全流量威胁取证系统

（Threat Forensics System，TFS）

技术白皮书

奇安信网神信息技术(北京)股份有限公司

2023 年 1 月

版权声明

商标声明

注意事项

您购买的产品、服务或特性等应受奇安信网神信息技术(北京)股份有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务 或特性可能不在您的购买或使用范围之内。除非合同另有约定，奇安信网神信息技术(北京)股份有限公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。如有修改，恕不另行通知。

公司信息

地址：北京市海淀区中关村军民融合产业园 D 座

网址： www.legendsec.com

邮编：100085

电话：010-88509780

客户热线：95015 (7×24 小时)

目 录

1 前言

随着新兴技术的不断发展，网络攻击手段和攻击工具层出不穷，网络安全环境日益复杂，网络安全威胁逐年严峻。以 APT 类高级威胁为代表，攻击团伙使用的攻击战术已经达到非常成熟的阶段，往往会组合多种技术形成高级攻击手段。即便部分攻击团伙的技术能力不高，但也能通过利用公开的或开源的脚本类或自动化攻击框架快速形成完备的攻击武器。攻击团伙不但使用针对个人 PC、服务器和目标内部网络的攻击向量技术，并且覆盖了移动设备和家用路由器，其攻击目标也延伸至政企、金融、能源、工业控制、军工、医疗、教育等领域。在新技术背景下，对安全威胁检测手段提出了更大挑战。

为了提高网络安全保障能力，各单位部署了大量的防火墙、IDS、IPS、WAF、审计等传统安全防御设备。传统安全设备核心原理是依靠攻击特征库的模式匹配完成对攻击行为的检测，基于大数据对检测日志进行关联分析，主要针对已知攻击。但传统安全设备检测手段单一，在高级威胁检测方面存在空白，无法有效发现未知漏洞（0day~Nday）等未知攻击的高级威胁安全事件。同时，可能存在日志被篡改、遗漏等问题，面对已经受到攻击或正在遭受攻击的行为，也无法进行攻击过程和攻击结果溯源分析。

为了提高网络安全保障能力，除了对流量进行实时监测分析，还需要具备事后审计以及还原事件真实场景的能力。基于关键网络流量，对原始 PCAP 进行留存和检索，加速威胁溯源分析和网络攻击取证过程。配合多种检测能力，对网络流量数据进行分析挖掘，发现 APT 等高级威胁的攻击线索，留存攻击证据。通过对网络攻击的线索、攻击过程信息进行多维分析，精准定位攻击源头，实现基于图和智能算法对攻击过程全链条追溯。

2 产品概述

2.1 产品概述

全流量威胁取证系统（Threat Forensics System，TFS）基于网络全流量分析技术，将采集到的流量以元数据和 PCAP 的形式存储。通过特征检测、威胁情报检测、网络异常行为检测和 AI 检测引擎，对原始流量进行交叉检测、验证，结合高效便捷的数据检索能力，对流量中存在的网络威胁进行有效的溯源取证。

全流量回溯是验证未知威胁、还原事发现场的重要手段。很多高级威胁产生的活动痕迹在大规模网络流量中只会占到非常小的比例，但正是这少量的通讯流量对于攻击检测分析尤为关键和重要，需要通过事后的多线索关联和全流量分析后才能有效定性和取证，要求必须对原始全流量数据包进行一段时间的完整保存，保全证据，并能快速回溯所有流量，有了原始流量的存储，就能够将当前检测到的攻击行为与历史流量进行关联，实现完整的攻击溯源和取证分析。

TFS 具备多维的数据分析及深度挖掘能力，通过回溯分析数据包特征、异常网络行为，能够实现数据包级的追踪取证，发现潜伏已久的高级未知攻击。系统能够接受态势感知平台的管理，能向态势感知平台上报告警信息；支持将告警日志/元数据外发给态势感知平台进行汇总展示和分析，日志传输接口支持 syslog 或 kafka 等常见日志传输协议，网络全流量分析技术是发现 APT 网络攻击的重要技术手段，帮助用户建立完备的网络安全检测分析架构。

2.2 系统架构

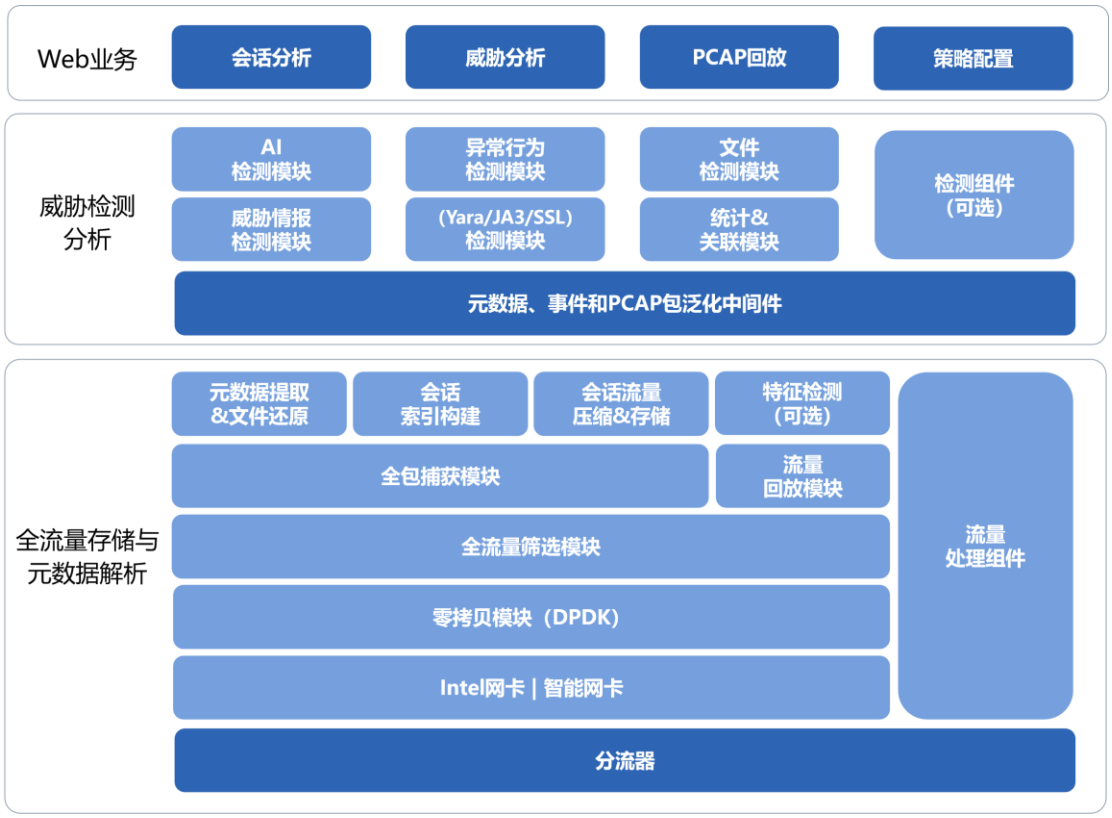

图 1 全流量威胁取证系统-系统架构图

TFS 系统架构如图 1 所示，TFS 监听口接收镜像/分光流量，通过 DPDK/PF_RING ZC 对数据包进行快速处理以及硬件资源调度。通过流量筛选模块过滤不必要的数据，将过滤后的数据进行二次处理，分别进行元数据解析、文件还原、特征检测、情报检测和全流量存储。将解析后的元数据，还原后的文件进行存储，并提交至特征检测引擎，发现基于特征的已知威胁；通过全流量存储模块实现原始流量全包留存。经过中间件将元数据和事件进行泛化处理，将处理后的数据提交至威胁情报、AI 等检测引擎，以威胁事件形式输出检测结果。最后，通过流量回溯和内容取证模块，提供威胁事件、元数据和原始流量溯源、取证能力。

