标准的19寸机架内，1U高。 |
| ★背板架构 | 无拥塞的背板架构 |
| ★全线速 | 所有FC端口支持16G全线速 |
| ★光模块特性 | 所有的光纤通道接口需支持16Gb光模块，可在线热插拔。 |
| 冗余性 | 双电源 |
| 支持区域划分 | 支持硬件分区 |
| 可管理性 | 支持SNMP、Telnet、Web管理/GUI界面 |
| 端口可扩展性 | 单台机器配置48个可使用端口 |
| ★端口需求 | 每台SAN交换机激活24个16Gb FC端口，并配置24个16Gb光模块。 |
| ★端口类型 | 支持D\_Port（诊断端口）、E\_Port、EX\_Port、F\_Port、M\_Port（镜像端口） |
| 基于交换机类型的自我发现（U\_Port），当Access Gateway 模式时，支持F\_Port 和N\_Port（支持 NPIV 技术）。 |
| ★加密和压缩 | 提供免费的加密和压缩功能 |
| ★多链路捆绑功能 | 支持基于Frame的多链路捆绑 |
| 保修 | 原厂免费保修3年（自货物交采购人验收合格之日起起算），7\*24电话支持，当天4小时备件更换，包括备件和人工。 |

**18.一体化运维管理平台**

|  |  |  |
| --- | --- | --- |
| 功能类别 | 技术要求及指标 | |
| 系统 | ★管理范围 | 监控节点数≥500 |
| ★硬件 | 采用2U软硬件一体化设备，千兆接口数量不少于6个，万兆接口不少于2个。 |
| 管理界面 | 全中文界面，采用HTML5技术，支持B/S模式的管理，界面友好，支持基于Web的图形用户界面（GUI），能够以简单、直观的方式显示信息，简化配置，在不改变现形网络架构前提下实现部署。 |
| 软件功能模块：综合监控、资产管理、运维辅助、动环监控、流量拓扑、日志及告警中心、报告报表、大屏展示、IP地址管理，系统管理 |
| ★数据分析大屏 | 支持≥3个独立大屏显示界面（非功能显示界面），包括内容信息：雷达大屏视图（含设备总类主视图、雷达扫描图、机房动力环境监控图、设备有效性排名、CPU利用率排名、主要出口数据流量曲线图、磁盘利用率排名、日志告警）；远程机房视图（各个机柜设备位置显示图（要求和官网设备图形一致）、设备状态显示图（针对设备是否存在故障能够有故障告警、告警信息等）；动态拓扑沙盘图（显示指定拓扑图、对故障设备能够动态红色标记显示、针对指定链路实时数据能够显示、对于指定的重要端口进出数据能够实时显示）。以上功能都能够在后台具有自定义功能，要求根据实际使用情况进行定制化大屏展示开发，可对接其他各类应用系统。 |
| ★时间同步 | 内置NTP时间同步功能 |
| ★操作系统 | 软件基于自主开发系统或是采用CentOS操作系统（64位） |
| 用户 | 支持基于角色的用户管理 |
| 监控管理 | 支持设备 | ★支持主流厂商交换机、路由器、网络安全设备，可添加定制所有支持SNMP协议的网络设备。 |
| 支持主流厂商存储设备 |
| 支持主流厂商UPS供电设备 |
| 监控方式 | 支持SNMP、WMI、SSH、TELNET、SHELL、IPMI、HTTP、Agent、Rsyslog、TCPDUMP等 |
| 服务及端口监控 | 支持基于TCP端口、UDP端口的监测监控 |
| 支持常见服务应用的监控（Apache、Nginx、IIS、Ftp、DNS、DHCP、WINS、Mysql、Oracle、POP3、Smtp、IMAP等） |
| 能够自定义要监控的服务和应用 |
| 能够对数据库和中间件等进行基本监控 |
| 网络监控 | 支持监控网络ICMP响应时间监控 |
| 支持网络端口的收、发数据包、错包、广播包等数据监控 |
| 支持主机设备的TCP/UDP网络连接状态监控 |
| 服务器/小机 | 支持Windows全系列主机和服务器、Linux全系列主机和服务器、AIX主机和服务器、HP-UX主机和服务器、Solaris主机和服务器 |
| 支持以上服务器的节点状态、CPU利用率、内存利用率、虚拟内存/SWAP、磁盘利用率、磁盘IO、网络连接、登录用户、运行时间、服务、运行进程等数据采集以及监控 |
| 应用监控 | 支持对Apache、IIS、Nginx等WEB应用运行性能参数的监控 |
| 支持对Oracle、MS SQL、MySQL数据库关键运行参数的监控 |
| 支持对WebLogic、WebSphere、Tomcat关键运行数据的监控 |
| 历史曲线 | 支持所有监控参数的历史数据查询 |
| 支持所有监控参数数据的1年内的数据查询 |
| 支持用户自定义时间段的历史数据查询 |
| 机房动环监控 | ★支持机房视频动环监控数据接入 |
| ★定制化监控 | 对现有网络所有可管理的IP设备进行统一的监控管理，各类应用及业务系统进行集中监控，需要对特殊应用进行定制化开发及达到监控的效果。 |
| 监控视图 | ★监控雷达 | 支持雷达扫描器 |
| 雷达扫描可以直观显示所监控的节点及正常与否 |
| 提供监控告警类型显示以及声音告警提示 |
| 节点视图 | 提供监控节点的设备类型、系统类型、运行服务状态的直观试图 |
| 提供节点运行正常率的最差TOP10排名 |
| 提供节点CPU、Memory、Disk的使用率的排名 |
| ★机柜视图 | 以设备实际面板图方式显示机柜实际布局 |
| 机柜内设备运行状态直观显示功能 |
| ★网络接口视图 | 真实的显示设备的网络接口 |
| 提供设备网络接口的状态、流量、收发错包/丢包直观显示 |
| **以上内容投标文件中提供产品截图** |
| 日志管理 | 支持设备 | 支持网络设备（交换机、路由器），安全设备（防火墙）系统日志管理。 |
| 支持Windows全系列主机和Linux/Unix全系列主机日志的管理 |
| 采集方式 | 日志采集方法支持Syslog、Syslog-ng、Windows Logs |
| 管理功能 | 支持自定义日志自动移除功能 |
| 内置丰富的日志告警规则，支持自定义日志告警规则。 |
| 支持日志实时告警功能 |
| 所采集日志可以按主机、时间、告警级别自动备份 |
| 统计图表 | 可按任意指定时间、指定设备、指定事件/告警类型等条件组合查询日志 |
| 提供日志告警级别的统计比例饼形图 |
| 提供日志告警主机的TopN图表 |
| 可按指定条件生成主机事件、日期、告警级别、告警事件来源、告警事件类型的统计图表 |
| 资产管理 | ★合同管理 | 支持合同管理 |
| 支持设备与合同的关联 |
| 维保折旧 | 支持设备的维保管理，具有维保到期提醒功能。 |
| 支持资产折旧管理 |
| ★二维码管理 | 支持设备二维码标签管理 |
| 通过智能手机扫描二维码可以查看设备的信息及状态，可以进行设备信息配置以及进行资产盘点。 |
| **以上内容投标文件中提供产品截图** |
| ★机房资产 | 支持机房机架物理拓扑显示，用户可以直观地看到每个机架上的每台设备的运行状态；可以看到设备的真实面板图。 |
| 支持通过鼠标拖动进行机柜内设备布局信息的调整 |
| **以上内容投标文件中提供产品截图** |
| 查询及图表 | 可按设备类型、品牌型号、存放位置、业务归属、管理归属、维保状态等信息进行查询 |
| 支持生成设备的使用状态、品牌分类、维保状态、业务归属、采购日期等图表 |
| 运维辅助 | IP地址管理 | 提过IP地址资源分配管理 |
| 提供IP地址使用历史回溯功能 |
| 可以对IP地址分配、使用数据生成Excel或PDF格式的统计报表 |
| 故障管理 | 支持对于运维中的故障问题记录、分类、统计功能 |
| 支持自定义故障级别 |
| 支持自定义故障分类 |
| 可以按时间周期、故障级别、故障类型提供故障记录的图表分析 |
| 提供故障记录的生成PDF格式文档并下载 |
| 运维文档管理 | 能够实现对运维文档的WEB管理 |
| 可以在线编辑、上传、下载运维技术文档 |
| 支持常用文档格式（WORD、EXCEL、PDF、JPG等） |
| 运维通讯录 | 支持运维应急通信录功能 |
| 通信录按公司划分 |
| 诊断工具 | 支持Ping和traceroute网络连通性诊断工具 |
| 拓扑管理 | ★拓扑功能 | 支持全网注册设备拓扑自动发现 |
| 支持多层次网络拓扑结构图 |
| 支持拖拽进行设备拓扑布局 |
| 支持托拽直接完成设备链路连接 |
| 支持端口流量数据映射到链路连接上，实时显示链路流量数据或占用情况并能够显示最近4小时变化量曲线图。 |
| 支持直观显示设备监控及性能监控状态，并以不同颜色进行显示（在线设备为绿色显示、非在线设备为红色显示）。 |
| 支持显示设备互联端口以及流量来源端口 |
| **以上内容投标文件中提供产品截图** |
| 拓扑配置 | 用户可以自定义、编辑、修改业务拓扑图，业务拓扑的元素包括主机、网络设备、安全设备、数据库、中间件、各种类型的服务和应用。 |
| 拓扑融合 | 通过点击拓扑中的设备，可直接进入对应设备流量汇总列表页面。 |
| 通过点击拓扑中的链路，可选择进入对应链路最近四小时、最近一周、最近一月的流量报表页面。 |
| 告警管理 | 监控告警 | 支持监控主机/设备的在线监控告警 |
| 支持各项性能监控数据的阀值监控告警 |
| 支持日志告警 |
| 告警方式 | 支持自定义告警分组 |
| 支持EMAIL、声音、短信告警方式 |
| ★告警记录 | 记录全部的告警事件 |
| 可以提供告警的发生时间、恢复时间信息 |
| 提供运维人员对于告警的确认以及处理记录功能 |
| **以上内容投标文件中提供产品截图** |
| 报告报表 | 报告报表 | 支持自动定义生成报告报表功能 |
| 可针对节点生成全数据统计报告 |
| 可生成节点运行可用性、节点资源利用率的统计报告 |
| 可生成资产数据统计报告 |
| 可生成告警报告文档 |
| 提供报告下载功能 |
| 服务 | 部署服务 | 提供产品安装、部署服务以及使用指导服务 |
| ★升级服务 | 提供三年免费升级并提供终身免费日常维护指导（自货物交采购人验收合格之日起起算） |
| 定制开发 | 可以按用户业务特点以及需求定制开发所需功能，如项目需要，提供驻场开发服务。 |
| 在线支持 | 提供电子邮件技术支持服务和QQ在线技术支持 |
| 其他 | ★证书 | 签订合同时提供原厂免费3年质保函（自货物交采购人验收合格之日起起算） |

