**长江石化网络等保2.0**

**二级项目技术规格书**

1. **总体技术要求：**

根据公安部关于开展重要信息系统和重点网站安全执法检查的工作要求，有效应对当前江苏长江石油化工有限公司网络安全面临的严峻威胁与挑战，全力做好江苏长江石油化工有限公司重要信息系统网络安全保卫工作，亟需对江苏长江石油化工有限公司的核心系统展开等保评测及等保加固工作，通过该评测工作及时发现系统安全隐患并迅速进行整改，从而全面提升江苏长江石油化工有限公司的网络安全防护水平，保障系统的安全、高效、稳定运行。

1. **网络安全升级改造**

基于我公司现有的网络情况进行整体升级改造，要求改造后实现三网分离、满足等保2.0标准，改造后拓扑图如下：



1. **安全等级二级等保认证**

测评数量：二级系统1个（系统名称：CA系统）

具体项目流程分为前期准备、现场实施、报告分析与编制、检查验收、总结验收五个阶段。，二级等保2年做一次，确保不过期至少5年内做2次测评，确保五年内等级保护证书不过期。，

1. **项目需采购设备如下：**

|  |  |  |
| --- | --- | --- |
| **序号** | **设备类型** | **数量** |
| 1 | 防火墙 | 2 |
| 2 | 零信任（设备/扩展模块） | 1 |
| 3 | 数据库审计 | 1 |
| 4 | 日志审计 | 1 |
| 5 | 堡垒机 | 1 |
| 6 | 威胁探针 | 2 |
| 7 | 态势感知平台 | 1 |
| 8 | WEB应用防火墙 | 1 |
| 9 | 办公网网闸 | 1 |
| 10 | 视频流网闸 | 1 |
| 11 | 工控防火墙 | 1 |
| 12 | 终端杀毒 | 100 |
| 13 | 数据备份一体机 | 1 |

1. **项目实施要求：**

所有采购的设备，供应商应按照我单位的要求安装、调试、测试后，等待验收。对于设备型号的选择，供应商应采用符合我单位技术与兼容性要求的一线设备品牌，根据参数性能的要求，提出最优的方案。

以上设备必须与我单位现有对应网络、服务器设备兼容。

中标方需要完全按照我单位要求，完成但不限于以下要求的工作，直至满足我单位对于该项的所有技术要求。

* 所有项目全部完成并通过国家安全第二级等级保护，并取得二级认证证书。
* 设备上架并按照要求完成所有的配置工作。
* 所有设备要提供5年质保及5年的特征库更新服务
* 协助制定符合国家二级等级保护要求的信息化规章和制度。
* 提供新设备与现有设备的连接与配置服务，且保障正常安全生产。
* 变更窗口约束：所有可能影响生产系统的操作（如防火墙策略调整、核心设备升级）需在甲方指定的非业务高峰时段（如每日00:00-05:00）进行，单次操作时长不得超过2小时，超时需立即回滚并提交故障分析报告。
* 灰度发布机制：网络拓扑变更或安全策略更新必须通过分段灰度发布，先在测试环境验证48小时，再选取≤10%的生产节点试运行72小时，确认无异常后方可全量部署。
* 4.2 生产环境隔离保护
* 网络分区：实施阶段需通过VLAN或物理隔离划分临时实施专区，与核心生产区域之间部署双向流量监控探针，实时捕获异常流量（如突发ICMP洪水、异常SQL连接）。
* 回滚快照：对受影响的生产系统（如数据库、工业控制服务器）提前生成全量数据快照，快照保存周期覆盖项目实施全程至验收后30天，支持一键回滚至变更前状态。
* 4.3 业务连续性保障
* 双活热备：涉及边界防护设备（如防火墙、IPS）更换时，需采用双机热备+心跳检测模式，切换过程业务中断时间≤30秒，且需提供备用设备性能不低于主设备90%的测试证明。
* 熔断机制：部署安全设备（如WAF）过程中，若触发生产系统CPU持续≥80%或内存溢出告警超过5分钟，自动切换至bypass模式并通知甲方运维人员介入。

