项目需求书

一、项目背景

本项目参照三级等级保护要求，补充完善天津市水资源监控管理信息平台的运行环境，购置综合日志审计系统，运维管理系统，负载均衡设备，漏洞扫描，抗 DDOS 设备，主机加固等设备，提升系统的运行安全。

本项目采购综合日志审计系统 1 项，运维管理系统 1 套，负载均衡设备 1 套，漏洞扫描 1 台，抗 DDOS 设备 1 台，主机加固 1 台，等相关服务工作。

二、技术需求

序号	采购项名称	需求条款	单位	数量
1	综合日志审计系统	*硬盘：内置 2T SATA 硬盘；接口：6 个千兆电口、2 个千兆光口；吞吐量：800M；SQL 处理性能：10000 条 SQL 语句/s；日志存储：10 亿条；标准 1U 机架式设备	台	1
		*采用 B/S 管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务。		
		支持 Oracle 数据库审计、SQL-Server 数据库审计、DB2 数据库审计、MySQL 数据库审计；支持同时审计多种数据库及跨多种数据库平台操作；		
		完整解析、记录、关联 SQL 操作语句绑定变量参数，并支持对超长 SQL 语句完整解析；		
		支持自定义数据库安全策略，可根据业务需要自定义各种场景的安全规则，对于违规的数据库访问可进行实时警告和阻断。		
		*可以对 SQL 语句进行安全检测，并识别当前的 SQL 操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施。		
		支持吞吐量分析，包括 SQL 语句吞吐量排行、SQL 语句吞吐量趋势、SQL 操作类型吞吐量排行、SQL 操作类型吞吐量趋势、数据库用户吞吐量排行、数据库用户吞吐量趋势、业务主机吞吐量排行、业务主机吞吐量趋势。		
		提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。 管理员支持下面几种角色 （1），超级管理员（仅 admin，不能新增，仅一个） （2），安全管理员（负责配置规则，无查看日志权限） （3），审计管理员（负责审计日志，仅有日志查看权限） （4），自定义角色：可以自选页面		

2	运维管理系统	流量分析：100M；系统监控：100 个；设备监控：100 个；系统主动探测：100 个；Oracle 监控：10 个；Weblogic 监控：10 个	台	1
		采用旁路镜像的方式部署，无需更改用户当前网络，也无需在用户服务器上安装客户端软件或插件；		
		*本次所需的运维管理系统能够实现对原有网络设备（防火墙，IPS，WAF 等设备）进行统一分析和管理；		
		提供部署向导工具，用户可根据实际需求选择对应的业务场景模式；		
		内建系统可用性、健康度评分模型，以仪表盘的方式对应用系统进行打分；系统出现异常时，可及时提醒用户；		
		支持 FTP、Lotus、SAP、Exchange 等各类 OA、ERP、Mail 系统；		
		提供系统状态、可用性、响应时延、告警状态等信息；		
		支持 TCP CONNECT、URL 探测、自定义探测，支持正则表达式；		
		可根据不同的健康等级定为阈值告警；		
		监视指定 Web 应用的性能、页面加载时间、所有页面元素的加载序，服务器时间、受影响用户数、错误等信息；记录下 Web 应用的 4XX、5XX 错误；		
		能够通过曲线等图表直观展示 WEB 服务的页面加载时间变化趋势、HTTP/TCP 错误数变化趋势、页面加载时间/网络延时变化趋势等；		
		可详细记录响应慢的页面中各子 URL 的详细信息，便于分析页面慢的原因；		
		*监控指标包括：weblogic 可用性、响应延迟等状态信息、JVM 信息、线程池使用、执行队列列表、等待处理的请求数、JDBC 信息、WEB 应用列表、会话数、Servlet 、EJB 应用缓存命中趋势、池的使用率、Bean 列表 、JTA 活动处理数、时间、次数、JMS 消息数、等待消息趋势、server 详情等；		
		可以与中间件关联的硬件、应用、网络等信息联动，而非局限在中间件；		
		可监控路由器、交换机、防火墙、服务器等基础硬件设备；		
		支持 SNMP（V1/V2C/V3）、WMI、SSH；		
		提供 CPU 执行队列、内存使用情况、磁盘（含分区）占用空间、网口流量、服务器进程等监控信息；		
		支持短信告警（短信猫或短信网关）、邮件告警；）		
		除内置告警规则，可针对硬件设备异常、网络异常、流量异常、系统异常、Oracle 异常、Weblogic 异常配置告警规则；		
		支持用户关注的若干分支网络整体可用性、质量报表；也支持指定某一分支网络可用性、质量报表；		
3	负载均衡	*吞吐量 10Gbps；并发会话数 1,000,000；4 层新建 80,000；7 层新建 40,000；网络接口：6 个千兆电口；可扩展到 24 个千兆电口，标准 1U 机架式设备	台	1