3 功能介绍

3.1 流量采集解析

3.1.1 流量采集

TFS 通过旁路镜像、高性能采集网络流量，并对网络协议进行实时解码，提取元数据，建立完整的日志、协议、数据包全字段索引库。同时，支持接入离线数据包，以便于快速提取多维度的网络元数据进行检测与分析，为后续异常数据挖掘、分析、取证建立牢靠的基础。

3.1.2 元数据解析

TFS 支持提取网络层、传输层、应用层的元数据，可解析还原 DNS、FTP、HTTP、IMAP、POP3、SMB、SMTP、SNMP、ICMP、DCE-RPC、DHCP、DNP3、IRC、krb、Modbus、MySQL、NTLM、RADIUS、RDP、RFB、SIP、SOCKS、SSH、SSL、Syslog、Oracle、Telnet、TFTP、TCP、UDP 等协议并以元数据/ PCAP 形式存储，用于威胁的溯源取证。

支持在线解析大于 3000 个协议的能力，涉及可达 14 万协议字段。

3.1.3 文件还原

TFS 支持还原流量中的文件，支持根据文件进行追溯取证，以及下载原文件。

3.1.4 正筛规则

TFS 支持在采集流量的过程中根据配置的正筛规则对会话进行标注，正筛规则包括源/目的 IP、源/目的端口、源/目的 MAC、协议等内容；同时支持配置仅保留匹配到正筛规则的流量，对重点站点进行观测及数据留存。

3.1.5 反筛规则

TFS 支持在采集流量的过程中根据自定义的反筛规则对流量进行过滤，反筛规则包括源/目的 IP、源/目的端口、源/目的 MAC、协议等内容；默认内置 Alex

Top 10000 白域名，对接入流量进行过滤。

3.2 全流量存储

TFS 具备高可靠、高性能数据包捕获及记录能力，将采集到的网络流量进行协议解析后并以元数据/PCAP 的形式存储，可根据需要进行正筛、反筛过滤流量内容，实现元数据/PCAP 的高性能采集和预处理，设备支持全流量存储采集，存储容量 48T、96TB、128T、192T 等多种存储类型。

3.2.1 PCAP 存储

TFS 支持全流量存储采集，支持对实时流量采集的 pcap 包进行全量存储，供追溯分析和取证使用，通过原始流量的偏移精准获取数据包，将原始流量包存储在 HDD，包括：全包存储和会话的前部分包存储，可根据需求调整存储包个数、周期，PCAP 存储可根据实际需求减少或扩容存储周期。

3.2.2 元数据解析

TFS 具备元数据存储能力。元数据基于流模式存储在 SSD，将同一个流的元数据进行聚合存储，可通过检索元数据的协议字段快速定位到会话，提高检索性能与存储空间的利用率，可根据需要保留三个月到半年的元数据。支持协议元数据解析，展示关键元数据字段内容，并支持按照元数据字段线索进行精确、模糊、组合等查询方式，调查取证攻击行为。

3.3 全流量回溯分析

TFS 具备对全流量进行快速数据挖掘和多维回溯分析能力，支持对网络流量根据会话进行关键字段的提取和展示，同时还可以完整还原数据交互的过程，并以可视化的形式展示交互过程及会话信息。支持从元数据、流日志界面等进行回溯功能，支持对主机进行可视化分析，呈现访问关系、资产画像、威胁标签、威胁信息等数据。

TFS 支持对告警日志的研判分析、标识和处置响应，包括自动呈现告警相关的基础信息、关联资产信息、关联情报信息、地理位置信息、IP 和域名的关联日

志，可查看告警对应的元数据（如 HTTP 请求头、请求体、回应头、回应体、请求方法、HTTP 主机名称、跳转前地址、请求头版本、返回码、返回信息等），可直接查看对应的 PCAP 原始报文信息.TFS 支持协议分析，对解析的关键信息字段进行数据统计、汇聚分析，并绘制趋势图表，从而发现流量当中的异常情况。TFS 支持数据统计分析，对不同关键字段的 value 分布进行数据统计及分析，可配置不同的展示结果、排序方式；根据会话、会话包数量、载荷进行可视化趋势图绘制。TFS 支持通联关系分析，根据配置的源、目的节点的 key 绘制通联关系图，可调整最小连接数、节点/连接权重等。例如源 IP、目的 IP 的通联关系；发件人、收件人的通联关系；文件信息及与该文件相关 IP 的通联关系等。

3.4 全流量威胁取证

TFS 通过多级索引的方式，对原始流量进行追溯，实现威胁快速取证能力。TFS 具备快速取证能力，基于五元组检索亿级数据，可秒级返回元数据。TFS 具备智能取证能力，支持自定义配置正筛、反筛策略，对任意解析后的字段进行条件和条件组检索，可秒级返回元数据。对于返回结果，支持查找并重组对应会话流的 PCAP。TFS 具备基于内容的取证能力，支持全文检索 PCAP 包，对搜索结果进行关键字匹配，并将检索结果以会话形式展示，提供相关 PCAP 下载能力。

3.4.1 智能检索

支持对全量数据包的快速检索功能，用于对入侵行为的取证分析。可对任意解析后的字段进行检索，同时和设定检索条件和检索条件组合，检索条件支持等于、不等于、小于、小于或等于、大于、大于或等于、包含在、不包含在、存在、不存在。

字符串搜索：支持通配符查询，例如，查询条件是：http.uri == *.baidu.com，表示将捕获包含 www.baidu.com 或 news.baidu.com 的 http.uri 字符串。IP 检索支持完整 IP、CIDR 等。

3.4.2 超快检索

流量检测能力范围 2Gbps-20Gbps，最大容量下数据查询时间范围内，PB 级别的原始流量，可做到 PB 级数据（百亿会话）秒内返回；

可对源/目的 IP、源/目的端口、源/目的 MAC 的字段进行检索，可设定单一检索条件和检索条件的逻辑与或非组合。

3.4.3 内容检索

系统具备内容 PCAP 包内容检索能力，从指定流量 PCAP 文件中检索满足用户指定字符串匹配的数据包。并且能够详细展示检索内容在 PCAP 中的位置，从而进一步分析字段前后相关联的数据。

3.5 多场景溯源取证

TFS 支持多场景溯源取证，支持对存储的原始流量进行重放，可灵活选择需重放的数据包，回放条件支持起止时间、采集接口、过滤规则、基于流的五元组过滤规则，用户基于检测探针告警和其他来源告警进行溯源取证，从告警、事件、元数据到原始流量 PCAP 文件，可按照数据粒度进行全链条追溯，真实还原黑客入侵的全过程，从而对网络安全事件进行精准的分析。

3.6 数据回溯与分析

TFS 支持对单个主机、IP 会话、TCP 会话、UDP 会话等多种维度的流量进行回溯分析，并支持趋势图展示结果。

支持对数据包内容多维度的统计分析，支持对传输层协议内容多维度的统计分析。

3.7 流量威胁检测

系统以威胁事件集中分析的角度出发，通过实时流量发现威胁事件并汇聚到关联分析引擎，从信息收集、暴力破解、欺骗攻击、漏洞利用、内网渗透等多个维度对多源告警信息进行聚类，并基于 web 可视化技术，对网络警报日志进行多种维度的聚合统计，形成对攻击者、被攻击者、攻击手法、攻击趋势、攻击路

