Neusoft

密级:秘密

NTARS v5.0
网络流量分析与响应系统
技术白皮书

东软公司 网络安全产品营销中心

目录

一、 前言

本文档适用于东软集团股份有限公司(以下简称东软公司、东软或者本公司)制造的NTARS 网络流量分析与响应系统的销售工作，力图从产品技术角度提供必要的参考说明。

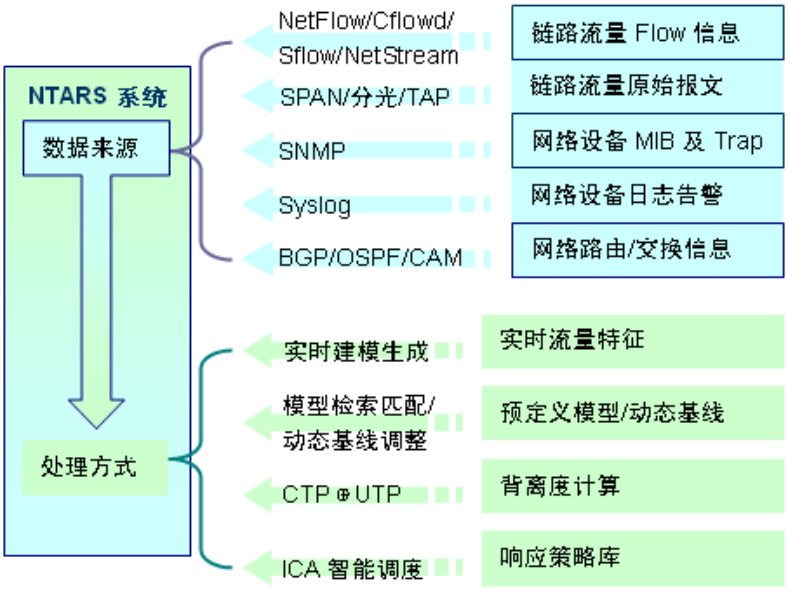
本文档主要内容包括 NTARS 产品体系构架、各功能单元说明和标称技术参数等方面的相关数据，便于阅读者快速掌握 NTARS 产品的基本概况，提高对项目需求判断和设备选型的正确率。

同时，需要指出的一点是，本文档所包含的各项数据，尤其是产品技术型号、指标参数，均为现阶段的一般性数据，仅供阅读者了解、理解 NTARS 产品的普遍情况使用。考虑到东软公司经营管理策略、技术研发进度和特定项目需求等因素，在实际供货时，所有数据指标均有可能发生更新变化，并将通过随机标准文档予以说明。

二、 NTARS 产品定位

2.1 NTARS 主要目标

NTARS(Network Traffic Analyse & Response System)网络流量分析与响应系统是东软公司面向高带宽网络领域推出的流量分析与动态响应系统，并由于一脉相承的血统缘故，NTARS 不仅具备一般网络流量分析系统的仪表功能，而且着重突出系统在异常流量分析方面的专长技能并提供多种自动的响应抑制能力。



NTARS 流量分析与响应系统技术原理示意图

NTARS 定位于高带宽网络流量图式的检测分析，通过对链路流量特征信息和设备状态信息的提取、建模，综合采用 DFI、SNMP 等多种方法进行分析，实时检测 DoS/DDoS 攻击、超限传输等网络异常事件，进而驱动响应系统进行阻断防御。同时，NTARS 系统面向管理员提供流量图式、趋势预测等各种针对网络运行状况的统计分析数据，帮助运管人员监控和掌握骨干链路及关键资源的运行情况。

在防护对象方面，与 FW、IPS、UTM 等传统安全设备相比，NTARS 的保护目标不再局限于如内网安全域、关键服务器等有形资产，而是将更加关注以网络使用效率、服务质量保证(SLA)为代表的无形资产。

在上一版本的基础之上，依据 NetEye 稳定的技术前瞻路线，秉承东软公司核心技术成果，并结合珍贵的客户反馈意见和可靠的现网观测数据，NTARS v5.0 在功能布局、系统平台、核心算法等方面均实现了跨越性提高。

2.2 值得推荐的协同产品

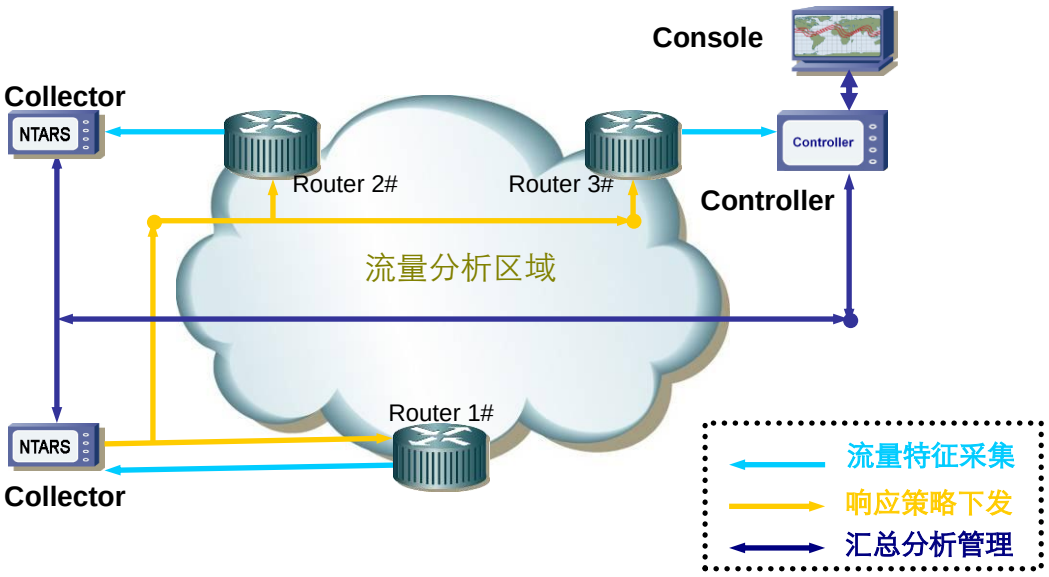
在东软公司 NetEye 产品线中，另有 NTPG 产品值得优先推荐以在网络流量分析与响应解决方案中与 NTARS 系统协同作业，从而形成“面<—>线<—>点”多防护层面之间遥相呼应、环环相扣的自适应防御体系。