**硬件参数要求：**

**防火墙：2套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 硬件要求 | 提供标准1U机型，提供≥1个MGMT（管理口），≥8个千兆电接口，≥8个千兆光接口，≥2个万兆光接口，≥1个接口卡扩展槽位，≥2个内置电源，≥10个并发SSL VPN用户授权，CPU和操作系统需满足国产化要求。提供IPS及AV防护规则库5年升级授权。 |
| 2 | 性能要求 | 整机吞吐量≥12G，每秒新建会话数≥13万，最大并发会话数≥200万，IPSec吞吐量≥4G，IPS吞吐量≥5.5G，AV吞吐量≥4.5G |
| 3 | 部署方式 | 支持虚拟线，二层透明，三层，混合，旁路监听，单臂接入方式 |
| 4 | 网络适配性 | 支持三层接口、三层子接口、环回接口、VPN接口 |
| 支持VLAN接口、VLAN间路由、单臂路由 |
| 支持汇聚接口，二层聚合、三层聚合、虚拟线聚合，能够手动绑定接口，聚合方式支持平衡轮询、手动负载分担和LACP |
| 支持配置虚拟线接口，可以通过配置虚拟线对，实现虚拟线的部署模式 |
| 支持VLAN划分、VLAN Trunk/Access，支持802.1Q，能进行封装和解封 |
| 支持静态路由及OSPFv2、RIPv1/v2动态路由协议 |
| 5 | 访问控制 | 支持基于IP地址、端口、协议、时间等多种方式进行综合过滤及访问控制 |
| 基于用户自定义安全策略的访问控制 |
| 支持IP和MAC地址绑定，防止IP地址盗用 |
| 支持动态网络地址转换（NAT） |
| 支持基于策略的源地址NAT、目的地址NAT和双向NAT， |
| 支持一对一、一对多、多对一等多种转换方式。 |
| 7 | 加密流量 | 支持HTTPS加密流量的安全检测，支持TCP代理和SSL代理，且代理策略中可同时配置多类过滤条件，提供功能截图 |
| 8 | DDoS防护 | 支持ARP/Ping/TCP/UDP/HTTP/DNS类型的Flood报文攻击 |
| 支持用户自定义触发流量阈值，保护流量上限，保护时长以及检测周期 |
| 9 | 日志管理 | 支持基础系统日志、系统升级日志、网络故障日志、高可用日志、审计日志 |
| 支持日志导出 |
| 支持基于日志字段进行筛选查询，并作出分类统计 |
| 支持日志展示的列自定义，展示用户关心的日志字段及信息 |
| 支持设置日志存储量阈值设置，对于超出阈值的日志，可以选择覆盖或者丢弃，并发送告警通知 |
| 10 | 管理方式 | 支持Web管理、串口管理、SSH管理  |
| 配置信息、过滤规则可以方便的备份、下载、恢复和上传 |
| 11 | 系统配置 | 支持系统重启、系统关机、应用层防护控制、web服务重启、引擎重启等操作 |
| 支持告警设置，例如CPU使用率、内存使用率、接口带宽值、告警频率 |
| 12 | 产品资质 | 产品具备《网络关键设备和网络安全专用产品安全认证证书》，提供有效证书的复印件 |
| 13 | 厂商资质 | 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全评估(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全建设(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商实施过程中具备成熟的能源管理体系，需具备能源管理体系认证证书，提供有效证书的厂商盖章复印件。 |

**零信任(可以是设备，也可以是防火墙拓展模块)**

|  |  |  |
| --- | --- | --- |
| **1** | **零信任** | ≥50个授权，支持基于UDP协议的单包授权机制，实现应用隐藏；支持通过SDP模式代理C/S或通过非http/https类协议通信的应用；支持访问控制策略，能够对用户接入进行访问控制，可设置策略匹配条件。 |
| 支持零信任服务端配置收集windows主机信息的具体内容项，包括：操作系统版本，系统补丁，防病毒软件、状态及病毒库更新，防火墙，防间谍软件及状态，IE版本及安全级别、已安装和正在运行的进程或服务、系统自动更新状态、文件路径、注册表信息等 |

**数据库审计：1套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 硬件参数 | 提供标准1U机架式设备，含交流单电源，提供≥2个USB、≥1个管理网口、≥4个千兆电口（2组bypass)、≥1个网络扩展位，网络吞吐≥1G，SQL处理性能≥10000条/s，纯数据库网络吞吐量(峰值)≥80M |
| 2 | 部署方式 | 支持多种部署方式，包括旁路镜像部署，Agent引流部署 |
| Agent部署支持在WEB端或DB端所在操作系统中进行部署。 |
| Agent支持数据传输加密，可通过界面快速开启或关闭加密传输，保证待审计数据安全传输，提供功能截图。 |
| 3 | 数据库类型 | 至少支持Oracle、SQLServer、MySQL、DB2、PostgreSQL、MariaDB等国际主流数据库审计。 |
| 至少支持ssh、telnet、nfs、smb、ftp、http、rdp、vnc等主流运维协议。 |
| 4 | 审计能力 | 支持记录数据库类型、数据库版本、登录时间、会话时长、语句类型、语句长度、语句执行回应、操作响应时长、影响行数等 |
| 支持多条规则支持策略组合。 |
| 支持审计策略自定义 |
| 支持审计查询条件自定义，至少包含：时间、数据库名称、数据库用户、主机名称、 客户端IP等查询条件。 |
| 同时支持高级查询，需包括：SQL关键字、结果集关键字查询。 |
| 支持根据行为操作等风险告警定义，按照高、中、低风险级别与响应方式关联进行告警。 |
| 5 | 日志管理 | 支持通过syslog、kafka接口外发数据，包括审计日志，告警日志等。 |
| 6 | 风险防御 |  |
| 7 | 系统管理 | 根据不同的安全级别采用不同的响应方式，响应方式包括记录、告警，告警方式包括：邮件、SYSLOG、SNMP、FTP等。 |
| 支持生成统计报表，支持以日、周、月等时间进行展示。 |
| 支持系统告警功能，包括设备异常类型以及当前状态。 |
| 支持系统资源监控与告警，支持磁盘使用率监控，当磁盘使用率达到预定的阈值时，系统会发出告警。 |
| 8 | 产品资质 | 具备中国网络安全审查技术与认证中心颁发的网络关键设备和网络安全品专用安全认证证书 |
| 9 | 厂商资质 | 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全评估(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全建设(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商实施过程中具备成熟的能源管理体系，需具备能源管理体系认证证书，提供有效证书的厂商盖章复印件。 |