径多种统计。并提供基于警报明细的警报日志，用户可以通过警报日志提取相关的原始数据包，通过在线解码功能对攻击发生时的原始流量进行分析，对攻击事件进行准确的研判。

3.7.1 下一代入侵检测

TFS 具备入侵检测功能，能够检测包括扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、URL 跳转、跨站攻击、WebShell、浏览器劫持、文件漏洞攻击等网络攻击事件。能够实时发现失陷主机，对入侵行为进行告警，多维度感知入侵，帮助用户分析入侵行为的攻击链路，从而让用户精准有效的发现并解决问题。

3.7.2 网络异常行为检测

TFS 支持网络异常行为检测，支持 C&C 通讯和 DGA 域名检测，发现僵尸网络或被控主机；支持非法外联和数据外发检测，发现隐蔽通道和窃取数据行为；可以监测发现 DoS 和 DDoS 攻击、SQL 注入、跨站攻击等；支持传输层和应用层网络异常行为，自定义基线（模型）异常检测，例如异地登录行为、异常时间登录行为等；

3.7.3 威胁情报检测

TFS 内置威胁情报模块，可进一步确认威胁来源的危害性。对流量进行威胁情报特征匹配，将存在威胁的 PCAP 进行标签批注。具备 APT 等高级威胁检测能力，内置主流 APT 家族的 IOC 数据库，可优先利用威胁情报引擎，进行 APT 攻击过滤，及时形成威胁告警。

3.7.4 人工智能检测

TFS 内置多个人工智能（AI）检测模型，支持对恶意加密流量、暗网流量、Shadowsocks 流量、VPN 流量、DNS 隐蔽隧道、ICMP 隐蔽隧道、HTTP 隐蔽隧道、DGA 域名、钓鱼欺诈邮件、Webshell、SQL 注入攻击、XSS 跨站脚本攻击进行检测、目标遍历攻击。

通过检测模型检测的方式可大幅度降低对特征规则数量的要求，具备更新频率低、数据量小、准确率高、误报率低、自动判断、人工干预少等优势。从告警、威胁事件、元数据到原始流量 PCAP，真实还原攻击者入侵的全过程，支持对检测的告警事件结合原始数据包和研判模型进行深层次研判给出告警事件的攻击结果，从而对高级威胁等网络安全事件进行精准的分析，进而迅速定位 APT 攻击。

3.8 数据外发

3.8.1 数据转存

支持将留存原始数据按照审计要求转存到审计服务器，支持 HTTP、FTP、SMB 三种转存协议；支持区分接入流量来源进行转存。

3.8.2 流量回放

支持将留存数据保序、不丢包的回放到第三方设备，回放数据源可通过时间范围、监听口、五元组条件进行过滤，便于第三方设备进行攻击回放检测；回放速率支持千兆、万兆光口，速率最高可到 20Gbps；可控制回放速度，通过倍速、pps、bps 三种方式限制速度。

4 核心技术

4.1 NUMA 动态感知技术

在通用服务器的架构中，CPU 的不同级别缓存访问延迟不同，跨 CPU 插槽的内存分布也提供不同的内存访问延迟。具体的访问成本描述如下：CPU 的 L1

缓存的访问成本是 3 个时钟周期，L2 缓存的访问成本是 11 个时钟周期，L3 缓存的访问成本是 32 个时钟周期，本地节点内存访问大约是 140 个时钟周期，远程节点内存访问大约是 300 个时钟周期。因此，技术挑战是如何在通用服务器上设计数据包最佳处理流程，充分利用 CPU 的缓存资源，进而减少昂贵的内存访问，特别是跨 NUMA 内存访问。

为了解决以上问题，奇安信网神基于专利技术，实现了一种非统一内存访问（Non Uniform Memory Access，NUMA）的感知框架，精心选择针对每个数据包处理阶段优化的算法和技术。该框架能够根据端到端的数据包处理路径，NIC 缓冲区、IO 存储、PCIe 总线、系统内存、CPU 缓存、CPU 的封装工艺和多核架构等各种硬件和相关软件套件，通过优化配置动态选择数据包处理管道和处理策略，实现单个 NUMA 节点线速处理 50Gbps 带宽。NUMA 感知框架提出了数据流处理逻辑单元概念，如图 2 所示，即 CPU 的 Die 核心处理的数据包仅在本地内存、本地 PCIe 网卡、本地 PCIe 的 Raid 卡以及 Raid 卡上的存储介质上进行流转，完整的数据包处理流程发生在其中。最后，为了提高通用服务器的总处理性能，可以在单个服务器的所有 NUMA 节点上复制多个此类单元，最终将数据包处理能力线性扩展到 100Gbps+流量速率。

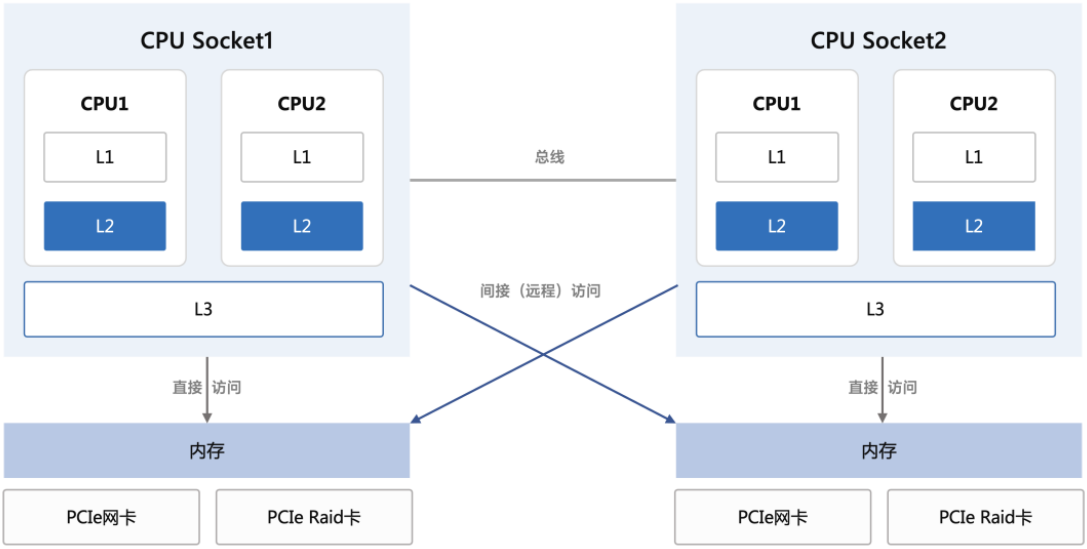

图 2 数据流处理逻辑单元

4.2 自适应接收端缩放的计算负载优化技术

捕获高速网络中的流量通常使用分片技术将计算资源切分以便并行处理流量，每个分片都以完全独立的方式进行流量处理，避免内核间的通信进而获得更高缓存命中效率。若传入负载在内核之间分配不平衡，会导致某些内核最终会缓冲比其他内核更多的数据包，导致过载而丢包。而此时，可能存在系统多个核心几乎处于空闲状态，但仍会出现这些高尾延迟（>10 毫秒）和数据包丢失，而且通过简单地配置并不能解决该问题。