NTPG(Network Traffic Purifying Gateway)网络流量净化网关：自适应防御体系中的“线”设备，能够通过 n*GE/2*10GE 端口提供深层次的流量清洗作业，实时过滤高带宽背景流量中夹杂的 DDoS、P2P、Worm 等 Bandwidth-Exhausted 类异常行为，并能够针对应用层提供协议识别、入侵防御和流量管理服务。同时，NTPG 支持集群阵列，并可实现各成员机之间的负载均衡和状态监控。NTPG 能够在 NTARS 的引导下面向特定数据流进行针对性过滤净化，并可将分析/处理结果上报 NTARS 系统，便于 NTARS 系统把对应的流量抑制策略向异常流量来源方向进行溯流上移，从而最大限度降低异常流量对目标区域的影响范围。

如需了解 NTPG 详细技术介绍，敬请参阅《NTPG 网络流量净化网关技术白皮书》。上述文档可从 Http://www.neusoft.com 下载或致电 86-10-82777777 免费索取。

三、 NTARS 系统架构

3.1 NTARS 系统单元构成



NTARS 流量分析与响应系统单元构成示意图

NTARS 在系统架构上包括流量收集、特征提取/建模、DFI 模式分析和策略响应多个模块，而在产品实现中主要采用收集器 + 控制器两部分物理实体的组成方式。

- 收集器(Collector)：主要完成流量收集及特征提取/建模两部分职能。该部分属于系统的低层模块，是系统面向网元设备的接口单元并进行数据上收和格式转换、

特征提取等预处理操作；

- 控制器(Controller)：主要完成模式分析、策略响应并最终提供人机交互 GUI 界面。控制器 Controller 是异常流量分析系统中逻辑运算高度集中的单元部分，在收集器上报数据的基础上进行行为判别及智能响应职能。

NTARS 支持 Collector 与 Controller 在一套硬件系统中的整机灌装形式，系统将通过许可证管理和管理员配置而按需切换至 Collector、Controller 或者 Collector + Controller 的工作状态。此外，NTARS 还提供专门的 Collector 设备以增大对网络设备的监控范围。

依赖于 Collector 与 Controller 的组合优势，NTARS 能够平滑实现从行业客户网络到大型运营商承载网络的升级扩容。Controller 将作为统一的管理分析单元同时实现对多个 Collector 流量模型的分析和告警，并提供集中、一致的报警处理界面。

通过产品架构的支持，NTARS 系统在实际部署时可以采用以下两种部署方式：

1) Collector + Controller 合二为一的单机部署方式。该方式可满足大部分行业用户和运营商网络的流量检测需求，NTARS 系统将在一套硬件体系中合并实现 Collector 和 Controller 两种职能；
2) Controller + N*Collector 的分布式部署方式。在该方式中，NTARS 系统将按照“一拖多”的方式，由 1 台 Controller 管理多个 Collector 系统，多个 Collector 相互独立，可广泛分布在网络中各关键节点周围进行数据采集/抽样和建模，并向 Controller 提交流量统计信息。Controller 将作为统一控制系统对所有 Collector 的流量信息进行集中分析和处理。对于大型运营商承载网，该方式可通过分布式部署满足对多个路由设备、总流量高达数百 G bps 的骨干链路提供实时流量分析和异常检测，并且抽样率不低于 1/500。

3.2 安全增值业务业务接口

以运营商行业为主要市场领域，NTARS 网络流量分析与响应系统非常重视对运营商在传统语音、数据主导业务之外开展安全增值业务提供技术支撑。对此，NTARS 系统采用“客户”概念用于配置定义安全增值业务，每个“客户”都对应到一个购买了运营商安全增业务服务的具体用户上。