**19.FC光模块**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 硬件指标 | 16Gb SFP+SW XCVR 模块 |

**20.千兆光模块**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 硬件指标 | SFP千兆模块(850nm，300m，LC) |

**21.入侵防御系统1**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 资质 | 厂商具有信息安全管理体系认证证书**（投标文件中提供复印件）** |
| 产品具有计算机信息系统安全专用产品销售许可证**（投标文件中提供复印件）** |
| ★厂商为国家级网络安全应急服务支撑单位**（投标文件中提供证明材料，如CNCERT网站截图）** |
| ★厂商为中国国家信息安全漏洞库（CNNVD）一级技术支撑单位**（投标文件中提供证明材料）** |
| 规格 | 标准2U专用万兆硬件平台 |
| 硬件架构 | 多核网络专用架构，使用64位MIPS多核处理器，非X86的多核架构或ASIC架构。 |
| 产品结构 | 最大功率≤300W，支持2对硬件接口Bypass，在设备断电、重启时，可自动切换到Bypass状态，当设备恢复时，可自动切换回工作状态。 |
| 网口数量 | 12\*GE电口，12\*SFP光口，4\*万兆光口，支持千兆光接口数量≥12，千兆接口总数≥24个，支持万兆光接口数量≥4，接口无路由/交换/LAN/WAN等固化区分，均可作为二三层接口使用。 |
| ★电源 | 内置双电源 |
| 性能 | 设备最大吞吐量≥40Gbps |
| 每秒新建连接数≥70万 |
| 最大并发连接数≥700万 |
| IPSec VPN隧道数≥1024 |
| SSL VPN接入数≥1500 |
| IPSec VPN性能≥4.8G |
| IPS吞吐量≥22G |
| 部署模式 | 支持路由模式、透明（网桥）模式、混模式，支持将多个物理网口加入一个网桥中，部署模式切换无需重启设备，支持镜像和被镜像。 |
| ★DDNS | 支持动态域名绑定功能 |
| NAT | 支持源地址转换、目的地址转换、双向地址转换、NAT44 |
| 路由支持 | 支持静态路由、策略路由、动态路由、ISP路由；策略路由支持七元组策略，动态路由支持RIP、OSPF等，ISP路由支持运营商地址自定义**（投标文件中提供web配置界面截图）。** |
| VRF | ★接口默认属于root，创建VRF后可把接口添加到VRF内，一个接口只能属于一个VRF。 |
| 不同vrf下的接口可以配置相同的ip地址 |
| ★支持vrf的静态路由 |
| 链路聚合 | 透明、路由模式下支持将多条链路带宽进行捆绑 |
| 安全域 | 支持将多个接口加入安全域中，并可对域内接口访问权限进行控制。 |
| 虚拟网线 | 支持设置虚拟网线透传并解析带VLAN TAG的报文 |
| 4G支持 | ★支持4G扩展网卡，支持在4G接口上运行IPSec VPN**（投标文件中提供web配置界面截图）。** |
| IPv6 | 支持IPv6环境，可创建IPv6地址和地址范围，支持展示地址对象被引用次数。 |
| 支持基于源和目的地址过滤IPv6地址和地址组，可选择时间、端口、接口、安全域等条件。 |
| ★支持针对IPv6内容进行管理和防护，包括应用、URL、入侵攻击、病毒行为等内容，IPv6应用策略支持选择全匹配或顺序匹配规则，可精细化管理应用的使用动作，针对社区类型，支持管控“上传”、“发表”、“浏览”、“登陆”等动作。 |
| ★支持IPv6数据包安全检测机制，可有效防御异常包攻击。 |
| 支持NAT64 |
| 安全通信 | 实际配置支持一对一、多对一、多对多等多种形式的NAT，支持H.323等应用协议ALG。 |
| 实际配置支持基于用户、应用、时间对象的流量管控和策略设置 |
| ★接口实际配置支持second IP地址，每个接口要求支持至少200个second IP**（投标文件中提供web配置截图）。** |
| ★至少支持telnet、ftp、imap、pop3、smtp、rlogin、http、oracle、mysql、postgres等10种常见协议的防暴力破解功能，针对每种协议可自定义检测时长、阈值和阻断时长**（投标文件中提供web截图）。** |
| ★支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口，支持通过流量自学习能获得服务器合法的外联行为，检测流量中的异常访问流量，可以自动拦截。学习时长可选择1小时、12小时、一天、一周等**（投标文件中提供web截图）。** |
| 入侵防御 | 支持基于源、目的、规则集的入侵检测 |
| 支持5种自定义动作 |
| 可记录攻击日志和报警 |
| 特征库库支持手动升级和自动升级 |
| ★支持自定义IPS特征，至少支持IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等8种协议自定义入侵攻击特征，可拓展协议字段，设置数据包中的匹配内容，支持选择包含、等于、不等于、大于、正则匹配等匹配方式，可选择多种匹配条件，支持设置“与”和“或”的匹配顺序**（投标文件中提供web界面配置截图）。** |
| 支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者syslog告警，不同告警规则可以发送给不同的用户**（投标文件中提供web界面配置截图）。** |
| ★系统定义超过4000+条主流攻击规则，包含Backdoor、bufferoverflow、dos、im、p2p、vulnerability、scan、webcgi、worm。 |
| 查杀邮件正文/附件、网页及下载文件中包含的病毒 |
| ★支持200万余种病毒的查杀，病毒库定期与及时更新。 |
| 支持启发式扫描查杀未知病毒 |
| ★支持ZIP/RAR等压缩文件的病毒查杀，默认支持检测到5层，最大可检测到20层**（投标文件中提供web界面配置截图）。** |
| 支持TAR等多种打包文件的病毒查杀 |
| ★支持HTTP协议的精确访问控制，可针对IP、URL、Method、Referer、User-Agent、Cookie、Url-args等字段设置内容，匹配内容包括但不少于：包括、不包含、等于、不等于、属于、不属于、长度小于、长度等于、长度大于、正则匹配等，日志级别包括但不少于：不记录、危急、告警、严重、错误、警告、通知、信息等**（投标文件中提供web界面配置截图）。** |
| ★支持防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护，应用隐藏可隐藏Server信息、X-Powered-By信息、替换客户端出错页面(4xx)、替换服务器端出错页面(5xx)等**（投标文件中提供web截图）。** |
| 支持网页防篡改，可手动清理缓存内容。 |
| 端口扫描 | ★支持针对IP、IP段进行端口扫描，可选择立即执行或定期执行，支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功能**（投标文件中提供web截图）。** |
| 弱口令扫描 | ★支持弱口令扫描功能，可针对IP和IP段对象做弱口令检测、空密码检测、用户名和密码相同检测，扫描任务可设置立即扫描或定期扫描，弱口令字典可自定义设置**（投标文件中提供web截图）。** |
| IPSec VPN | 实际配置支持IPSec VPN接入，内置VPN硬件协处理器 |
| 实际配置支持DES、3DES、AES加密算法**（投标文件中提供截图）。** |
| ★IPSec VPN支持第三方对接和快速配置，自有设备对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址，支持配置国密**（投标文件中提供web界面配置截图）。** |
| HA可同步IPSec VPN状态，当HA主备切换时无需VPN重建。 |
| 支持统计隧道持续时间，支持统计隧道流量。 |
| 支持用户强制下线 |
| 支持IPSec VPN链路备份功能，未运行的VPN隧道不接收，不发送报文。 |
| ★支持IPSec VPN连接断开邮件告警 |
| 支持移动终端IPSec VPN拨入 |
| SSL VPN | 支持自定义资源类型，可定义发布的协议和端口，资源支持导入导出，可快速完成配置，支持自定义门户页面中的标题、logo和公告内容。 |
| 支持SSL VPN用户防暴力破解功能，可根据用户和IP设置防护阈值。 |
| 支持SSL VPN账号与VPN资源唯一绑定，针对拨入用户设置拨入时间段和强制下线时间，精细管控用户访问权限。 |
| 应用协议识别 | 支持主流P2P、IM、在线视频、网络游戏、网络炒股等应用识别，可识别应用数大于3500种 |
| 支持BYOD特征库，可识别iOS版和安卓版移动互联网软件如微博、微信等特征**（投标文件中提供web界面配置截图）；** |
| 支持基于端口、协议等自定义服务 |
| 应用特征库可提供在线升级和手动升级 |
| 支持自定义应用，可基于协议、端口、IP、域名等维度定义未知应用，支持指定应用组。 |
| ★支持智能和快速识别模式配置**（投标文件中提供web界面配置截图）** |
| 支持自定义URL过滤，并支持URL的模糊匹配**（投标文件中提供web界面配置截图）。** |
| 可广泛识别恶意网站、违法网站 |
| SSL加密内容审计 | 支持HTTPS解密功能，支持管理界面及命令行配置解密策略，包括入接口、源地址对象、目的地址对象、https对象、域名排除等；支持HTTPS域名库，预定义域名以及自定义域名。 |
| ★支持审计HTTPS加密邮箱，支持审计主题、内容、附件等，支持本地下载邮件原件。 |
| 支持针对HTTPS网站、HTTPS门户搜索等内容进行审计 |
| 流量管理 | 支持通道化的QoS，支持基于源地址、用户、服务、应用、时间进行带宽控制，并支持配置保障带宽、限制带宽、带宽借用、每IP带宽、每用户带宽、带宽优先级等QoS动作，时间选择支持基于日计划、周计划、单次计划等。 |
| 支持4级层次化QoS、支持多级用户/用户组嵌套。 |
| ★支持日流量限额、时长限额，超过阈值提供弹窗提示且可自定义，支持流量和时长的月限额**（投标文件中提供web界面截图）。** |
| ★支持流量惩罚通道和限速通道**（投标文件中提供web界面截图）** |
| 支持应用、用户流量统计，应用流量支持趋势图、饼状图呈现，可查看某一应用的流量趋势图和其Top流量用户。 |
| 会话管理 | 支持进行IP、整机会话限制和新建会话限制**（投标文件中提供web界面配置截图）** |
| 支持会话源目标、目的目标排名统计，实时显示当前会话会话数和历史1小时、1天、1周会话数**（投标文件中提供web界面截图）。** |
| ★会话监控界面展示全部会话数信息，显示会话属性至少包含用户、用户组、源地址、源端口、目的地址、目的端口、协议、类型、应用、策略ID、发送包数、接收包数、总包数、发送流量、接收流量、总流量、会话状态、本地连接、策略动作、创建时间、超时时间、存在时间、入接口、出接口、源NAT地址、源NAT端口、目的NAT地址、目的NAT端口等25项，并且可根据任意条件进行查询和排序**（投标文件中提供web界面截图）。** |
| 防私接路由 | ★可识别私接主机个数，并可制定策略分别设置私接终端类型个数为阀值进行封堵，支持自定义阻断时间，同时支持基于IP及IP段配置白名单**（投标文件中提供web界面配置截图）。** |
| 支持识别和封堵360随身wifi、猎豹wifi、无线路由器等软硬件网络共享方式 |
| 支持私接用户的PPPoE账号展现**（投标文件中提供web界面配置截图）** |
| 支持状态监控、解锁操作 |
| 支持基于用户、MAC、终端数量的监控和搜索 |
| 用户认证功能 | ★支持WEB Portal认证功能，支持本地认证、Radius认证、LDAP认证 和LDAP用户同步，支持对接IMC、AAS、SAM等常见AAA服务器，支持配置强制重新认证间隔，支持配置认证通过后重定向URL，要求本机自身支持短信认证功能**（投标文件中提供web界面配置截图）。** |
| 支持portal服务器联动，支持radius服务器联动，支持实现NAS-Identifier(32)在无线场景携带AC名字。 |
| 支持认证页面自定义，支持免责声明。 |
| 支持针对HTTPS网页推送portal页面 |
| 支持伪portal推送抑制 |
| ★支持微信认证功能，使用微信连WiFi2.0接口，限制微信流量放通（pc和移动端，认证通过放通），支持基于http获取access\_token，支持微信内部浏览器http弹portal，强制关注功能（定时检查用户是否关注公众号）**（投标文件中提供web界面配置截图）。** |
| 支持短信认证，登录后方可认证上网 |
| 支持AD域单点登录 |
| 支持认证用户有效期限制 |
| 支持临时用户策略，当次登录有效**（投标文件中提供web界面配置截图）。** |
| 支持混合认证，支持界面配置选择多种认证方式，用户可根据需要更换认证方式。 |
| 用户管理 | 支持同步LDAP用户，支持标准AD服务器和OPEN LDAP服务器的用户导入，支持针对同步的用户和用户组配置策略。 |
| 支持用户树形组织架构显示，快速统计当前用户用组包含的用户数。 |
| ★支持创建临时用户，能够指定用户有效时间。 |
| 支持用户批量操作功能，可选择当前页和所有用户进行删除和移动，支持一键删除所有的用户，用户组，支持批量修改用户密码、批量启用/禁用用户。 |
| 支持强制用户首次登录修改密码 |
| ★支持模糊搜索用户名、用户组名 |
| 为统一维护、统一管理，需与入侵防御系统2同一品牌。 |
| 应用缓存 | ★支持文件缓存，支持安卓和IOS形式的文件，文件形式不限于视频、APP、文本文件等。 |
| ★支持自学习性缓存，设备可自动缓存特定服务器的所有终端应用。 |
| 支持模糊匹配 |
| 服务质量管理 | 支持PING、TCP、DNS探测 |
| 支持接口探测、域名探测 |
| ★支持统计探测目标的成功率和延时，方便运维人员清晰的了解网络运行状态。 |
| 支持自定义间隔时间探测 |
| 广告推送 | ★支持配置在用户上网时弹出广告页面，支持本地和第三方广告**（投标文件中提供web配置截图）。** |
| 支持配置广告跳转链接和广告推送间隔 |
| ★支持PC端推送4个方位的广告，手机端支持推送全屏广告。 |
| 链路负载均衡 | ★支持7元组的链路负载均衡策略 |
| ★支持基于域名的负载均衡策略 |
| 基于支持直连网段和特定网段的负载均衡排除 |
| 负载均衡接口支持pppoe，dhcp，链路聚合，物理接口等三层接口。 |
| 基于源地址hash的链路负载均衡 |
| 服务器负载均衡 | ★支持5元组的负载均衡策略 |
| 负载算法支持权重、源地址散列+权重 |
| 支持服务器健康检查和会话保持 |
| DNS透明代理 | ★支持基于优先级、权重、流量的DNS透明代理，支持DNS负载均衡。 |
| ★支持静态域名配置，支持特定域名特定DNS服务器解析，静态域名和特定域名支持模糊匹配。 |
| 支持DNS域名匹配顺序 |
| 支持DNS透明代理缓存管理 |
| 双机热备 | 支持双机热备，支持主主模式、主备模式，支持同步配置、会话、运行状态、VPN状态、特征库，支持配置抢占模式和抢占延时，支持配置HA监控接口。 |
| 支持地址代理 |
| 支持非对称路由 |
| 配置管理 | 支持本地中英文Web界面管理及命令行管理，支持基于SSL协议的远程安全管理。 |
| 支持通过管理平台进行集中管理，统一升级，下发配置，收集日志。 |
| ★支持U盘零配置上线，设备端无需预配置，将U盘插入设备USB接口中，即可实现快速上线实施，配置文件内容支持加密，支持按需升级系统版本，可自动快速升级系统版本，支持导入多份配置文件，用于业务需求，变更业务运行，保障可靠性。 |
| ★支持多配置切换，配置文件之间相对独立，灾备场景可快速恢复业务，保障业务正常运行。 |
| PKI | 支持X.509 V3数字证书，支持CER/PEM/PKCS12多种证书编码。 |
| 支持内置CA，为其他设备或移动用户签发证书。 |
| 支持本地CA根证书、根私钥的更新 |
| 支持在线CRL列表 |
| 系统维护 | ★web管理界面支持Ping、Traceroute、TCP Syn诊断工具，可支持基于接口、协议、IP地址、端口、应用进行网络抓包，并可下载导出分析**（投标文件中提供web界面配置截图）。** |
| ★支持三权管理方式，包括账号管理员、权限管理员、审核员，各管理员权限制约，权限管理员支持分配权限，可细致分配界面中每一个模块的读写权限。 |
| 支持设备管理端口的自定义，包括HTTPS、HTTP、TELNET、SSH等常用管理方式的端口。 |
| ★支持管理员双因子认证 |
| 支持命令行、Web界面管理 |
| SNMP | ★支持v1、v2、v3版本，支持跨三层自学习MAC地址，支持IP和MAC绑定。 |
| 系统日志 | 支持本地日志记录和远程日志输出，支持专用的日志审计管理软件。 |
| 业务告警 | 支持针对设备健康状态，业务信息等维度告警，支持预设告警阀值，告警日志支持导出。 |
| ★告警事件支持邮件方式 |
| 统计报表 | 支持统计设备健康状态、用户行为、网络质量、网络安全等报表**（投标文件中提供web页面截图）** |
| 支持HTML、PDF等报表格式，并可通过邮件、FTP等方式外发。 |
| 支持丰富的用户行为数据统计 |
| 服务要求 | 不少于免费3年原厂质保服务（自货物交采购人验收合格之日起起算） |
| 不少于免费3年原厂7\*24小时上门现场服务支持（自货物交采购人验收合格之日起起算） |
| 原厂工程师实施及提供设备相关的培训，提供原厂产品培训1天。 |
| 提供原厂常驻浙江省内不少于7个经中国信息安全测评中心认证的注册信息安全专业人员-云安全工程师（CISP-CSE）（投标文件中提供证书复印件），以便提供快速的售后服务。 |