为了解决以上问题，基于专利技术，实现了一种自适应的接收端缩放技术 ARSS，（Adaptive Receive Side Scaling，ARSS），通过动态规划算法在分片之间迁移 RSS 间接桶来解决数据包调度问题。ARSS 跟踪每个 RSS 桶接收到的数据包数量。然后，ARSS 统计哪些桶向每个 CPU 核心发送数据包，计算每个桶对每个 CPU 核心负载的贡献程度。之后，修改 RSS 间接表从过载的 CPU 核心移动到负载不足的 CPU 核心。需要时，ARSS 可以通过将存储桶移动到新内核或重新分配计划移除的内核存储桶来动态扩展内核数量。通过保存每个桶的流表，当一个桶被重新分配给另一个 CPU 核心时，所有相应的流都可以一次迁移完成。为了防止在迁移过程中数据包重新排序，ARSS 会跟踪 CPU 核心清空其队列的时间，然后释放其关联的每条流状态。ARSS 通过实现有状态的服务器内负载平衡，使得即使在 200Gbps 链路的速度下也能充分确保对 CPU 的极高利用率。它通过强制数据包流到具有更高亲和力的核心、优化并最小化核心之间的每条流状态传输以及利用网卡中存在的基于硬件的 RSS 负载平衡方案来实现 ARSS。

4.3 海量数据的原始流量超快检索

基于专利技术，实现了一种面向会话的超快检索算法，具备以下特点：

① 流生成：采用面向会话的处理、索引和检索方法，优于传统面向数据包的处理方法，极大的提高存储、索引和检索效率；

② 索引生成：采用五级索引和二级过滤定位用户关注的会话 PCAP 文件，如图 3 所示。其中，五级索引包括时间索引、布隆过滤器索引、压缩位图索引 RBM、KV 索引和会话数据包索引；二级过滤，元数据过滤用于筛选时间粒度不够引入

的误差，BPF 过滤（可选）用于进行最后包特征匹配；

③ 检索过程：采用 CPU 缓存、内存、SSD 阵列和 HDD 阵列四级存储结构。通过将检索进程绑物理核心方式避免 CPU 核心的频繁上下文切换，将用户访问最频繁的会话索引放入 CPU 缓存，以最近的会话索引放入的内存作为热索引，其他索引存储在 SSD 阵列中，PCAP 文件存储在 HDD 阵列中，确保最慢的硬件尽量少的访问。

TFS 能够做到单台设备在 PB 级的 PCAP 数据（对应 320 亿会话元数据）中，1 秒内快速检索到会话级原始流量，并提供下载。可检索源/目的 IP、源/目的端口、源/目的 MAC，在 1 秒内返回，并且查询无时间范围限制，实现真正的全流量溯源取证。超快检索结果页面如图 4 所示。

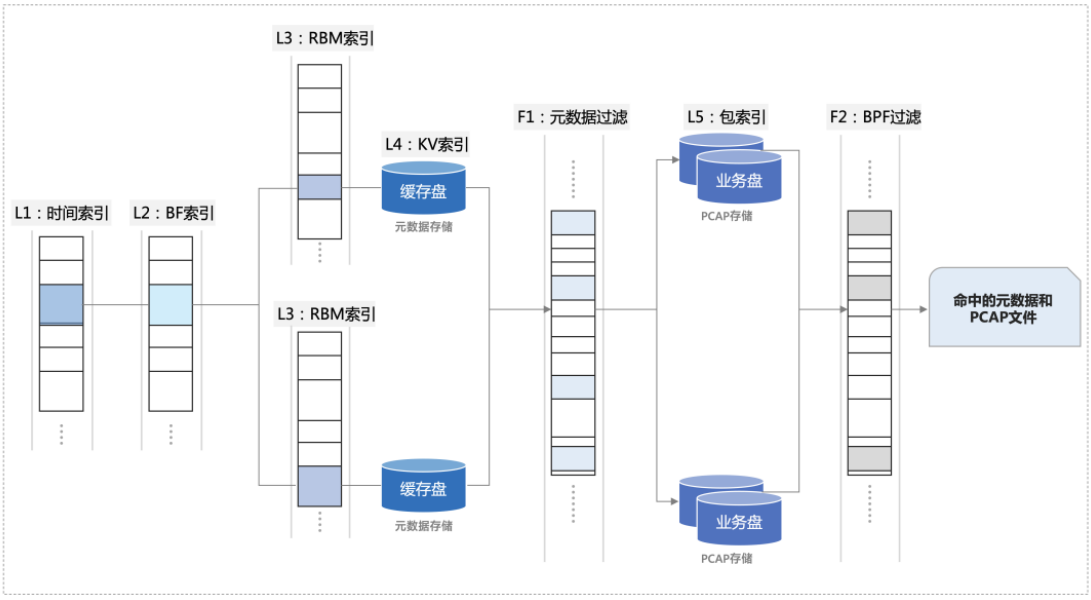

图 3 超快索引原理

图 4 超快检索结果页面

4.4 基于数据包分段压缩算法的高效流量压缩存储技术

为了满足高速链路的网络流量落盘留存、原始流量溯源并显著降低存储成本，提出了一种基于高效压缩算法的全流量存储技术。如图 5 所示，该技术包含三个关键模块：

① 面向流的数据重组和索引，将数据包流转换为面向流的形式，提高了检索和数据压缩效率；

② 高效的数据压缩算法：针对数据包包头和载荷，分别使用有效的数据压缩技术降低总存储成本。其中，包头压缩技术，通过利用同一流中数据包的包头冗余来减少数据包包头的存储大小，即冗余压缩技术；载荷压缩技术，利用可变长度块重复数据删除与每块字典压缩相结合来压缩有效负载；