**日志审计：1套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 硬件要求 | 提供标准1U机架式设备，交流冗余电源，≥2\*USB接口，≥1\*RJ45串口，≥1\*GE管理口，≥4\*千兆SFP插槽，≥6\*GE电口，≥1个接口扩展槽位，≥32G内存，≥128G SSD，≥2TB SATA硬盘，≥授权接入40个日志源，日志处理性能（峰值）≥2000EPS |
| 2 | 产品部署 | 系统应基于B/S架构，支持SSL加密模式访问，可通过web方式直接对系统进行管理 |
| 3 | 日志采集 | 系统支持的数据采集范围包括但不限于网络安全设备、交换设备、路由设备、操作系统、应用系统等 |
| 系统支持的数据采集方式包括但不限于SYSLOG、RSYSLOG、SNMP Trap、FTP等方式采集日志 |
| 4 | 日志管理 | 系统应能实现日志数据的采集并保存原始日志数据 |
| 系统应能够对异构日志格式进行统一化处理并保存统一化处理后的日志数据 |
| 系统应支持IPv4日志数据的采集、范式化、分析、展示 |
| 系统应支持日志源监控能力，包括资产维度支持展示资产详细信息 |
| 5 | 日志备份 | 系统应支持设置日志存储备份策略，可设置备份周期、备份日志类型 |
| 系统应支持备份日志导入查询 |
| 6 | 日志查询 | 系统应支持全文检索、模糊检索等多种方式 |
| 系统应支持日志检索结果展示为统计图，并可将统计图下载 |
| 7 | 事件告警 | 系统应内置事件分类，并支持自定义事件分类，可定义事件分类的风险级别 |
| 系统应内置丰富的事件规则，应支持自定义事件规则 |
| 系统应支持基于事件分类的告警规则，支持短信、声音、邮件、界面提示等多种告警方式 |
| 8 | 报表管理 | 系统应支持统计分析报表与多种文件格式导出 |
| 9 | 系统管理 | 系统应支持用户自定义账号 |
| 系统应支持管理员、审计员、操作员多种权限设置 |
| 系统应支持密码配置策略 |
| 系统应支持自身日志记录并可查询、自身CPU、内存和磁盘使用率可监控并以图形化方式动态显示，且支持状态监控和主动告警； |
| 系统应支持系统基本参数管理、基本配置管理。 |
| 10 | 产品资质 | 具备公安部计算机信息系统安全产品质量监督检验中心颁发的网络安全专用产品安全检测证书 |
| 11 | 厂商资质 | 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全评估(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全建设(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商实施过程中具备成熟的能源管理体系，需具备能源管理体系认证证书，提供有效证书的厂商盖章复印件。 |

**堡垒机：1套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 硬件参数 | 提供标准1U机架式设备，单电源，≥4T SATA硬盘，≥4\*GE电口，≥1\*GE管理口，≥1个接口扩展槽位。授权管理≥40台设备。 |
| 2 | 产品架构 | 软硬件一体化产品。系统应基于B/S架构，支持SSL加密模式访问，可通过web方式直接对系统进行管理 |
| 支持基于SDP技术的远程接入，无需额外部署VPN设备。支持服务隐藏功能，开启后，攻击者无法扫描到对应服务端口 |
| 支持服务端口代理功能，支持可将多个服务端口代理成一个，提供功能截图 |
| 3 | 组织管理 | 支持划分多级组织架构，支持管理员批量导入用户信息，可通过勾选账户进行管理。 |
| 支持划分多级组织架构，不同层级有独立的用户管理，支持不同角色相互组合。 |
| 支持对IPv6和IPv4双栈网络下托管设备运维管理和用户访问 |
| 4 | 用户认证 | 堡垒机具有用户角色权限自定义功能，可对用户进行细粒度权限划分 |
| 支持多种认证方式，包括本地静态密码认证、LDAP认证、RADIUS认证、USBKEY认证、PIN+软件OTP等身份认证方式。 |
| 5 | 资产管理 | 支持资产托管账号密码检查，配置包含但不限于：密码强度检查规格，最小长度，检查后可通过列表展示。 |
| 6 | 运维管理 | 支持RDP、X11、VNC、SSH、TELNET、等协议的运维。  |
| 支持通过PC/Web Portal唤起本地浏览器来访问目标网页，包括chrome、edge、firefox等常用浏览器。 |
| 支持可通过参数配置开启或关闭字符、图形、文件、数据库等协议运维行为审计。 |
| 7 | 支持终端合规检查策略，包含针对Windows补丁检测、操作系统版本检测、端口检测、进程检测和安装应用检测。支持可由管理员自定义配置合规策略，自定义范围包括但不限于检查项、告警等级、执行操作等 |
| 8 | 运维审计 | 支持运维审计，审计日志包括认证日志、图形审计、字符审计、文件审计、数据库审计、系统日志。 |
| 支持自动化运维，支持自定义自动化脚本，可在线编辑和本地导入。支持设定任务为手动、定时和周期执行方式。支持登录后自动执行脚本，执行完后堡垒机保存运维记录。 |
| 支持FTP和NFS备份，支持手动备份和自动备份，支持备份指定的日志类型，支持日志从FTP恢复和从文件恢复。 |
| 支持超限和超时自动清理日志，日志超限自动清理。 |
| 9 | 产品资质 | 具备中国网络安全审查技术与认证中心颁发的网络关键设备和网络安全专用产品认证证书拥有软件著作权证书，厂家需具备产品自主知识产权，禁止OEM贴牌投标（提供证明文件）。 |
| 10 | 厂商资质 | 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全评估(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全建设(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商实施过程中具备成熟的能源管理体系，需具备能源管理体系认证证书，提供有效证书的厂商盖章复印件。 |