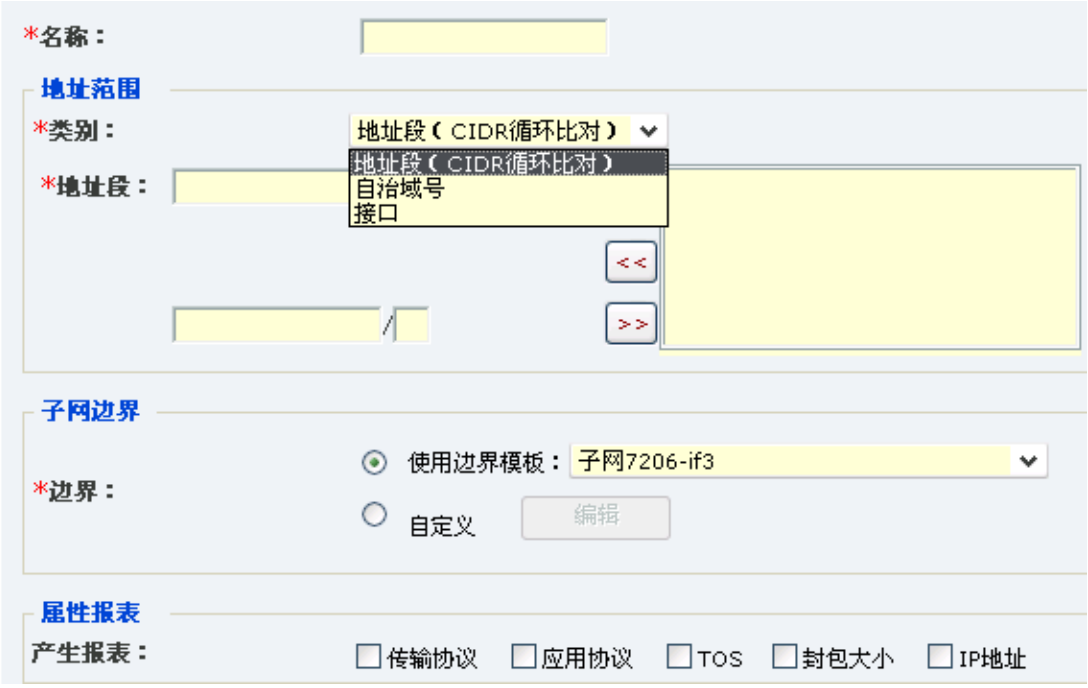
为便于运营商开展基于 NTARS 系统的安全增值业务，NTARS 系统提供以下几种机制予以保障：

1) “客户”账号管理机制：系统提供专门的客户账号管理界面，管理员可在此对客户进行账号创建、修改、启用/禁止、边界定义、增值服务分配、自动报表设置等操作；
2) “客户”操作行为审核制度：客户在登录系统之后，能够对其网络范围内的配置进行自助式操作，其中大部分操作无需管理员进行审核。但对于一些可能会涉及到系统整体安全或网络系统稳定的关键操作，NTARS 系统将会将其放入审核队列中，待管理员批准后方可生效。这些关键操作主要包括检测规则/基线的定义、响应策略的配置和对执行该响应策略的网络设备的指定；
3) 独立的客户接入通道。在业务规模较小的情况下，NTARS 系统可允许客户经 Flow 采集端口或 Admin 端口登录系统以访问其安全增值业务，而当面对较高的安全防护策略要求是，NTARS 系统还可提供专门的网络接口专门用于客户登录，并且系统内将严格限制从该端口登录用户的访问权限，从而实现系统业务流量与管理流量的分离。

四、 NTARS 功能特色

4.1 完善的网络单元描述

在错综复杂的骨干区域访问关系中，NTARS 系统可通过多种手段进行网络单元实体的描述说明，为异常流量检测、流量流向分析、自动抑制策略等工作流程提供基本的对象定义。如：



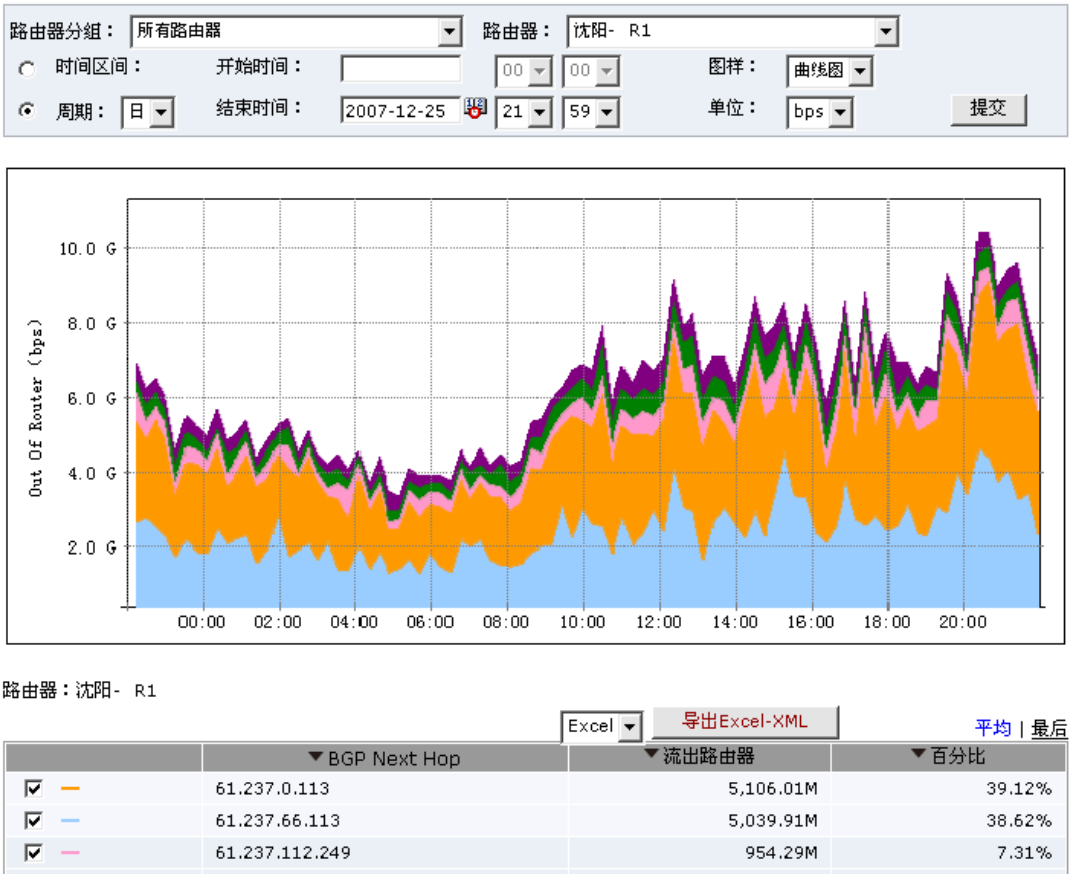
- 本地网络：支持 IP 地址段、AS 自治域号等属性；
- Internet 区域：支持路由器、路由接口、AS 自治域号等属性；
- 路由器及其接口：支持 IP 地址、SNMP 团体字、Flow 配置、BGP 配置等属性；