**22.入侵防御系统2**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 资质 | 厂商具有信息安全管理体系认证证书**（投标文件中提供复印件）** |
| 产品具有计算机信息系统安全专用产品销售许可证**（投标文件中提供复印件）** |
| ★厂商为国家级网络安全应急服务支撑单位**（投标文件中提供证明材料，如CNCERT网站截图）** |
| ★厂商为中国国家信息安全漏洞库（CNNVD）一级技术支撑单位**（投标文件中提供证明材料）** |
| 规格 | 标准2U专用万兆硬件平台 |
| 硬件架构 | 多核网络专用架构，使用64位MIPS多核处理器，非X86的多核架构或ASIC架构。 |
| 产品结构 | 最大功率≤300W，支持2对硬件接口Bypass，在设备断电、重启时，可自动切换到Bypass状态，当设备恢复时，可自动切换回工作状态。 |
| 网口数量 | 12\*GE电口，12\*SFP光口，4\*万兆光口，支持千兆光接口数量≥12，千兆接口总数≥24个，支持万兆光接口数量≥4，接口无路由/交换/LAN/WAN等固化区分，均可作为二三层接口使用。 |
| ★电源 | 内置双电源 |
| 性能 | 设备最大吞吐量≥20Gbps |
| 每秒新建连接数≥50万 |
| 最大并发连接数≥500万 |
| IPSec VPN隧道数≥1024 |
| SSL VPN接入数≥1500 |
| IPSec VPN性能≥2G |
| IPS吞吐量≥12G |
| 部署模式 | 支持路由模式、透明（网桥）模式、混模式，支持将多个物理网口加入一个网桥中，部署模式切换无需重启设备，支持镜像和被镜像。 |
| ★DDNS | 支持动态域名绑定功能 |
| NAT | 支持源地址转换、目的地址转换、双向地址转换、NAT44 |
| 路由支持 | 支持静态路由、策略路由、动态路由、ISP路由，策略路由支持七元组策略，动态路由支持RIP、OSPF等，ISP路由支持运营商地址自定义**（投标文件中提供web配置界面截图）。** |
| VRF | ★接口默认属于root，创建VRF后可把接口添加到VRF内，一个接口只能属于一个VRF。 |
| 不同vrf下的接口可以配置相同的ip地址 |
| ★支持vrf的静态路由 |
| 链路聚合 | 透明、路由模式下支持将多条链路带宽进行捆绑 |
| 安全域 | 支持将多个接口加入安全域中，并可对域内接口访问权限进行控制。 |
| 虚拟网线 | 支持设置虚拟网线透传并解析带VLAN TAG的报文 |
| 4G支持 | ★支持4G扩展网卡，支持在4G接口上运行IPSec VPN**（投标文件中提供web配置界面截图）。** |
| IPv6 | 支持IPv6环境，可创建IPv6地址和地址范围，支持展示地址对象被引用次数。 |
| 支持基于源和目的地址过滤IPv6地址和地址组，可选择时间、端口、接口、安全域等条件。 |
| ★支持针对IPv6内容进行管理和防护，包括应用、URL、入侵攻击、病毒行为等内容，IPv6应用策略支持选择全匹配或顺序匹配规则，可精细化管理应用的使用动作，针对社区类型，支持管控“上传”、“发表”、“浏览”、”登陆“等动作。 |
| ★支持IPv6数据包安全检测机制，可有效防御异常包攻击。 |
| 支持NAT64 |
| 安全通信 | 实际配置支持一对一、多对一、多对多等多种形式的NAT，支持H.323等应用协议ALG。 |
| 实际配置支持基于用户、应用、时间对象的流量管控和策略设置 |
| ★接口实际配置支持second IP地址，每个接口要求支持至少200个second IP**（投标文件中提供web配置截图）。** |
| 内网资产监控 | ★支持内网资产自动发现功能，可以显示内网资产的风险级别、IP、操作系统、浏览器、应用杀毒软件、服务等属性**（投标文件中提供web截图）。** |
| 安全防护 | 支持IPv4、IPv6双协议栈异常包防御，至少包含：Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP选项、IP Spoof、Jolt2等。 |
| ★至少支持telnet、ftp、imap、pop3、smtp、rlogin、http、oracle、mysql、postgres等10种常见协议的防暴力破解功能，针对每种协议可自定义检测时长、阈值和阻断时长**（投标文件中提供web截图）。** |
| ★支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口，支持通过流量自学习能获得服务器合法的外联行为，检测流量中的异常访问流量，可以自动拦截，学习时长可选择1小时、12小时、一天、一周等**（投标文件中提供web截图）。** |
| 入侵防御 | 支持基于源、目的、规则集的入侵检测 |
| 支持5种自定义动作 |
| 可记录攻击日志和报警 |
| 特征库库支持手动升级和自动升级 |
| ★支持自定义IPS特征，至少支持IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等8种协议自定义入侵攻击特征，可拓展协议字段，设置数据包中的匹配内容，支持选择包含、等于、不等于、大于、正则匹配等匹配方式，可选择多种匹配条件，支持设置“与”和“或”的匹配顺序**（投标文件中提供web界面配置截图）。** |
| ★支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者syslog告警，不同告警规则可以发送给不同的用户**（投标文件中提供web界面配置截图）。** |
| ★系统定义超过4000+条主流攻击规则，包含Backdoor、bufferoverflow、dos、im、p2p、vulnerability、scan、webcgi、worm。 |
| 查杀邮件正文/附件、网页及下载文件中包含的病毒 |
| ★支持200万余种病毒的查杀，病毒库定期与及时更新。 |
| 支持启发式扫描查杀未知病毒 |
| ★支持ZIP/RAR等压缩文件的病毒查杀，默认支持检测到5层，最大可检测到20层**（投标文件中提供web界面配置截图）。** |
| 支持TAR等多种打包文件的病毒查杀 |
| ★支持HTTP协议的精确访问控制，可针对IP、URL、Method、Referer、User-Agent、Cookie、Url-args等字段设置内容，匹配内容包括但不少于：包括、不包含、等于、不等于、属于、不属于、长度小于、长度等于、长度大于、正则匹配等，日志级别包括但不少于：不记录、危急、告警、严重、错误、警告、通知、信息等**（投标文件中提供web界面配置截图）。** |
| ★支持防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护，应用隐藏可隐藏Server信息、X-Powered-By信息、替换客户端出错页面(4xx)、替换服务器端出错页面(5xx)等**（投标文件中提供web截图）。** |
| 支持网页防篡改，可手动清理缓存内容 |
| 端口扫描 | ★支持针对IP、IP段进行端口扫描，可选择立即执行或定期执行，支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功能**（投标文件中提供web截图）。** |
| 弱口令扫描 | ★支持弱口令扫描功能，可针对IP和IP段对象做弱口令检测、空密码检测、用户名和密码相同检测，扫描任务可设置立即扫描或定期扫描，弱口令字典可自定义设置**（投标文件中提供web截图）。** |
| IPSec VPN | 实际配置支持IPSec VPN接入，内置VPN硬件协处理器 |
| 实际配置支持DES、3DES、AES加密算法**（投标文件中提供截图）** |
| ★IPSec VPN支持第三方对接和快速配置，自有设备对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址，支持配置国密**（投标文件中提供web界面配置截图）。** |
| HA可同步IPSec VPN状态，当HA主备切换时无需VPN重建。 |
| 支持统计隧道持续时间，支持统计隧道流量。 |
| 支持用户强制下线 |
| 支持IPSec VPN链路备份功能，未运行的VPN隧道不接收，不发送报文。 |
| ★支持IPSec VPN连接断开邮件告警 |
| 支持移动终端IPSec VPN拨入 |
| SSL VPN | 支持自定义资源类型，可定义发布的协议和端口，资源支持导入导出，可快速完成配置，支持自定义门户页面中的标题、logo和公告内容。 |
| 支持SSL VPN用户防暴力破解功能，可根据用户和IP设置防护阈值。 |
| 支持SSL VPN账号与VPN资源唯一绑定，针对拨入用户设置拨入时间段和强制下线时间，精细管控用户访问权限。 |
| 应用协议识别 | 支持主流P2P、IM、在线视频、网络游戏、网络炒股等应用识别，可识别应用数大于3500种 |
| 支持BYOD特征库，可识别iOS版和安卓版移动互联网软件如微博、微信等特征**（投标文件中提供web界面配置截图）。** |
| 支持基于端口、协议等自定义服务 |
| 应用特征库可提供在线升级和手动升级 |
| 支持自定义应用，可基于协议、端口、IP、域名等维度定义未知应用，支持指定应用组。 |
| ★支持智能和快速识别模式配置**（投标文件中提供web界面配置截图）** |
| 支持自定义URL过滤，并支持URL的模糊匹配**（投标文件中提供web界面配置截图）。** |
| 可广泛识别恶意网站、违法网站 |
| SSL加密内容审计 | 支持HTTPS解密功能，支持管理界面及命令行配置解密策略，包括入接口、源地址对象、目的地址对象、https对象、域名排除等，支持HTTPS域名库，预定义域名以及自定义域名。 |
| ★支持审计HTTPS加密邮箱，支持审计主题、内容、附件等，支持本地下载邮件原件。 |
| 支持针对HTTPS网站、HTTPS门户搜索等内容进行审计 |
| 流量管理 | 支持通道化的QoS，支持基于源地址、用户、服务、应用、时间进行带宽控制，并支持配置保障带宽、限制带宽、带宽借用、每IP带宽、每用户带宽、带宽优先级等QoS动作，时间选择支持基于日计划、周计划、单次计划等。 |
| 支持4级层次化QoS、支持多级用户/用户组嵌套 |
| ★支持日流量限额、时长限额，超过阈值提供弹窗提示且可自定义，支持流量和时长的月限额**（投标文件中提供web界面截图）。** |
| ★支持流量惩罚通道和限速通道**（投标文件中提供web界面截图）** |
| 支持应用、用户流量统计，应用流量支持趋势图、饼状图呈现，可查看某一应用的流量趋势图和其Top流量用户。 |
| 会话管理 | 支持进行IP、整机会话限制和新建会话限制**（投标文件中提供web界面配置截图）** |
| 支持会话源目标、目的目标排名统计，实时显示当前会话会话数和历史1小时、1天、1周会话数**（投标文件中提供web界面截图）。** |
| ★会话监控界面展示全部会话数信息，显示会话属性至少包含用户、用户组、源地址、源端口、目的地址、目的端口、协议、类型、应用、策略ID、发送包数、接收包数、总包数、发送流量、接收流量、总流量、会话状态、本地连接、策略动作、创建时间、超时时间、存在时间、入接口、出接口、源NAT地址、源NAT端口、目的NAT地址、目的NAT端口等25项，并且可根据任意条件进行查询和排序**（投标文件中提供web界面截图）。** |
| 防私接路由 | ★可识别私接主机个数，并可制定策略分别设置私接终端类型个数为阀值进行封堵，支持自定义阻断时间，同时支持基于IP及IP段配置白名单**（投标文件中提供web界面截图）。** |
| 支持识别和封堵360随身wifi、猎豹wifi、无线路由器等软硬件网络共享方式 |
| 支持私接用户的PPPoE账号展现**（投标文件中提供web界面截图）** |
| 支持状态监控、解锁操作 |
| 支持基于用户、MAC、终端数量的监控和搜索 |
| 用户认证功能 | ★支持WEB Portal认证功能，支持本地认证、Radius认证、LDAP认证和LDAP用户同步，支持对接IMC、AAS、SAM等常见AAA服务器，支持配置强制重新认证间隔，支持配置认证通过后重定向URL，本机自身支持短信认证功能**（投标文件中提供web界面配置截图）。** |
| 支持portal服务器联动，支持radius服务器联动，支持实现NAS-Identifier(32)在无线场景携带AC名字。 |
| 支持认证页面自定义，支持免责声明。 |
| 支持针对HTTPS网页推送portal页面 |
| 支持伪portal推送抑制 |
| ★支持微信认证功能，使用微信连WiFi2.0接口，限制微信流量放通（pc和移动端，认证通过放通），支持基于http获取access\_token，支持微信内部浏览器http弹portal，强制关注功能（定时检查用户是否关注公众号）**（投标文件中提供web界面配置截图）。** |
| 支持短信认证，登录后方可认证上网。 |
| 支持AD域单点登录 |
| 支持认证用户有效期限制 |
| 支持临时用户策略，当次登录有效**（投标文件中提供web界面配置截图）。** |
| 支持混合认证，支持界面配置选择多种认证方式，用户可根据需要更换认证方式。 |
| 用户管理 | 支持同步LDAP用户，支持标准AD服务器和OPEN LDAP服务器的用户导入，支持针对同步的用户和用户组配置策略。 |
| 支持用户树形组织架构显示，快速统计当前用户用组包含的用户数。 |
| ★支持创建临时用户，能够指定用户有效时间。 |
| 支持用户批量操作功能，可选择当前页和所有用户进行删除和移动，支持一键删除所有的用户，用户组，支持批量修改用户密码、批量启用/禁用用户。 |
| 支持强制用户首次登录修改密码 |
| ★支持模糊搜索用户名、用户组名 |
| 为统一维护、统一管理，需与数据库审计系统同一品牌。 |
| 应用缓存 | ★支持文件缓存，支持安卓和IOS形式的文件，文件形式不限于视频、APP、文本文件等。 |
| ★支持自学习性缓存，设备可自动缓存特定服务器的所有终端应用。 |
| 支持模糊匹配 |
| 服务质量管理 | 支持PING、TCP、DNS探测 |
| 支持接口探测、域名探测 |
| ★支持统计探测目标的成功率和延时，方便运维人员清晰的了解网络运行状态。 |
| 支持自定义间隔时间探测 |
| 广告推送 | ★支持配置在用户上网时弹出广告页面，支持本地和第三方广告**（投标文件中提供web配置截图）。** |
| 支持配置广告跳转链接和广告推送间隔 |
| ★支持PC端推送4个方位的广告，手机端支持推送全屏广告。 |
| 链路负载均衡 | ★支持7元组的链路负载均衡策略 |
| ★支持基于域名的负载均衡策略 |
| 基于支持直连网段和特定网段的负载均衡排除 |
| 负载均衡接口支持pppoe，dhcp，链路聚合，物理接口等三层接口。 |
| 基于源地址hash的链路负载均衡 |
| 服务器负载均衡 | ★支持5元组的负载均衡策略 |
| 负载算法支持权重、源地址散列+权重 |
| 支持服务器健康检查和会话保持 |
| DNS透明代理 | ★支持基于优先级、权重、流量的DNS透明代理，支持DNS负载均衡。 |
| ★支持静态域名配置，支持特定域名特定DNS服务器解析，静态域名和特定域名支持模糊匹配。 |
| 支持DNS域名匹配顺序 |
| 支持DNS透明代理缓存管理 |
| 双机热备 | 支持双机热备，支持主主模式、主备模式，支持同步配置、会话、运行状态、VPN状态、特征库，支持配置抢占模式和抢占延时，支持配置HA监控接口。 |
| 支持地址代理 |
| 支持非对称路由 |
| 配置管理 | 支持本地中英文Web界面管理及命令行管理，支持基于SSL协议的远程安全管理。 |
| 支持通过管理平台进行集中管理，统一升级，下发配置，收集日志。 |
| ★支持U盘零配置上线，设备端无需预配置，将U盘插入设备USB接口中，即可实现快速上线实施，配置文件内容支持加密，支持按需升级系统版本，可自动快速升级系统版本，支持导入多份配置文件，用于业务需求，变更业务运行，保障可靠性。 |
| ★支持多配置切换，配置文件之间相对独立，灾备场景可快速恢复业务，保障业务正常运行。 |
| PKI | 支持X.509 V3数字证书，支持CER/PEM/PKCS12多种证书编码。 |
| 支持内置CA，为其他设备或移动用户签发证书。 |
| 支持本地CA根证书、根私钥的更新 |
| 支持在线CRL列表 |
| 系统维护 | ★web管理界面支持Ping、Traceroute、TCP Syn诊断工具，可支持基于接口、协议、IP地址、端口、应用进行网络抓包，并可下载导出分析**（投标文件中提供web界面配置截图）。** |
| ★支持三权管理方式，包括账号管理员、权限管理员、审核员，各管理员权限制约；权限管理员支持分配权限，可细致分配界面中每一个模块的读写权限。 |
| 支持设备管理端口的自定义，包括HTTPS、HTTP、TELNET、SSH等常用管理方式的端口。 |
| ★支持管理员双因子认证 |
| 支持命令行、Web界面管理 |
| SNMP | ★支持v1、v2、v3版本，支持跨三层自学习MAC地址，支持IP和MAC绑定。 |
| 系统日志 | 支持本地日志记录和远程日志输出，支持专用的日志审计管理软件。 |
| 业务告警 | 支持针对设备健康状态，业务信息等维度告警，支持预设告警阀值，告警日志支持导出。 |
| ★告警事件支持邮件方式 |
| 统计报表 | 支持统计设备健康状态、用户行为、网络质量、网络安全等报表**（投标文件中提供web页面截图）** |
| 支持HTML、PDF等报表格式，并可通过邮件、FTP等方式外发。 |
| 支持丰富的用户行为数据统计 |
| 服务要求 | 不少于免费3年原厂质保服务（自货物交采购人验收合格之日起起算） |
| 不少于免费3年原厂7\*24小时上门现场服务支持（自货物交采购人验收合格之日起起算） |
| 原厂工程师实施及提供设备相关的培训，提供原厂产品培训1天。 |
| 提供原厂常驻浙江省内不少于6个经中国信息安全测评中心认证的注册信息安全专业人员-大数据安全分析师（CISP-BDSA）（投标文件中提供证书复印件），以便提供快速的售后服务。 |