**安全探针：2套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 硬件要求 | 标准1U机架式硬件，交流冗余电源，≥64G SSD，≥4\*GE电口，≥1\*GE管理口，网络层吞吐≥1Gbps。需提供日志威胁管理、全流量威胁管理、脆弱性管理、资产管理、一键响应、态势感知等功能 |
| 2 | 流量采集及存储 | 支持IPV4/IPV6流量解析。 |
| 支持流量白名单，过滤掉不关注资产流量 |
| 3 | 协议解析 | 支持常见应用的识别 |
| 支持对包含：TCP、UDP、ICMP、SCTP、HTTP、FTP、SMTP、DNS、POP3、LDAP、TELNET、SSL、RDP、SNMP、SSH、VNC、等常见协议的深度解析和还原。 |
| 支持对流量中出现的文件进行发现和还原，支持还原的协议包括：HTTP、FTP、SMTP、POP3、IMAP、SAMBA、WEBMAIL。 |
| 4 | 入侵检测 | 应覆盖多种攻击特征，可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测  |
| 支持常见应用服务爆破检测。 |
| 支持常见数据库协议的口令暴力破解检测。 |
| 5 | 告警白名单 | 支持对告警进行一键例外，快速屏蔽掉业务异常告警。 |
| 支持自定义告警白名单。 |
| 6 | 威胁告警 | 支持不同条件检索告警日志，包含时间、威胁等级、攻击IP、攻击端口、受害IP、受害端口等 |
| 告警详情日志支持关联会话日志和元数据日志，并支持通过页签对报文多维度展示 |
| 支持对网络中的流量统计，统计类型包括应用流量的构成和占比、协议的构成和占比、接口流量统计和接口流量趋势。 |
| 支持从攻击者角度进行分析，对攻击者进行画像，攻击者属性包括攻击时间、详情等。 |
| 支持从受害者角度进行分析，对受害者进行画像，受害者属性包括资产IP、资产组、资产类型和风险级别和详情。 |
| 7 | 系统管理 | 系统应提供基于Web的远程GUI管理完成策略配置、警报查询、攻击响应、集中管理等各种任务。 |
| 系统应具备系统运行状态监控功能，能够实时查看CPU使用率、内存使用率、磁盘剩余空间、系统运行时间、接口状态、流量等信息。 |
| 支持威胁检测规则的开启/关闭 |
| 系统内置故障诊断模块，支持对硬件故障、系统资源故障进行检测 |
| 故障诊断模块支持查看故障告警图表、故障告警趋势图表 |
| 系统应提供多种升级方式，至少提供自动在线升级、离线升级两种方式 |
| 8 | 产品资质 | 具备公安部安全与警用电子产品质量检测中心颁发的网络安全专用产品安全检测证书 |
| 9 | 厂商资质 | 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全评估(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全建设(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商实施过程中具备成熟的能源管理体系，需具备能源管理体系认证证书，提供有效证书的厂商盖章复印件。 |

**态势感知：1套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 硬件要求 | ≥256G SSD系统盘，≥8TB SATA硬盘，≥6个千兆电口，≥2个千兆光口，≥2个接口扩展槽位，含交流单电源模块，需提供国产化CPU和操作系统。网络层吞吐量≥3G |
| 2 | 产品架构 | 软硬件一体化产品。系统应基于B/S架构，支持SSL加密模式访问，可通过web方式直接对系统进行管理 |
| 3 | 态势中心 | 支持以地图、指数、雷达图、柱状图、趋势图等形式展示监测网络安全的整体安全态势，可投放大屏并兼容分辨率要求、易于操作，可动态提醒当前网络最新的安全威胁态。态势呈现包括但不限于综合态势、威胁态势、脆弱性态势、环境感知态势、运维响应态势、日志审计态势、扩展分析响应态势；支持配置大屏轮播、弹窗提醒、声音提醒 |
| 4 | 事件中心 | 支持事件的查询统计，包括如TOP源IP、TOP目的IP、TOP事件名称、TOP事件类型等 |
| 支持Base64解码、URL解码、Unicode解码、ASCII解码、UTF-8解码 |
| 支持可视化大屏的自定义，包括但不限于：威胁态势统计项自定义以及新增基于内置接口统计项的自定义大屏 |
| 支持系统状态监控，包括主机名、IP、CPU利用率、负载、磁盘使用展示。 |
| 支持创建综合威胁报表任务，支持列表展示报表任务，展示报表名称、任务名称等，支持导出WORD报表。 |
| 5 | 分析中心 | 支持界面化配置规范化规则采集第三方日志实现异构日志格式归一化。解析规则支持正则表达式等前置过滤方式及json、kv、csv、正则表达式类型的解析规则，支持界面划取字段配置、多级解析提取嵌套字段、配置规范化规则对解析提取的字段进行字段类型、名称、取值规范化 |
| 支持场景化展示事件的关键信息，根据威胁的不同特性，提取研判的关键攻击特性在详情中展示，帮助研判分析 |
| 支持提供威胁事件统一运维入口，并支持运维人员自定义威胁运维页签，实现关注IP、资产、攻击类型、攻击结果、来源设备、置信度等多维度自定义的运维事件 |
| 8 | 厂商资质 | 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全评估(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全建设(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商实施过程中具备成熟的能源管理体系，需具备能源管理体系认证证书，提供有效证书的厂商盖章复印件。 |

