

NTARS v5.0

网络流量分析与响应系统

技术白皮书

目录

一、 前言.....	1
二、 NTARS 产品定位.....	2
2.1 NTARS 主要目标.....	2
2.2 值得推荐的协同产品.....	3
三、 NTARS 系统架构.....	5
3.1 NTARS 系统单元构成.....	5
3.2 多层次的集中管理.....	7
3.3 运营级的安全增值业务 Portal.....	7
3.3.1 安全增值业务的分类.....	8
3.3.2 安全增值业务的自身安全保护.....	8
3.3.3 安全增值业务的性能扩展.....	9
四、 NTARS 功能特色.....	11
4.1 完善的网络单元描述.....	11
4.2 详尽的流量流向分析.....	12
4.3 广泛的检测范围覆盖.....	14
4.4 智能的 ICA 复合机制.....	15
4.5 自学习的动态基线调整.....	16
4.6 高效率的特征沉降加速.....	17
4.7 深度协议分析及攻击检测.....	18
4.8 细粒度的异常溯源定位.....	19
4.9 灵活驱动的抑制响应机制.....	20
4.10 契合业务的客户访问界面.....	21
4.11 快捷便利的辅助工具包.....	22
4.12 免维护的长期运行能力.....	22
五、 功能描述.....	24

六、 典型应用场景.....28

6.1 电信运营 IP 承载网 28

6.2 园区网络骨干区域 30

6.3 计算资源集中区域 31

七、 产品型号及标称参数.....32

7.1 NTARS 12800 32

7.2 NTARS 8800 33

7.3 NTARS 6800 34

7.4 NTARS 6500 35

7.5 NTARS 6000 36

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。

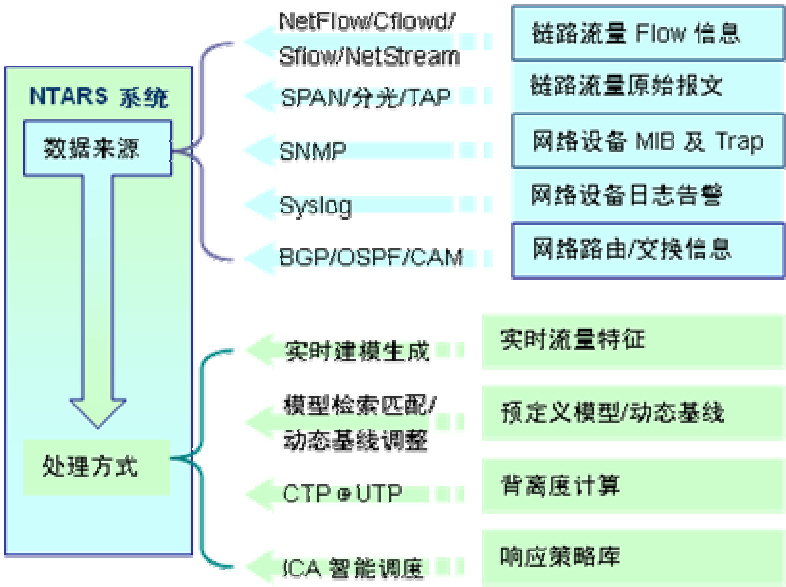
本文档使用权及解释权归东软公司所有,并由东软公司网络安全产品营销中心编纂维护。未经东软公司书面明确允许/授权,本文档禁止任何个人或机构用于商业/非商业用途,如复制、修改、引用、索引等。

本文档的任何阅读者缺省负有对本文档及其所含数据的保密义务,或者将本文档即时销毁。

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**、**DPI**、**SNMP** 等多种方法进行分析，实时检测 **DoS/DDoS** 攻击、超限传输、路由抖动及其他网络异常事件，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、路由抖动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** 在模块布局、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。

