天融信网络流量分析系统

技术白皮书

北京天融信公司

二〇一三年

目 录

第一章 背景

1.1 概述

随着网络应用的日益增多，互联网用户对互联网带宽的要求越来越高，不仅体现在运营商万兆级别物理链路出口瓶颈上，也体现在网络非健康环境下运营困境，随着骨干网中DoS/DDoS 攻击、蠕虫病毒、垃圾邮件事件频发，无时无刻不威胁着网络健康。

天融信网络流量分析系统(简称“TA-FLOW”)系统采用旁路式流量摘要提取技术，通过对帧数、帧长、协议、端口、标志位、IP 路由、物理路径、CPU/RAM 消耗、带宽占用等直接特征的监测，基于时间、拓扑、节点等统计分析手段，建立现行流量分布数学模型并结合已知模型进行实时比对分析，实现网络流量分布异常监测。系统采用 Collector 结合 Controller 技术对网络流量进行分析、检测，实时监控、检测网络中 DoS/DDoS 攻击、蠕虫病毒、垃圾邮件及其他网络异常事件，提取异常特征，并启动报警和响应系统进行过滤、阻断和防御。

1.2 网络流量现状与问题

1.2.1 网络带宽资源有限

随着互联网不断地飞速发展，网络上的各类应用越来越多，占用带宽资源越来越大。在带宽资源有限的情况下，一些应用如迅雷、BT、视频、病毒等抢占大量的带宽，很难对这些流量做出详细的分析和网络流量的分布情况做出准确了解，企业业务无法得到正常的保障。

1.2.2 网络流量应用异常

网络流量异常，企业内部用户用于工作（访问业务服务器）的流量有多大？用于上网的流量有多大？谁占用的网络带宽最大，这些占用是必要的吗？谁在非法扫描网络？谁提供非法的下载服务？

1.2.3 网络流量分布不明

流量的分布问题：在全网中，哪些点流量大，哪些点流量小？流量的构成问题：对于特定的点，流量的组成是什么？由谁发起的？目的地在哪里？网络流量的应用不明，是我们急切需要了解的。

第二章 产品功能

2.1 综述

采用旁路式流量摘要提取技术，通过对帧数、帧长、协议、端口、标志位、IP 路由、物理路径、CPU/RAM 消耗、带宽占用等直接特征的监测，基于时间、拓扑、节点等统计分析手段，建立现行流量分布数学模型并结合已知模型进行实时比对分析，实现网络流量分布异常监测。系统采用 Collector 结合 Controller 技术对网络流量进行分析、检测，实时监控、检测网络中 DoS/DDoS 攻击、蠕虫病毒、垃圾邮件及其他网络异常事件，提取异常特征，并启动报警和响应系统进行过滤、阻断和防御。

2.2 流量分析

系统基于流的流量分析功能，可通过旁路抓包采集数据，也提供收集 NetFlow 信息的能力；可以对接口、传输协议、应用协议、源目的地址、源目的端口、会话进行统计分析，可以多条件组合分析；支持流量趋势分析；支持流量分析的下钻与上卷；可对数据包的字节数、包个数、传输速率进行统计、分析、告警。

系统可对设备总流量、接口流量、上下行流量、接口进出流量进行统计分析，包括流量字节数、包个数、速率等，用户可自定义查询时间段和查询条件。

可基于流量某种属性进行 TOP 排名，以该属性为出发点进行下钻，可多次下钻，最终定位到最细粒度（源 IP、目的 IP、应用协议、传输协议）的会话流量字节数、包个数、历史趋势图等。

分析方法包括：

- 总流量分析
- 基于连接信息分析
- 基于应用协议分析
- 基于传输协议分析
- 基于源地址分析
- 基于目的地址分析

- 原始流量留存
- 原始数据包留存

2.3 基线自学习

设备可基于正常网络流量进行基线自学习，学习出正常网络情况下，单个主机被访问的数据包个数速率、主机之间的数据包传输个数速率，该基线值可用于异常流量检测、DDOS 检测等。

2.4 异常流量监控

系统可实时进行网络异常流量监控，对于异常流量，产生告警信息。针对网络设备、设备接口、主机、主机分组等的异常流量监控包括：

- 应用协议流量速率、字节数、包个数异常告警；
- 协议组流量速率、字节数、包个数异常告警；
- 设备接口流量速率、字节数、包个数异常告警；
- 协议比例异常告警，包括 TCP、UDP、单播、组播、广播等分布异常；
- IP/MAC 绑定异常告警；
- 总流量超常告警，包括流量速率、字节数、包个数超常告警；
- 包大小分布异常，包括 64、128、512、1024 等包分布异常告警