**WEB应用防火墙：1套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 硬件要求 | 提供1U机架式设备，≥2个USB口，≥4个千兆电口，应用层吞吐≥3G，HTTP层吞吐≥300M，包含5年规则库升级授权 |
| 2 | 产品架构 | 软硬件一体化产品。系统应基于B/S架构，支持SSL加密模式访问，可通过web方式直接对系统进行管理 |
| 3 | 部署方式 | 部署灵活，支持透明桥部署，串联部署，路由旁路部署，镜像模式，反向代理模式等部署模式 |
| 4 | 攻击防护 | 支持基于规则体系构建黑名单安全策略和自学习白名单机制  |
| 支持识别和防护各类WEB攻击，至少包括：SQL注入，XSS注入，命令行注入，PHP代码注入，JAVA代码注入，PHP反序列化，JAVA反序列化等。 |
| 支持可配置的内置规则；且支持自定义规则，规则属性要求支持“检测方向”、“检测对象”、匹配操作等丰富要素。 |
| 支持ARP攻击防护，支持MAC地址绑定。 |
| 6 | Web防护 | 支持针对主流Web服务器及插件的已知漏洞防护。Web服务器应覆盖主流服务器：apache、tomcat、NGINX、IIS等 |
| 支持HTTP访问控制功能，可以提供针对HTTP元素和客户端的组合访问控制策略。支持对多种HTTP方法执行访问控制，包括：GET、POST、HEAD、PUT |
| 支持对注入（包括SQL注入、LDAP注入、XPATH注入及命令行注入）、XSS、SSI指令、路径穿越、远程文件包含、WebShell防护。 |
| 支持非法下载防护，可以根据文件大小及文件扩展名灵活定义下载限制策略  |
| 支持多达多种的防护动作，包括了放过、阻断、接受等。可针对不同安全风险提供多种可选方案。 |
| 7 | 系统管理 | 支持显示接口状态，引擎状态、系统CPU、内存及硬盘使用率，系统当前时间及系统运行时间 |
| 支持标准SNMP V1/V2c/V3以及 trap；支持Syslog接口 |
| 支持配置同步，包括离线同步和在线同步，  |
| 8 | 厂商资质 | 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全评估(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全建设(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商实施过程中具备成熟的能源管理体系，需具备能源管理体系认证证书，提供有效证书的厂商盖章复印件。 |

**办公网网闸：1套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 硬件要求 | 标准2U机架式硬件，提供。内外网分别满足：≥2个万兆光口，≥6个10/100/1000BASE-T接口（含1个HA口），≥1个CON口，≥2个usb口，≥1个扩展槽，支持跨域访问（邮件、网页、文件、数据库通用）、数据库同步、文件同步、关键字过滤等功能。 |
| 2 | 性能要求 | 网络层吞吐量≥1G，最大并发连接数≥50万 |
| 5 | 可视化 | 展示设备基本信息，主要但不限于设备运行状态、运行时长、版本信息、磁盘信息、设备序列号、入侵事件信息等。 |
| 6 | 部署模式 | 支持代理、路由、透明工作模式，管理员可依据实际网络状况进行相应的部署。 |
| 7 | 文件同步 | 支持内到外、外到内的单向同步和双向同步。 |
| 支持全量、增量同步方式。 |
| 支持覆盖、跳过、重命名同步策略。 |
| 8 | 数据库同步 | 支持全量、增量同步方式。 |
| 支持数据库单向同步或双向同步。 |
| 9 | 厂商资质 | 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全评估(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全建设(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商实施过程中具备成熟的能源管理体系，需具备能源管理体系认证证书，提供有效证书的厂商盖章复印件。 |

**视频流网闸：1套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 硬件要求 | 标准2U机架式硬件，提供。内外网分别满足内网机：≥2个万兆光口，≥6个10/100/1000BASE-T接口（含1个HA口），≥1个CON口，≥2个usb口，≥1个扩展槽，  |
| 2 | 性能要求 | 网络层吞吐量≥4G，最大并发视频路数3000路D1视频 |
| 5 | 功能要求 | 产品采用“2+1”（即双主机系统+物理隔离数据通道控制系统）体系结构；通过嵌入式数据通道控制系统隔离外部网络，而不是采用DMA、SCSI、网卡等方式实现；采用特有控制逻辑和专用通讯协议完全控制数据的实时交换，确保可信网络（域）和非可信网络（域）之间任何连接的断开，彻底阻断TCP/IP协议及其他网络协议 |
| 6 | 部署模式 | 支持代理、路由、透明工作模式，管理员可依据实际网络状况进行相应的部署。 |
| 7 | 功能要求 | 支持海康、大华、华为、华三、公安一所、天地伟业、天视达、宇视、科达、数码视讯、藏愚、合众、汉邦，东方电子，中星等视频厂商； |
| 支持文件名命名黑名单、扩展名类型黑名单过滤（提供功能截图） |
| 支持覆盖、跳过、重命名同步策略。 |
| 8 | 厂商资质 | 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全评估(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全建设(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商实施过程中具备成熟的能源管理体系，需具备能源管理体系认证证书，提供有效证书的厂商盖章复印件。 |

