ANZHOU-TECH
安州科技

安州全流量分析系统

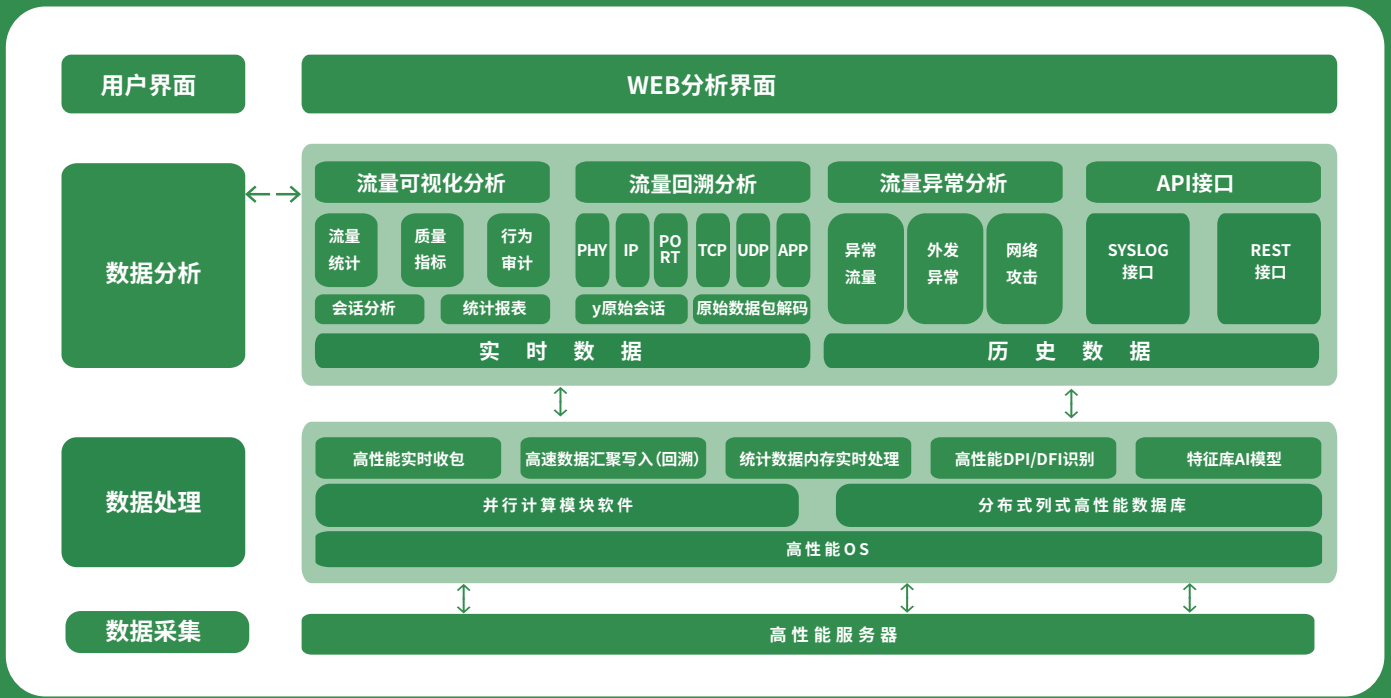
1.产品概述

网络流量分析系统是一款大容量存储的高性能数据包采集和分析平台，可以分布部署在网络的关键节点，实现了对网络通讯数据包级的高性能实时分析。

通过采集网络数据流量，进行数据包存储。通过数据挖掘、结构化的数据处理、可视化的呈现，来实现对网络数据的实时流量可视分析、流量回溯分析、流量异常分析，直观掌握网络情况，快速分析定位故障，提升对关键业务的运行保障和问题处置效率。

网络流量分析系统通过旁路部署在网络中。通过网络设备的端口镜像，或者分光器、分流器将需要进行分析网络流量发给网络流量分析系统，进行存储、解码、统计，通过各种图表直观的进行可视化呈现。相比过去通过人工现场临时抓包，网络流量分析系统可以长时间对流量采集和存储，大大加快了网络问题的处置效率，更好的保障网络业务的开展。