	设备	支持串接部署、旁路部署；支持三角传输模式。		
		*必须独立专业负载设备，非插卡式扩展的负载均衡设备。		
		提供针对多条出口线路的链路负载均衡功能，实现 inbound 和 outbound 流量的均衡调度，以及链路之间的冗余互备。 提供针对 L4/L7 内容交换的服务器负载均衡功能，可在单一设备上支持多个应用和服务器集群，可以根据多种算法和要求分配用户的请求。 单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能，三种功能同时处于激活可使用状态，无需额外购买相应授权。		
		支持多种链路检测方法，能够通过 PING、TCP、HTTP 等方式监控链路的连通性。 支持链路冗余机制，当某一条链路故障时，可将访问流量切换到其它链路，保障用户业务的持久通畅。		
		*对 Oracle 数据库、Weblogic 中间件的关键性能指标监控，并通过报表的形式多维度实时展现关键性能参数，提供历史健康状态分析。界面友好直观，无需在服务器上安装任何插件，不会对网络造成任何影响。		
		内置完备的 ISP 地址库，无需手动导入并支持自动更新，可点击查看并编辑全球任意国家的 IP 地址段。		
		对于超过服务器的连接数上限或者请求数上限的新建连接缓存起来放入队列中，后续分批逐步发送给服务器，而不是直接丢弃数据包		
		*利用读写分离技术实现 MYSQL 数据库的七层负载且无需在服务器上安装任何插件或软件。通过对数据库操作请求报文内容解析，将其中的写操作调度到指定服务器，读操作则调度到所有节点，减少服务器压力，提高数据库资源利用率，提升业务响应速度。		
		同时支持国密和通用商密算法		
		*支持四七层 DDoS 攻击防护：ICMP-Flood、SYN-Flood、UDP-Flood、DNS Query Flood、Script-Flood 、TCP 全连接攻击、并发连接耗尽攻击、SSL-Flood、HTTP Flood、CC 攻击、慢速攻击、Smurf 攻击、Fraggle 攻击、ARP/ND 等攻击防护。 支持实时漏洞检测功能，通过对实时流量进行安全性分析来评估业务系统的漏洞风险，结合黑客攻击行为进行关联分析，帮助用户找到真正存在高风险的安全薄弱环节，并通过报表的方式展现安全风险和解决方法。		
		支持与 VMware vSphere 服务器虚拟化环境深度结合，提供 VMware vCenter 的插件，可以实现在 vCenter 上管理负载均衡设备，自动同步配置。		
		支持与 VMware vCenter 联动，可根据业务高峰期与空闲时段进行主动判断，针对应用系统的虚拟机负荷		
		支持智能的托管处理机制，可针对应用假死，虚拟机宕机等业务不可用情况，自动通知 vCenter 重启虚拟机进行恢复业务，并通过短信、邮件等形式及时告知管理员，提升 IT 部门应急响应能力		
4	漏洞	*扫描数据包吞吐量≥5Gbps，扫描网络接口≥2 个千兆电口，评估服务器数无限制，扫描 IP 授权无限制；标准 1U 机架式设备，标配 6 个 10/100/1000 Base-T 千兆电口，	台	1