- 大客户接入：支持 IP 地址段、边界模版、收集器、路由器等属性；
- CIDR 子网：支持 IP 地址段、边界模版、路由器、路由接口等属性；
- BGP Prefix 分段：支持 IP 前缀、掩码等属性，也可由 BGP 路由信息中自动导入。

在基本单元定义的基础之外，NTARS 系统还支持进行分组、模版等复合定义，从而提高策略配置的灵活性和可复用性。

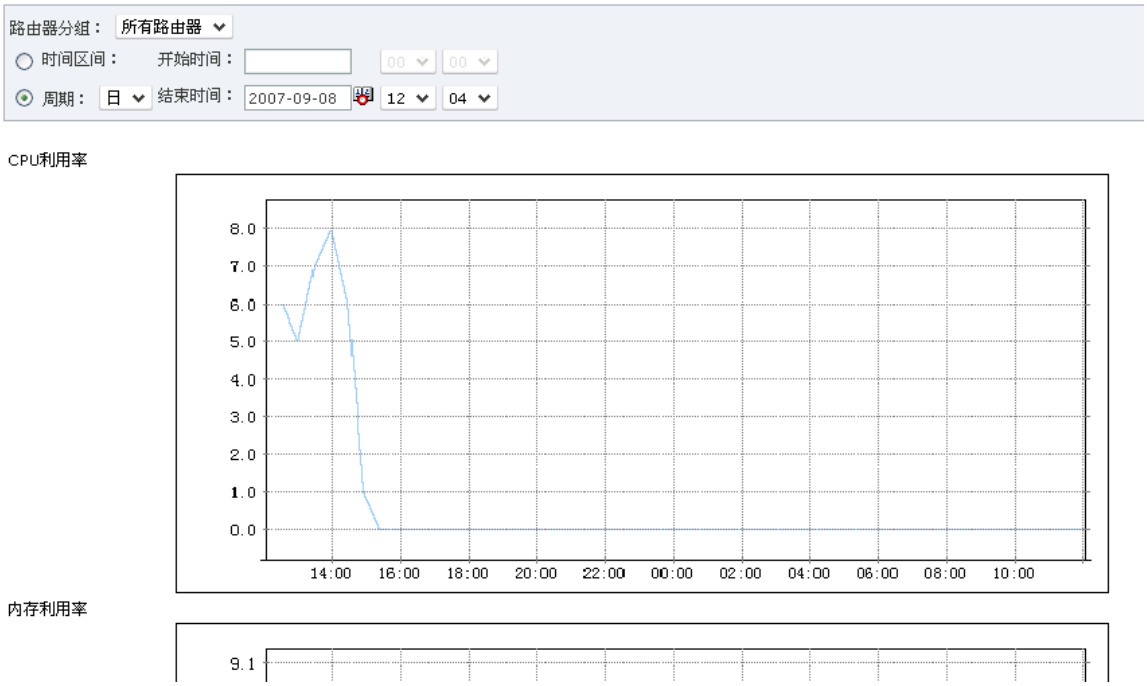
4.2 详尽的流量流向分析

依据所采集的 Flow 数据，NTARS 系统能够自动产生各网络单元的流量流向分析报告，采用图形、列表等形式对网络链路流量分布进行精确描述。



- 横向层面：支持 Internet 流量、路由器流量、下一跳流量、路由接口流量、子网流量、大客户流量、检测规则流量等类型，NTARS 可按照不同流量属性(如 AS 发出流量、AS 过境流量、AS 互连流量等)生成分类别的统计分析、对比/排序等报告；
- 纵向层面：以 bps、pps 为单位，纵向涵盖 Frame size、IP、TOS、传输协议、应用协议等各类属性，NTARS 能够对此生成针对性的成分统计分析报告。

4.3 广泛的检测范围覆盖



与单纯依赖于 Flow 技术的同类产品不同，NTARS 广泛支持了所有可能被利用的基础数据。因此，除了 NetFlow V1/V5/V7/V9、SFlow V4/V5、Cflowd V5/V8、NetStream V5/V8/V9 之外，NTARS 还支持 SNMP、SPAN、CLI、NAP 等方式，对流量分布、设备状态等进行实时采集，大幅度提高流量分析结果的准确率，而且通过对网元设备的主动调节还可有效缓解其影响。