**23.WEB应用防火墙**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 资质 | ★产品具有计算机信息系统安全专用产品销售许可证**（投标文件中提供复印件）** |
| ★产品具有IT产品信息安全认证证书**（投标文件中提供复印件）** |
| ★产品通过国家保密局检测中心检测并获得检测证书**（投标文件中提供证明材料）** |
| ★厂商具有信息技术产品安全测评证书（EAL3+）**（投标文件中提供复印件）** |
| 规格 | 标准2U专用千兆硬件平台，标配1+1冗余电源，电源可热插拔。 |
| 网口数量 | 标配：2\*GE电管理口，8\*工作口（4\*GE电口，4\*GE光口）。 |
| 扩展：工作口最大可扩展16\*GE光/电口 |
| 性能参数 | 应用吞吐量不小于4000Mbps，HTTP并发连接不小于30万，HTTP新建连接(CPS)不小于3万。 |
| 部署方式 | 透明桥部署：防护口不占用IP地址，实现完全透明部署，无需以先终结用户的TCP会话后再发起新的TCP会话到服务器方式处理，并支持路由不对称场景。 |
| 透明代理部署：防护口不占用IP地址，实现应用层透明部署，支持TCP连接复用，并优化服务器会话处理改善服务器处理性能。 |
| 端口镜像部署：镜像服务器流量即可实现安全审计和告警。 |
| ★反向代理部署：可支持代理和路由牵引两种模式，客户端源IP可采用透明和非透明两种转发机制，非透明可指定字段进行识别，支持前后端口分离，支持多台WAF设备冗余和集群部署**（投标文件中提供界面截图）。** |
| ★支持虚拟化部署，支持KVM、Xen、VMWare等虚拟机环境，并支持WAF镜像导入**（投标文件中提供公安部计算机信息系统安全产品质量监督检验中心检测报告）。** |
| 支持链路聚合，提升网络带宽、增加容错性和链路负载均衡。 |
| 支持VLAN子接口，业务口可承载多个VLAN通道。 |
| 高可用性 | 支持全透明集群模式、主-主模式、主备模式、硬件BYPASS、软件BYPASS。 |
| 保护对象 | 支持多条链路数据的防护，防护网段数量不限。 |
| 支持以域名和IP多种方式进行防护 |
| 支持ipv4/ipv6双协议栈 |
| WEB服务自发现 | ★支持WEB站点服务自动侦测功能，支持自动识别VLAN信息**（投标文件中提供界面截图）。** |
| 防御功能 | 能够识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括SQL注入、命令注入、Cookie注入、代码注入、LDAP注入、SSI注入文件注入等）、跨站请求伪造等应用攻击行为。 |
| 支持对HTTP请求分割攻击和HTTP响应报文截断攻击的防护 |
| 能够识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷 |
| 能基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力。 |
| 能识别网站中的网页木马程序，通过策略可防止木马网页被用户访问。 |
| 内置主流Webshell特征库，对上传内容进行检查，防止恶意Weshell上传。 |
| WAF能自动识别扫描器的扫描行为，并智能阻断如Nikto、Paros proxy、WebScarab、WebInspect、Whisker、libwhisker、Burpsuite、Wikto、Pangolin、Watchfire AppScan、N-Stealth、Acunetix Web Vulnerability Scanner等多种扫描器的扫描行为。 |
| 内置开源CMS漏洞和WEB服务器插件漏洞防护规则 |
| 支持阻断提交政冶敏感、违反法规相关的言论信息 |
| 支持丰富的自定义规则，可以针对多个条件组合，形成深度的WEB防护规则。 |
| 支持服务器隐藏，可配置删除服务器响应头信息。 |
| ★内置身份证、银行卡等服务器敏感信息库，对服务器响应敏感内容进行隐藏，并支持自定义**（投标文件中提供界面截图）。** |
| 支持Cookie安全机制，支持Cookie自学习，防止Cookie被篡改和劫持，并支持Cookie Httponly。 |
| 智能自学习功能 | 支持网站自学习建模功能，能通过自学习形成网站URL树，通过自学习能生成安全防护策略，通过自学习能发现参数的名称、类型、匹配频率，可配置匹配到自学习特征后放行，可配置匹配不到自学习特征直接阻断请求**（投标文件中提供界面截图）。** |
| 智能攻击者锁定 | 支持智能识别攻击者，对网站连接发起攻击的IP地址进行自动锁定禁止访问被攻击的网站，可配置攻击者识别策略和算法，可配置攻击者锁定时间，可配置将攻击者直接加入网络黑名单，可展示攻击者发生的时间和攻击者所在的地理位置**（投标文件中提供界面截图）。** |
| 基于时间的访问  控制 | 可基于时间对客户端IP进行黑白名单控制**（投标文件中提供界面截图）** |
| 防御动作 | 针对触发安全规则的行为进行阻断并发出告警页面 |
| 告警页面支持重定向至其它URL |
| 能将攻击者列入网络黑名单进行网络阻断该IP的访问 |
| 对攻击报文丢弃 |
| WEB访问行为合规 | ★可实现访问流程的校验，向网站提交表单前必须先访问指定的网页，并等待可配置的时间长度后才能正常提交表单**（投标文件中提供公安部计算机信息系统安全产品质量监督检验中心检测报告）。** |
| CC防护功能 | ★可根据URL、请求头字段、目标IP、请求方法等多种组合条件对CC攻击进行检测，检测指标为URL访问速率和URL访问集中度，可根据IP、IP+URL和IP+User\_Agent等算法对客户端进行检测，并支持应用层字段解析和自定义检测字段功能，支持挑战模式，支持基于地址位置的识别，支持对特定的IP地址进行CC规则白名单放行，支持CC慢攻击防护，通过学习业务流量模型，在业务流量异常时开启CC防护，并支持启动配置阈值**（投标文件中提供公安部计算机信息系统安全产品质量监督检验中心检测报告）。** |
| 地图态势分析 | ★按地理区域对攻击次数等进行统计，通过地图展示，并在地图上可以指定某一地理区域进行访问控制，阻断此区域IP的访问**（投标文件中提供公安部计算机信息系统安全产品质量监督检验中心检测报告）。** |
| IP信誉库 | ★根据国际权威机构提供的恶意IP名单库，对恶意IP的访问实施告警或阻断**（投标文件中提供界面截图）。** |
| 篡改监控 | 系统提供防篡改功能，能够防止被篡改内容被浏览者访问到，一旦检测到被篡改，实时发送告警信息给管理员。 |
| 安全审计 | 能详细记录攻击事件的HTTP请求头信息，含请求的URL、UserAgent、POST内容，cookie等所有的请求头内容。 |
| 能详细记录服务器响应头信息，服务器响应内容。 |
| 日志分析 | ★根据产生的安全日志进行智能分析，提高人工分析效率，减小规则误判概率**（投标文件中提供界面截图）。** |
| 报表 | 根据PCI-DSS要求，对用户的应用进行合规性评估，生成合规报表。 |
| 支持自定义报表、定时报表、支持各类导出格式（WORD，PDF等） |
| 报表可自动发至管理员邮箱 |
| 告警方式 | 支持Syslog、手机短信、邮件等多种告警方式 |
| 访问审计 | 具备审计网站正常访问流量的能力，提供按小时，日期、月份生成报表。 |
| 能记录、查询所有用户对网站的访问情况 |
| 能分析出访问量最大的URL、IP地址 |
| 能分析出访问流量最大的文件类型 |
| 加速功能 | 系统内嵌应用加速模块，通过对各类静态页面及部分脚本高速缓存，提高访问速度。 |
| 支持响应内容压缩，并支持对压缩的响应内容识别。 |
| SSL透明代理 | 支持HTTPS服务器的防护，可支持第三方认证机构颁发的证书链，WEB应用防火墙前端与后端均为HTTPS加密链路，实现HTTPS应用系统的防御。 |
| 支持对HTTPS站点上传的公钥、私钥、证书链的内容格式进行检查，同时自动检测公钥和私钥是否配对、公钥和证书链是否配对，避免无效证书引起的业务不通的问题。 |
| 一个保护站点支持上传多个域名证书 |
| ★可以选择需要支持的SSL/TLS协议版本**（投标文件中提供界面截图）。** |
| 部署在SSL网关后面，能够解析到真实的访问者IP，并能对真实的IP进行防护和阻断。 |
| 移动安全运维 | 可通过移动端实现设备安全运维监控，APP具备以下功能：支持查看当前WAF的告警数量包括最近24小时内以及总的告警数量，支持对攻击的服务器IP以及客户端IP进行统计**（投标文件中提供界面截图）。** |
| 智能联动 | ★支持与同品牌的APT设备进行联动，对未知威胁流量进行检测和拦截**（投标文件中提供界面截图）。** |
| 设备管理 | 规则库支持手工、在线升级两种方式，在线升级可支持规则定时检查新版本和在线更新，确保WAF能够针对新型的、突发型的Web攻击进行防护。 |
| 支持HTTPS方式进行设备管理 |
| 设备管理采用管理员与审计员分离 |
| 操作界面支持全中文界面 |
| 支持LDAP认证 |
| 支持标准网管SNMPv3，并且兼容SNMP v1和v2c。 |
| 支持NTP时间同步 |
| 为统一维护、统一管理，需与APT攻击预警系统同一品牌。 |
| 服务要求 | 不少于免费3年原厂质保服务（自货物交采购人验收合格之日起起算） |
| 不少于免费3年原厂7\*24小时上门现场服务支持（自货物交采购人验收合格之日起起算） |
| 原厂工程师实施及提供设备相关的培训，提供原厂产品培训1天。 |
| 提供原厂常驻浙江省内不少于6个经中国信息安全测评中心认证的注册信息安全专业人员-大数据安全分析师（CISP-BDSA）（投标文件中提供证书复印件），以便提供快速的售后服务。 |

**24.APT攻击预警系统**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 硬件规格 | 软硬一体化2U标准机架式设备 |
| 1+1冗余电源 |
| 可用磁盘空间不小于2T，带RAID1。 |
| 标配千兆管理口\*2，千兆业务口RJ45网口\*4，千兆业务SFP光口\*4。 |
| 千兆RJ45网口\*4或千兆SFP光口\*4或万兆SFP光口\*2 |
| 高可用性 | 旁路镜像模式部署，不影响服务器处理性能和网络架构。 |
| ★支持旁路部署和分布式部署，对探测器可以添加、删除，显示探测器版本、状态和IP，管理中心可实现告警统一管理，可自定义管理中心和探测器之间的数据传输速率、时间、发送目录等参数。 |
| 性能规格 | 网络层：4Gbps，应用层：2Gbps。 |
| HTTP最大并发数：10万/秒 |
| 邮件处理数：200万封/24小时 |
| 10万个/24小时 |
| 支持管理节点30个 |
| 攻击检测 | ★支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、Mysql、MSSQL、DB2、Oracle等协议报文，并提供审计协议类型的端口号配置，可根据需要变更端口号，并支持LDAP登录行为识别、VXLAN镜像流量解析检测及HTTPS流量解析能力。 |
| ★支持检测WEB攻击、异常访问、恶意文件攻击、C&C IP/URL、WEB后门访问、发件人欺骗、邮件头欺骗、邮件钓鱼欺骗、邮件恶意链接、DGA域名请求、SMB远程溢出攻击、WEB行为分析等风险**（投标文件中提供截图）。** |
| ★支持对文件白名单、发件人邮箱白名单、发件人域名白名单、黑域名白名单、黑IP白名单、域名白名单、客户端IP白名单、服务端IP白名单、WEB风险特征白名单进行设置。 |
| ★支持对私网地址IP地理位置信息添加，在产生告警时，定义IP可正常显示所属地理位置信息。 |
| ★支持对Telnet、FTP、POP3、SMTP、IMAP等协议进行弱口令检测 |
| 可支持详细展现告警级别、时间、威胁名称、状态、客户端IP、客户端IP所在地理位置、服务端IP、服务端IP所在地理位置、报文、操作等信息，包含请求URL、请求类型、请求内容、请求头、Host、User-Agent、Accept、Accept-Language、Accept-Encoding、Accept-Charset、Keep-Alive、Connection、Cookie请求参数、响应码、返回长度等信息。 |
| ★可自动对内网主机进行威胁指数分析，详细展示具体的威胁指数、威胁活动、历史威胁指数、遭受的攻击类型、攻击次数、攻击状态等**（投标文件中提供截图）。** |
| 可根据不同威胁指数的主机实现攻击溯源和攻击过程的可视化分析 |
| 可通过攻击源、攻击目的对攻击路线进行统计，包括攻击的行为、告警，并以直观的图形化形式展示。 |
| 可自动学习网络流量中包含的各种可疑C&C IP/URL，包含各种可能对内网存在影响的IP和域名。 |
| 快速识别网络中存在的恶意回连行为，包含回连主机IP、服务器IP、时间、行为等。 |
| 对基于木马回连的非法数据传输等行为进行取证分析，包括回连主机IP、服务器IP、传输数据大小、协议类型等。 |
| 可通过攻击源和目的的地理位置信息，以世界地图和中国地图的形式展示，并实现世界地图和中国地图自动切换直观展示攻击路径。 |
| WEB攻击检测 | 支持 HTTP协议解析，检测WEB攻击。 |
| 支持双向审计，对请求和响应都进行审计。 |
| ★支持SQL注入、命令注入、跨站脚本、代码注入、协议错误攻击检测**（投标文件中提供截图）** |
| ★支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等**（投标文件中提供截图）。** |
| ★支持根据来源IP、MAC、HTTP请求方法、URL、请求头、请求参数、响应码等内容设置审计规则高、中、低等风险等级**（投标文件中提供截图）** |
| ★自动关联行为分析的详细展现，包含SQL注入取数据、表单破解、XSS测试、目录穿越读取文件、多人访问Webshell、APT攻击等**（投标文件中提供截图）。** |
| ★支持场景化的分析能力，对发现的告警进行二次关联，支持对勒索病毒、网站后门、邮件APT攻击等事件进行预警**（投标文件中提供截图）。** |
| ★具备DNS协议分析能力，发现受感染主机、危害程度、被感染病毒类型、回连C&C域名、DNS返回详情、恶意主机明细等行为**（投标文件中提供截图）。** |
| ★支持将分析到的WEBSHELL攻击、木马回连和恶意攻击行为同步到WAF，实现APT深度威胁分析与WAF联动阻断**（投标文件中提供截图）。** |
| Mail攻击检测 | 支持解析webmail、SMTP、POP3类型报文**（投标文件中提供截图）** |
| 支持基于webmail攻击类型检测，包括sql注入、跨站、命令注入等攻击检测。 |
| ★对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接**（投标文件中提供截图）。** |
| 支持邮件恶意附件行为检测 |
| 文件攻击检测 | 支持HTTP、FTP、SMB、SMTP、POP3等协议传输文件检测 |
| 支持doc, xls, ppt, swf, pdf, java, rar, zip, rar, exe, vbs, scr, html，js等多种文件解析。 |
| ★可添加或删除指定审计文件类型**（投标文件中提供截图）** |
| 对文件进行特征匹配，利用已知的特征库发现恶意可以执行代码。 |
| 对文件进行特征匹配，利用已知的特征库发现恶意的非可执行文件。 |
| ★通过分析文件中的二进制代码，找到文件溢出攻击的代码，并能找到APT攻击中的0day攻击**（投标文件中提供截图）。** |
| 对存在问题的文件输出完整的二进制动态分析报告 |
| ★动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险**（投标文件中提供截图）。** |
| 对文件关键行为进行截图**（投标文件中提供截图）** |
| ★可展示文件中版本信息、段信息、资源信息、导入表、字符串信息、删除文件信息等内容**（投标文件中提供截图）** |
| ★可展示ROP行为检测**（投标文件中提供截图）** |
| ★可展示具体文件的行为，包括所有的注册表行为、进程行为、互斥量、进程运行的函数、返回结果、返回值等信息**（投标文件中提供截图）。** |
| 对文件内部嵌入的子文件可进行二次扫描，分析安全性**（投标文件中提供截图）。** |
| 可以提取出攻击的完整样本文件，并提供对该文件下载的能力。 |
| ★可展示威胁程度最高的文件样本MD5、威胁指数、传播次数，病毒检测、静态检测和动态检测结果等内容**（投标文件中提供截图）** |
| ★根据文件传播情况分析受感染主机、接受云端威胁情报、关键威胁行为可视化、回连主机host和完整沙箱分析报告**（投标文件中提供截图）** |
| ★根据云端威胁情报展示云端是否确认、传播协议类型、传播次数、云端确认结果等**（投标文件中提供截图）** |
| 抓包检测功能 | ★同时支持至少16个抓包任务抓包，每个抓包任务可配置抓包规则，按照IP、端口、协议等信息进行抓包，将抓取的原始流量包保存于本地以供后续分析和取证使用，每抓包任务最大抓包20MB**（投标文件中提供截图）。** |
| 管理 | 支持根据需要对风险状态进行选择处理中、处理完成、延迟处理、拒绝处理等 |
| ★支持一键登录排错平台，对系统进行深度配置和排错，支持一键检测故障、配置核对、表分区检查、表检测、同步验证、信息收集等功能**（投标文件中提供截图）。** |
| 支持对设备的CPU、内存等状态进行监控，并在设备界面中进行展示。 |
| ★根据不同的风险信息，提供风险分析和处置建议知识库**（投标文件中提供截图）。** |
| 为统一维护、统一管理，需与数据库审计系统同一品牌。 |
| 日志报表 | 告警可详细展示风险级别、发生时间、告警名称、客户端IP、服务器IP、报文内容（URL、请求头、请求参数、请求内容） |
| 可根据需要针对单个告警添加白名单 |
| ★支持kafka、短信、邮件、syslog、snmp、ftp等告警方式**（投标文件中提供截图）** |
| ★支持同时发送多人、单条发送、发送统计等高级告警功能**（投标文件中提供截图）** |
| 报表能够支持WORD、PDF等格式导出 |
| 日志数据管理 | ★审计数据保留策略应至少满足天数和百分比两个控制参数，支持web界面可配置，且恢复数据不影响正常的审计功能，对审计日志可自动备份并加密，必须导入设备才能进行恢复查看，并可自动释放磁盘空间**（投标文件中提供截图）。** |
| 资质 | 产品具有软件著作权登记证书**（投标文件中提供复印件）** |
| ★产品具有销售许可证（APT安全检测类）**（投标文件中提供复印件）** |
| ★产品具有国家信息安全产品认证证书（ISCCC）**（投标文件中提供复印件）** |
| ★产品具有国家保密科技中心颁发的恶意代码检测系统涉密信息系统检测证书**（投标文件中提供复印件）** |
| 产品具有第三方权威机构检测报告（误报率低于3%，无背景流量情况下检出率不低于98%，有背景流量情况下检出率不低于97%）**（投标文件中提供复印件）** |
| 产品具有公安部APT安全检测报告**（投标文件中提供复印件）** |
| 服务要求 | 不少于免费3年原厂质保服务（自货物交采购人验收合格之日起起算） |
| 不少于免费3年原厂7\*24小时上门现场服务支持（自货物交采购人验收合格之日起起算） |
| 原厂工程师实施及提供设备相关的培训，提供原厂产品培训1天。 |
| 提供原厂常驻浙江省内不少于6个经中国信息安全测评中心认证的注册信息安全专业人员-大数据安全分析师（CISP-BDSA）（投标文件中提供证书复印件），以便提供快速的售后服务。 |