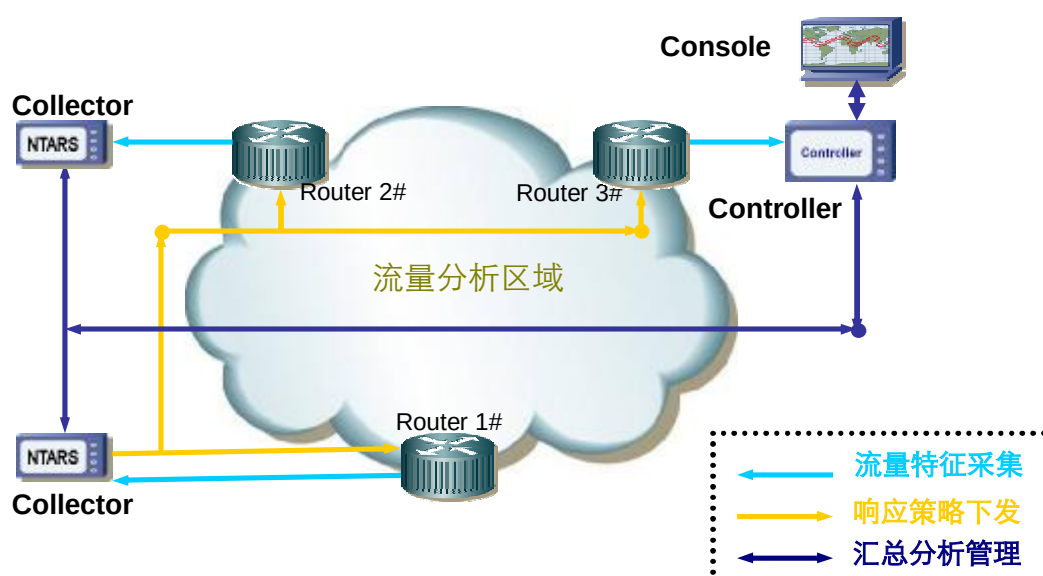
NTPG(Network Traffic Purifying Gateway)网络流量净化网关：自适应防御体系中的“线”设备，能够通过 **n*GE/2*10GE** 端口提供深层次的流量清洗作业，实时过滤高带宽背景流量中夹杂的 **DDoS**、**P2P**、**Worm** 等 **Bandwidth-Exhausted** 类异常行为，并能够针对应用层提供协议识别、入侵防御和流量管理服务。同时，**NTPG** 支持集群阵列，并可通过阵列前端控制系统实现各成员机之间的负载均衡和状态监控。**NTPG** 能够在 **NTARS** 的引导下面向特定数据流进行针对性过滤净化，并可将分析/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](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、**DPI** 深度检测、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 **NTARS-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 and 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 多层次的集中管理

NTARS 集中管理平台 CMP(Central Monitor Platform)是针对超大型电信运营商构建全网统一的流量分析平台而推出的解决途径。

CMP 是在 **NTARS Controller** 和 **Collector** 之外独立的集中管理 **Console**，能够面向多台分布式的 **Controller** 提供事件汇总、策略下发、状态监控、关联分析等集中处理作业。通过 **CMP**，**NTARS** 系统可实现“**1+M*(1+N)**”的多层次的分布式架构，从而很好的适应运营商行业“总公司+省分公司+地市分公司”的组织结构体系。同时，通过 **CMP** 的“摘要集中，数据分散”的工作流程特点，**NTARS** 系统成功解决了海量日志数据在远程传输实时性、系统开销、网络开销、存储介质开销之间的矛盾。

相对于“**1+N**”的 **Controller** 和 **Collector** 产品组成模块而言，**CMP** 呈现出更多的垂直管理职能色彩，既可单独组建全网流量分析中心，又为 **NTARS** 系统无缝融入电信运营商现存的网络管理中心系统和安全管理中心系统而提供规范、可靠、便捷的集成接口。

CMP 采用 **License** 销售策略，通过所管理的 **Controller**、**Collector** 的数量及各自的 **License** 情况进行许可权限计算。

3.3 运营级的安全增值业务 Portal

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值业务服务的具体用户上。

3.3.1 安全增值业务的分类

NTARS 可将安全增值业务分为四个类别以供选择：

- 1) 流量流向分析：提供客户网络范围内的流量及成分统计、数据流向分析、信息热点排名等基础数据；
- 2) 异常流量检测：可按照客户指定基线进行异常流量检测，系统将通过策略限制该客户能够启用的检测规则/基线的最大数量，策略限制的具体数量可在客户属性中进行指定；
- 3) 异常流量抑制：在异常流量检测服务的基础之上，系统将对检测到的异常流量进行自动干预，干预方式主要包括 **Black hole** 或 **ACL**，干预位置可在 **PE**、**CE** 中任选，客户可启用的检测规则/基线和干预措施的最大数量同样受到策略限制；
- 4) 异常流量净化：此业务可将系统检测到的异常流量牵引至专门的流量净化网关中进行 **DPI** 检测和过滤，因此本服务需要额外的过滤网关提供支持。**NTARS** 系统与过滤网关之间按照指定接口协议进行交互，以获得过滤网关对被牵引流量的处理情况的反馈并最终呈报客户。除了检测规则/基线之外，被牵引流量的最大带宽同样受到系统策略限制。