2.5 攻击检测

2.5.1 入侵检测

系统内置 4000 余条入侵检测规则库，可自动识别、监测蠕虫攻击、木马攻击、SQL 注入、RPC 调用、溢出攻击等检测。此为，用户也可以自定义安全行为特征。

2.5.2 DDOS 检测

系统可检测 FLOOD 攻击、异常包攻击，对产生的攻击进行日志留存、告警处理，对于客户重点关注的设备，如服务器、路由器等，如被 DDOS 攻击，可直接查看当前的资源耗用情况。

可自动识别的 FLOOD 检测包括：SYSFLOOD、UDPFLOOD、ICMPFLOOD、DNSFLOOD、DHCPFLOOD、Pingsweep、Portscan。

可自动识别的异常包 DDOS 攻击包括：land、smurf、pingofdeath、winnuke、tcpsscan、ipoption、teardrop、targa3、ipspoof、dns 异常包、dhcp 异常包。

2.6 性能监控

可自动发现网络设备，可对网络设备进行分类，如交换机、路由器、服务器等，可针对客户重点关注的网络设备，如服务器、交换机等，实时监控设备状态，包括网络设备的链路连接状态、端口启停、开启服务、CPU、内存、存储、流量等状态；

系统可结合设备的相关告警信息进行整个设备的风险评估分析。

2.7 应用识别

系统内置 12 类 300 条应用协议识别规则，可根据数据包进行深度检测。用户可自定义使用识别规则。

2.8 报表与告警

2.8.1 报表

系统可将流量信息、告警信息、日志信息等生成各种格式报表及报表组合；可计划任务生成日、周、月等报表，支持的报表格式包括：Pdf、Excel、Csv、Html、word

2.8.2 告警

系统可将异常流量告警、入侵检测告警、DDOS 攻击告警、设备性能告警等信息通过多种方法外发，通知管理员。

告警方式包括：Syslog 告警、SNMP Trap 告警、邮件告警、防火墙联动

第三章 关键技术

3.1 高效数据采集机制

综合采用FLOW、SNMP、SPAN数据采集技术和带外数据传输机制，能够透明部署在大型运营商承载网省级骨干出口链路上，对原有系统的稳定性和性能无负面影响；

3.2 良好的兼容性和扩展能力

基于行业标准的数据采集协议和Collector + Controller的方案架构，能够提供对不同品牌设备良好的兼容能力，并可以较小代价实现系统的扩充升级，有效保护客户既有投资；

3.3 流量趋势预警

实时监控、分析网络的通信流量情况，及时提供关于流量变化趋势的报表，显示网络运行状况。系统可通过缺省或定制的预警阈值和流量基线及时报警并告知负责人员；

3.4 异常行为判别

实时检测因大量数据包的泛滥式攻击造成的网络流量异常，包括网络中的DoS/DDoS攻击、蠕虫病毒、大量的垃圾邮件等异常流量；

3.5 异常行为溯源

通过异常行为特征信息和IP路由、端口CAM信息关联分析，可将异常流量源头准确定位到网元设备物理端口级别上，为实施针对性的防护响应提供明确指引；

3.6 应用层攻击检测

采用数据流智能重组、特征检测、协议分析相结合的检测方法，根据强大的攻击特征库检测各种攻击，并提供攻击报告和补救建议措施；

3.7 应用层行为检测

采用应用层内容检测、协议解码分析、行为分析等多种检测技术，实现对网络通信行为

的检测分析，可检测敏感信息越界传输和大部分P2P流量发生；

3.8 通信服务质量实时监控

通过对网络设备和网络流量的实时监控，提供多种详细的设备、系统、带宽资源占用情况和服务进程响应情况的图形和报表显示，便于管理员了解和掌握全网运行状况和通信服务质量，保证关键业务安全稳定的正常运行；

3.9 攻击实时响应

对于检测到的异常流量，将通Syslog、Email、SNMP Trap等进行报警，并可将异常流量隔离进行重点监控和深度检测，如调整ACL、黑洞路由、防火墙、防垃圾邮件系统等安全设备对各种异常流量进行防御等；