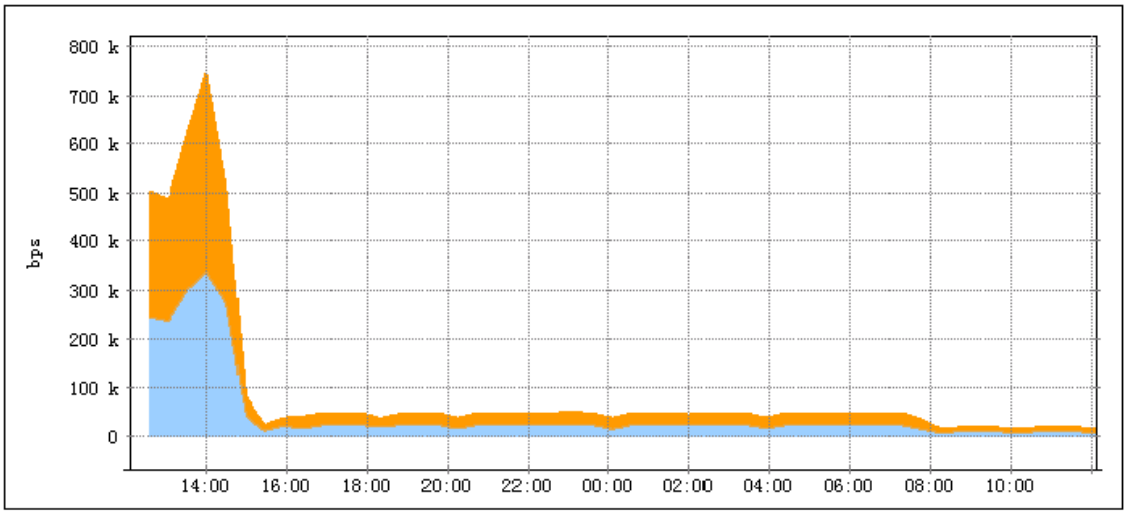
4.4 智能的 ICA 复合机制

ICA©复合技术是 NTARS 系统的技术灵魂。通过 ICA©的智能调度，NTARS 系统能够依据一种机制的输出结果而动态调整其他机制的输入策略，自动完成异常事件检测与反向抑

制指令之间的策略驱动，提高了系统针对异常流量做出抑制响应动作的时效性和自动化程度，大幅度降低同类其他设备所必需的人工介入负担。

4.5 自学习的动态基线调整

NTARS 系统支持固定基线和动态基线两种类型，其中固定基线可由管理员根据以往历史流量数据或应用业务已明确的流量特点进行人工定义，而动态基线则赋予 NTARS 系统有效检测未知异常流量特征的能力。

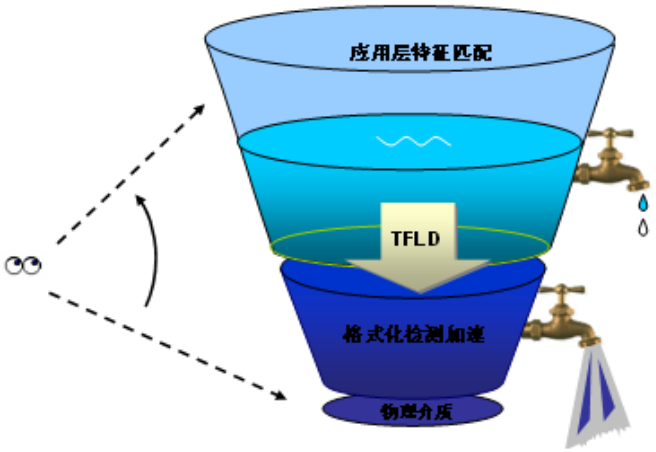


如同大海中的浪与涌一样，在网络环境中也存在着相似的流量变化现象：“浪”型流量一般具备相对稳定的“平均水位”和较为清晰的波峰波谷界定，其对网络整体服务质量的影响是短暂的，比较适合固定基线和传统动态基线的工作；然而，“涌”型流量却呈现长周期、慢增长、低曲率、大振幅等特点，无法通过固定基线及传统动态基线予以识别，却能够对网络服务质量造成长期、广泛的危害。

对此，NTARS 系统动态基线采用了由东北大学、东软信息学院和 NetEye 网络安全实验室持续多年的联合研究成果，实现了多种网络流量趋势预测算法，能够通过对未知特征的网络流量进行一定周期的采样分析后，自动完成对该部分流量的图式建模和基线描述，并持续

跟踪实际流量的变化曲率而对基线进行动态调整，从而保证了 NTARS 系统对于网络流量演变趋势的自学习能力，能够有效避免随机杂波的偶发干扰、显著提高系统检测命中率。

4.6 高效率的特征沉降加速



NTARS 系统的工作层面可简化为“链路层、网络层、传输层、应用层”四部分，其中传输层以下层面的检测速度是最快的，系统扩容能力也是相对平滑、便利的，而应用层的异常识别则需涉及高 CPU 消耗的逐比特匹配检测。在保证系统处理性能的前提下，如何有效提高检测深度，是 NTARS 及其同类产品都必须面对的技术课题。

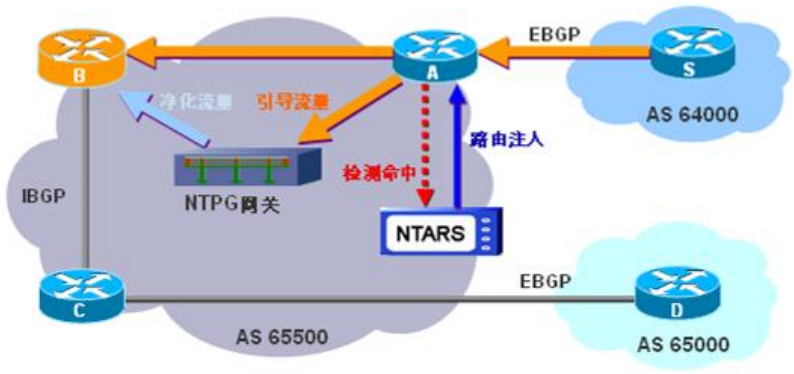
NetEye 网络安全实验室为此提供了 TFLD© (Top_layer Features, Low_layer Detection)应用层特征沉降加速技术。通过 TFLD©技术，NTARS 能够将应用层异常特征直接映射到低层格式化数据中，并通过优化算法完成快速检测和反向映射，从而能够在高效的低层处理中实现应用层的异常命中，提高了系统整体检测效率。

