全流量回溯分析产品彩页

1、产品介绍

1.1 产品简介

全流量回溯分析产品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。

通过对数据存储，挖掘、分析，实现对关键业务中的网络异常、业务性能异常和网络行为异常实时发现、以及异常原因的回溯分析，提升对关键业务的运行保障和问题处置效率。

1.2 产品形态

软硬件一体机，通过交换机、路由器、分光器等镜像网络中的流量旁路部署在网络中。

1.3 核心功能

流量回溯分析：支持任意时间段1秒/10秒/1分钟/10分钟/1小时/1天多种分析精度回溯历史流量，支持IPv4/IPv6混合分析，多种指标趋势分析；通过多个维度进行快速检索，通过IP、应用、会话等多级钻取，进行在线WEB协议解码，多角度还原历史流量原始数据。

网络流量分析：识别3000+协议与应用，基于数据中心、接入网、广域网多个场景，对服务器、用户、应用、站点、链路的流量、质量、行为进行全量统计分析。

告警分析：支持对流量、应用、IP主机、邮件、域名等多对象维度进行告警；内置了垃圾邮件、域名黑名单告警规则，进行智能告警；支持实时告警、多时间精度/频率告警；支持多种告警指标组合实现与或非的灵活告警。

业务分析：支持对业务性能关键指标进行分析，支持通过多节点采集进行业务端到端全链路对比分析，支持对业务IP画像分析，支持分析业务访问关系，支持对业务进行梳理，支持灵活条件自定义应用，支持对100+种文件类型进行还原，支持对伪装文件进行还原。

元数据日志分析：支持应用层协议元数据解析，解析结果通过协议详单呈现，包括 HTTP、FTP、DNS、EMAIL（IMAP/POP3/SMTP）、Mysql 等 30 多种协议详单分析。

1.4 产品优势

- **高处理性能：**单机支持 1G-40Gbps 实时采集及原始报文落盘处理能力；
- **丰富的分析精度：**1 秒~1 天的多种流量分析精度，支持 30+类型元数据 1000+字段提取分析；
- **全能一体化：**B/S 架构一体化，一机完成流量采集、回溯分析、性能分析、数据包存储及解码；
- **长时间回溯：**支持长达 186 天的历史数据溯源分析；TB 级原始流量数据包秒级溯源；10 亿级会话秒级检索能力；
- **灵活集成：**支持 REST API 集成调用，同时支持通过 syslog/kafka/zmq/ftp 等方式共享数据；

2、产品主要功能

2.1 网络流量采集

✓ 平台采用旁路部署方式，通过以太网端口镜像、分流器方式采集网络流量数据，不改变企业原有网络架构；

✓ 支持基于 VLAN、VXLAN、MPLS、网段等方式配置子链路口，实现对云数据中心、SDN 网络、分流交换汇聚流量进行灵活采集；

✓ 可提供链路流量实时数据包抓取及历史数据回溯功能，并可自定义捕获条件与参数，可回放原始数据包文件。

2.2 应用协议解析

✓ 平台采用 DPI（Deep Packet Inspection）深度包检测技术进行应用层协议解析，可准确高效识别 3000 余种网络协议和预定义应用，1000 多种自定义应用，充分分析网络流量构成、性能、流速等；支持 HTTPS 流量识别、解码；

✓ 支持离线报文在线解码分析，支持源端回溯系统存储报文通过 WEB 界面进行在线报文解码、时序图展示、数据流内容还原；

2.3 流量回溯分析

- ✓ 能够分布式部署在各个监控的网络节点，实时分析捕获流量,实时保存捕获到的网络通讯数据包，进行长时间、大容量的数据存储能力；
- ✓ 能发现网络中存在的窃密行为，对捕获的原始数据包、数据流、网络会话、应用日志等各种统计数据；
- ✓ 能够通过对原始数据包的数据流还原分析，诊断网络故障、应用故障，界定故障责任范围；
- ✓ 具备快速的数据检索能力、随时分类查看及调用任意时间段的数据，具有回溯分析的能力；
- ✓ 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。

2.4 网络流量分析

- ✓ 贴合运维管理工作的场景化，基于数据中心、接入网、网段场景化进行网络流量统计分析，对用户、应用、服务器实时流量分析
- ✓ 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。
- ✓ 针对网络流速、时延、异常等情况进行实时分析和趋势分析，对故障定位、链路升级、带宽规划、策略调整等进行数据支撑；
- ✓ 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，协助判断用户体验时延偏差是由于网络影响导致还是应用影响导致；

2.5 元数据日志分析

- ✓ 元数据日志分析：支持应用层协议元数据解析，解析结果通过协议详单呈现，包括 HTTP、FTP、DNS、EMAIL（IMAP/POP3/SMTP）、Mysql、TNS、Mongodb、DB2、Postgres、telnet、Radius、arp、bgp、dhcp、dtls、https、icmp、isis、krb5、ldap、memcache、msnms、nntp、quic、rdp、rtsp、sip、snmp、socks、ssh、stun、syslog、tds、tftp、vnc 等协议详单分析。

2.6 异常告警分析

- ✓ 通过行为模型分析，实现流量数据实时异常检测、长时间回溯异常检测，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；
- ✓ 丰富的流量预警分析，支持对链路流量、邮件敏感字、可疑域名、报文 ASCII/HEX 特征值告警；

3、典型应用场景

3.1 接入网流量分析

- ✓ 业务接入端用户、终端的进出流量细粒度全景呈现
- ✓ 业务接入端用户、终端流量多维度呈现
- ✓ 流量回溯分析故障、责任界定
- ✓ 提升运维管理效率和响应速度

3.2 骨干网流量分析

- ✓ 骨干网络 WAN 链路流量细粒度全景呈现
- ✓ 骨干网络 WAN 链路进出流量多维度呈现
- ✓ VPN 虚链路网络流量与质量监控
- ✓ 流量回溯分析故障、责任界定
- ✓ 提升运维管理效率和响应速度

3.3 数据中心流量分析

- ✓ 虚拟链路网络流量与质量的监控
- ✓ 关键业务多维度呈现、分析
- ✓ 流量回溯分析故障、责任界定
- ✓ 异常流量监测与发现
- ✓ 提升运维管理效率和响应速度
- ✓ 监控处置空载服务器