3.10网络信息审计

通过对于网络流量的检测、应用特征的分析分析和响应形成完整的网络审计日志，便于管理员对骨干网络运行情况进行全面地监控、记录、审计和重放，为网络策略优化提供数字依据。

第四章 产品优势

4.1 全网络关联的实时性

实现全网关联的关联性流量分析，满足客户对全网流量状况的整体把握。主要采通过核心 Controller 对网络中流量情况进行汇总，实现多出口整体的关联性分析，提供整体的出口状况的整体性分析，针对某个热点地区和用户的全网关联流量分析等，有助于从整个网络的角度来把握全局的流量特征。

4.2 适用于较大型网络

采用Collector对多台路由设备进行实时分析，通过核心Controller对Collector进行管理和对Collector分析到的数据进行汇总关联。当网络扩容时，随着网络中路由气台数的增加通过增加Collector方式即可实现扩展，保护用户的投资。

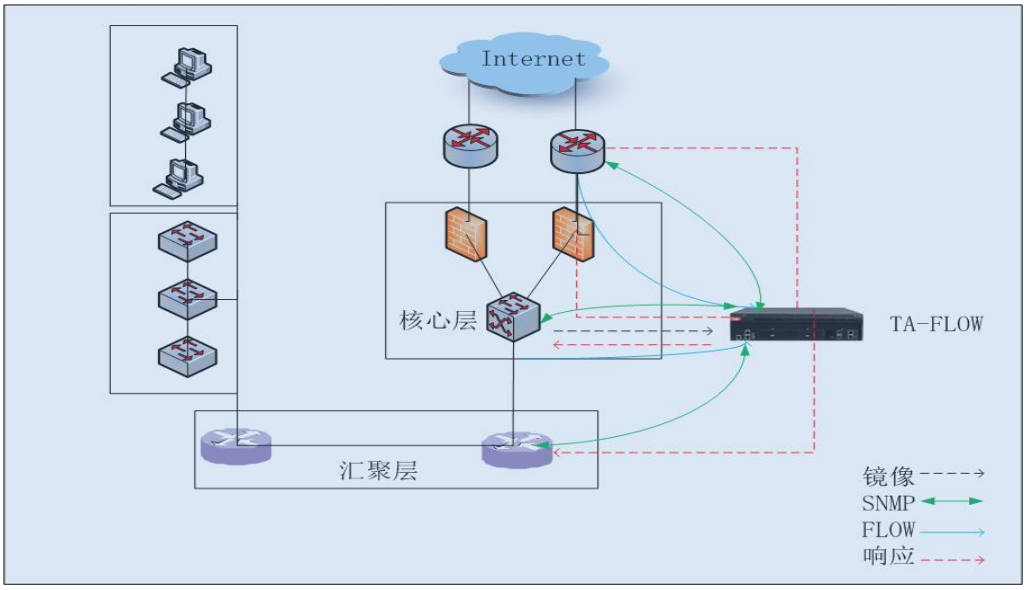
4.3 具备良好的扩展性

采用镜像端口收集数据具有更佳的扩展性。 单个收集器就能从网络中多个路由器收集数据而且没有对网络增加任何故障点。可以根据用户的网络规模和流量的增加而进行平滑的升级，只需要根据网络流量的情况增加收集器即可增加系统的处理能力。系统的分析服务器能够对新增的收集器进行统一的管理，并可以在增加收集器时将原配置在其它收集器的路由器无缝移植到新增的收集器中以减少原有收集器的负载，原有的数据和结果并不会丢失。

第五章　产品部署

5.1 部署示意图

网络中核心层采用两台防火墙部署在网络出口位置，汇聚层通过核心交换机接入到防火墙。其中 TA-FLOW 监控对象为 IP 网络的边界路由器、核心层交换机和汇聚层交换机设备，这样的设置不仅可以监控外部网络和 IP 网络之间的流量，同时也可以监控 IP 网络内部的网络流量状况。如下图：



5.2 部署配置说明

- 通过配置边界路由设备接口的 FLOW 功能，对进出 IP 网络的流量采用标准的 Flow 协议进行数据采集并加以分析；
- 通过配置核心交换机的 FLOW 功能，对 IP 网络的内部流量采用标准的 FLOW 协议进行数据采集并加以分析；
- 通过将连接到核心交换机的 SPAN 接口上，使 TA-FLOW 系统对 IP 网络的全部流量进行原始数据包分析；
- 通过配置所有网络设备的 SNMP 功能，对所有网络设备的物理接口进行管理和监控。上述配置的完美搭配，帮助用户实现。

