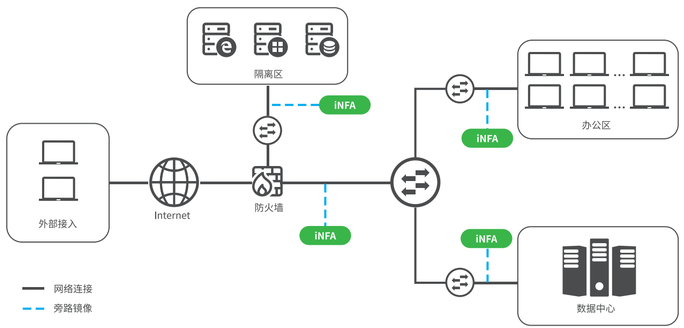
部署方式

聚铭网络流量智能分析审计系统（iNFA）采用旁路SPAN部署方式和TAP部署方式，两种部署方式均不会改变用户现有网络架构和网络配置，且不会对用户现有的生产业务或应用产生任何影响；设备部署的示意图如下：



产品规格

聚铭网络流量智能分析审计系统（iNFA）可根据不同客户需求进行选择，以下为硬件规格型号：

型号	JUMING-iNFA-200	JUMING-iNFA-500	JUMING-iNFA-1000	JUMING-iNFA-5000	JUMING-iNFA-10000
吞吐量	200Mbps	500Mbps	1000Mbps	5000Mbps	10000Mbps
网络接口数	2个千兆电口	2个千兆电口	4个千兆电口	2个千兆电口/2个万兆光口	2个千兆电口/2个万兆光口
每秒新建连接数	2万	5万	10万	50万	100万
最大并发连接数	50万	100万	200万	400万	900万
硬盘	2T	4T	2*4T	3*4T	4*4T
内存	16G	32G	32G	64G	64G
电源	单电源	单电源	单电源	冗余电源	冗余电源
设备尺寸	2U	2U	2U	2U	2U

注：规格配置仅供参考，实际交付以合同约定为准。

关注微信公众号

关注新浪微博

JUMING 聚铭

地 址：江苏省南京市雨花台区软件大道180号南京大数据产业基地07栋406室
电 话：025-52205520 / 025-52205570　　传 真：025-52205565
全国统一服务热线：400-1158-400

欢迎访问公司官方网站 http://www.juminfo.com

JUMING 聚铭

网络流量智能分析审计系统

Intelligent Network Flow Analysis Audit System

网络威胁的探查者

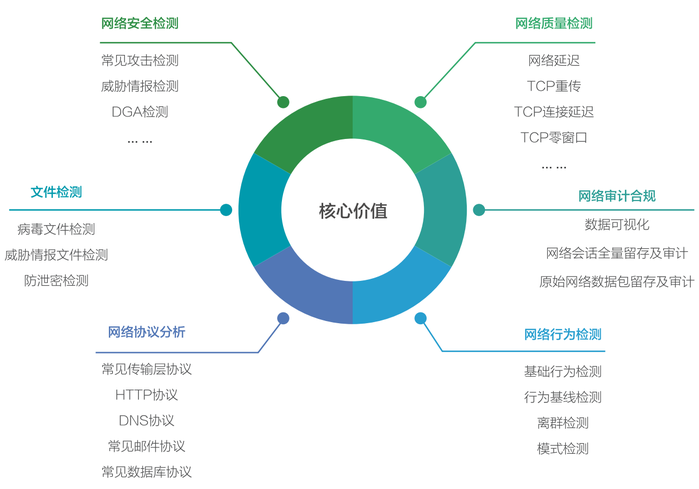
南京聚铭网络科技有限公司
Nanjing JuMing Network Technology Co., Ltd

2018年10月 第一版

产品概述

聚铭网络流量智能分析审计系统（iNFA）是南京聚铭网络科技有限公司研发的具有自主知识产权的专业网络流量分析及审计系统。它具有独特而强大的网络流量审计和分析功能，结合攻击检测技术、异常流量检测技术、威胁情报技术、文件检测技术、大数据安全分析技术、安全态势感知技术以及丰富的安全事件报告功能，可有效检测外部攻击、内部非法连接、网络会话模式异常等安全威胁，是对传统安全防御系统的完善和补充，成为企业提升安全防御水平的有力武器和必要工具。