	扫描	并含 2 个高速 USB2.0 接口，1 个 RJ45 串口		
		*此次所需漏洞扫描设备能够与现有的安全设备（防火墙，IPS,WAF 等）进行安全防护联动，实现日志统一管理		
		产品内置漏洞特征库：6000+ ，并且能够自动或者手动升级		
		有单独的实时漏洞特征分析识别库，支持被动检测网络系统实时漏洞，实时漏洞库数量在 1200+		
		支持对 web 整站系统漏洞的扫描		
		支持自定义漏洞，包可定义漏洞 ID、漏洞名称、漏洞描述、攻击对象、危险等级、参考信息、地址、字符串、正则表达式等		
		*可识别 1000 种以上应用 3000 种以上的应用动作，包括 P2P、IM、OA 办公应用、数据库应用、ERP 应用、软件升级应用，木马外联、炒股软件、视频应用、代理软件、网银等协议		
		包括蠕虫/木马/后门/DoS/DDoS 攻击探测/扫描/间谍软件/利用漏洞的攻击/缓冲区溢出攻击/协议异常/ IPS 逃逸攻击等		
		支持 ftp、mysql、oracle、mssql、ssh、RDP、网上邻居 NetBIOS、VNC 等多种应用的漏口令评估与扫描		
		支持目标 IP 进行端口、服务扫描		
		支持被动检测方式，通过旁路部署被动进行报文特征匹配、协议异常检测（需提供截图证明）		
		支持 APT 检测功能，防止僵尸网络感染 PC 终端用户		
		包括 SQL 注入/xss 跨站脚本漏洞/CSRF/目录遍历/文件包含/命令注入/敏感信息泄露等 OWASP TOP10 高危漏洞		
		支持服务器、客户端的漏洞风险评估功能		
		漏洞详细信息显示：漏洞 ID、漏洞名称、漏洞描述、攻击对象、危险等级、参考信息、地址等内容		
		*支持对终端被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为；（需提供截图证明并加盖厂商公章） 具备独立的僵尸网络特征库，恶意软件识别特征总数在 52 万条以上； 具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，下发威胁行为分析报告；（需提供云端恶意软件分析报告并加盖厂商公章）		
		*设备必须支持内置数据中心（需提供截图证明并加盖原厂商公章）。		
		*支持对经过设备的流量进行分析，发现被保护对象存在的漏洞（非主动扫描），并根据被保护对象发现漏洞数量进行 TOP 10 排名，列出每个服务器发现的漏洞类型以及数量，支持生成和导出威胁报告，报告内容包含对整体发现的漏洞情况进行分析；（提		

		供威胁报告并加盖厂商公章） 支持在首页多维度的展示发现的安全威胁，如攻击风险，漏洞风险，终端安全威胁和数据风险等，并支持将所有发现的安全问题进行归类汇总，并针对给出相应的解决方法指引； *提供安全报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，可以查看到有效攻击行为次数和攻击趋势；（提供安全报表并加盖厂商公章） 支持自定义统计指定 IP/用户组/用户/应用在指定时间段内的服务器安全风险、终端安全风险等内容，并形成报表； 支持每天/每周/每月自动生成报表，并将报表自动发送到指定邮箱，可以自定义报表内容；		
		*可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则；（需提供截图证明并加盖厂商公章）		
		支持虚拟化/云环境软件化部署，提供虚拟化版本，虚拟化版本支持以虚机的形式部署在 VMware 虚拟化平台中，并完全适配 vCenter 和 Vmotion 的监管，支持虚机的克隆和迁移等配置和操作，实现最高的易用性 虚拟化版本支持扩展部署在自有品牌虚拟化平台上，支持扩展部署在 KVM、XEN 等其他虚拟化平台		
		中国反网络病毒联盟成员；		
		国家信息安全漏洞共享平台(CNVD)用户组成员；		
5	抗 DDOS 设备	*提供的产品不能少于 6 个千兆接口，此外还具有至少 1 个 RJ45 管理接口 1 个 RJ45 串口，2 个 USB 接口。 *单台抗拒绝服务系统处理能力在 64 字节的小报文的环境下要求攻击处理速度≥70 万 pps，转发延迟小于 42μs，最大并发连接数≥200 万。	台	1
		支持对欺骗与非欺骗的 TCP（SYN，SYN-ACK，ACK，FIN，fragments）、UDP（random port floods，fragments）、ICMP（unreachable，echo，fragments）、(M)Stream Flood 及混合类型攻击的防护。 设备具备针对 UDP53、TCP53 及 DNS 提供专用的 DNS Query Flood 防护手段。 设备具备针对 HTTP Get Flood 攻击具备专门的防护手段，能够对 HTTP 进行解码。其中，针对 HTTP Get Flood 攻击防护的算法不少于 8 种。		
		要求可扩展能够与攻击流量分析系统进行联动，由攻击流量分析系统对网络中的流量进行实时检测，当发现拒绝服务攻击事件时，攻击流量分析系统能够和抗拒绝服务系统联动，将需要被防护的信息通告给抗拒绝服务系统，由抗拒绝服务系统实现拒绝服务攻击的防护。		
		要求扩展支持与 WEB 防火墙联动功能，WEB 安全防火墙与抗拒绝服务系统联合提供完善的 Flood 防护的功能，当 Flood 流量超过 WEB 安全防火墙的防护能力即所设置的联动通告阈值时，向抗拒绝服务系统发出牵引通告，由清洗能力更强的抗拒绝服务设备		

