中国医学科学院肿瘤医院

回溯分析

技术需求

**信息中心/计算机室**

**2017年9月**

目录

[中国医学科学院肿瘤医院 0](#_Toc494181503)

[回溯分析 0](#_Toc494181504)

[技术需求 0](#_Toc494181505)

[一、 项目概述 2](#_Toc494181506)

[1.1产品描述 2](#_Toc494181507)

[二、 技术要求 2](#_Toc494181508)

[2.1清单 2](#_Toc494181509)

[2.2技术参数表格 2](#_Toc494181510)

[三、 服务 5](#_Toc494181511)

[四、 资质 5](#_Toc494181512)

# 项目概述

伴随我院信息化建设的不断发展，所面对的网络问题越来越多、越来越复杂。网络所面临的的攻击各种各样，黑客恶意攻击、网络入侵、病毒感染等事件此起彼伏。

信息安全等级保护要求，网络应具备回溯能力，对入侵及攻击具备配合取证调查的功能。对于我们自己的应用系统，同样需要应用性能、网络性能分析的工具，来排查、定位各种问题、故障。提高监控、预警、分析、解决故障的能力。

###

### 1.1产品描述

回溯分析系统通过对网络通讯进行7×24小时的捕获、存储、回溯、挖掘以及对海量网络数据的定性分析，如针对数据上报平台重点的通讯数据分析、异常HTTP/HTTPS通讯分析、木马心跳包分析、境外DNS检索、特征回查等，能够准确发现网络中的各种隐蔽、狡猾的高级网络攻击窃密行为，是一个基于全量网络数据取证分析的数据平台设备。

能够从任意地点连接到任一的远程分析服务器，实现对全网的分析与故障诊断，能够并发、独立地监控和分析多个网段。分布式支持跨地域，可实现不同城市，不同物理地域的网络分析监测。负责和分析服务器建立连接通讯，传送控制指令和回传分析数据。提供各种视图交互界面，实时显示服务器传回的分析数据。

# 技术要求

### 2.1清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **配置描述** | **数量** |
| 1 | 回溯分析、应用性能分析 | 实时流量采集和分析能力不低于4Gbps；支持多网卡数据采集；存储空间不低于6Tb; 网络协议和应用识别解析不低于1000种； | 1套 |