**工控防火墙：1套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 硬件要求 | 标准1U机架式硬件，交流冗余电源，有风扇，≥64G SSD，≥2组BYPASS，≥4\*千兆光口，≥2\*USB接口，≥1\*RJ45串口，整机吞吐≥3.5G，新建连接数≥5万，最大并发连接≥500万 |
| 2 | 产品架构 | 软硬件一体化产品。系统应基于B/S架构，支持SSL加密模式访问，可通过web方式直接对系统进行管理 |
| 3 | 可视化 | 支持显示系统状态信息，包括CPU、内存大小及使用率，磁盘大小及使用率、系统版本等；  |
| 支持显示网络流量趋势、IP资产流量排行、应用流量统计等统计图、趋势图展示；  |
| 4 | 部署方式 | 支持虚拟线、二层（或透明）、三层（或路由）接入方式，适应各种网络环境需求； |
| 5 | 网络适配性 | 物理接口：支持二层、三层、监听、虚拟线、监听、镜像、汇聚成员等接口 |
| 逻辑接口：支持VPN、VLAN、汇聚、三层子接口等接口； |
| 汇聚接口：虚拟线、二层汇聚接口类型 |
| NAT:支持基于策略的SNAT和DNAT，不限于“一对一”、“一对多”、“多对一”、“多对多”； |
| 路由：支持基于源/目的地址、接口的、基于服务、应用类型、用户的策略路由；  |
| 路由：支持动态路由协议：RIP、OSPF；支持反向路由功能。 |
| 6 | 防护策略 | 提供基于源/目的IP地址、安全区、应用/应用过滤器、协议/端口、时间、安全模板/模板组的精细粒度的安全访问控制；  |
|  |
| 支持资产识别、发现，并可对其资产信息进行管理，提供界面截图 |
| 支持配置工业白名单，可设置源地址、目的地址、时间、网络协议、端口号等单一或者组合生成可信任白名单规则 |
| 工业白名单：支持自定义白名单应用；  |
| 7 | 系统管理 | 支持包括防火墙日志、工业白名单日志系统日志查询，同时可根据条件类型生成相应的报表。 |
| 日志类型包括但不限于调试、信息、警告、错误等多个级别  |
| 8 | 厂商资质 | 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全评估(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全建设(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商实施过程中具备成熟的能源管理体系，需具备能源管理体系认证证书，提供有效证书的厂商盖章复印件。 |

**杀毒软件：100套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 防病毒 | 支持全盘扫描、快速扫描、自定义扫描、拖动扫描等多种扫描方式 |
| 实时防护支持高、中、低三种防护级别 |
| 支持扫描内存、关键位置、本地磁盘、网络驱动器等 |
| 具备基因特征引擎，支持对引导区、内存、脚本、压缩包、宏病毒等进行威胁检测 |
| 支持检测挖矿木马通信协议和连接矿池地址，实时阻断挖矿木马挖矿行为 |
| Windows/Linux/国产操作系统提供相同的杀毒UI界面，提供证明截图 |
| 支持目录白名单、文件哈希白名单、签名证书白名单四种方式 |
| 支持设置积极、均衡和谨慎三种工作模式，提供功能截图 |
| 支持活动文件、内存中活跃进程和模块、网络访问的进程实时监控 |
| 支持邮件监控，支持对接收和发送的邮件进行病毒检测 |
| 2 | 基线检查 | 支持身份鉴别策略组基线核查，包括密码策略、账户策略等 |
| 支持访问控制策略组基线核查，包括账号、共享检查等 |
| 支持安全审计组策略基线核查，包括审核策略更改、登录事件、过程跟踪、目录服务访问、特权使用、系统事件等 |
| 支持检测操作系统弱口令 |
| 支持用户自定义字典，支持自定义组合密码，弱密码检测过程不受登录策略的影响，不产生大量系统或应用登录日志，支持字典库导入。 |
| 3 | 终端管理 | 支持采集终端基础信息，包括终端名称、IP地址、MAC地址、健康状态、硬件架构、操作系统、组件等信息 |
| 支持采集终端硬盘信息，包括硬盘名称、型号、固件、物理序列号、总线、大小、是否固态、是否nvme、硬盘温度等 |
| 支持采集终端进程列表，包括进程ID、进程创建时间、CPU占用率、物理内存占用、映像文件路径、启动命令行、用户名等 |
| 支持采集终端服务信息，包括服务名称、运行账号、主程序路径、模服务类型、启动方式、服务状态等信息 |
| 支持采集终端启动项信息，包括启动项名称、执行文件路径、启动项位置、所属用户、是否启用等信息 |
| 4 | 外设管控 | 具备外设管控能力，支持对终端各种外设（USB存储、光驱、USB外置网卡、无线网卡、蓝牙、手机、平板等）、接口（USB接口、串口、并口、1394、PCMIA）设置使用权限，支持添加外设和端口黑白名单例外 |
| 5 | 违规外联 | 提供违规外联监测能力，支持互联网或专网的外联探测功能，发现外联后能够设置告警、断网等违规处理手段 |
| 具备外设管控能力，支持对终端各种外设（USB存储、光驱、USB外置网卡、无线网卡、蓝牙等）、接口（USB接口、串口）设置使用权限，支持添加外设和端口黑白名单例外 |
| 6 | 管理平台 | 管理平台具备整体安全概览展示，包括威胁趋势、安全概况、防护概况、安全合规、高危终端TOP10、高危病毒TOP10、待办事项等 |
| 支持以柱状图的形式统计全网基线核查、终端版本、杀软安装、补丁修复的运维概况 |
| 管理平台支持以组织架构的方式管理全网终端，能够显示终端基本信息；终端资产支持显示终端详情包括性能、硬件、软件、进程、网络、漏洞等；包括策略分发、卸载、关机、重启等 |
| 管理平台支持终端安全策略的整体管控配置，包括：基本策略、病毒查杀、实时防护、信任名单、异常告警、漏洞修复、桌面管控、安全评分安全策略 |
| 7 | 厂商资质 | 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全评估(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商具备数据安全服务能力，需具备中国计算机行业协会数据安全专业委员会中国软件评测中心颁发的数据安全服务能力评定资格证书，证书需满足**数据安全建设(二级)**，提供有效证书的厂商盖章复印件。 |
| 为保证原厂商实施过程中具备成熟的能源管理体系，需具备能源管理体系认证证书，提供有效证书的厂商盖章复印件。 |