		将流量牵引过去，提供完善的Flood防护。		
		要求抗拒绝服务系统能够支持安全云技术，支持与厂商的云安全平台联动。		
		管理界面要友好、易用性强，应支持集中管理、本地管理、远程管理等多种管理方式，并能实时显示攻击事件、流量、系统运行状况等信息。		
		在集群部署时支持对多台设备的集中管理，日志收集，运行状态监控，策略下发。		
		要求原厂提供三年配套的7X24小时安全运营服务，包括安全基线设置、DDoS攻击监测与防护、设备维护，并出示详细SLA文档说明服务内容和过程。		
6	主机加固	*支持多个Windows操作系统平台，包括Windws 2003/XP/2008所有32bit和64bit的操作系统，以及Linux、AIX、HP-UX、Solaris等操作系统。	套	1
		一个控制台可以同时对多个平台的客户端进行管理和维护，可实现集中管理。		
		对系统的CPU、内存、磁盘、网络资源进行监控，当这些资源的使用状况超过设置的阀值时将进行报警，以提前发现资源不足、滥用等问题。		
		具备良好的系统自身的保护功能，保护系统自身进程不被异常终止、伪造、信息注入，系统自身文件不被恶意修改和删除。		
		可灵活配置系统用户密码的复杂性和登陆失败处理，以此来增强系统用户身份鉴别的安全性。		
		*提供安全管理员和审计官员的USB KEY+密码的双因子认证功能，还可对系统用户配发USB KEY实现双因子认证，对于远程登陆和虚拟化系统而无法识别USB KEY的服务器，提供可配置两个密码组合的登陆认证方式，只有掌握密码的两个人同时存在才能登陆系统，以此确保自然人的可信。		
		具备内核级文件/目录强制访问控制，允许对文件/目录配置用户或进程以读、写、禁止访问等权限访问的安全策略。		
		具备内核级注册表强制访问控制，允许对注册表项配置进程以读、写等权限访问的安全策略。		
		具备内核级进程强制访问控制，允许对进程配置进程以读内存、写内存、复制句柄、终止进程等权限的安全策略。		
		具备内核级服务强制访问控制，能够阻止新增的服务及驱动在系统中的加载，阻止已安装服务的启动类型的更改。		
		具备内核级别帐户强制访问控制，能够阻止对系统帐户的破坏，如新增帐户、删除帐户等。		
		保护功能开启时，可防止病毒和入侵者恶意格式化磁盘，同时降低管理员意外格式化磁盘的风险		
		通过把用户认为信得过的进程添加到信任列表中，该进程的操作则会畅通无阻，同时对此进程也可以设置策略进行保护，这样保证了系统的安全性，也保证了一些特殊操作的正常进行，减少用户的操作量		
		具备文件完整性检测，通过记录和对比指定目录中所有文件的基本属性及内容校验和		

		来进行完整性检测，以识别哪些文件被篡改。		
		具备服务完整性检测。通过记录和对比系统中所有服务的基本属性及内容校验和来进行完整性检测，以识别哪些服务被篡改。		
		保护系统重要的可执行程序，比如 exe，dll，com，sys 等文件，可发现可执行程序被篡改并进行恢复。		
		可设置是否允许系统开启和关闭共享，以及设置系统本地帐户的安全策略以及帐户身份认证时的安全传输方式，以此来增强系统帐户的安全性。		
		可设置用户对磁盘的使用配额来避免磁盘空间的滥用，当用户的磁盘使用量超过配额限制时进行报警。		
		*提供至少 7 次以上的文件和目录反复擦写，做到真正的信息清除，防止数据恢复。		
		*提供一键式清理用户上网记录、文档访问记录、临时文件等信息，防止用户隐私数据泄密。		
		*提供经过验证的分等级的安全策略模板，全面保护系统，方便易用，降低用户的使用难度。		
		当用户担心自己配置的策略是否会影响系统和应用时，可开启此功能，此时将只记录违规的日志而不进行阻止，便于管理员在不造成业务中断的情况下调整策略。		
		记录系统内的所有违反强制访问控制策略的事件，并提供日志的查询、删除、备份、导出、日志分析和 syslog 转发功能。		
		记录安全管理员和审计管理员的所有操作事件，如登陆、功能停用等，并提供日志的查询、删除、备份和导出		
		记录安全管理员设置的一些报警事件，比如文件完整性定时自检，服务完整性定时自检，违规日志报警，系统信息报警等。		

三、技术支持

*1. 负载均衡设备具备公安部颁发的《计算机信息系统安全专用产品销售许可证》（提供复印件，正本为红色公章）。

2. 负载均衡设备具备国家工业和信息化部颁发的《电信设备进网许可证》（提供复印件，正本为红色公章）。

3. 为确保项目后续技术支持，投标人须提供生产厂商研发体系通过国际认证 CMMI L4