4.7 灵活驱动的抑制响应机制

在高效的异常检测之后，NTARS 还会做些什么？

NTARS 名字中的“R”(esponse)清晰地传达出系统对于 DDoS 等异常行为的主动干预能力，从而将其与单纯的检测报警类仪表设备泾渭分明的区别开来。

NTARS 支持各种针对不同类别设备抑制响应指令的模版配置和预定义，并在异常流量发生时，由 ICA©复合技术进行自动触发，无须管理员人工介入，即可对异常流量进行自动的、可复用的实时抑制干预，从而避免后续异常流量的发生。



NTARS 可通过以下协议接口进行抑制响应：

- → CLI：可针对设备进行 ACL、SPAN、QoS、路由配置等策略调整；
- → NAP：v1.0/v1.2，可对所有支持 NAP 协议的安全产品进行联动，如 NTPG 网络流量净化网关系统，从而能够驱使可疑流量接受进一步的、具有针对意义的定性分析过滤。

4.8 安全增值业务访问界面

NTARS 不仅重视用户从产品部署中所获得的安全防护收益，而且更为强调该安全防护收益能够给用户带来的增值业务收入能力。为此，NTARS 系统提供了专门的功能单元，遵循用户现有盈利模式，提供契合业务需求的增值业务支撑能力。

对于拥有众多客户的网络接入服务商而言，NTARS 系统可从以下几方面为用户带来直接的增值业务收入：

- 以较低的投入成本，向全部客户提供全面服务；
- 细粒度的权限划分，便于向客户提供定向、定量的增值业务销售；
- 为每个客户提供其所得到的服务质量的履行情况分析报告，增强服务质量的量化分析能力；
- 为每个客户提供专门的访问接入界面，客户可在权限范围内获得对各类分析数据的直接访问，保证数据的真实性和透明度。

4.9 快捷便利的辅助工具包

NTARS 系统重视对客户一站式管理运维需求的满足度，在统一的管理界面中集成各类有益的网络管理工具，避免用户在多种管理工具之间的频繁切换，为网络流量分析工作提供良好的辅助作用：

→ IP 地址地理位置和归属快速查询

→ 主机端口服务探测

→ NTARS 设备系统状态监控

4.10 免维护的长期运行能力

NTARS 系统提供运营级的稳定运行质量，并通过各类强化机制以实现零人工介入的续航能力：

- 流量分析报告自动生成；
- 流量数据自动备份与空间维护；
- 流量抑制指令的 ICA 智能加载与撤销；
- 外挂协同设备的 ICA 智能联动；
- 存储介质硬件化的容灾、扩容机制；
- 关键部件(如 CPU、电源)冗余备份。