### 2.2技术参数表格

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 软件要求 | 软件架构：要求系统与数据库于一体，基于类Linux操作系统工作；  |
| 无节点授权数限制； |
| 旁路镜像、分光等方式部署采集数据； |
| 支持多网卡数据采集； |
| 硬件要求 | 实时网络流量处理能力不低于4Gbps； |
| 存储容量不低于6TB，支持外接存储； |
| 数据包采集量不小于500000pps；  |
| 数据采集端口不少于4个； |
| 设备规格，标准机架尺寸，标准2U； |
| 性能要求 | 网络协议和应用识别解析不低于1000种； |
| 实时数据刷新频率不大于1分钟； |
| 对KPI/KQI的历史状态存储；对网络通信原始数据包实时存储； |
| 历史数据保存时间不小于3年； |
| 功能要求 | **Web应用分析：**支持对http协议会话监控；对http实时会话的监控指标包括但不限于：源和目的IP、服务器端口、完整的URL、返回码、加载类型、页面加载时间、http响应时延、服务端时延、客户端时延、网络通信时延等； 对Web性能的分析使用不同的展示方式，例如：线图、饼图、柱图等分析并展示刷新间隔不大于1分钟； |
| **网络应用分析：**智能化分析应用的交易处理响应时间，包括对交易处理的全过程响应时间以及连接建立、服务器的响应时间、网络延迟、重传延时、客户端交易处理数据在网络中的传输时间等；针对特定应用或特定主机某时段的最大交易处理响应时间、平均交易处理响应时间、最小交易处理响应时间分析，同时提供趋势分析；支持应用响应时间的测量，提供性能最差的客户端分析、响应时间分布图、响应次数分布图、重传分布图、网络延迟等； |
| **自定义应用分析：**支持对自定义协议实时会话监控；对实时会话的监控指标包括但不限于：源和目的IP、服务器端口、包数、重传包数、应用中断数量、通信中断数量、应用处理时延、服务端时延、客户端时延、网络通信时延等；分析过程中均为在线自动完成，无需人工通过离线或者半离线方式；对自定义性能的实时分析使用不同的展示方式，例如：线图、饼图、柱图、健康图等；分析并展示刷新间隔不大于1分钟，基于会话级的分析均为在线自动完成，无需人工通过离线或者半离线方式； |
| **网络流量分析：**网络流向分析，分析各应用的流量流向；网络吞吐量，分析各应用的流量历史与趋势；异常预警分析，从网络流量的突变中，发现网络异常并告警；流量趋势分析，分析网络流量与应用延时等的趋势；单个用户单个应用带宽占有分析，分析单个应用、单个ip机器、单个用户、单个用户群的带宽利用率；根据客户IP地址、TCP/UDP端口、及URL定义应用，监控设备让管理人员采用不同方式，或几种方式，新增自定义应用；以多种指标进行Top N应用/流量/主机/用户排序分析（不只以吞吐量），监控设备能按照不同KPI，进行应用的TopN排行；可自定义不同指标在同一图形对比分析，监控设备能在同一个图里，显示不同的KPI，方便对比分析； |
| **网络性能分析：**支持TCP会话级的网络通信质量实时监控；对网络通信质量监控指标包括但不限于：实时流量、实时会话数量、网络丢包率、应用中断数量、通信中断数量、尝试连接数量、小包速率、数据包大小分布、应用层协议分布等；支持TCP会话级的子网网络通信质量实时监控；对网络通信质量监控指标包括但不限于：实时流量、实时会话数量、网络丢包率、应用中断数量、通信中断数量、尝试连接数量、小包速率、数据包大小分布、应用层协议分布等；支持TCP会话级的主机通信质量实时监控；对网络通信质量监控指标包括但不限于：实时流量、实时会话数量、网络丢包率、应用中断数量、通信中断数量、尝试连接数量、小包速率、数据包大小分布、应用层协议分布、流量最大的IP排名、丢包最大的IP排名、会话数量最大的IP排名等； |
| **快速故障定位：**带宽占有过大问题分析，高流量快速原因查找（相关应用、主机和会话）；网络延时过大问题分析，高网络延时的快速原因查找（相关应用、主机和会话）；丢包率过大问题分析，高丢包率的快速原因查找（相关应用、主机和会话）；服务器响应慢原因分析，服务器响应慢的快速原因查找（相关应用、主机和会话）；失败连接数过高原因分析，连接失败率高的快速原因查找（相关应用、主机和会话）；网络延时过高原因分析，提供对主机查找网络延时瓶颈。 |
| **告警功能：**要求能对影响网络和数据业务系统运行的重要流量参数进行实时监控，并能够设定阀值，主动产生告警；告警的内容和级别可订制；阀值告警：可以是应用响应代码、服务器响应时间、客户端响应时间、网络响应时间、网络带宽、某项应用的网络带宽或延迟等参数，比如某个应用系统出现http 500错误时立刻告警； |
| **报表要求：**能够提供对网络中的流量进行长期的定制化报表，提供全面详尽及准确的网络流量分析周报表和月报表；可订制不同的报表定期以邮件方式发送到不同的邮箱内。报表可以是图片、pdf、csv等格式中的一种或多种。报表的呈现形式包括饼图、柱状图、折线图等。报表提供可开发的程序接口。 |
| **API接口要求\*：**Restful API；易于和商业或者开源软件集成。能够满足各种业务场景的实时性需求，能够提供数据给风控、BI、大数据平台；API支持读取功能要求中的所有分析数据； |
| 其他要求 | 计算机软件著作权登记证书； |
| 软件产品登记证书； |

# 服务

1. **7×24小时技术支持：**
* 电话支持服务： “7×24”的电话支持服务，由原厂公司工程师接听来电，提供专业的技术支持服务。
* 每年六次免费现场数据流量分析服务。
* 每年二次技术培训服务。
* 硬件设备每年4次安全巡检报务。
1. **现场支持**
* 市内4小时内现场响应。
1. **质保服务**
* 上述硬件平台、所有软件功能模块提供合同规定时间内叁年原厂保修和升级服务。

# 资质

**★**计算机软件著作权登记证书；软件产品登记证书。