**数据备份系统（软硬件一体机）：1套**

|  |  |  |
| --- | --- | --- |
| **序号** | **指标项** | **指标和性能** |
| 1 | 硬件参数 | 2U机架服务器，国产化双路32核2.6G处理器， 64GB内存，2个千兆以太网口，2个万兆网口（含光模块），2块480GB SSD，4块8TB企业级硬盘，热插拔双冗余电源。 |
| 2 | 产品主要功能 | 1、提供集中统一的备份管理平台，包含客户端保护、虚拟化保护、NAS保护、备份管理、恢复管理、客户端管理、存储管理、日志管理、归档管理等，并支持集中管理全部客户端主机的数据备份、恢复、虚拟化无代理、瞬时恢复、远程复制、数据查询、数据清理等操作。2、要求基于Single Linux（非Windows）的64位操作系统。采用B/S管理架构，https方式登录，无需安装辅助程序，所有功能同一界面统一管理； 3、支持对虚拟服务器、物理服务实现操作系统的整体定时备份。本次配置不少于20TB容量授权，在容量授权范围内，不限制虚拟化无代理备份服务器、物理服务器及虚拟机数量，不限制虚拟化分钟级快速接管虚拟机数量，不限制操作系统和数据库数量备份和恢复功能。（须提供授权管理界面截图证明，并加盖原厂公章）4、支持基于飞腾、鲲鹏、海光等国产平台上的文件、操作系统的在线备份与恢复功能。支持基于Windows、Linux及统信、欧拉、麒麟等国产化操作系统定时备份和恢复功能。5、支持主流虚拟化平台无代理备份，包括vSphere ESXi、Hyper-V、Huawei FusionCompute、H3C CAS/UIS、EVEREST、RedHat RHV/Ovirt、SmartX、OpenStack、ZStack、QingCloud、云宏CNware等主流虚拟化平台虚拟主机无代理备份，提供完全、增量等多种备份类型，无需在虚拟主机上安装任何客户端代理，实现虚拟主机整机、整盘备份。（须提供多品牌虚拟化平台无代理备份功能配置过程截图证明，并加盖原厂公章）6、支持虚拟机同平台及跨平台瞬时恢复功能，可支持同时启动多个时间点数据副本瞬时恢复至同平台或异构平台，用于备份数据演练、验证、应急接管，而无需真实恢复故障虚拟机进行验证。（须提供瞬时恢复功能，包含同平台、跨平台恢复功能截图证明，并加盖原厂公章）7、支持虚拟化环境下的细粒度恢复功能，无需进行整机恢复，即可快速找回虚拟主机内某单一文件或文件夹，节省恢复效率。（须提供虚拟化环境下单一文件及文件夹恢复功能截图证明，并加盖原厂公章）8、支持对SQL Server、Oracle、MySQL等主流数据库和应用进行在线备份保护，创建配置过程中全部采用图形化向导式完成，无需编写任何的脚本。9、支持Oracle/Oracle RAC、SQL Server等主流数据库及集群高可用环境下，内置数据库坏块告警、数据库故障检查/校验机制，可针对进行数据库数据文件逻辑、物理坏块检测或检查所有数据库是否损坏，一旦查到数据库损坏或逻辑坏块，系统自动根据告警机制将告警日志信息以发送邮件形式，通知设备管理员。（须提供数据库坏块告警、数据库故障检查/校验机制及系统邮件告警功能截图证明，并加盖原厂公章）10、支持提供副本数据管理功能，兼容基于Linux和Windows环境下的Sql Server、Oracle等主流数据库，在对生产数据进行数据一致性处理后，以原生格式进行数据备份、存储，不进行任何的格式转换处理，可在分钟级别时间内对任意数据量大小的副本数据，通过iSCSI或者FC的方式快速挂载，挂载后的数据副本可用于应急、软件开发测试、备份数据有效性验证、恢复演练等场景。（须提供副本数据管理及iSCSI/FC挂载功能截图证明材料并加盖原厂公章）11、支持海量小文件在线备份，在备份拥有百万级、千万级，甚至亿万级小文件的文件系统时，提供加速备份功能，如永久增量、小文件合并、源端消重等技术实现超百万数量级小文件的高速备份；万兆网络环境下备份性能不低于1GB/s；（须提供文件系统加速功能，数量超过百万场景下包含备份数据量、文件数量、备份耗时等信息的任务截图并加盖原厂公章）12、支持操作系统备份和裸机恢复功能，支持主流Linux/Window及国产平台的操作系统在线备份，可快速从裸机状态直接恢复操作系统，无需重新安装操作系统、驱动程序和应用软件。13、支持对备份数据进行加密传输和存储，支持提供AES256、SM4等多种加密传输功能，提升传输过程以及存储的安全性。在备份任务开启加密功能后，在执行备份任务过程中备份客户端将生产端数据，在Client端先行加密，再传送给备份设备，确保备份数据传输过程中无泄密风险。（须提供多种加密传输功能截图证明，并加盖原厂公章）14、支持提供磁带库离线归档功能，兼容市场主流磁带机、磁带库、虚拟带库设备，可将备份数据再次进行数据归档到磁带或磁带机设备上，实现离线备份，满足相关法律法规。（须提供离线归档至磁带库或磁带机详细过程截图证明，并加盖原厂公章）15、支持普通和三权分立多种用户访问控制模式，可根据实际需求进行普通模式和三权分立模式随时切换；普通用户模式包含管理员和操作员两种访问角色类型；三权分立模式包含审计员、安全员、管理员、操作员四种访问角色类型。（须提供多种用户访问机制管理功能截图证明，并加盖原厂公章）16、支持可指定操作员分配客户端、存储空间、授权数量、授权类型等管理资源。不同操作员分配到资源相互独立，完全隔离，任意操作员进行备份与恢复操作，均不影响其他操作员管理。（须提供多个操作员相互独立管理操作截图证明，并加盖原厂公章） |
| 3 | 售后服务 | 提供原厂五年硬件、含免费升级，软件打补丁，邮件、电话支持服务。 |