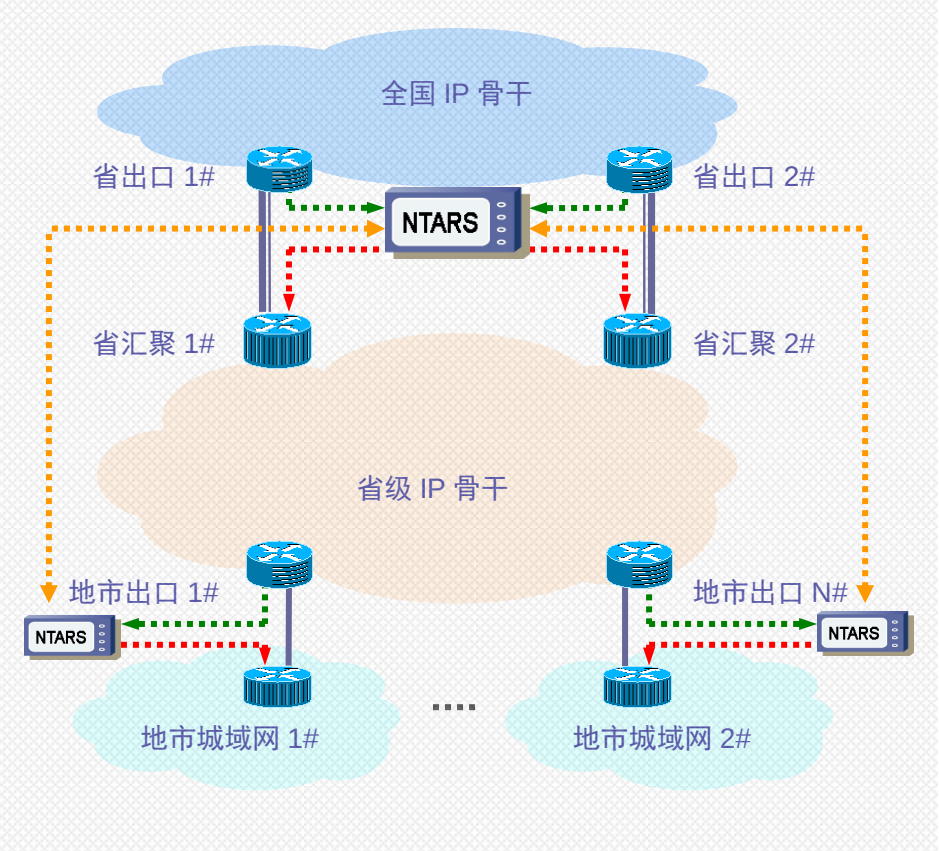
五、 功能描述

基础信息	
产品定位	网络流量分析及响应抑制产品
体系架构	软硬一体化设计
管理方式	基于 SSL 的 B/S 界面
功能单元	Controller + Collector
功能	
Flow 版本	NetFlow V1、 V5、V7、V9
	SFlow V4、V5
	cFlowd V5、V8
	NetStream V5、V8、V9
流量流向分析	以图表形式，对网络全局、单独链路、子网、客户、检测规则、地域和 TOP N 等层面显示流量流向分析数据，并可按照 IP、协议、端口、AS 等进行分类归并分析
异常流量分析	实时检测因协议滥用造成的网络流量异常，包括超限带宽下载、DoS/DDoS 攻击等异常流量
流量图式基线	支持固定阀值、静态基线、动态基线三种类型
异常检测及响应抑制策略的定制化能力	支持系统缺省检测策略及管理员定制检测策略的加载，可针对全局、会话、安全事件等层面设置不同的检测策略和事件描述并进行针对性的响应抑制动作定义

异常流量自动响应	可在正确检测异常流量发生的前提下，自动作出响应抑制动作，包括黑洞路由、ACL 过滤、可疑流量牵引等措施
联动响应兼容性	可通过 CLI、NAP 等方式支持主流路由器、交换机、防火墙、NTPG 流量净化网关、IPS 等设备联动
原始报文 Flow 提取	对于无法生成 Flow 的链路，系统能够利用原始报文自行提取 Flow 信息
网络设备状态监控	对主流网络设备状态进行实时监控，提供系统资源利用情况、链路资源利用情况多种信息，并通过图形和报表显示，便于管理员了解和掌握全网运行状况和通信服务质量
事件报警方式	支持 Email、SNMP Trap、Syslog 等方式进行事件报警，便于管理员及时掌握网络安全状态
系统时间校正	支持 NTP 自动校时和管理员手工校时等方式
辅助工具包	系统集成提供 IP 归属查询、主机端口服务探测等辅助功能
安全增值业务接口	提供专用访问接口，可支持内建批量客户账号并通过严格的鉴权机制保证客户账号在指定范围内的流量分析权限
日志审计功能	系统内置数据库系统，具备本地海量存储空间并可自动维护
	可按照日志类型、时间等条件进行数据备份和导入导出操作
	可针对源/目的 IP、时间段、事件类型、事件来源等条件进行审计
	自动生成日报、周报、月报、季报、年报等报表
管理	
管理角色划分	提供账号管理、策略管理、审计管理等权限角色
管理权限控制	按照具体操作功能对管理员账号进行细粒度的权限控制
管理界面语言	简体中文
管理通信加密	基于数字证书的会话加密机制

