天融信全流量威胁溯源系统TopTTT

www.topsec.com.cn

产品概述

天融信全流量威胁溯源系统是一款高性能的，对全量流量采集存储和解析检索的软硬一体化平台。该平台在捕获流量的同时进行数据包深度解析，并将解析结果与流量数据关联存储，为后续检索分析提供强有力的数据支撑。通过该平台可以发现网络事件中的蛛丝马迹，是威胁回溯分析和数据挖掘的利器。

产品特点

全流量留存-滴水不漏

天融信全流量威胁溯源系统具备数据全流量存储的能力，7*24小时实时抓取流量，将所有的数据以PCAP文件的形式留存于本地，无论是正常包，还是异常包，滴水不漏，全部留存，提供了具有法律效力的流量会话记录，供用户随时调取。

系统基于先进的多核处理器硬件平台，采用64位高性能多核并行处理技术，同时配置了大容量硬盘，具备出色的稳定性能和超强的存储能力。

全流量回溯-识包寻踪

天融信全流量威胁溯源系统具备深度包解析能力，通过拆解网络封包，透视网络中的数据传输。支持识别十多种应用协议，能够解析协议中的每个字段，支持将会话数据包以ASCIL、UTF8、十六进制等格式在界面展示，可供用户直接调用，同时系统拥有异或（XOR）运算解密能力和Base64解码能力，具备了高便捷性、高实用性的特点，助力用户在海量数据中快速寻得关键数据包。

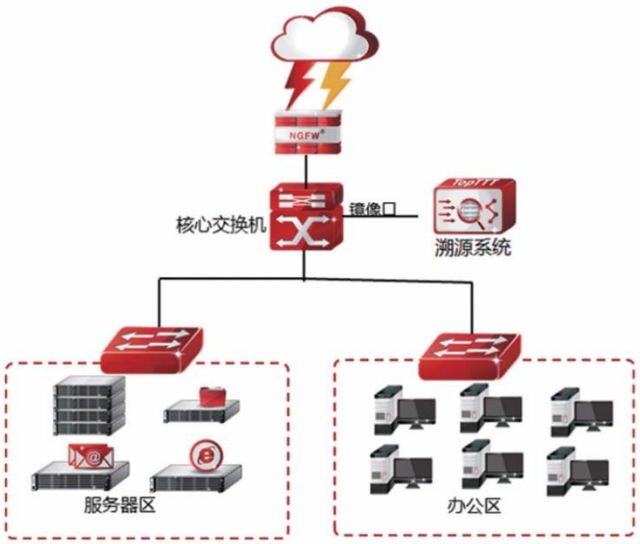
全流量检索-快如闪电

天融信全流量威胁溯源系统运用Elasticsearch技术，具备快速的数据检索能力，千万级数据，秒级查询。系统提供了视图检索模块，使检索方式更加便捷，同时支持标签功能，用户可以对关注的流量数据打上标签，通过检索标签，使得流量回溯更快更高效。此外，系统运用了异步加载技术，可最大程度的保障检索效率，实现了闪电般的检索速度。

典型应用

旁路部署

天融信全流量威胁溯源系统采用旁路镜像部署模式，将区域内所有的网络流量镜像到产品上，从而实现全流量数据采集。该模式无需改变用户原有的网络拓扑结构，系统上线方便快捷。



产品规格

TA-61508-TTT	
参数	**技术要求**
运行温度	0~40℃
电压	100-240VAC、50-60Hz
功率	550W (MAX)
接口	4 个 SFP+接口、7 个千兆电接口
尺寸（深宽高）	660mm(D)*430mm(W)*88mm(H)
产品形态	2U
电源	冗余双电源
设备形态	软硬一体化 2U 机架式设备，B/S 技术结构；
性能指标	内存容量 128GB；存储总容量 64TB；支持站点数量无限制

功能列表

TA-61508-TTT	
协议解析	包括但不限于 Cert、DHCP、DNS、Email、HTTP、IRC、Krb5、IDAP、 MySQL、Oracle、PostgreSQL、QUIC、RADIUS、SMB、SOCKS、SSH、TLS 等协议解析
实时监控	支持实时监控流量，显示时间粒度支持到 1 秒
本机状态监控	支持对探针状态监控，包括但不限于实时时间、会话数量、可用空间、CPU 状态、内存、包队列、磁盘队列、ES 队列
数据预处理	支持依据会话流统计信息，包括：会话持续时间、上传数据包数、下载数据包数、上传总字节数、下载总字节数
	支持关键应用提取，能够对 DNS、HTTP、ICMP、E-Mail 等进行协议还原，提取并记录协议中请求和对应响应的关键信息
特定协议深度分析功能	支持对常见的编码格式进行解码，包含 Base64 和十六进制，以及 ASCII、UTF-8 等。
人性化设计	界面中包含中文解释，图表可视化程度高

产品资质

TA-61508-TTT	
产品资质	**认证机构**
软件著作权证书	中华人民共和国国家版权局