核心价值



主要功能

多种应用解码

提供HTTP、TLS、SMTP、POP3、IMAP、FTP、SMB、RDP、SSH、Telnet等应用协议以及IEC、MMS、Modbus、OPC、OPCUA、EthernetIP CIP等工控协议的解码、元数据提取及存储、搜索、统计功能，并对可疑网络流量进行了全包留存。

威胁检测

通过对网络流量进行非入侵性的侦听检测，在威胁发生全生命周期的多个阶段识别攻击者的攻击负荷、恶意行为和网络通信。

安全事件分析

对安全事件对应的会话、入侵检测特征、网络访问域名信息、C&C回连信息、动态算法生成域名（Dynamic Generating Algorithm，即DGA）等通过多视图展示，全方位快速展示攻击或网络异常事件背后的信息。

威胁情报分析

支持动态域名、Spyware IP / Bot IP / Spammer IP、被黑主机、扫描器结点，C&C回连域名、钓鱼URL/虚假防病毒网站、TOR、VPN/Socket代理等多类的攻击情报，提升对可疑高级持续威胁的攻击检测能力。

网络会话分析

对网络中的会话正常行为模式进行建模，分析网络流量速率分布、会话趋势、会话目的端口分布、会话协议分布、会话包数分布、会话字节数分布、会话源地址分布、会话目的地址分布、会话应用协议分布相关统计情况，通过分析会话流量对于正常行为模式的偏离而识别网络攻击，隐蔽传输与内网探测检测等问题。

态势感知

可按安全事件类别、安全事件名称、系统网络流量速度、C&C（即Command And Control，恶意软件回连地址或域名）、IDP（即Intrusion Detection and Prevention，入侵检测防御）安全事件的分布及趋势评估总体安全态势，分别在客户所属国地图与世界地图上显示安全攻击分布态势、会话分布态势，并可对安全事件信息进行深层次钻取分析。

追溯挖掘

基于大数据，可快速的回溯和定性分析历史的HTTP、TLS、SMTP、POP3、IMAP、FTP、SMB、RDP、SSH、Telnet等应用协议相关流量，识别其中未被发现的攻击行为，当推出新的检测算法时可依据历史流量数据训练、事后挖掘先前未发现的威胁。

产品优势

高速的网络抓包及模式匹配技术

聚铭网络流量智能分析审计系统（iNFA）采用零拷贝、全程无锁化技术处理网络流量数据包，而且充分利用CPU向量化指令对各类模式进行识别或匹配，故即使在超大流量情况下，系统整体处理几无延时。

协议的深度识别，更全面、更精确分析恶意行为

独有的智能协议识别技术，可高速、准确地识别上千种应用，检测各种协议伪装行为；

支持HTTP、TLS（含HTTPS）、SMTP、POP3、IMAP、FTP、SMB、SSH、Telnet等协议的3-7层元数据提取、存储、搜索，分析，可二次挖掘可疑攻击行为。

多维度纵深检测机制，提供最佳的检测率和最低的误判率

从已知签名检测、行为检测、网络会话异常检测、威胁情报检测及事件关联分析等多个维度对URL、邮件、网络通道、流量等威胁载体中各类安全威胁进行深度检测，并在高级持续威胁的漏洞利用、后门植入、后门网络通道，C&C回连、流量异常等多个阶段、多个攻击环节上形成纵深、完备的检测体系，从而提供最佳的检测率和最低的误判率。

高度智能化的分析能力

产品采用多种人工智能包括机器学习分析方法（包括支持向量机、马尔科夫转移概率分析、距离分析、参数及非参数假设检验分析等）对各类网络连接/流量进行深度分析，对可能隐藏的问题进行深层级挖掘，以提供更广范围、更深层次的安全检测能力。

情报为王，把握行动先机

整合包括最全的全球C&C黑名单库在内的多类的威胁情报库，可快速、准确发现已知的、可疑的高级持续威胁的攻击来源，使安全管理人员可以专注于实际风险及关键的威胁信息，把握先机，快速解决问题。

大数据安全分析，持续改进分析效能

对HTTP、TLS、SMTP、POP3、IMAP、FTP、SMB、RDP、SSH、Telnet等应用协议的元数据及会话数据的通过大数据技术全量存储、搜索分析，识别、挖掘其中可疑的攻击行为，当推出新的检测算法时可依据历史流量数据训练、事后挖掘先前未发现的安全威胁，促使安全分析效能持续改进。