**25.数据库审计系统**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 硬件指标 | 专用工控机硬件架构，非普通PC服务器，MTBF(平均故障间隔时间)≥65000小时。 |
| ★系统启动采用CF卡加硬盘方式**（投标文件中提供产品图片）** |
| 处理器：Intel酷睿第四代I7系列CPU，主频至少3.4G，至少4核8线程。 |
| 内存：≥16GB DDR3 1600Mhz |
| 电源模块：具备冗余热插拔双电源 |
| 硬盘可用容量：≥2TB，2T\*2，支持RAID1、RAID5，最大支持扩展到16T存储空间。 |
| ★网络端口：支持监听接口扩展，配备至少2个千兆电口管理口。 |
| 支持千兆网络环境下的监听能力，标配至少4个千兆电口和4个千兆光口。 |
| 硬件至少另外支持3个扩展板卡，最高支持扩展28个千兆电口或光口，或6个万兆口。 |
| 处理能力 | 审计性能：能够稳定、流畅地同时支持16个数据库数审计能力，不会产生漏审。 |
| ★峰值处理能力：≥40000条/秒**（投标文件中提供第三方权威机构测试报告）** |
| 审计日志检索能力：≥1500万条/秒 |
| 部署方式 | 旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计 |
| ★支持在目标数据库安装agent解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计**（投标文件中提供第三方权威机构测试报告）；** |
| 支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询。 |
| 管理中心和探测器都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展。 |
| 管理中心和探测器直接的数据传输速率、时间、端口都可自定义**(投标文件中提供功能截图)** |
| ★支持大数据平台部署，具有成熟的大数据hadoop平台处理，支持后期无缝扩展大数据版本，支持审计数据外送至大数据平台，检索性能高达100亿数据仅需6-8秒，存储数据量高达3000亿以上。 |
| 协议支持 | 支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL六种主流数据库审计 |
| 支持PostgreSQL、HANA、Teradata、Cache、人大金仓、达梦、南大通用数据库审计**(投标文件中提供功能截图)** |
| ★支持MongoDB、Hbase非关系型数据库审计 |
| 支持主流业务协议HTTP、Telnet、FTP、SMTP、POP3、DCOM |
| ★支持对SQL server（2005及以上版本）数据库采用加密协议通讯，可以通过导入证书的方式实现审计和防护**（投标文件中提供第三方权威机构测试报告）。** |
| 支持对各种协议自动识别编码及在web界面手工配置特定编码。 |
| 审计功能 | 支持数据库操作类、表、视图、索引、存储过程等[各种对象的所有SQL操作审计](#_支持各种对象的SQL审计_1) |
| ★支持数据库请求和返回的双向审计，特别是返回字段和结果集、执行状态、返回行数、执行时长等内容，支持通过返回行数和内容大小控制返回结果集大小**（投标文件中提供第三方权威机构测试报告）。** |
| 支持跨语句、跨多包的绑定变量名及绑定变量值的审计**（投标文件中提供功能截图）** |
| ★支持与堡垒主机自动关联审计通过ssh、rdp等加密协议操作数据库行为**（投标文件中提供第三方权威机构测试报告）** |
| 智能发现 | 自动识别流量中存在的数据库 |
| ★支持定期[自动扫描数据库漏洞](#_支持定期扫描数据库漏洞)和不安全配置，提供漏洞扫描报告**（投标文件中提供第三方权威机构测试报告）。** |
| 应用关联 | ★支持B/S业务系统三层关联审计**（投标文件中提供第三方权威机构测试报告）** |
| 支持通过[部署agent](#_Agent三层关联)实现java web环境100%准确关联**（投标文件中提供功能截图）** |
| 支持[旁路自动学习三层审计](#_旁路自学习三层关联)关联功能**（投标文件中提供功能截图）** |
| 安全审计 | 支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义**（投标文件中提供功能截图）。** |
| 内置安全特征库不少于300条，如SQL注入、缓冲区溢出、弱口令等。 |
| 可自定义审计规则，审计规则至少支持18个条件**（投标文件中提供功能截图）。** |
| 规则各条件之间支持[与或非逻辑](#_支持与或非逻辑关联)关系**（投标文件中提供功能截图）** |
| 告警数量需[支持最大告警数量限制](#_最大告警数限制)，超过告警阈值之后便不告警**（投标文件中提供功能截图）。** |
| 告警查询应支持根据登陆用户、客户端工具名、客户端IP、规则进行归并分析，能详细展示每类告警占总告警数量百分比，便于告警分析处理**（投标文件中提供截图）。** |
| 审计查询 | 具有高效的查询性能，后台采用[SPHINX](#_SPHINX全文索引)全文检索引擎检索**（投标文件中提供功能截图）。** |
| 查询条件易于使用，[审计查询条件](#_查询条件)均为非正则表达式形式进行。 |
| 支持采用部分[匹配模糊](#_支持模糊查询)查询方式检索审计日志 |
| 支持基于数据库[访问日期、时间、源/目的IP、来源](#_多维度查询)、数据库名、数据库表名、字段值、数据库登陆账号、SQL关键词、数据库返回码、SQL响应时间、数据库操作类型、影响行数等条件的审计查询。 |
| 统计报表 | ★内置[多种报表模板库](#_内置多种报表模板)，内置的报表不少于35种**（投标文件中提供功能截图）。** |
| 报表支持严格按照[塞班斯（SOX）法案、等级保护标准](#_SOX、等级保护合规多维度)要求生成多维度综合报告 |
| 支持按照数据库[访问行为](#_按行为分析)生成报表，智能识别帐号的增删、权限变更、密码修改、特权操作等行为。 |
| 支持按照[时间曲线统计流量](#_时间曲线等报表)、在线用户数、并发会话、DDL操作数、DML操作数、执行量最多的SQL语句等报表**（投标文件中提供功能截图）** |
| 支持[性能分析](#_按性能分析)，准确提炼出SQL语句执行频率和执行时间异常的报表。 |
| 支持[Word、PDF、ppt](#_导出格式)等格式的报表导出 |
| 支持[报表自定义](#_报表自定义)，自定义的条件不少于20个**（投标文件中提供功能截图）。** |
| 模型分析 | ★支持对数据库[自动建模及智能对异常行为告警功能](#_自动建模告警)**（投标文件中提供第三方权威机构测试报告）** |
| 可通过行为[轨迹图方式](#_轨迹图方式展示)展示数据库访问行为**（投标文件中提供功能截图）** |
| ★可基于账号、IP地址、访问权限、客户端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警**（投标文件中提供功能截图）** |
| 可以自动[对比不同时期的行为模型](#_不同时期对比)，以区分其审计日志数趋势、用户、IP地址、工具、访问权限的差异情况。 |
| 数据管理 | 支持根据保留天数和占用百分比[自动清理](#_自动清理)最早的数据 |
| 提供审计策略和[系统配置信息的单独导入、导出](#_系统配置单独导入导出)功能 |
| 系统管理 | 支持用户界面告警、Syslog、SNMP、邮件、短信、ftp六种方式告警 |
| 采用B/S架构管理，[支持中英文两种管理界面](#_中英文切换)。 |
| 支持[系统安全配置](#_系统安全配置)（会话锁定、超时退出、IP地址访问控制、密码复杂性管理、验证码登陆等措施） |
| 支持[NTP时间同步、SNMP](#_NTP、SNMP)(v1、V2、V3)网络管理协议 |
| 为统一维护、统一管理，需与运维审计系统同一品牌。 |
| 故障排错 | ★系统内置独立的故障排错系统，支持一键导出系统调试日志，一键检测服务、许可证、流量等常见故障，支持流量分析功能，包括抓包、包内容查看、[自动探测sql语句](#_流量分析)等。 |
| 资质 | ★具有计算机信息系统安全专用产品销售许可证**（投标文件中提供复印件）** |
| ★具有[信息技术产品安全测评证书](#_国家信息安全测评EAL3+)，级别EAL3+**（投标文件中提供复印件）。** |
| ★通过国家信息安全认证中心[3C](#_3C_认证)认证检测，级别增强级以上**（投标文件中提供复印件）。** |
| 具有软件著作权登记证书**（投标文件中提供复印件）** |
| ★具有国家保密局涉密信息系统安全保密测评中心颁发的[涉密信息系统产品检测证书](#_涉密信息系统产品检测证书)**（投标文件中提供复印件）** |
| 服务要求 | 不少于免费3年原厂质保服务（自货物交采购人验收合格之日起起算） |
| 不少于免费3年原厂7\*24小时上门现场服务支持（自货物交采购人验收合格之日起起算） |
| 原厂工程师实施及提供设备相关的培训，提供原厂产品培训1天。 |
| 提供原厂常驻浙江省内不少于6个经中国信息安全测评中心认证的注册信息安全专业人员-大数据安全分析师（CISP-BDSA）（投标文件中提供证书复印件），以便提供快速的售后服务。 |

**26.运维审计系统**

|  |  |  |
| --- | --- | --- |
| 功能类别 | 技术要求及指标 | |
| 硬件配置 | 软硬件一体化产品，2U、磁盘空间不少于2T、硬盘须配置RAID1、至少配备4个100/1000M自适应电口和2个1000M光口（并配2个SFP多模模块）、并支持至少1个端口扩展槽，最大端口数可达10个，1+1冗余电源。 | |
| 可管理设备数量 | 可管理设备数量≥1000个，运维用户无限制。 | |
| 并发性能 | ★单台堡垒机字符类并发会话≥1000个、图形类并发会话≥300个**（投标文件中提供第三方权威机构测试报告）** | |
| 系统安装与存储 | ★系统安装在专用的CF卡或固态盘中，审计数据存储在磁盘中，防止操作系统故障导致审计数据丢失**（投标文件中提供真实硬件结构图）。** | |
| 设备部署 | 采用旁路部署，不得影响业务环境，支持HA主备模式，管理口和心跳口支持多链路端口绑定功能，防止单网卡或单线故障**（投标文件中提供功能截图）。** | |
| 支持多台堡垒机异地备份部署，每台设备都能提供运维和审计服务，配置数据自动同步。 | |
| ★支持集群部署模式，中心采用HA，节点可以横向扩展，实现统一登录入口、统一配置同步、审计日志集中存储、实时会话集中监控，以满足业务增长需求**（投标文件中提供功能截图）。** | |
| 用户管理要求 | 用户角色 | 支持用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理。 |
| 用户管理和用户策略 | 支持用户的批量导入/导出，按用户类型等分组方式；支持用户安全策略功能，如密码锁定次数、密码有效期、密码复杂度、用户有效期、用户登录时间限制、用户登录IP范围等。 |
| 部门层级管理 | ★支持按部门组织架构（至少5个层级的部门）管理用户数据、资产数据、授权数据、审计数据**（投标文件中提供相关截图）** |
| 部门用户管理 | ★每个部门可以管理本部门及下级部门的用户角色：部门管理员、运维管理员、审计管理员、运维员**（投标文件中提供相关截图）** |
| 部门资源管理 | 每个部门的部门管理员可以管理本部门及下级部门的主机、授权关系、策略**（投标文件中提供相关截图）** |
| 部门审计管理 | ★每个部门的审计管理员可以管理本部门及下级部门的运维会话日志**（投标文件中提供相关截图）** |
| 身份认证要求 | 与第三方认证对接 | 支持与AD、LDAP、RADIUS、吉大正元、北京CA认证系统联动登录堡垒机，[支持自动同步AD/LDAP用户](#_AD/LDAP用户同步)。 |
| 短信口令认证对接 | ★支持与get、post、soap发送方式的http短信网关平台进行联动，实现短信动态口令双因素认证机制，如与阿里云短信服务、SendCloud联动**（投标文件中提供相关截图）。** |
| 手机APP动态口令认证 | ★支持手机APP动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定APP动态口令**（投标文件中提供相关截图）** |
| 双因子认证 | 堡垒机须内嵌动态令牌和usbkey认证引擎，可同时使用动态令牌和USBkey**（投标文件中提供相关授权和资质复印件）** |
| 配置5个USBkey和5个动态令牌 |
| 多种双因子认证同时使用 | ★基于不同的用户设置不同的双因子认证模式，如user1用动态令牌、user2用USBkey、user3手机APP动态口令认证**（投标文件中提供相关截图）。** |
| 多种认证组合使用 | 支持域认证与双因子认证结合使用，如同时使用AD/LDAP用户名+AD/LDAP密码+手机APP动态口令登录堡垒机、同时使用AD/LDAP用户名+AD/LDAP密码+短信口令登录堡垒机。 |
| 认证窗口全局设置 | ★支持认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口**（投标文件中提供相关截图）** |
| 设备管理要求 | 支持的协议和应用 | 支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具。 |
| 主流数据库运维管理 | ★支持DB2、oracle、mysql、sqlserver主流数据库协议代理运维，可直接调用本地windows系统的数据库客户端工具，支持自动登录、无需应用发布前置机**（投标文件中提供相关截图）。** |
| IE代填 | ★IE代填应用发布：HTTP/HTTPS协议的web设备，且可以直接代填账号和密码**[（投标文件中提供国家权威机构证明）](#_IE代填应用发布专利证明)** |
| 混合云管理 | ★可以通过socks5/http/ssh等代理协议连接管理异地云资源区中私有网络的云主机 |
| 分组管理 | 支持对设备进行按设备类型分组、按部门分组，支持设备批量导入/导出。 |
| 登录模式 | 支持设备帐户和密码的自动登录、手工登录、二次自动登录模式。 |
| 自动收集和自动授权 | ★支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，甚至可自动完成授权**[（投标文件中提供国家权威机构证明）](#_IE代填应用发布专利证明)。** |
| 设备密码管理 | 导出的设备信息文件加密存储，解密时须由2个管理员同时解密才能查看到设备信息文件内容**（投标文件中提供相关截图）。** |
| 工单流程要求 | 申请工单 | 运维人员可以向管理员申请需要访问的设备，申请时可以选择：设备IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理员**（投标文件中提供相关截图）。** |
| 审批工单 | 管理员对运维工单进行审核之后以邮件方式通知给运维人员，如果允许，则运维人员才可访问，否则就无法访问。 |
| 自动改密要求 | 自动改密 | 支持定期自动修改windows服务器、网络设备、linux/unix等目标设备密码功能 |
| 改密保护机制 | ★支持完善的自动改密安全保护机制，包括：改密前备份、备份失败不改密、改密后备份、密码文件加密。 |
| 支持发送方式，包括邮件、FTP、SFTP等**（投标文件中提供相关截图）。** |
| 密码容错机制 | ★支持自动密码恢复、手工验证密码、密码强度控制等 |
| 运维方式要求 | 多种浏览器登录 | Web访问方式：至少支持使用IE、谷歌、火狐三种浏览器打开堡垒机的Web页面直接调用mstsc、VNC、Xshell、SecureCRT、Putty、winscp、flashFXP、FileZilla、SecureFX等运维客户端工具 |
| ★H5运维方式：支持ssh、telnet、rlogin、rdp、vnc协议的H5运维，无需本地运维客户端工具。 |
| 数据库运维 | ★支持通过堡垒机页面直接调用本地Windows系统里的plsql、sqlplus、toad、sqlwb、ssms、mysql.exe等数据库客户端工具。 |
| 客户端工具登录 | 客户端访问方式：支持使用本地的mstsc/Xshell/SecureCRT/Putty等客户端工具登录堡垒机访问图形或字符设备，视图界面一致性、搜索能力 |
| SFTP/FTP的客户端登录 | ★支持使用本地的winscp/flashFXP/SecureFX等客户端工具登录堡垒机访问SFTP/FTP设备 |
| SSH网关代理直连 | ★支持使用本地的SecurCRT/Xshell/OpenSSH工具通过SSH网关代理方式直接登录字符设备 |
| 数据库代理直连 | ★支持在mac电脑里使用navicat工具通过堡垒机登录mysql、oracle等数据库服务器 |
| 批量自动登录字符主机 | ★支持批量登录字符设备功能：能自动生成SecurCRT/Xshell工具的批量登录文件，实现在工具中批量自动登录多台设备**（投标文件中提供配置界面截图）。** |
| 域用户自动登录主机 | ★AD/LDAP环境，支持直接使用登录堡垒机的AD/LDAP用户及密码可以直接自动登录到服务器里**（投标文件中提供配置界面截图）。** |
| 审计日志要求 | 运维审计日志 | 支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志。 |
| Zmodem传输审计 | ★支持保存SSH的sz/rz命令（zmodem）传输的原始文件**（投标文件中提供第三方权威机构测试报告）** |
| SFTP/FTP传输审计 | ★支持保存SFTP/FTP传输的原始文件**（投标文件中提供第三方权威机构测试报告及功能截图）** |
| RDP粘贴板审计 | ★支持保存RDP粘贴板（桌面之间复制-粘贴）传输的原始文件**（投标文件中提供第三方权威机构测试报告及功能截图）** |
| RDP磁盘映射审计 | ★支持保存RDP磁盘映射传输的原始文件**（投标文件中提供第三方权威机构测试报告及功能截图）** |
| RDP文字记录 | 支持对RDP屏幕文字内容、标题窗口、键盘输入的记录和搜索定位 |
| SQL记录 | ★支持审计主流数据库（如DB2、oracle、mysql、sql server）运维中的SQL语句，可进行关键信息定位查询。 |
| 全文检索 | ★支持全局搜索审计日志，无需区分图形/字符/文件/应用类型，只需通过关键信息直接搜索定位**（投标文件中提供功能截图）。** |
| 日志数据归档 | ★审计数据支持通过SFTP/FTP方式自动归档，并在页面中可以查询哪些数据是否归档，可以设置归档成功之后自动删除数据，归档后的数据可以用专用播放器离线查看。 |
| 安全策略要求 | 运维规则策略 | 支持通过基于时间、IP/IP段、用户/用户组、设备/设备组、设备账号、命令关键字、控制动作、黑白名单等组合访问控制策略，授权用户可访问的目标设备。 |
| 二次审批 | 对重要设备启用登录审核功能，运维人员须向管理员申请登录，管理员允许之后才可登录，否则无法登录 |
| 命令审批 | 支持对重要命令进行审核：运维人员执行命令后，须等到管理员审批通过后才可执行成功**（投标文件中提供国家权威机构证明）** |
| 自动运维任务 | 支持自动推送命令任务，如可自动备份交换机/路由器的配置信息、可自动执行周期任务，并将结果以邮件/FTP/SFTP的方式发送给相关管理员**（投标文件中提供功能截图）。** |
| 运维空闲时间限制 | ★支持运维空闲会话时间全局设置限制功能**（投标文件中提供功能截图）。** |
| 报表统计要求 | 运维报表格式 | 内置丰富的报表统计模板，可点击柱状图、饼状图或曲线图进行数据钻取分析，且支持PDF、doc、html格式导出**（投标文件中提供效果截图）。** |
| 运维报表内容 | 内置根据运维人员和组生成各种维度的分析报表，维度包含总为运维次数、时长、活动时长、会话起止时间、会话大小、命令数、上传下载文件数，分别从全局及平均值、最大值、最小值、单次运维、单个会话等角度提供非常有价值有意义的报表**（投标文件中提供效果截图）。** |
| 自动发送报表 | 支持运维报表自动定期发送，提供一键导出符合等级保护、SOX法案要求的综合分析报告**（投标文件中提供报表样本）。** |
| 系统管理要求 | 系统自审 | 支持自身审计，包括但不限于：系统状态检测、登录日志、用户配置日志、设备配置日志、授权配置日志、策略配置日志、运维访问日志、系统配置日志等。 |
| 系统日志报表 | 支持系统日志报表统计功能，包括但不限于登录日志统计、配置日志统计、运维访问日志统计等，可以导出报表**（投标文件中提供效果截图）。** |
| 告警输出 | 支持邮件/syslog方式输出告警日志 |
| SNMP输出 | 支持SNMP方式输出系统信息 |
| 排错功能 | 提供排错工具：ping、TCP端口检测、UDP端口检测、路由跟踪等 |
| API接口 | ★提供用户、资产、授权的增删改查等API接口，允许第三方平台调用堡垒机的API接口，实现用户、资产、权限自动同步到堡垒机，简化堡垒机配置工作量**（投标文件中提供功能截图）。** |
| 与同品牌数据库审计联动 | ★支持和同品牌数据库审计系统进行联动，将通过SSH/RDP等加密方式操作数据库的行为整合到数据库审计中，实现数据库行为的统一集中查询、展示、审计分析等**（投标文件中提供功能截图）。** |
| 与同品牌SOC联动 | ★支持和同品牌的SOC系统进行联动，对绕过堡垒机而登录主机的行为，SOC进行实时告警，并且与SOC进行日志关联性分析。 |
| 管理 | 为统一维护、统一管理，需与综合日志审计系统同一品牌。 |
| 资质 | ★产品[具有公安部产品销售许可证](#_销售许可证)**（投标文件中提供复印件）** | |
| ★[产品具有国家涉密产品资质证书](#_21、涉密资质)**（投标文件中提供复印件）** | |
| ★产品符合国家《运维审计产品安全技术要求》测试标准，[并获得中国信息安全认证中心3C资质](#_中国信息安全认证中心3C资质)**（投标文件中提供证明材料）。** | |
| 原厂具有产品自主知识产权，非OEM贴牌**（投标文件中提供证明材料）。** | |
| 提供原厂常驻浙江省内不少于6个经中国信息安全测评中心认证的注册信息安全专业人员-大数据安全分析师（CISP-BDSA）（投标文件中提供证书复印件），以便提供快速的售后服务。 | |