③ 冷热分离存储，将频繁使用和随机访问的索引数据存储到 NVME SSD 上，存储介质上保留不经常访问的批量数据，例如 PCAP 包，从而改善检索延迟。

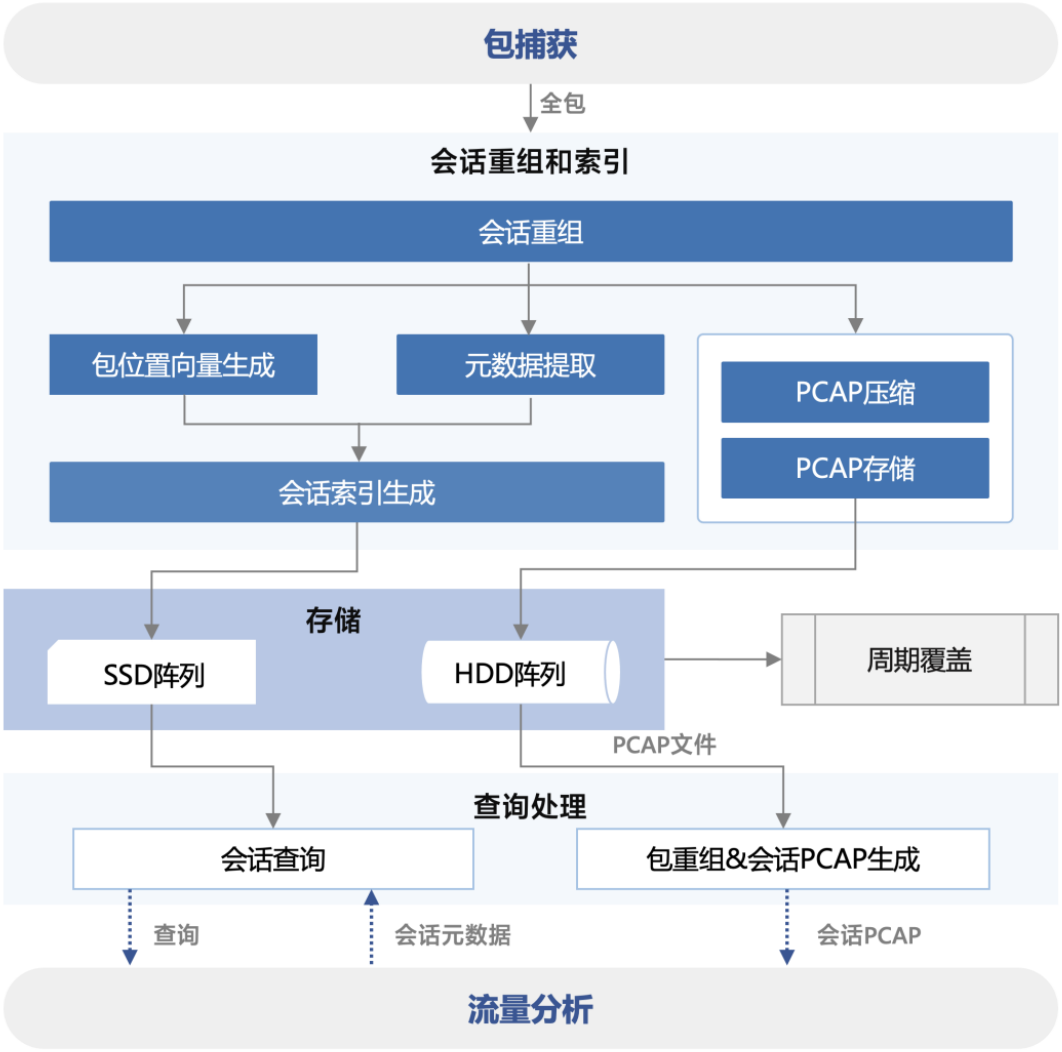

图 5 基于高效压缩算法的全流量存储技术关键模块

4.5 全面的流量统计分析

流量分析是网络分析中的重要手段，TFS 可分析出网络流量中各协议的占比情况、各主机在流量中的占比情况、接收/发送数据包的情况等。解析后的字段，可协助用户排查网络中是否存在网络扫描、DDOS 等网络威胁。

4.6 基于会话的流量数据展示

TFS 可以基于会话流量数据，使原始的网络流量具备更高的可读性，对网络流量根据会话进行关键字段的提取和展示。支持完整还原数据交互的过程，并用

可读可视化的形式展示，能够清晰看到每次交互过程及数据。展示页面如图 6、图 7 所示。

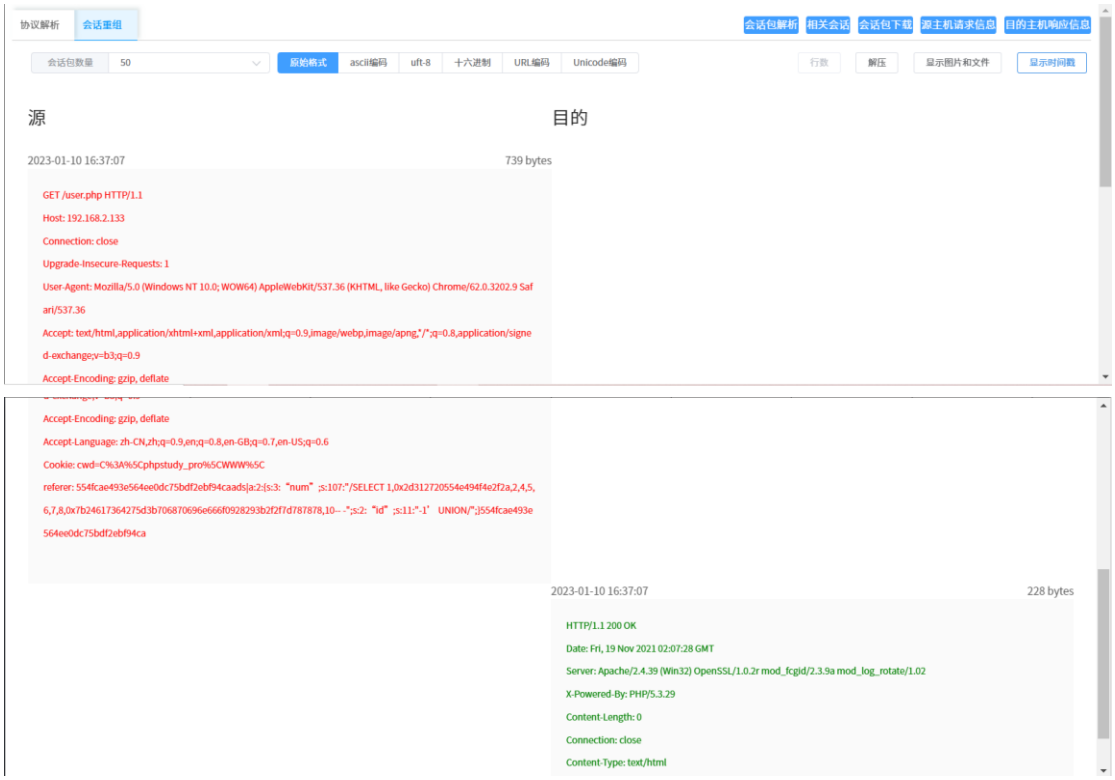

图 6 流量会话编码重组

图 7 基于会话展示协议解析

4.7 基于内容快速取证

TFS 支持基于内容进行取证，对于未解析为元数据的内容支持对原始流量进行取证，支持根据关键字、正则表达式进行检索，可通过元数据检索缩小内容取证范围，提高检索效率，如图 8 所示。

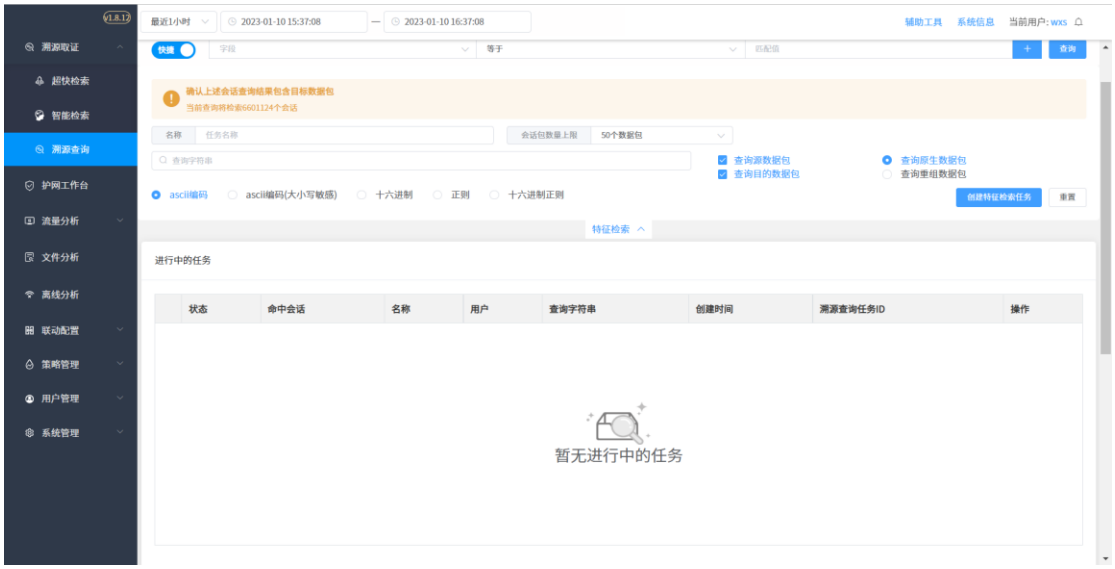

图 8 基于内容取证

4.8 基于多级索引的智能检索

TFS 支持 TCP、UDP、ICMP 等传输层协议解析，支持 20 多种主流的应用层协议解析，140 多种网络元数据解析。建立数据索引并存储在数据库中，提供快速的检索效率，支持灵活的检索条件及组合，可检索条件包括：时间范围、五元组、情报 IOC、威胁检测结果、协议元数据字段。同时，可根据会话精准定位原始数据包并提供下载，如图 9 所示。