NTARS 系统提供专门的客户账号管理界面。在该界面中，管理员可以调整客户账号的网络范围定义和服务类别选择，并能够配置每种服务相关的属性，如最大检测规则数量、最大牵引流量带宽等。

3.3.2 安全增值业务的自身安全保护

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) “客户”集中认证机制：**NTARS** 可通过内置的帐号数据库对客户进行认证授权，也可利用 **Radius** 协议支持第三方认证系统；
- 4) 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。更极致的是，在业务规模逐步扩大以后，**NTARS** 系统还可提供专门的 **OSP(Open Service Portal)**主机以应对客户登录需求，**OSP** 主机将与 **NTARS** 系统维持安全、可靠的数据通道，可同时处理数百客户的登录会话。

3.3.3 安全增值业务的性能扩展

在客户数量较少的情况下，**NTARS** 系统可通过内置模块完成客户流量处理和登录接入工作，而在客户数量较多的情况下，**OSP** 主机可帮助 **NTARS** 系统实现安全增值业务处理能力的线性扩展。**OSP** 主机将集中实现以下四个功能，从而可有效降低 **NTARS** 系统开销并提高安全增值业务性能：

- A) 统一的客户接入界面：在 **OSP** 部署之后，**NTARS** 系统本身将不再允许客户的直接登录，并且也不再维护客户账号信息。客户可通过 **OSP** 访问其全部安全增值业务；
- B) 集中的客户帐号管理：**OSP** 自行维护所有客户账号信息，也可接受第三方认证系统支持。在 **OSP** 采用内置的客户账号数据库时，管理员可在 **OSP** 中完成全部的客户账号维护工作；
- C) 独立的数据分析处理：安全增值业务所涉及的数据统计、异常检测等工作将从 **NTARS** 系统中分离出来，转由 **OSP** 来完成。**NTARS** 系统将通过 **OSP** 获得其所关注的客户边界范围，并在 **Flow** 初始处理阶段便将相关记录转发给 **OSP** 系统，从而降低自身处理负担；
- D) 多机集群部署能力：**NTARS** 系统最多可支持 **4** 台 **OSP** 构成多机集群，从而可应对最多 **2000** 客户的安全增值业务需求。在同一集群中，各成员 **OSP** 共享所有的客户认证信息并明确分别所负责的客户账号群，客户可选择在任何一台 **OSP** 上进行登录，认证通过后该 **OSP** 将根据该账号归属而将会话自动重定向到相应 **OSP** 中，因此对于客户侧而言是完全透明的。

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：

The screenshot displays the NTARS configuration interface with the following sections:

- *名称：** A text input field.
- 地址范围**
 - *类别：** A dropdown menu with options: 地址段 (CIDR循环比对), 地址段 (CIDR循环比对), 自治域号, and 接口. The first two options are currently selected.
 - *地址段：** A text input field.
 - Buttons: << and >>.
- 子网边界**
 - *边界：** Radio buttons for 使用边界模板 (selected) and 自定义. The 使用边界模板 option has a dropdown menu showing 子网7206-if3. A 编辑 button is next to the dropdown.
- 属性报表**
 - 产生报表：** Checkboxes for 传输协议, 应用协议, TOS, 封包大小, and IP地址.