**6. 验收测试与权益保障要求**

6.1 **验收指标（生产稳定性部分）**

 项目实施期间生产系统可用性≥99.9%（单次故障≤10分钟不计入统计）.

 安全策略变更导致的业务异常率≤0.1%（基于APM工具监控的HTTP 500错误率）。

 等保二级必检项（如身份鉴别、访问控制）100%通过技术检测，且无高风险项遗留.

 **渗透测试**：乙方需提供第三方机构出具的渗透测试报告，覆盖应用层、网络层、数据层的攻击模拟（如SQL注入、0day漏洞利用、横向渗透），关键系统漏洞修复率需达100%，中低风险漏洞修复率≥95%。

 **流量审计**：部署流量探针验证安全设备（如WAF、IDS）的告警准确率（≥99%）与阻断率（≥98%），需提供连续30天无干扰流量日志作为基线证据。

数据完整性：通过哈希校验与区块链存证技术，确保安全配置变更记录、日志文件的防篡改性，甲方可随时抽查任意时间节点的数据快照。

6.2 **合规性闭环**

 **标准对齐**：验收文档需明确标注每项技术指标对应的法规/合同条款，未覆盖项需书面说明豁免理由。

 **供应链审计**：乙方需提交所有第三方组件（开源/商业）的SBOM（软件物料清单）及已知漏洞清单，并提供5年内漏洞响应承诺函。

6.3**违约救济条款**

 若验收中发现重大设计缺陷（如防火墙策略绕过的POC验证），乙方需在5个工作日内提交修复方案，每超期1日按合同总额0.5%支付违约金。

 验收通过后1年内，若因乙方技术原因导致安全事故，乙方需承担第三方取证费用及监管罚款的150%补偿。

**7. 交付物清单**

 威胁建模报告（含ATT&CK矩阵映射）

 安全设备原始日志（含SIEM平台解析结果）

**8．应急响应要求**

**** 7×24小时护航：项目实施期间至验收后7天内，乙方需配备至少1名网络安全工程师+1名甲方业务系统专家组成联合保障组，提供分钟级响应的现场/远程支持。

 故障分级：明确生产事件等级（如P0级：业务完全中断；P1级：关键功能降级），P0级故障需在15分钟内启动应急预案，2小时内提供根本原因分析报告。

**9. 等保合规专项要求**

**** 安全审计不中断：所有实施操作必须通过堡垒机+视频录屏双记录，确保账号权限变更、策略调整等操作可追溯，日志保存周期≥6个月。

 最小权限控制：乙方人员账号权限按“工作日+小时”维度动态分配（如仅允许每周三03:00-05:00拥有防火墙策略修改权），超时自动回收。