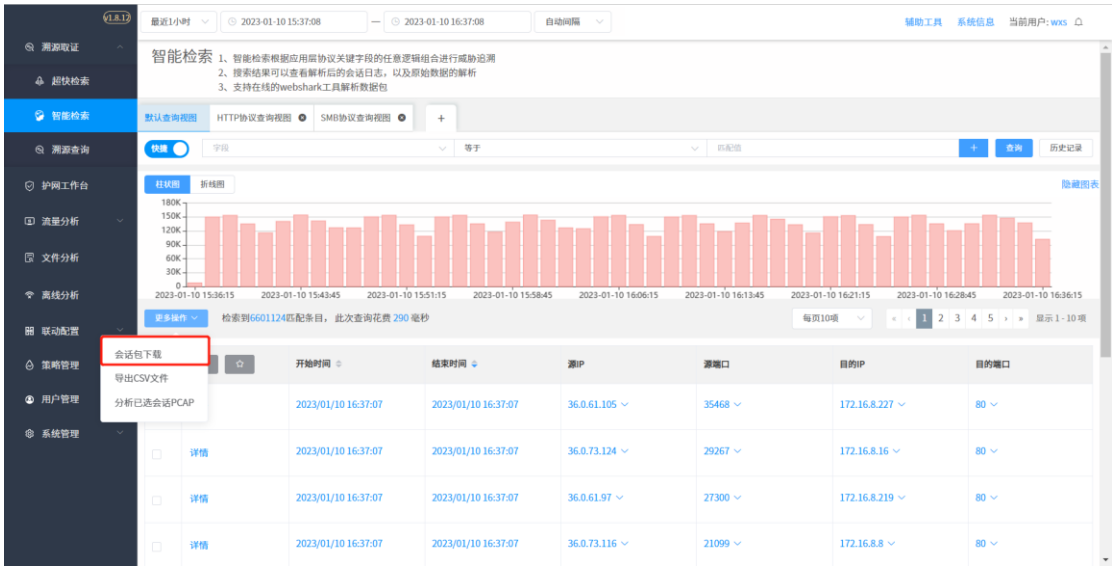

图 9 基于会话展示流量数据

4.9 在线 PCAP 深度分析

TFS 内置与 Wireshark 兼容的数据包分析工具，能够对用户定位的会话 PCAP 包进行类 Wireshark 在线分析。支持解析 3000+协议的多种编码格式的编解码，并支持追踪流进行分析。减少了用户下载 PCAP 文件并利用第三方工具分析的过程，使用便捷，如图 10 所示。

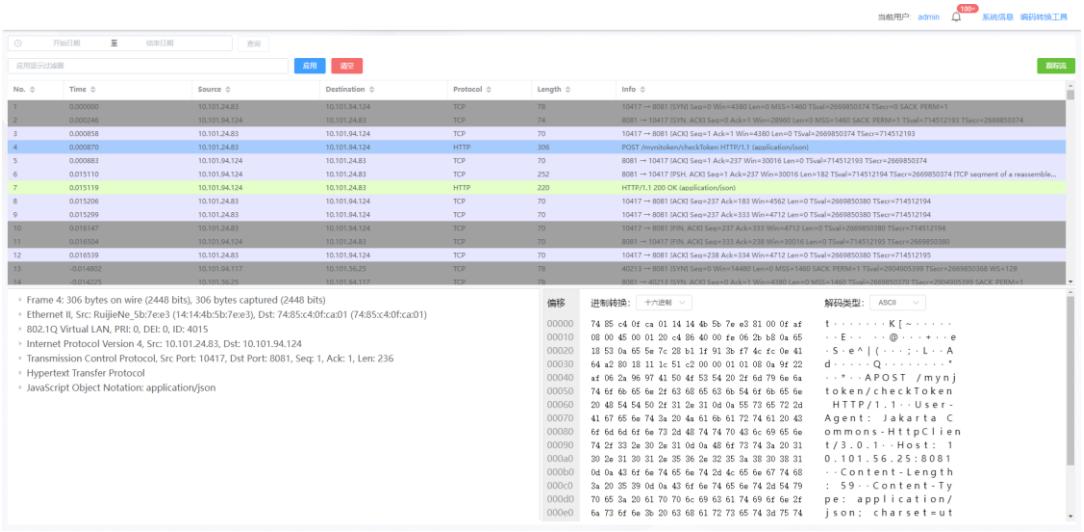

图 10 在线 PCAP 深度分析

4.10 详细的通联关系分析

TFS 利用图标的形式更好的展示节点间的通联关系，其中的源/目的节点可配置为各种不同的对象字段，线可配置为不同的连接阈值，可根据需求查看对象的通联关系，例如图中的源/目的 IP 的通联关系，还可以查看文件与主机间的通联关系，邮件收发的通联关系等，如图 11 所示。

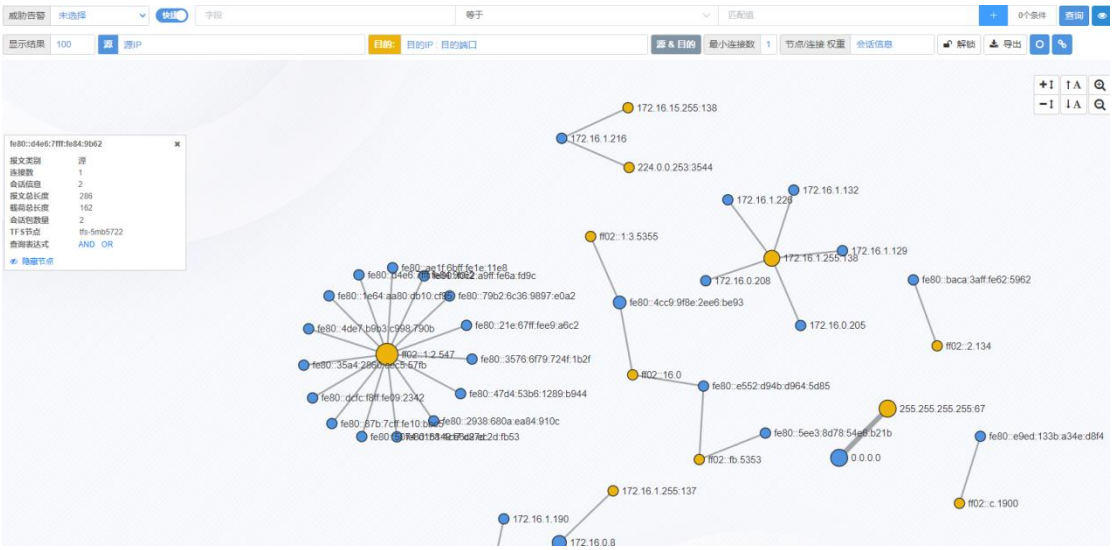

图 11 通联关系分析

4.11 丰富直观的图表展示

TFS 提供给了强大的图表自定义功能，为用户提供丰富的图形化流量实时监控视图，可以自定义选择关注的内容以及各种阈值。可选择根据解析出的不同字段进行数据分析，例如根据 TFS 节点、报文长度、会话包数量、IP、主机等已记录的元数据字段，同时可选择关注的该字段的 TopX，排序方法、刷新时间等，如图 12 所示。