5.3 部署配置效果

TA-FLOW 通过对边界路由设备和核心交换设备采用标准的 FLOW 协议完成数据采集，通过对网络流量中异常行为的鉴别，实时检测因大量数据包的泛滥式攻击造成的网络流量异常，包括网络中的 DoS/DDoS 攻击、蠕虫病毒、大量的垃圾邮件等异常流量。

TA-FLOW 通过采用标准的 SNMP 协议完成核心交换设备信息的收集，关联异常流量行为特征的分析结果，迅速将异常流量源头准确定位到核心交换设备的物理端口级别上，管理员可通过采用限制端口速率、设置 ACL 或者直接关闭端口等措施实施防护响应。

TA-FLOW 自动发送指令启动核心交换机指定端口的 SPAN 功能，完整采集原始数据源，采用数据流智能重组、特征检测、协议分析相结合的检测方法，根据强大的攻击特征库准确检测 IP 网络内部的攻击行为，并提供攻击报告和解决方案。针对特殊的应用协议，进行内容检测、协议解码分析，可检测隐藏在正常应用协议中的非法网络流量，如：P2P 流量等。TA-FLOW 对于检测到的攻击入侵、蠕虫病毒、DoS/DDoS 攻击、垃圾邮件以及其他网络异常事件，将通过声音、Syslog、Email、SNMP Trap 等方式进行报警，并可进行深度防御和响应，如调整 ACL、配置黑洞路由，与防火墙、防垃圾邮件系统等安全设备互动。

第六章　产品资质

资质证书	颁发单位
计算机信息系统安全专用产品销售许可证	公安部公共信息网络安全监督局
涉密信息系统产品检测证书	国家保密局涉密信息系统安全保密测评中心
军用信息安全产品认证证书（军 C+级）	中国人民解放军信息安全测评认证中心
计算机软件著作权登记证书	中华人民共和国国家版权局
ISCCC 信息安全产品认证证书	中国信息安全认证中心
软件产品登记证书	北京市经济和信息化委员会
IPv6 Ready 2 金牌认证	全球 IPv6 测试中心
信息技术安全测评 EAL3 证书	中国信息安全测评中心

第七章 关于天融信

天融信是中国领先的信息安全产品与服务解决方案提供商。基于创新的 “可信网络架构”以及业界领先的信息安全产品与服务，天融信致力于改善用户网络与应用的可视性、可用性、可控性和安全性，降低安全风险，创造业务价值。

构建可信网络安全世界

随着人类文明的进步，全球已经进入到信息化时代，并带给我们前所未有的高科技高品质生活，同时也带给我们前所未有的信息安全危机。面对日益严峻的信息安全 形势，致力于全面实现信息安全性与可用性的的天融信公司，正朝着成为“民族安全产业的领导者、领先安全技术的创造者、世界级信息安全提供商”这一目标坚实迈进。

面对鱼龙混杂、混沌无序、创新不断的网络世界，从用户、应用、内容、安全、服务、位置、时间七个层面，天融信正不断构建强大的网络感知体系。有感知才有安全，从终端、管道到云端，天融信致力于全面保护用户信息，为客户构建可信网络及安全世界。

中国安全硬件市场领导者

从 1996 年率先推出填补国内空白的自主知识产权防火墙产品，到自主研发的可编程 ASIC 安全芯片，到云时代超百 G 机架式“擎天”安全网关，天融信坚持自 主创新完成了国产防火墙跟随、跟近甚至超越国际知名产品的过渡。连续 10 年以上位居中国信息安全市场防火墙、安全网关、安全硬件第一，天融信始终引领和见 证着中国信息安全产业发展的每一个里程碑。

快速成长的安全管理业务

不仅仅是防火墙，不仅仅是保护网络边界，天融信安全管理软件业务快速成长，并在进入的所有领域获得或者正在获得领先。天融信的终端虚拟化技术帮助客户构建 一个可控的、可信的关键网络应用环境，彻底避免了来自于互联网的安全威胁对网络关键应用及数据的灾难性影响。统一用户及终端安全管理帮助客户有效管理多种 应用，实现多应用环境下的统一用户管理以及用户终端数据保护，并涵盖了快速增长的移动智能终端。合规管理帮助客户更好的实现数据库、业务、网络及运维的审 计与监控。涵盖安全设备管理、应用性能管理、数据安全管理、安全事件管理等功能的大数据安全分析与挖掘平台，正成为天融信下一代安全管理平台、互联网安全 云服务平台的核心。

