Product
Introduction

网络服务监控系统

1 产品介绍

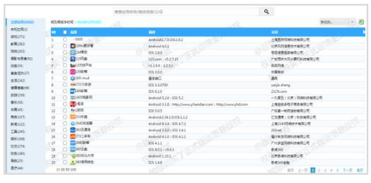
适用范围： 本系统为湖南友道信息技术有限公司出品的网络流量、性能监测、行为分析的产品，适用于需要使用网络来提供公共服务的企事业单位、运营商等，尤其是需保证网络和核心应用正常运行的单位，与其他网络管理产品是相互协作关系，更是对网络运维的重要补充之一。

核心功能： 以“流量透视、性能监控、安全检测、监测告警、回溯分析、用户行为分析”作为核心功能模块，以报表分析和系统管理作为辅助功能，协助用户实现网络资源合理配置、行为监测、安全分析，保障网络的高效、可靠、稳定运行。

技术特征： 采用自行研发的高性能流量监控板卡，具有专利化的数据包处理、硬件加速、精确业务识别、网络行为建模、内容还原和审计技术，通过分布式部署在网络关键节点的探针，实时全量捕获数据包级网络通讯流量，能提供最精确、最全面的网络流量、性能、业务、安全等统计数据，达到对网络流量任何时间任何地点的可视性监视。

2 系统特色

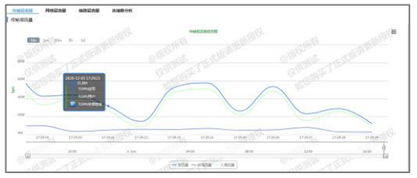
1、系统内置有应用识别特征库，对主流网络应用识别数量达到3200种以上，包括内网私有应用与主流工控协议；支持对S7、Modbus-TCP、EtherNet/IP、PROFINET、OPC、DNP3等主流工控协议的识别；内置安全规则数据库，覆盖42000条以上；内置有学术地址库，识别全球1300种以上学术地址网站及其他资源库。



2、支持对网络安全态势和网络攻击状态进行解读分析：支持在地图上分攻击方与被攻击方角度查看安全事件轨迹、展示攻击类型、攻击严重等级、攻击严重地区、攻击以及被攻击部门、机构、个人最严重TOP等信息，并能直观展示安全事件变化趋势。

3、支持对网络流量的多维数据关联分析，支持应用、应用组、用户、用户组，国家、城市、外部地址、虚链路、学术等维度数据进行跳转关联下钻分析，可以将其中任一个作为起点，并在各维度间任意游走；支持总/出境/入境流量及所占百分比、连接数统计及趋势图展现。支持6级用户组的多维度动态关联下钻及用户组自定义管理。

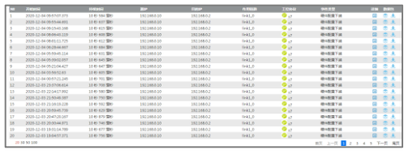
4、支持时间粒度为秒级的实时监控流量，并可实时查看当前流量的应用、用户、外部地址的成分;支持对网络连接数的分析，分析的类型包含并发流、新增流、老化流，并能对上述指标的变化趋势进行可视化展示，以此监测网络负载的变化。



5、支持对TCP会话记录的回溯分析，指标支持中文化，监测指标包括cwr、ece、urg、ack、psh、rst、syn、fin、纯ack、payload、重传、乱序、错误、sack等45个以上tcp协议指标参数的展示，可以让我们全方位了解该会话TCP连接状态。

6、支持按照服务端和客户端查看自定义时间段的网络性能指标，支持时延、传输字节数、连接数、重传、拥塞、零窗口、重置等指标查看其对应的网络性能状态，同时根据各指标进行对应的TOP10排名。

7、支持工控网络异常流量检测分析，对发现的异常流量进行预警；扩展支持对用户误操作、用户违规操作（对工程师站组态变更、操控指令变更、PLC下装、程序异常退出）等关键事件进行检测，并能对事件的全流程监控。



8、可集成主动端到端拨测设备功能，实现对应用层常用业务（HTTP、SMTP、POP3、FTP、DNS等）的测量和端到端时延、丢包率、时延抖动、带宽、路由及传输层TCP、UDP协议的主动测量。