- ◆ 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。

路由器分组：

所有路由器

 路由器：

沈阳- R1

时间区间：

开始时间：

00

00

图样：

曲线图

周期：

日

结束时间：

2007-12-25

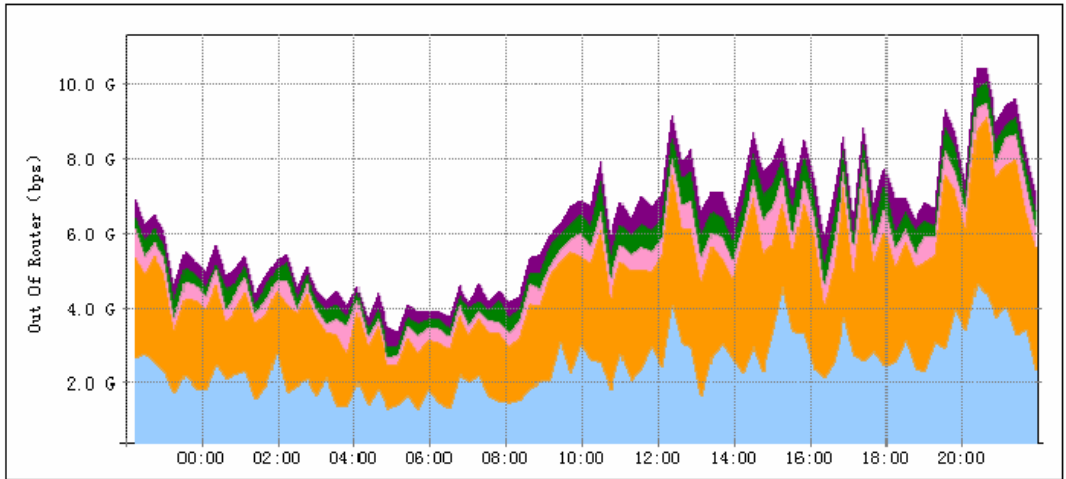
21

59

单位：

bps

提交



路由器：沈阳- R1

Excel

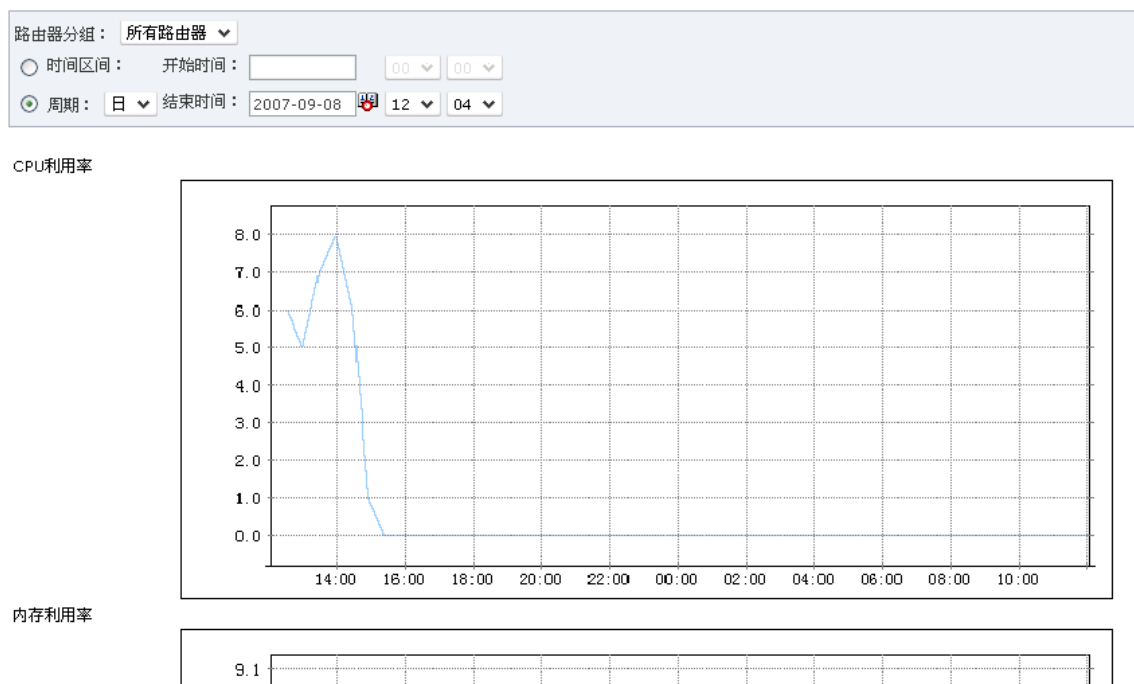
导出Excel-XML

平均 | 最后

	BGP Next Hop	流出路由器	百分比
☒ —	61.237.0.113	5,106.01M	39.12%
☒ —	61.237.66.113	5,039.91M	38.62%
☒ —	61.237.112.249	954.29M	7.31%