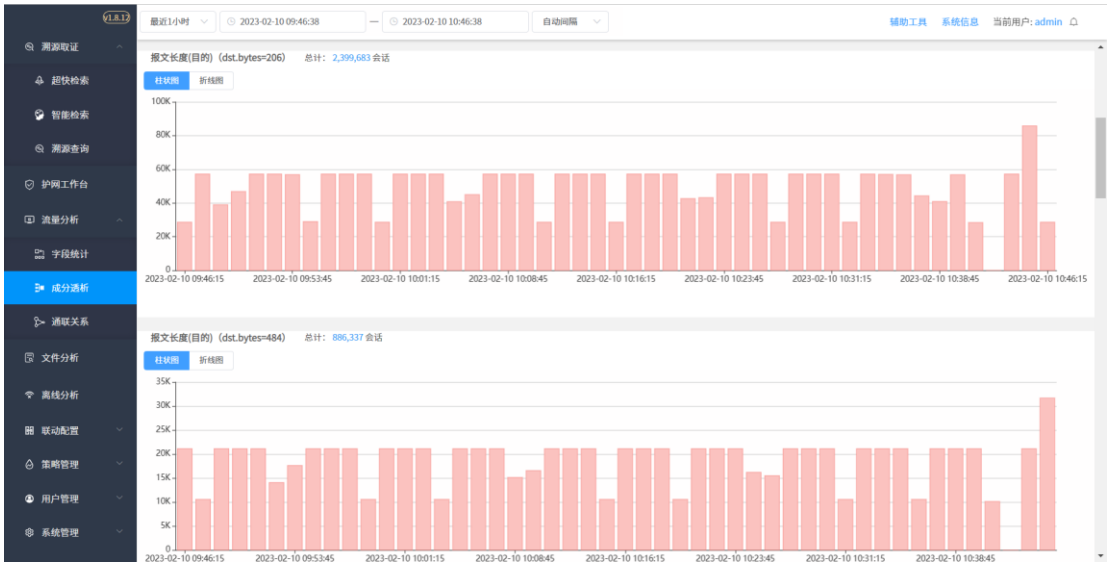

图 12 图表展示

5 产品优势

- **高性能全流量留存**

高可靠、高性能的数据包捕获及记录，高磁盘数据存储压缩比。支持抓包策略灵活配置，基于五元组、域名、BPF 规则和应用等策略的流量过滤。

- **高效的网络协议分析及异常行为检测能力**

具备基于特征、威胁情报和 AI 智能检测的威胁检测分析能力，从源头快速发现网络恶意行为，有效发现高级威胁。

- **完善的溯源取证能力**

可对任意解析后的数据字段进行快速过滤检索及对留存的 PCAP 包原始内容检索，基于图和智能算法进行事件追溯。

- **秒内超快检索**

秒内检索到 PB 级数据（百亿会话）中的指定会话及 PCAP 文件。

- **强大的处理性能**

提供强大的溯源取证能力，单台流量处理能力最高可达 20Gbps，并可按需扩展处理能力和存储周期,适用于用户对业务网络高度、实时化监控保障的要求。

6 部署场景

6.1 全流量威胁取证与回溯分析场景

全流量威胁取证系统通过分光或镜像网络流量的方式,旁路部署在各单位网络进出口处，对企业办公网、生产网或数据中心环境全流量威胁溯源取证，部署方式如图 13 所示：

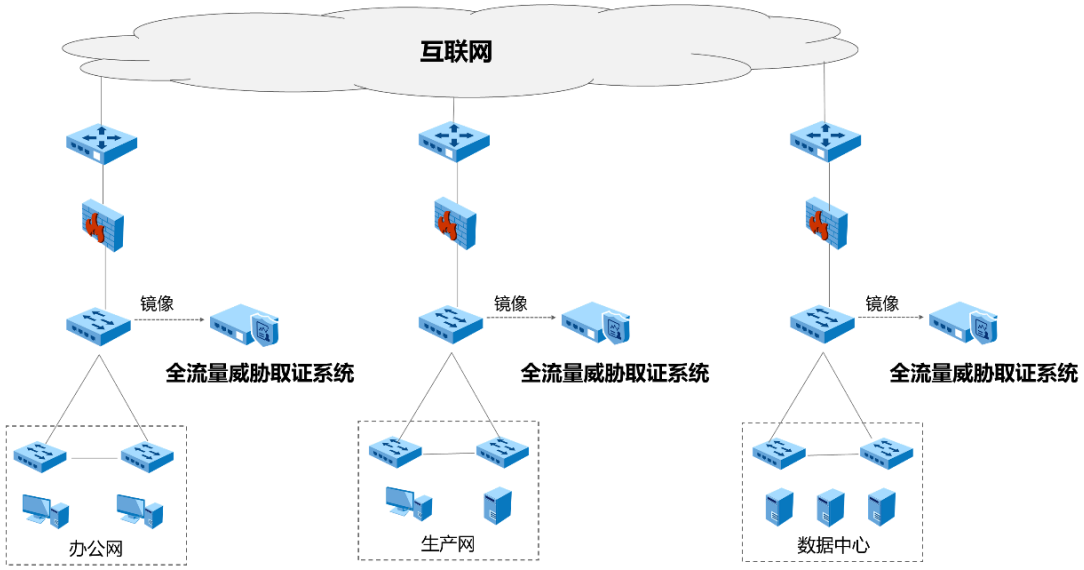

图 13 全流量威胁取证系统-单节点部署方式

全流量威胁取证系统通过分光或镜像网络流量的方式，集群部署在运营商城域网的流量进出口处，实现对城域网等大流量场景进行威胁溯源取证，部署方式如图 14 所示：

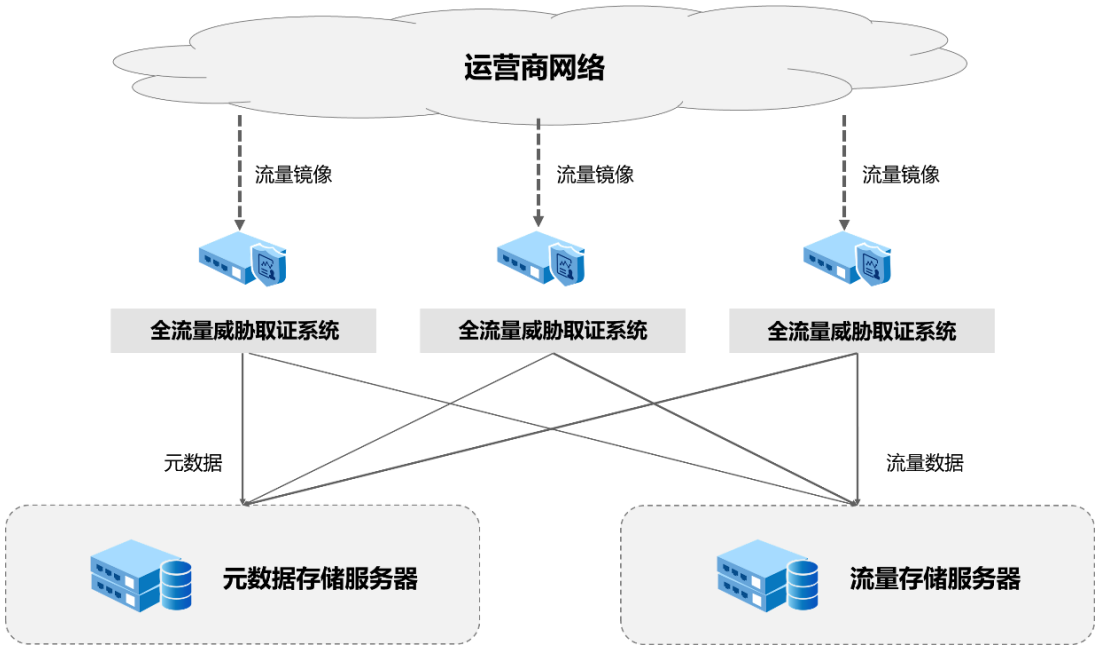

图 14 全流量威胁取证系统-集群部署方式

6.2 全流量滚动存储（TRS）场景

全流量滚动存储场景的设计目标是为检测类、审计类、安全运营类产品提供低成本的全流量威胁取证支持。该系统可提供全包存储、威胁溯源，通过缓存模

式和永久模式确保所有与威胁相关的流量都被长时间存储，与威胁无关的流量在超过缓存时间后将被删除，使得 TRS 系统具备极高的处理能力和较低的拥有成本。全流量滚动存储 TRS 最大可实现 100G 全流量存储能力，需根据实际流量需要进行产品硬件配置。