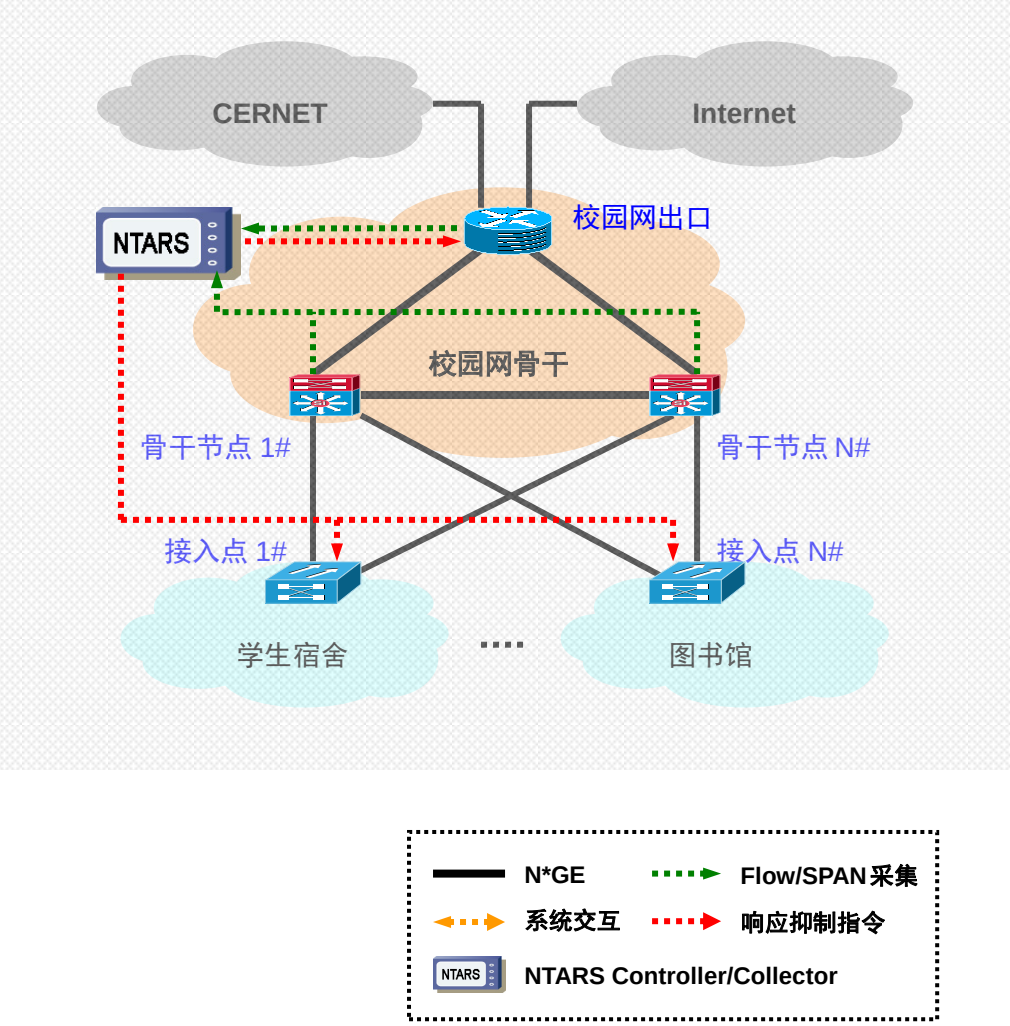
六、 典型应用场景

6.1 电信运营 IP 承载网



- 网络环境：电信运营商 IP 承载网省级出口及各地市省内骨干。
- 主要需求：流量流向分析、异常流量检测、自动响应抑制。
- 方案简述：采用“1 + N”模式，通过多台 Collector 设备对总出口链路及所辖各地市节点进行流量分析，构建分布式流量监控体系，并依靠 Controller 实现对全局所有流量数据的汇总检测与分析呈报。此外，系统还可根据流量分析所命中的异常流量定位将可疑流量自动牵引至预设的流量净化处理单元，从而实现面向全局海量带宽的动态流量清洗作业。

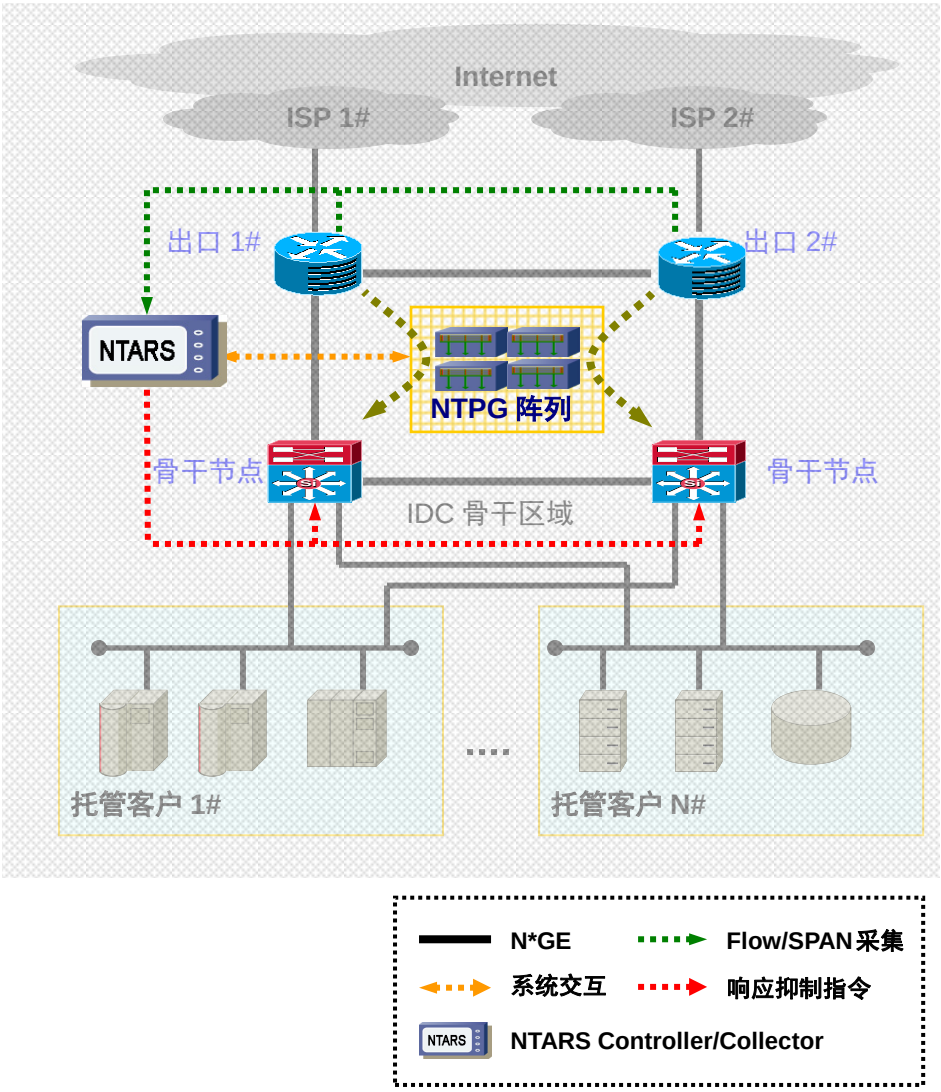
6.2 园区网络骨干区域



- 网络环境：高等院校校园网出口及骨干链路、大型行业性网络。

- 主要需求：异常流量检测、带宽资源分配。
- 方案简述：采用单机模式，监控多个采集点的流量图式分布，并能够通过 ICA 机制为下一步的应用层深度检测分析提供流量牵引。

6.3 计算资源集中区域



- 网络环境：大型商业化 IDC 机构、行业客户数据中心。
- 主要需求：异常流量检测、QoS 策略调整、异常流量清洗过滤。
- 方案简述：采用 NTARS+外挂协同单元模式，不仅可根据业务应用动态调整网络服务质量，还可通过 ICA 驱动以 NTPG 阵列为代表的外挂协同单元，构建伪串联的 DDoS 防范堡垒。