**27.综合日志审计系统**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 资质 | 产品具有计算机信息系统安全产品销售许可证以及公安部信息安全产品检测中心出具的检测报告，检测报告符合《信息安全技术日志分析产品检验规范》**（投标文件中提供复印件）。** |
| 产品具有IT产品信息安全认证证书**（投标文件中提供复印件）** |
| 产品具有软件著作权登记证书**（投标文件中提供复印件）** |
| 产品通过国家保密科技测评中心检测并获得涉密信息系统产品检测证书，需符合《涉及国家秘密的信息系统安全监控与审计产品技术要求》**（投标文件中提供检测报告复印件）。** |
| 厂商具有信息安全应急处理服务资质（一级）**（投标文件中提供证明材料）** |
| 厂商为国家级网络安全应急服务支撑单位**（投标文件中提供证明材料，如CNCERT网站截图）** |
| 厂商具有信息安全服务资质证书（安全工程类二级及以上）**（投标文件中提供复印件）** |
| 厂商具有信息安全管理体系认证证书**（投标文件中提供复印件）** |
| 工作模式 | 独立完成审计日志采集，不依赖于设备或系统自身的日志系统。 |
| 审计工作不影响被审计对象的性能、稳定性或日常管理流程 |
| 审计结果存储于独立存储空间 |
| 自身用户管理与设备或主机的管理、使用、权限无关联 |
| 提供全中文WEB管理界面，无需安装任意客户端软件或插件。 |
| 硬件规格 | 2个工作管理口，1个console口。 |
| 内存：16GB，磁盘：2T\*2 raid1。 |
| 双电源 |
| ★采用CF卡启动**（投标文件中提供第三方检测报告）** |
| 可扩展项：内存可扩展至32GB |
| 单个磁盘可扩展至4T(4个盘位)，支持HBA卡扩展。 |
| 网口可扩展（4电4光、8电、8光、2万兆光） |
| 处理性能 | 支持审计200个日志源 |
| 平均处理能力（每秒日志解析能力EPS）：9000EPS |
| 峰值处理能力（每秒日志解析能力EPS）：12000EPS |
| 功能扩展 | ★采用解决方案包上传对产品进行功能扩展，无需要代码开发。 |
| 日志收集 | 支持Syslog、SNMP Trap、OPSec、FTP协议日志收集 |
| 支持使用代理(Agent)方式提取日志并收集 |
| 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等 |
| 设备厂家包括但不限于：Cisco(思科)，Juniper，联想网御/网御神州，F5，华为，H3C，微软，绿盟，飞塔(fortinet)，Foundry，天融信，启明星辰，天网，趋势，东软，Nokia，CheckPoint，Hillstone(山石)，安恒，珠海伟思，BEA，中国电信，安氏，帕拉迪，apc，arbor，clam，戴尔（dell），digium，东方电子，EMC，中国电力科学研究院，Eudora，google，冠群金辰，linksys，Mcafee，netapp，NAS（美国国家安全局），永达，sonicwall，vigor，天存，西岭，Symantec（赛门铁克），Hardened-PHP，foundertech(方正)，三零盛安，allot，蓝盾，IBM，金诺网安，网威，nortel(北电)，citrix(思杰)，watchguard，中兴，阿帕奇，WINDOWS系统日志，Linux/UNIX syslog、IIS、Apache等； |
| ★支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。 |
| 日志分析 | 可以以日志等级进行过滤 |
| 可以通过自定义配置将用户不关心的日志过滤掉 |
| 支持对收集到的重复的日志进行自动的聚合归并，减少日志量。 |
| 支持可由用户定义和修改的日志的聚合归并逻辑规则 |
| 支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备。 |
| 支持对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展。 |
| 可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息（公网情况）。 |
| 具备安全评估模型，评估模型基于设备故障、认证登陆、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数，安全评估模型可以显示总体评分、历史评分趋势，安全评估模型各项指标可钻取具体的评分扣分事件**（投标文件中提供截图）。** |
| 内置非法访问、可疑入侵、病毒爆发、设备异常、弱点针对等5大类50子类的安全分析场景**（投标文件中提供截图）** |
| ★支持基于内存的实时关联分析，跨设备的多事件关联分析**（投标文件中提供第三方检测报告）**。 |
| ★支持自定义条件的事件进行聚合 |
| ★进行关联分析的规则可定制 |
| ★支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析（三维关联），所有的三维关联算法和准则以CVE、Bugtraq、OWASP公开协议和标准为为基础**（投标文件中提供第三方检测报告）。** |
| 日志备份 | 可设置日志存储备份策略，包括系统日志保存期（天）、磁盘使用率百分比。 |
| ★支持日志备份自动传送到远程服务器 |
| 日志查询 | 支持B/S模式管理，支持SSL加密模式访问。 |
| 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询。 |
| 支持用任意关键字对所有事件进行高性能全文检索 |
| 支持可指定多个查询条件进行组合查询 |
| 支持将查询的条件存储为查询模版，方便再次使用。 |
| ★极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。 |
| 应用性能监控  （APM） | 支持如下应用的性能监控（Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris）、数据库（mysql、oracle）、应用服务器（weblogic、tomcat）、web服务器（apache） |
| 支持应用性能历史详情回溯查看 |
| 支持监控Windows操作系统如下参数：cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数 |
| 支持监控Linux操作系统如下参数：一分钟系统负载、5分钟系统负载、15分钟系统负载、cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数 |
| 支持监控Mysql如下参数：查询缓存命中率、键缓存命中率、立即获得锁数、连接数、线程数、每秒SQL查询数、每秒发送字节、每秒接收字节 |
| 支持监控Oracle如下参数：库缓存命中率、内存排序比率、词典缓存命中率、SGA数据缓存命中率、重做日志缓存命中率 |
| 支持监控Apache如下参数：总访问数、写日志次数、每秒发送字节数、长连接数、关闭连接数、空闲活动数、查询DNS数、正在发送数、请求完成数、负载、等待连接数、总数据量、读操作数、工作线程数、空闲线程数、CPU占用率 |
| 支持监控应用服务器（tomcat、weblogic）如下参数：活动线程数、堆内存（已用）、守护线程数 |
| 脆弱性管理 | 支持从IBM Rational AppScan导入资产弱点漏洞信息 |
| 支持从安恒明鉴Web应用监测工具导入网站弱点漏洞信息 |
| 支持从安恒明鉴数据库弱点扫描器导入数据库弱点漏洞信息 |
| 支持从NetSparker Web应用扫描器导入网站弱点漏洞信息 |
| 支持从Nessus网络扫描器导入网络弱点漏洞信息 |
| 支持从OpenVAS扫描器导入弱点漏洞信息 |
| 内置73000+条CVE漏洞数据知识库 |
| 内置数十项符合OWASP的Web漏洞数据知识库 |
| 地理安全系统 | 内置GeoSec地理安全子系统，内置世界以及中国安全GIS地图。 |
| 支持用地理地图展示来源威胁的趋势 |
| 支持用地理地图展示目的威胁的趋势 |
| 支持在地理地图上标注威胁事件的发生分布 |
| 内置IP地址到经纬度的转换库 |
| 支持以地理信息类进行统计的数据报表 |
| 支持切换Google地图（需要连通互联网） |
| 告警功能 | 可预设置安全告警策略 |
| 支持数据阀值设置，超过阀值将产生告警。 |
| 可以通过邮件、短信和屏幕显示进行告警 |
| 支持自动防止报警信息在短时间内大量发送(告警抑制) |
| 具备报警合并和在一个时间段内抑制报警次数的能力 |
| 综合查询及报表  管理 | 内置合规性报表1000+种 |
| ★内置SOX、ISO27001、WEB安全等解决方案包 |
| ★内置完善的等级保护合规报表 |
| 内置综合性自动化审计报告 |
| 支持用户自定义报表 |
| 自定义的报表支持多个统计维度的数据集合 |
| 支持报表导出为PDF和Word格式文件 |
| 为统一维护、统一管理，需与远程安全评估系统同一品牌。 |
| 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容，日志员只负责完成对系统本身的用户操作日志管理。 |
| 系统自带自身管理日志 |
| ★注册用户资产时，提供自动发现识别能力。 |
| ★提供一键式故障排除功能 |
| 提供自助式的升级接口，支持对产品升级、规则升级。 |
| 部署方式 | ★支持分布式部署 |
| ★支持集中式管理和升级模式 |
| 支持分级管理模式 |
| 采用B/S架构操作方式，无需客户端安装。 |
| 支持监控设备自身CPU、内存、磁盘等工作运行状况 |
| 售后服务支持 | 提供3年免费升级维护（自货物交采购人验收合格之日起起算） |
| 提供安装调试后1天本地操作培训 |
| 提供24小时支持热线 |
| 本地应急响应时间<=2小时 |
| 服务要求 | 不少于免费3年原厂质保服务（自货物交采购人验收合格之日起起算） |
| 不少于免费3年原厂7\*24小时上门现场服务支持（自货物交采购人验收合格之日起起算） |
| 原厂工程师实施及提供设备相关的培训，提供原厂产品培训1天。 |
| 提供原厂常驻浙江省内不少于6个经中国信息安全测评中心认证的注册信息安全专业人员-大数据安全分析师（CISP-BDSA）（投标文件中提供证书复印件），以便提供快速的售后服务。 |

**28.远程安全评估系统**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 产品要求 | 安全的Linux操作系统 |
| 硬件环境 | 1U机架式：管理口2\*GE电口(管理口\*1，HA口\*1)，工作口 4\*GE电口，一个可扩展模组（4光），单电源，i5处理器，16G内存，1T硬盘双核或双核以上CPU，16G以上内存，至少1T硬盘空间。 |
| 部署方式 | 支持旁路部署，无需改变原有的网络架构，分布式部署。 |
| 扫描对象 | Web漏洞扫描、数据库漏洞扫描、主机软件漏洞扫描、基线配置核查，每个模块支持256个IP。 |
| 功能要求 | 界面友好，并有详尽的技术支持文档，所有图形界面要求中文。 |
| 系统为B/S架构，并采用SSL加密通信方式，用户可以通过浏览器远程方便对产品访问操作，支持多用户同时登陆操作。 |
| 提供分布式部署，上级管理设备能够方便查看下级设备状态。 |
| 提供三权分立的账户体系，支持上下级部门管理，非上下级的不同部门任务、资产隔离。 |
| 提供审计功能，能够对登陆日志、操作日常进行记录和查询，并可以将日志导入导出操作。 |
| ★提供日志自动审计功能，根据指定的审计标准自动、定时审计，并将审计结果发送到指定邮箱当中。 |
| ★厂商漏洞策略库大于35000条，提供详细的漏洞描述和对应的解决方案描述，漏洞知识库与国际CVE、国内CNNVD漏洞库标准兼容。 |
| 系统内置不同的策略模板如针对Linux、Windows操作系统等模板，同时允许用户定制扫描策略，用户可定义扫描范围、定义扫描端口、扫描使用的参数集等具体扫描选项。 |
| 支持Windows系列操作系统，支持Linux主流操作系统（Centos、Redhat、Debian、Fedora、Ubuntu、Suse等），支持Unix主流操作系统（AIX、HPUX、Solaris等）。 |
| 支持对Web、FTP、电子邮件等应用系统、Apache等web中间件服务器以及Office等常用软件进行漏洞扫描 |
| 可以自定义扫描端口范围、端口扫描策略 |
| 提供采用SMB、SSH等协议对Windows、Linux系统进行登录授权扫描 |
| ★具备弱口令扫描功能，提供多种弱口令扫描协议，包括SMB、RDP、SSH、TELNET、FTP、SMTP、IMAP、POP3、MySQL、MSSQL、REDIS、RTSP等协议进行弱口令扫描，允许用户自定义用户、密码字典。 |
| 支持发现非默认端口启动的服务，支持服务的协议识别、版本。 |
| ★可根据端口识别出的软件版本提供可能存在的相关漏洞列表 |
| 支持HTML、WORD、PDF、XLS报告格式 |
| 为统一维护、统一管理，需与全流量深度威胁检测平台同一品牌。 |
| 配置核查模块 | 提供系统安全配置核查功能，能够对主流操作系统、中间件的安全配置项目进行检查。 |
| Web扫描模块 | 提供Web应用漏洞扫描功能，支持对Discuz、大汉CMS、PHPCMS、DEDECMS、ECSHOP、WordPress、eWebEditor、FCKeditor、Struts2等国内外常见第三方组件扫描。 |
| 能够检测GET、POST、User-Agent、Cookie等多种方式提交的HTTP请求参数，并进行相应检测。 |
| 能够通过Cookie的方式支持对带验证码的应用系统进行扫描 |
| 存在误报漏洞可通过产品在扫描结果处一键反馈给厂商协助修改 |
| ★支持识别国内外主流Web应用防火墙品牌 |
| ★支持识别被扫描目标对象的网站响应状态，能根据不同的响应状态直观呈现不同颜色标识。 |
| 管理人员可根据系统给出的漏洞参数、HTTP请求/响应数据，快速验证，一键验证漏洞。 |
| 数据库模块 | 支持Oracle、Mysql、SQLServer、DB2、informix、达梦、人大金仓的授权数据库漏洞扫描 |
| 资质 | 产品具有软件著作权登记证书**（投标文件中提供复印件）** |
| 产品具有计算机信息系统安全专用产品销售许可证**（投标文件中提供复印件）** |
| 产品具有国家保密局涉密信息系统安全保密测评中心的涉密信息系统产品检测证书**（投标文件中提供复印件）** |
| ★产品具有国家信息安全漏洞库兼容性证书**（投标文件中提供复印件）** |
| 服务要求 | 不少于免费3年原厂质保服务（自货物交采购人验收合格之日起起算） |
| 不少于免费3年原厂7\*24小时上门现场服务支持（自货物交采购人验收合格之日起起算） |
| 原厂工程师实施及提供设备相关的培训，提供原厂产品培训1天。 |
| 提供原厂常驻浙江省内不少于6个经中国信息安全测评中心认证的注册信息安全专业人员-大数据安全分析师（CISP-BDSA）（投标文件中提供证书复印件），以便提供快速的售后服务。 |