场景 1： 缓存模式

在缓存时间内，全流量威胁检测/安管平台可以根据告警会话 ID 查询 TRS，TRS 将会话完整 PCAP 包返回给检测设备或安管平台。最大支持 10 万次查询/秒，即 10 万 QPS；在缓存模式下， TRS 滚动删除落盘时间超过缓存时间的会话 PCAP。

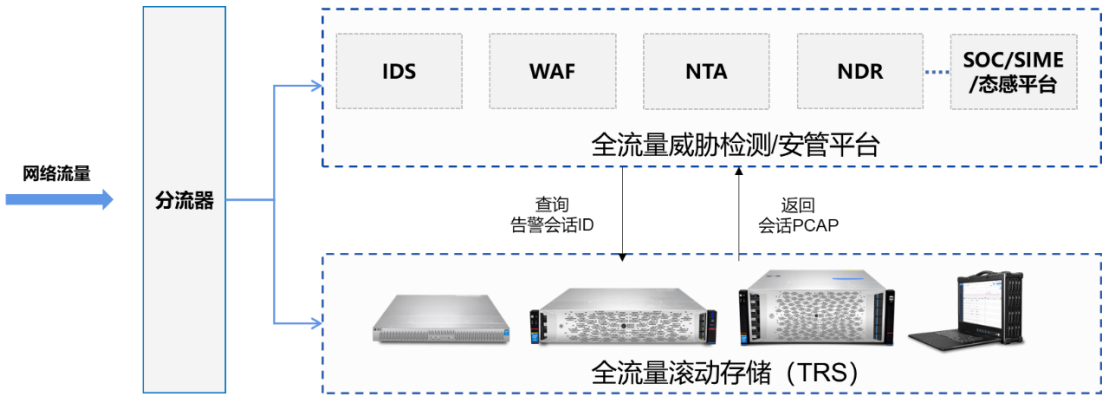

图 15 缓存模式

场景 2： 永久模式

TRS 通过 Syslog 接收威胁事件日志或查询告警会话 ID，根据告警会话 ID 查询到完整会话 PCAP 文件，将 PCAP 文件从 TRS 缓存存储区转移到永久存储区，长期留存供后续溯源取证使用。在永久模式下，告警 PCAP 将被存储到永久存储区；对于未命中告警的 PCAP 文件，将被 TRS 滚动覆盖删除。

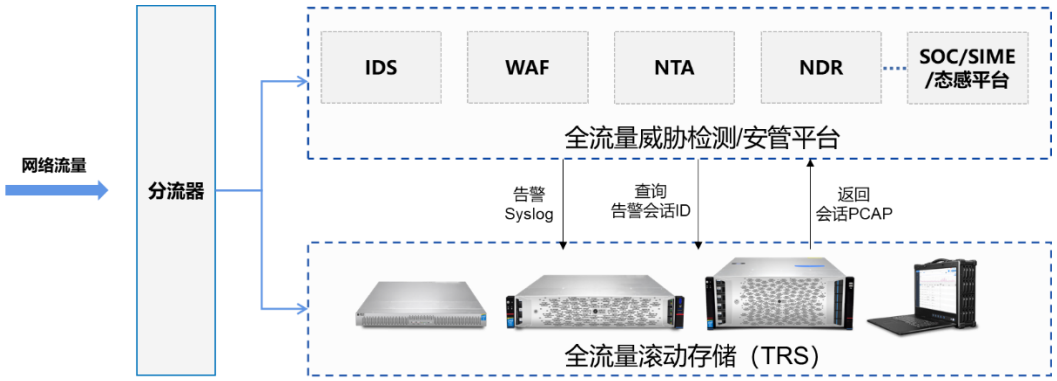

图 16 永久模式

6.3 云端全流量威胁溯源取证场景

部署全流量威胁取证系统 TFS 和大数据安全分析系统 CIC 在云环境的云主机中；

通过引流 Agent 或云厂商提供的流量镜像功能（API）将待监测流量牵引至 TFS 进行威胁检测与溯源。

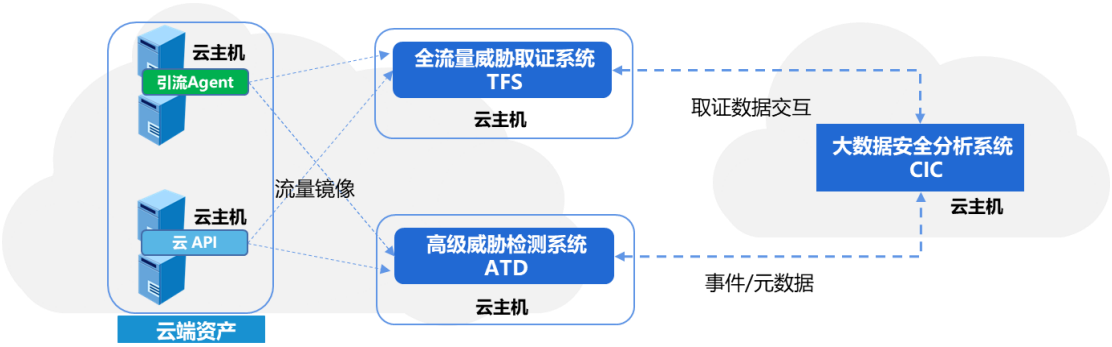

图 17 云端全流量威胁溯源取证部署

7 产品规格表

产品规格表

CPU	处理器	14 核心 28 线程*2
	芯片组	intel 芯片组-2.4GHZ
内存	大小	192GB
存储	大小	系统盘：SSD：240GB；缓存盘：7.6TB 存储盘：HDD：176TB（11*16TB）
	RAID	有
性能	检测能力	5Gbps
	查询时间	最大容量下数据查询时间不高于 1 秒
网口	接口数量	4
	监听端口	1 个 1000Mbps RJ45+2 个万兆 SFP
	管理端口	1 个 RJ45
其他接口	VGA 接口	1*VGA
	串行接口	1*Console 口
	USB 接口	2*USB 前，4*USB 后
工作环境		温度：5℃～45℃；湿度：20%～90%（非凝结）
存储环境		温度：-10℃～70℃；湿度：5%～95%（非凝结）
平均功率		550W
电源	冗余电源	双电源，交流
	电源（A）	25A
尺寸（W*D*H）mm		445 x 700 x 87 mm（无机柜挂耳） 483 x 720 x 87 mm（有机柜挂耳）
设备重量（净重）		18.85kg
设备重量（毛重）		26.75kg
设备类型		2U、机架式安装