2.产品部署



3.产品优势

高性能：10G-40Gbps实时处理能力　高精度：多种精度实时统计分析（1秒~1天）　大容量：强大数据存储（内置最大 200TB）

回溯：TB级原始流量数据秒级定位　扩展性：提供Restful API接口，Syslog接口

4.产品功能

一.流量回溯分析

能够分布式部署在各个监控的网络节点;能发现网络中存在的窃密行为;具备快速的数据检索能力。

二.流量全景呈现

平台对网络流量实现OSI 7层流量监控分析，可显示全双工接口的收、发和全部的流量、数据包信息;提供对主机、协议、会话等维度的分析内容呈现，并支持关联分析、智能排序、模糊查询、多级钻取等功能;针对用户、业务应用及服务器对象，即可呈现历史数据统计分析结果，也可提供实时流量、会话信息的呈现与条件检索，让用户对网络流量、业务状态一目了然。

三.网络质量呈现

针对网络流速、时延、异常等情况进行实时分析和趋势预测;支持网络异常的监控与呈现。包括网络层、应用层的异常连接、异常会话的统计分析结果呈现;支持网络响应时延和应用响应时延的监控与呈现;支持应用交易分析。

四.视频质量分析

进行视频监控网络质量分析;针对单个摄像头、区域内所有摄像头、业务服务器进行统一质量呈现;支持视频监控网络流量异常告警。包括流量中断、突发、时延、抖动、超标等。

五.应用行为分析

针对内部用户访问内部资源与外部资源以及外部用户访问内部资源的多种用户行为进行画像分析和数据关联分析，准确识别异常用户访问和用户异常访问;针对用户各种访问资源和行为进行细粒度日志审计，并根据日志信息与用户正常访问基准进行比对，实现用户访问合规性分析与安全趋势分析。

六.异常流量分析

通过对流量数据异常检测，快速发现网络攻击、蠕虫、木马、异常连接、敏感数据外发、违规操作等危害网络安全的异常行为;快速发现高级定向攻击行为，准确获取攻击痕迹与证据，及时阻止进一步扩散和渗透。

5.应用场景

一.接入网场景

典型的接入网场景：生产或业务接入网络，如企业的营业厅、政府机构的业务办理大厅以及办公室办公网络等，有多种接入终端和业务类型。

用户收益：1.通过在网络核心交换节点、或者汇聚交换节点，旁路部署大数据网络流量分析系统，采集接入网络侧的数据流量，开展网络运行状态监控、用户端流量可视化分析。

2.图表化分析所有用户端实时和历史数据，大大提升网络故障处理效率，降低工作复杂度，减少繁琐的跑现场连线抓包排查工作、减少效率极极低的协调工作。

3.方便易用、B/S架构多功能集成一体化。

4.全流量全量可视化。

二.广域网场景

广域网，是网络的主干，连接着总部、各级分部。

大型企业、政府机构、行业性骨干网，有省级、国家级规模的骨干网。如省级电子政府网络、公安信息专网、银行骨干网络等。

用户价值：1.通过在广域网汇聚路由器、核心路由器节点。旁路部署网络流量分析系统，开展网络运行状态监控、广域网流量可视化分析。2.广域网链路流量可视化。全面监控运行状态，实时掌握运行状态，访问关系、突发流量情况，高效分析多种应用、多类业务的流量以及运行状况。3.链路质量分析。保障网络质量，掌握传输链路网络质量，快速判断问题范围，提升跨单位、跨部门的协调工作的效率。4.虚拟链路分析。多层次化监控分析重要链路，监控IP到IP的虚拟网络、MPLS VPN链路流量。

三.数据中心场景

企业、政府机构、事业单位、高校的数据中心：几十台到上百台服务器的小型数据中心网络、上千台服务器的中大型数据中心网络。

用户价值：1.通过在数据中心汇聚交换机或接入交换机部署网络流量分析系统，开展网络运行状态监控、服务器端流量可视化分析。2.服务器流量可视化分析，随时掌握网络变化。3.质量分析，分清网络和应用/业务问题边界。4.服务器侧回溯故障处理，有效溯源问题根源，分清责任边界。5.业务分析，按业务进行服务器组分析流量，监控业务运行状态。6.僵尸服务器（幽灵服务器）监控分析，避免浪费资源。

电话：010-60606994　售后热线：400-188-5118
网址：http://www.anzhou.net.cn　邮编：100193
地址：北京市海淀区西北旺东路10号院东区4号楼科锐大厦206房间