互联网安全云服务的开拓者

早在 2004 年，天融信就成立了“天融信安全运维中心”，为企业用户提供安全运维外包服务，这是国内第一个商业化的安全运维服务组织。2007 年起，天融 信分别与电信、联通合作，成立了两家安全运维中心，充分利用双方的优势资源为广大企业客户提供安全运维服务。2012 年天融信互联网安全云服务中心成立， 可为全国范围内的企业用户提供 7*24 小时远程安全事件监控、分析、预警和响应服务，同时可提供本地化的现场运维服务，帮助用户快速、有效地解决安全问 题。经过八年多的探索与发展，天融信已经累计为 5800 多家企业提供过远程安全运维服务。

实现安全的业务交付

天融信不仅帮助客户保护网络及信息安全，还帮助客户实现安全的、快捷的业务交付，提升业务价值。上网行为管理、精确的应用流量控制以及负载均衡帮助客户高 效地管理带宽的使用，保障关键应用的性能，抑制非关键应用对带宽的占用，并实现对互联网内容访问的有效控制，提高员工工作效率。广域网加速、安全网关内置 的加速模块及云加速软件可以加速以 Web 为代表的众多互联网应用服务，并显著提高长距离访问、跨运营商访问及无线网络访问的用户体验。

安全研究与前沿探索

国内首屈一指的漏洞挖掘、攻防分析、软件代码分析、安全研究、安全服务人员负责跟踪和分析互联网的安全威胁形势，为所有天融信公司产品提供安全技术、内容 及支持，实时保证了安全产品的有效性。自动化的互联网应用与内容分析平台及持续人员投入保障天融信各类产品拥有领先的应用识别与内容分析能力。可编程 ASIC 安全芯片及高性能加密芯片的研制开发为相关安全硬件产品提供了强大的动力，实现了安全产品的高性能。云计算、工业系统、物联网、IPV6、 WLAN 等新兴产业或业态的安全研究也取得众多阶段性成果或者局部应用。

技术创新引领发展

虚拟化及安全技术的创新性研究将极大地提升终端安全及云端安全的防护水平。国内可靠性最高、性能最强、网络适应性最好的网关专用安全操作系统保证了天融信 防火墙在银行、证券、电力等关键行业的大规模应用与高占有率。高度集成的一体化智能过滤引擎技术

能够在一次数据拆包过程中，对数据进行并行深度检测，保证 了协议深度识别的高效性。基于更大规模、更多种类的数据采集、存储、处理、关联分析的安全管理平台将真正成为客户安全运维与管理神经中枢。

国家安全企业责任

2008 年奥运会安全保卫工作核心技术支撑单位、2010 年世博会网络安全神经中枢系统建设单位、2010 年广州亚运会信息系统（AGIS）网络安全系统 集成商、2011 年天宫一号与神州八号对接工程安全管理系统提供商及 2012 年国家下一代互联网安全专项防火墙、VPN、互联网审计的承接单位……，天融 信在多个重要行业信息系统或项目建设中成为主力军，并不断践行着维护国家信息安全的使命与责任。

全球视点中国领先

网络无界、安全无限，天融信正以全球视点，推动安全业务的稳步发展。天融信是微软 MAPP 合作伙伴，可第一时间获得微软相关漏洞，同时天融信还是中国第一批可以查看微软源代码的企业。天融信是 INTEL 全球信息安全合作伙伴，并在北京建有联合实验室，致力于 INTEL 架构平台在安全领域的开拓性研究。天融 信还在美国硅谷建设了中国第一个海外安全分析与监测实验室，全面跟踪国际互联网安全态势。

正是对技术创新的不断追求以及对信息安全事业的不懈努力，为天融信赢得了无数荣誉，也确立了天融信在中国信息安全市场的领先位置。中关村 10 大软件品牌企 业、中国电子政务 100 强企业、德勤亚太高成长 100 强企业、中国软件 100 强企业、《福布斯》中国最具潜力非上市企业、国家规划布局重点软件企业、国家 重点高技术企业等等，既是对天融信的肯定，又是对天融信的激励。回顾过去、放眼未来，天融信开启、探索、引领信息安全市场，全力帮助客户构建安全能力，提升业务价值。