**29.全流量深度威胁检测平台**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 硬件外形 | 软硬一体化2U标准机架式设备 |
| 硬盘容量 | 可用磁盘空间不小于1T |
| 接口数量 | 标配千兆管理口\*2，千兆业务口RJ45网口\*4。 |
| 吞吐率 | 1Gbps |
| 部署方式 | | 旁路镜像模式部署，不影响服务器处理性能和网络架构。 |
| 分布式部署 | | 支持分布式部署，管理中心可实现告警统一管理。 |
| 支持添加和删除探测器配置 |
| 支持根据添加探测器情况，配置探测器名称、发送时间、发送目录等信息。 |
| 支持显示不同探测器的IP、版本、状态和最近24小时的风险信息 |
| 为统一维护、统一管理，需与远程安全评估系统一品牌。 |
| 自定义配置 | | ★管理中心和探测器之间的数据传输速率、时间、发送目录都可自定义**（投标文件中提供截图）** |
| 审计功能 | | 支持全流量审计，包含网络第2-7层数据流量**（投标文件中提供截图）。** |
| 可选择特定协议或IP地址自定义检测**（投标文件中提供截图）** |
| 支持自定义IP地址访问监测**（投标文件中提供截图）** |
| 详细记录所有的审计数据包，可展现审计数据包的时间、客户端IP、服务端IP、应用层协议、报文、返回码、详细信息等。 |
| 协议解析 | | ★支持解析应用层协议不低于100多种，如HTTP、SSL、FTP、SMTP、POP3、TFTP、TCP、UDP、NFS、SNMP、ICMP、RTMP、DNS、IRC、SMB等。 |
| ★支持对应用层协议HTTP/DNS/FTP/IMAP/POP3/SMTP/SMB/DNP3等可做深层解析还原，并进行全审计**（投标文件中提供截图）。** |
| ★支持对Modbus、IEC-104、DNP3、Ethernet/IP、S7等工控协议流量的解析还原**（投标文件中提供截图）** |
| 支持对传输层TCP/UDP流量统计**（投标文件中提供截图）** |
| 对应用流量可做流量统计分析**（投标文件中提供截图）** |
| 敏感信息识别 | | ★实现对关键字、数据来源等的自定义，通过内容深度匹配流量中的敏感信息，并对敏感信息快速定位，实现对敏感信息访问行为的有效监测**（投标文件中提供截图）。** |
| 登录信息识别 | | ★识别网络中WEB、QQ、迅雷等各种应用的登录行为，提取登录IP、登录账户、登录网站域名等登录信息**（投标文件中提供截图）。** |
| 加密流量解析 | | ★支持对HTTPS流量的解析还原**（投标文件中提供截图）** |
| 流量代理分析 | | ★处理和分析第三方接入流量，满足用户对其他平台流量无法分析溯源需求**（投标文件中提供截图）。** |
| 威胁分析 | | 支持流量异常行为检测，如网络蠕虫、木马、后门、僵尸、间谍软件、网络漏洞、网页漏洞、跨网站攻击、钓鱼邮件、暴力攻击、数据库注入攻击、ARP欺骗、DoS攻击等。 |
| 支持详细展现发现的威胁内容，包含时间、攻击源IP、攻击目的IP、网络层协议、应用层协议、规则描述、风险相关参照等信息。 |
| 流量构成分析 | | ★可展现某IP在指定时间范围内的总流量、上下行流量大小及该IP下所有应用的总流量、上下行流量大小 |
| ★可展现某应用在指定时间范围内的总流量、上下行流量大小及该应用下所有IP的总流量、上下行流量大小 |
| 流量趋势分析 | | 支持最近1小时、3小时、6小时、12小时、24小时和自定义时间段的协议统计分析，包含应用层流量统计和传输层流量统计信息。 |
| ★支持对2800多种应用流量数据进行统计，包含但不限于QQ、迅雷、VPN、PPTV、天猫等各种应用**（投标文件中提供截图）。** |
| 支持对传输层和网络层流量数据进行统计，包含但不限于TCP、UDP、IP、ICMP等。 |
| 三权分立用户管理 | | 提供三权分立的用户管理能力：配置员、用户管理员、审计员相互独立，支持自定义管理用户权限和角色。 |
| 设备状态监控 | | 支持对设备的CPU、内存等状态进行监控，并在设备界面中进行展示。 |
| 告警与报表 | | 告警可详细展示风险级别、发生时间、告警名称、客户端IP、服务器IP、报文内容（URL、请求头、请求参数、请求内容） |
| ★支持SYSLOG、FTP、KAFKA等接口进行审计、风险等各种信息外送**（投标文件中提供截图）** |
| 报表能够支持WORD、PDF、EXCEL等格式导出 |
| 日志数据管理 | | 审计数据保留策略应至少满足天数和百分比两个控制参数，且支持web界面可配置，且恢复数据不影响正常的审计功能**（投标文件中提供截图）。** |
| 支持自动备份审计日志，备份完后通过FTP方式外送到外部设备。 |
| 备份文件需要进行加密，且必须导入设备才能够进行恢复查看。 |
| 当磁盘空间达到一定的阀值，支持自动清理最早的数据释放空间 |
| 资质 | | 产品具有软件著作权登记证书**（投标文件中提供复印件）** |
| ★厂商具有信息安全服务资质证书（安全工程类三级及以上）**（投标文件中提供复印件）** |
| 厂商具有信息安全应急处理服务资质（一级）**（投标文件中提供证明材料）** |
| 厂商具有信息安全管理体系认证证书**（投标文件中提供复印件）** |
| 服务要求 | | 不少于免费3年原厂质保服务（自货物交采购人验收合格之日起起算） |
| 不少于免费3年原厂7\*24小时上门现场服务支持（自货物交采购人验收合格之日起起算） |
| 原厂工程师实施及提供设备相关的培训，提供原厂产品培训1天。 |
| 提供原厂常驻浙江省内不少于6个经中国信息安全测评中心认证的注册信息安全专业人员-大数据安全分析师（CISP-BDSA）（投标文件中提供证书复印件），以便提供快速的售后服务。 |

**30.网站卫士（网页防篡改）**

|  |  |  |  |
| --- | --- | --- | --- |
| 功能类别 | 技术要求及指标 | | |
| 资质 | 产品[具有公安部产品销售许可证](#_销售许可证)**（投标文件中提供复印件）** | | |
| 厂商具有信息安全应急处理服务资质（一级）**（投标文件中提供证明材料）** | | |
| 厂商为国家级网络安全应急服务支撑单位**（投标文件中提供证明材料，如CNCERT网站截图）** | | |
| 为了实现网页防篡改系统与WEB应用防火墙的的联动，网页防篡改系统与WEB应用防火墙为同一厂商生产的产品。 | | |
| 基本要求 | 产品形态 | 软件 | |
| 支持的操作系统 | Windows2000,2003,2008 32&64位。 | |
| Redhat,CentOS,SUSE,Asianux等32&64位。 | |
| UNIX系列：AIX,HP-UX,Solaris。 | |
| 支持WEB服务器 | IIS，apache。 | |
| java系列(weblogic,websphere,tomcat,jboss等) | |
| nginx | |
| 管理方式 | B/S管理方式 | |
| 核心技术 | 采用先进内核驱动、WEB核心内嵌和实时触发机制结合 | |
| ★数据库弱点扫描模块 | 产品形态：软件，提供光盘介质及其加密狗。 | | |
| 扫描数据库漏洞，防止通过修改数据库来执行网站的页面篡改。 | | |
| 通过模拟黑客攻击的方式，利用数据库本身存在的漏洞，获取数据库管理员的权限并登录到数据库中。 | | |
| 能够实时检测出黑客入侵数据库后对数据库系统对象的篡改，还能探测出黑客创建的一些隐藏对象，比如隐藏的具有DBA权限的用户，并提供详细的扫描报告。 | | |
| 防篡改功能 | 文件保护 | | 支持各类网页文件的保护，包括静态和动态网页以及各类文件信息。 |
| 目录保护 | | 支持对指定文件夹以及子文件夹的保护，避免上传非法文件及木马等恶意文件或插入恶意代码。 |
| 断线检测和防护 | | 在与其它模块网络断开的情况下能防止文件被篡改 |
| 许可设置 | | 支持基于目录、进程、文件、文件类型等进行设置许可 |
| 支持正则表达式设置许可策略 |
| 支持对符合许可策略的更新发布进行审计 |
| 自我保护 | | 防篡改程序的进程被kill，防篡改功能不会失效。 |
| 防篡改程序有自我保护机制 |
| ★防攻击功能 | WEB安全防护 | | 能够有效防止SQL注入攻击、跨站攻击、溢出代码攻击、对危险文件类型的访问、对危险系统路径的访问、特殊字符构成的URL利用、防止构造危险的Cookie等。 |
| 防字段溢出 | | 支持自定义HTTP头的各字段溢出自定义**（投标文件中提供功能截图）** |
| 规则自定义 | | 支持防护规则基于HTTP头的各字段进行自定义**（投标文件中提供功能截图）** |
| 基于时间，IP调整规则 | | 能根据时间段，IP段进行规则调整**（投标文件中提供功能截图）。** |
| 管理控制 | 站点管理 | | 对WEB服务器的CPU，内存，磁盘等信息进行监控展显。 |
| 用户管理 | | 支持多用户分级管理 |
| 管理端支持ACL设定允许的源IP才能访问**（投标文件中提供功能截图）。** |
| 日志 | | 支持多种日志级别，并支持日志导出。 |
| 相同日志支持归并展现 |
| 告警方式 | | 支持SYSLOG、邮件、短信、界面提示等多种告警方式 |
| 性能指标 | 最大保护对象 | | 不限 |
| 最大保护深度 | | 不限 |
| 占用资源情况 | | CPU，内存占用资小于3% |
| 文件保护：在保护目录下，用任意进程，对任意类型的文件，进行任意的修改，确保文件不能被篡改，并保证被修改的操作都能记录日志**（投标文件中提供功能截图）。** | | | |
| 文件更新：对于被保护的目录进行文件更新，需要能通过进程、文件类型、目录路径等三个维度进行许可设置，并能对更新操作进行日志记录**（投标文件中提供功能截图）。** | | | |
| 防攻击模块：对被保护的网站进行各种sql注入攻击、xss脚本探测都能正常的防护，并详细记录日志**（投标文件中提供功能截图）。** | | | |
| 其他要求 | 通过对http字段的溢出防护长度限制进行修改，在访问的时候以超过长度的请求进行访问，服务器返回403是被网站卫士拦截；主要是rfc2616规范，对http头各字段的长度有明确的要求，超过长度的请求可能被作为恶意攻击而利用。 | | |
| 管理端支持ACL：设置允许的源IP，确保最大限度的保障管理端的安全。 | | |
| 同步端HA功能：验证方法在部署同步端的时候在两台机子上安装同步端，关闭其中一台，看看另一台是不是能正常发布，主要的应用场景是对发布端有高可用要求的。 | | |
| 基于时间调整规则：验证的方法是对某条规则设置自动生效时间，在规则的时候能阻断符合特征的请求，不在规则的规定的时间内不能生效（时间以web服务器的系统时间为准），主要应用于某些系统在特定的时间内有特定的访问请求。 | | |
| 用户自定义规则：应用层的安全防护不像网络层那样简洁明了，产品内置了非常精练的规则，但在实际的应用中能防护95%以客户的90%需求，对于未能覆盖的需求，产品提供了非常友好配置界面，让用户可以自定防护规则，基本上不需要非常专业的知识，完全可以根据日志里的提示信息进行规则调整。 | | |
| 售后服务 | 提供原厂3年免费升级维护（自货物交采购人验收合格之日起起算） | | |
| 提供原厂产品培训服务 | | |
| 提供原厂常驻浙江省内不少于6个经中国信息安全测评中心认证的注册信息安全专业人员-大数据安全分析师（CISP-BDSA）（投标文件中提供证书复印件），以便提供快速的售后服务。 | | |

**31.网站安全监测服务**

|  |  |  |
| --- | --- | --- |
| 功能类别 | | 技术要求及指标 |
| 期限及频率 | | 一年，7\*24小时 |
| 网站安全监测服务 | | 对网站进行7\*24小时漏洞、木马、篡改、可用性、关键字监测 |
| 单位与资产管理 | ★资产识别 | 能够对辖区在线系统自发现的能力，并可提供发现设备的详细基础数据列表，数据类型如下：信息系统域名，域名所有者，域名解析者，网站与业务系统名称，IP地址，资产IP归属地，网站备案号。 |
| 资产指纹 | 能够为用户的在线资产进行指纹信息的采集，并为用户提供发现设备的指纹信息数据，支持的指纹类型包括如下：应用服务器指纹，操作系统指纹信息，开发语言指纹信息，CMS指纹信息，开发框架指纹。 |
| 单位与资产管理 | 支持可以通过IP段、网站注册单位等方式自动关联网络资产与所属单位 |
| 支持对网站进行资产类型配置 |
| 单位下可设立安全联系人、安全负责人等类型角色，以适用在不同的通报场景。 |
| 安全监测预警功能 | ★漏洞扫描 | 支持常见的WEB应用弱点检测，支持OWASP TOP 10等主流安全漏洞，如：SQL注入、Cookie注入、Base64注入、XSS跨站脚本、框架注入、链接注入、隐藏字段、CSRF跨站伪造请求、命令注入、命令执行、代码注入、遍历目录、弱口令、表单绕过、文件包含、管理后台、敏感信息泄漏、第三方组件、其他各类CGI漏洞等各种类型。 |
| ★篡改监测 | 支持对页面中非法变更智能监测，可实现图片篡改、代码篡改、内容篡改等类型识别，要求能够过滤正常变动，提取出黑客篡改行为。 |
| ★暗链监测 | 支持对页面中的隐藏链接、UA作弊内容等非法内容植入的监测，包括对广告、游戏、博彩、色情、医疗、推广等类型进行监测。 |
| 0day预警 | 支持对0day漏洞进行指纹配置，通过指纹与版本的识别，对网站进行定向精准0day预警。 |
| 安全通报 | ★安全通报 | 平台支持对安全问题的通报，且满足：通报时可以自动匹配网站建设方和上级监管单位，当网站未预先设置联系人时可以手工添加。 |
| ★安全跟踪 | 在事件通报后，管理单位可以对问题进行跟踪：可以自动化的对漏洞进行跟踪，可以对问题的处置状态进行跟踪，支持自定义超期时间且当下级超时未处理时，提示超期且可以进行二次通报。 |
| 安全处置 | 问题通报后，下级单位可以通过账号登录平台进行反馈处置：下级可以在平台上提交处置，包括已修复，已关闭等反馈，当出现通报资产不属于下级资产时，下级可以进行回退上报操作。 |
| 管理功能 | 报告与报表 | 为满足监管需求，可以对监管数据进行多维度的统计：对发现事件总数、处置数和处置率等进行统计，根据不同的事件类型，如漏洞、暗链等分别统计发现量、通报量和处置量，按照不同的事件状态和事件进行趋势展示，根据下级被监管单位的类型分别统计漏洞和暗链的发现量、通报量和处置量，对下级单位可以按照不同的安全问题类型和问题发生数量进行排行。 |
| 考核评分 | 支持对下级单位发生事件，处置事件时效性等维度进行考核评分，并可定期对评分进行排行公布。 |
| 公告通知 | 支持监管单位可以对指定的下级单位推送公告通知，包括会议通知、公告等类型，支持反馈回执。 |
| 报平安功能 | 支持在指定的报平安时段内，要求指定的下级单位每天报送平安或者异常情况，执行零汇报制度。 |
| 安全资讯 | 支持每日接收外部各类安全资讯进行展示 |
| 为统一维护、统一管理，需与远程安全评估系统一品牌。 |
| 安全运营服务 | 7\*24安全值守 | 服务提供7\*24小的安全专家值守服务，实时发现各类安全威胁，第一时间安全告警通知。 |
| 资质 | ★厂商具有信息安全管理体系认证证书**（投标文件中提供复印件）** |
| 产品具有公安部销售许可证**（投标文件中提供复印件）** |
| 产品具有软件著作权登记证书**（投标文件中提供复印件）** |
| 产品具有国家信息安全产品认证证书（ISCCC）**（投标文件中提供复印件）** |
| 产品具有[信息技术产品安全测评证书](#_国家信息安全测评EAL3+)，级别EAL3**（投标文件中提供复印件）。** |

**32.安全评估服务**

|  |  |  |
| --- | --- | --- |
| 功能类别 | 技术要求及指标 | |
| 资质 | ★产品制造商具有信息安全管理体系认证证书**（投标文件中提供复印件）** | |
| 产品具有公安部销售许可证**（投标文件中提供复印件）** | |
| 产品具有软件著作权登记证书**（投标文件中提供复印件）** | |
| 产品具有国家信息安全产品认证证书（ISCCC）**（投标文件中提供复印件）** | |
| 产品具有[信息技术产品安全测评证书](#_国家信息安全测评EAL3+)，级别EAL3**（投标文件中提供复印件）。** | |
| 期限及频率 | 一年4次 | |
| 服务范围 | 对重要系统的系统层、应用层、业务层进行安全扫描、渗透测试和人工审计 | |
| 工具要求 | ★提供自主研发的专业WEB应用弱点扫描工具 | |
| ★提供自主研发的数据库弱点扫描工具 | |
| ★提供自主研发的等级保护检查工具 | |
| ★提供自主研发的网页后门检查工具 | |
| ★提供自主研发的应急处置工具箱 | |
| ★提供自主研发的计算机终端审查工具 | |
| WEB应用弱点扫描工具 | 产品具有[信息技术产品安全测评证书](#_国家信息安全测评EAL3+)，级别EAL3+级别**（投标文件中提供复印件）。** |
| ★产品具有IT产品信息安全认证证书**（投标文件中提供复印件）** |
| ★支持对各种挂马方式的网页木马进行全自动、高性能、智能化分析，并对网页木马传播的病毒类型做出准确剖析和网页木马宿主做出精确定位**（投标文件中提供截图）。** |
| 支持常见的WEB应用弱点检测，支持OWASP TOP 10等主流安全漏洞，支持指纹识别、暴力猜解、Webshell、暗链扫描。 |
| 支持指纹识别、暴力猜解、Webshell、暗链扫描 |
| 支持自动化漏洞验证和沙盒技术，对目标应用进行深入安全分析，取得系统安全威胁的直接证据。 |
| 数据库扫描工具 | ★支持针对数据库每张表每个字段的内容进行敏感数据探测；敏感信息用户可以自定义添加，可以让用户了解自己的数据库系统有哪些敏感数据，存放的具体位置，便于在信息保护和审计中重点关注。 |
| 提供自动搜索功能，可以自动搜索出某一网段或指定IP范围内（端口号可默认或指定范围）的活动数据库，轻松获得数据库的基本信息（包括IP、数据库类型、服务名、端口号、数据库版本、操作系统类型、主机名等），可按时、按日、按周定制扫描计划，到时间自动进行扫描。 |
| 使用具有DBA权限的数据库用户，执行选定的安全策略实现对目标数据库的检测。 |
| 用户在没有授权的情况下（即：不需要数据库的用户名和密码），依据数据库版本号并根据选定的安全策略对目标数据库进行的检测。 |
| 能够实时检测出黑客入侵数据库后对数据库系统对象的篡改，还能探测出黑客创建的一些隐藏对象，比如隐藏的具有DBA权限的用户，并提供详细的扫描报告。 |
| 按漏洞类型分类：（1）缓冲区溢出漏洞（2）访问控制漏洞（3）提权漏洞（4）PL-SQL注入漏洞（5）执行权限过大漏洞（6）访问权限绕过漏洞（7）弱口令（8）数据库内  核入侵探测（9）安全信息查看（10）敏感数据探测 |
| 按风险级别分为类：（1）紧急（2）高危（3）中危（4）低危（5）信息 |
| 提供扫描策略可自定义模式，操作者可以灵活选择默认策略的同时也可以自定义添加策略。 |
| 支持CVE、CNNVD标准 |
| 提供直观的风险危害等级图表和风险类型统计图表、漏洞的描述、漏洞的风险级别、加固建议 |
| 输出报告格式包括PDF、WORD、XLS等 |
| Webshell后门检查工具 | 支持各类WEB编程语言的应用的深度网页后门漏洞扫描 |
| 支持常见的asp、php、jsp、aspx等多种WebShell的有效扫描 |
| 支持实时结果的展现 |
| 支持生成统计报表 |
| 扫描对象：支持IIS、Websphere、Weblogic、Apache等所有的应用服务器，支持Asp、Jsp、.Net、J2EE、Php、Perl等所有的WEB应用编程语言。 |
| 扫描功能：  具有快速扫描功能：支持根据文件类型自动选择内置扫描策略进行扫描，例如当进行扫描index.ASP文件时程序会自动选择ASP对应的策略进行扫描而忽略其他的扫描策略；  具有全盘扫描功能，支持扫描所有内置的策略以及用户自定义策略；  具有自定义扫描功能，支持文件类型、优先级、扫描策略等用户自定义。 |
| 报告输出：  支持提供详细的检测报告，报告内容包括不限于扫描的URL信息、漏洞类型、安全加固建议等，同时支持对所有弱点的相关背景提供详细描述、引用，以及相应的修复和改进建议；  支持PDF、html、xml等多种格式的报表输出。 |

**33.应急演练服务**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 期限及频率 | 一年，一年1次 |
| 服务范围 | 提供全方位的应急演练场景模拟策划、方案编制和组织实施 |
| 资质 | ★厂商具有信息安全管理体系认证证书**（投标文件中提供复印件）** |
| 产品具有公安部销售许可证**（投标文件中提供复印件）** |
| 产品具有国家信息安全产品认证证书（ISCCC）**（投标文件中提供复印件）** |
| 产品具有[信息技术产品安全测评证书](#_国家信息安全测评EAL3+)，级别EAL3**（投标文件中提供复印件）。** |

**34.应急响应服务**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 期限 | 一年 |
| 服务范围 | 当安全威胁事件发生后迅速采取的措施和行动，最快速恢复系统的保密性、完整性和可用性。 |
| 应急响应服务能力 | 服务内监测的任意系统由于安全事件、安全问题崩溃、系统性能严重下降等情况，导致停止服务或者造成恶劣影响的，服务提供须在浙江省内配有较强的专业技术队伍进行应用响应服务。 |
| 资质 | ★厂商具有信息安全管理体系认证证书**（投标文件中提供复印件）** |
| 产品具有公安部销售许可证**（投标文件中提供复印件）；** |
| 产品具有[信息技术产品安全测评证书](#_国家信息安全测评EAL3+)，级别EAL3**（投标文件中提供复印件）。** |
| 应急处置工具箱 | 任务管理：  支持从应急处置管理平台下发处置任务，也可以新建应急处置任务；  处置任务的内容应包括事件描述、事件类型、事件级别、事发时间、事发单位、单位联系人、单位联系人电话、系统名称、保护等级、处置人员、资产信息等。 |
| 访谈记录：  根据事件的级别，询问调查表分为简表和完整表，简表针对一般事件，完整表针对重大事件；  支持对情况记录表单进行编辑、导入、导出、打印；  支持处置过程访谈记录的上传、下载、删除。 |
| 攻击发现：  支持将漏洞验证工具检测结果与资产进行关联，并在工具箱上查看相应的扫描结果；  ★支持数据库漏洞检测、系统漏洞检测、网站漏洞检测、病毒检测、木马检测；  支持一键导入功能，将验证工具集检测结果自动导入到工具箱；  支持手动导入工具检测结果到工具箱及关联任务验证对象。 |
| 关联分析：  日志取证模块采用只读锁的方式提取保证现场主机证据不会被破坏；  日志提取应包括操作系统日志、中间件日志及相关网站后台操作日志。  支持在线取证；  能够对开启的主机的内存、硬盘进行证据固定，支持DD、E01、aff的镜像格式；  能够对开启的主机直接进行安全事件取证；  支持离线取证：  能够对关闭的主机的硬盘进行证据固定，支持DD的镜像格式；  能够对关闭的主机直接进行安全事件取证；  取证设备对象支持存储设备、边界设备、主机/服务器；  在不改变设备运行状况的前提下，不拆机箱对应急处置对象硬盘进行取证，可以获取包括整个硬盘、分区、目录和文件等各个级别的数据；  对于开机情况下的设备，在不改变设备运行状况的前提下，在线对应急处置对象进行取证，可以获取内存信息、运行状态信息、已保存的密码、硬盘、分区、目录和文件等各个级别的数据；  支持基于IA32架构的笔记本、PC和服务器；  支持IDE、SATA、SCSI、RAID等各种接口硬盘和数据架构；  支持Dos/Windows文件系统，包括：FAT、FAT32、NTFS；  支持常见的其它文件系统，包括：EXT2/3/4、UFS、XFS、HFS、JFS、MINIX、HPFS等；  数据获取速率最高可以能达到2.5GB/分钟；  取证过程中，支持对中间硬盘进行数据擦除，确保多次取证不会造成互相干扰；  支持自动关联；  能够自动查找外接设备中的镜像文件、日志信息并获取其中的安全事件相关信息；  支持手动关联；  能够手动指定镜像文件、日志信息所在的位置，获取其中的安全事件相关信息；  支持自动分析；  能够自动从镜像文件、日志信息中分析出事件名称、源地址、源端口、目标地址、目标  端口；  能够按照事件类型：基本事件、聚合事件、关联事件、三维关联事件进行查询；  支持按照事件威胁等级、关键字、时间进行查询；  支持专家分析；  能够从镜像文件、日志信息中分析出源IP、方法、报文；  能够对分析出的记录进行多条件的关键信息查询，支持“和”“或”两种查询组合；  提供简洁易用的的操作界面，以位对位的硬盘复制形式，保证对象计算机的硬盘数据没有任何的改变，提供现场快速获取和介质分析的功能；  支持Unix/Linux/Mac os/Windows等多种操作系统的在线或离线取证。  事件处置：  支持对应急处置进行结果定性；  支持存在的漏洞、事件发生过程、事件发生的原因、事件处置及结果的填写。  处置报告：  支持手动导入工具检测结果到工具箱及关联任务验证对象；  资产安全漏洞应包含网站安全漏洞、网站恶意代码、sql注入验证、操作系统及应用软件漏洞、数据库安全漏洞等安全风险；  应急处置情况应包含事件发生的过程、发生的原因及分析、事件如何处置及处置结果；  支持生成不同类型的应急处置报告。  知识库：  知识库内容包含各种操作系统常用命令，如windows系统、linux系统；  知识库内容包含提权常用命令；  知识库内容包含各种sql注入点；  知识库内容包含多种常见、高危漏洞的描述及原理。 |

**35.网站云防护服务**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 资质 | 厂商具有信息技术服务管理体系认证证书**（投标文件中提供复印件）** |
| ★厂商为国家级网络安全应急服务支撑单位**（投标文件中提供证明材料，如CNCERT网站截图）；** |
| ★厂商通过国家信息安全等级保护三级**（投标文件中提供证明材料）** |
| 服务年限 | 一年 |
| 平台要求 | 全国范围内具备至少50个云防护和CDN加速节点 |
| ★支持不小于300Gbps拒绝服务攻击流量防护能力 |
| ★安全防御平台为一体化平台，应同时具备网站漏洞监测、可用性监测、攻击防御状态、防护报表、页面防篡改等功能，所有的功能集成在同一产品上实现，所要求的功能提供可视化界面配置，能为每个网站单独创建用户账号，用于查看网站的安全状况，管理员用户账号可关注、查看网站整体情况**（投标文件中提供截图）。** |
| 为统一维护、统一管理，需与数据库审计系统同一品牌。 |
| 部署方式 | 无需在网站前端安装任何安全设备、软件，通过DNS流量指向到云端进行安全防护。 |
| 支持将防护网站NS解析到云防护DNS服务器，支持将防护网站CNAME别名指向云防护。 |
| 防御功能 | 支持检查提交的报文是否符合HTTP协议框架，如异常的请求方法、特殊字符、重点字段的缺失、超长报文造成的溢出攻击以及对高危文件的访问等。 |
| DDOS畸形报文过滤，过滤frag flood、smurf、stream flood、land flood、攻击ip畸形包、tcp畸形包、udp畸形包。 |
| 传输层DDoS攻击防护，过滤syn flood、ack flood、udp flood、icmp flood、rstflood。 |
| 连接型DDoS攻击防护，过滤TCP慢速连接攻击、连接耗尽攻击、tcp新建连接限制等攻击和loic、hoic、slowloris、Pyloris、xoic等慢速攻击。 |
| 特征过滤，4层ip+port过滤和7层payload部分内容过滤。 |
| 支持识别恶意请求含：跨站脚本(XSS)、注入式攻击（包括SQL注入、命令注入、Cookie注入等）、跨站请求伪造等应用攻击行为 |
| 支持识别服务端响应内容导致的缺陷：敏感信息泄露、已有的网页后门、错误配置、目录浏览等缺陷 |
| 支持基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力。 |
| 支持识别网站中的网页木马程序，通过策略可防止木马网页被用户访问。 |
| 支持对用户上传的文件后缀名和文件内容进行全方面检查，杜绝Webshell的上传和访问。 |
| ★支持区域访问控制，限制国外用户或者国内以省市为单位的区域进行访问控制。 |
| 支持对WEB服务器容器、应用中间件、CMS系统等第三方组件漏洞进行有效防护 |
| 支持页面缓存，通过水印匹配算法防止页面被篡改。 |
| ★支持智能识别攻击者，对网站连接发起攻击的IP地址进行自动锁定禁止访问被攻击的网站**（投标文件中提供界面截图）。** |
| ★支持一键虚拟补丁功能，网站出现0day漏洞时能快速完成修复**（投标文件中提供界面截图）。** |
| ★支持按地理区域对攻击次数等进行统计，通过地图展示，用户可在地图上可以指定某一地理区域进行访问控制，阻断此区域IP的访问**（投标文件中提供界面截图）。** |
| ★支持一键关停功能，当网站出现紧急安全事件时，可在一分钟内通过手机APP和浏览器一键完成关停，防止产生恶劣影响**（投标文件中提供界面截图）。** |
| 安全审计 | 能详细记录攻击事件的HTTP请求头信息，含请求的URL、UserAgent、POST内容，cookie等所有的请求头内容。 |
| 能详细记录服务器响应头信息，包括状态码、服务器类型等信息。 |
| 防护内容 | 对单位在阿里云平台中的门户WEB应用系统实行云端防护建设，防护黑客发起的Syn-flood、upd-flood、tcp-flood、应用层CC等攻击，并对黑客发起的注入、跨站、网页木马、扫描器、组件0day攻击、盗链等攻击进行防护。 |
| 告警方式 | 支持Syslog、手机短信、邮件、密信等多种告警方式 |
| CDN内容加速 | ★全国范围内具备至少20个CDN加速节点支持页面缓存和压缩 |
| 云监测 | ★支持服务质量监测，支持全国多省服务是否中断或报错告警、访问延时分析、域名劫持监测、页面加载质量分析、CDN服务质量监测。 |
| ★支持钓鱼监测，通过大数据监测网络中是否存在与防护对象相匹配的钓鱼网站，发现钓鱼网站后及时与用户沟通并协助上报处置。 |
| ★支持漏洞检测，对网站存在的脆弱性进行探查，包括SQL注入漏洞、跨站脚本漏洞、开放服务漏洞、网站第三方应用漏洞等，及时发现漏洞。 |
| ★支持篡改监测，监测出网站是否被嵌入暗链地址、监测网站是否存在非法外部链接、监测网站内容是否存在敏感内容、监测网站是否篡改为黑页。 |
| 手机APP管理 | ★通过手机APP查看网站整体防护态势，包含网站漏洞监测、可用性监测、攻击防御状态、防护报表、页面防篡改等状态信息。 |
| ★通过手机APP完成防护配置，包括一键关停、防护模式、永久在线等功能。 |
| 服务能力 | ★具有云端7\*24远程安全专家服务能力**（投标文件中提供相关的证明材料，含办工场地，人员情况，服务过程性材料截图等）。** |

**36.智能排查软件系统**

|  |  |
| --- | --- |
| 功能类别 | 技术要求及指标 |
| 功能要求 | 支持Windows、Linux平台及MS SQL、Oracle数据库，支持B/S架构； |
| ★实现一站式智能运维界面功能，通过智能运维门户可以提供向导式的网络运维，设备管理、故障排查、维护大全、开局助手、控制台、云图、工具宝箱等功能（**投标文件中提供相关证明材料并进行现场演示）。** |
| ★实现故障排查及脚本管理功能，可通过选择故障设备、选择故障类型、确定前置条件，然后通过信息收集，信息分析，提供向导式解决方法**（投标文件中提供相关证明材料）。** |
| 实现自定义脚本、公共协议、交换技术、路由技术、无线、安全产品、交换机产品、路由器产品的脚本管理功能**（投标文件中提供相关证明材料）。** |
| ★实现云图功能，提供网络公共协议、交换技术、路由技术、无线产品、安全产品、管理软件、云计算产品、路由产品、交换机产品向导式运维方式，提供从解决各个问题最开始到解决问题的各种方法**（投标文件中提供相关证明材料）。** |
| 实现远程控制台功能，通过控制台可实现设备集中远程控制功能，通过新建设备连接，提供设备远程控制及运维。 |
| ★实现工具宝箱功能，用户可自定义常用功能界面，提供常用协议号查询、常用端口号查询、MAC厂商查询、FTP客户端查询、FTP服务器查询、TFTP服务器查询、IP地址划分、IP地址归属查询、条件申请查询、设备维保查询、板卡配套查询、快速Ping扫描查询、报文格式查询、日志转读查询、序列号二维码、命令查询、ACL信息查询等（**投标文件中提供软件功能截图及相关证明材料并进行现场演示）。** |
| 个性化要求 | ★中标人应根据之江实验室实际需求，无偿进行系统表格、样式及功能模块调整，调整费用包含在合同总价中。 |
| ★各类应用系统对接工作由中标人自行负责，系统集成的对接费用包含在合同总价中，不得另行收费。 |

**除招标文件中所明确的技术规格和品牌外，欢迎其他能满足本项目技术需求且性能相当于或高于所明确品牌的产品参加投标报价，同时在需求偏离表中作出详细对比说明。**