- 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

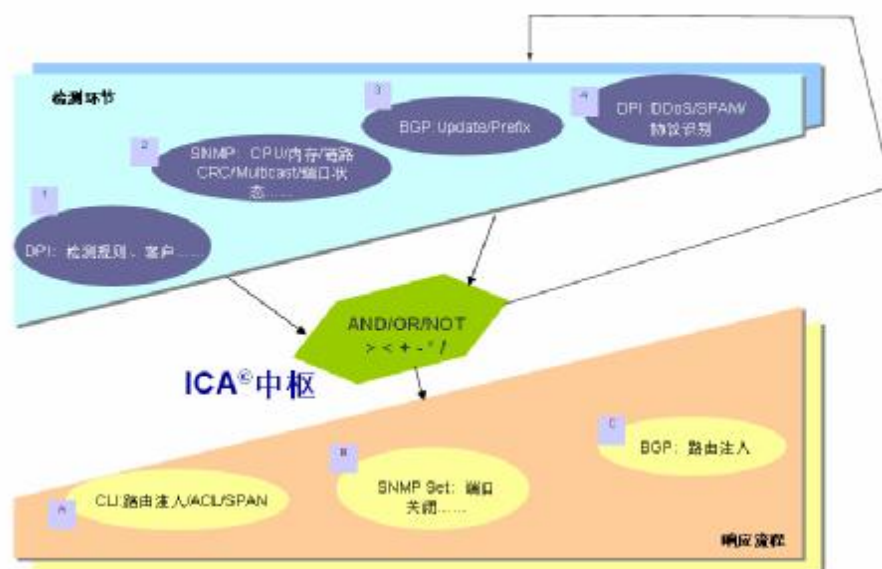


与单纯依赖于 **Flow** 技术的同类产品不同，**NTARS** 广泛支持了所有可能被利用的基础数据。因此，除了 **NetFlow V1/V5/V7/V9**、**SFlow V4/V5**、**Cflowd V5/V8**、**NetStream V5/V8/V9** 之外，**NTARS** 还支持 **SNMP**、**BGP**、**SPAN**、**CLI**、**NAP** 等方式，对路由设备状态、路由表项、动态路由协议交互、**IP/MAC** 影射、**MAC/Port** 影射、原始报文内容等进行实时采集，把链路流量图式和网元节点状态同时纳入到系统分析基础数据库中并在二者之间进行高度关联分析，不仅大幅度提高流量分析结果的准确率(如通过流量分析得出的“流量异常”表象往往有可能是由于网元设备错误策略配置等内在因素所诱发的)，而且通过对网元设备的主动分析/调节还可较精确的定位异常流量来源并有效缓解其影响。

4.4 智能的 ICA 复合机制

NTARS 所支持的 **Flow**、**SPAN**、**SNMP**、**BGP**、**CLI**、**NAP**®等采集方式并不是孤立并行的，而是在各种采集方式之间采用了 **ICA**®复合技术进行智能调度。

ICA®二次分析



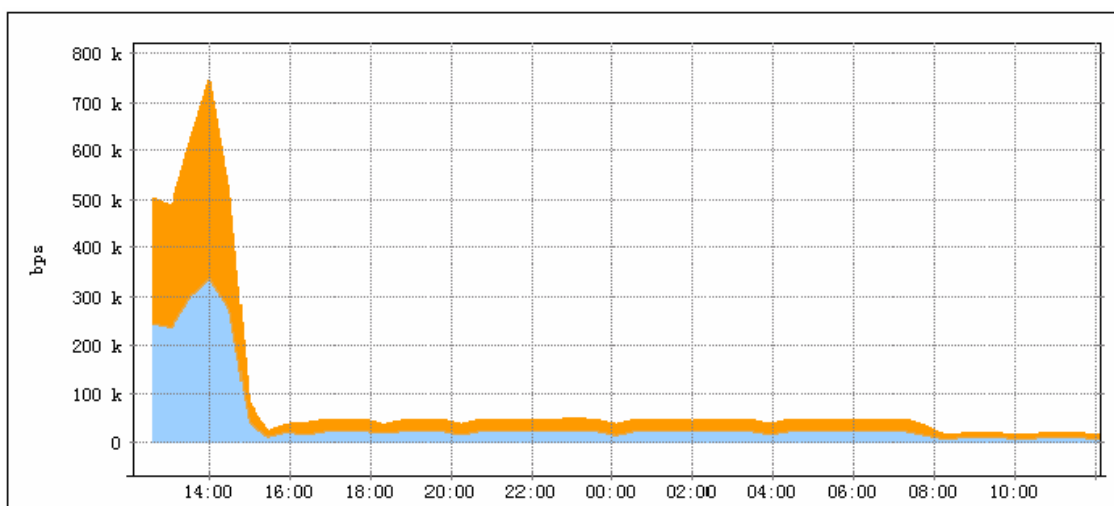
不同的采集技术在处理效率、检测精度和数据负荷等方面存在巨大差异，如 **Flow** 技术能够面向数百 **G** 流量提供整体上的流量分析与检测、**SPAN** 可针对 **Gigabits** 级别以下带宽进行逐比特的特征匹配和文本比对，而 **SNMP/CLI/BGP** 和 **NAP**®协议则更适合在网元层面进行状态提取和策略干预。如何有效地在各种技术之间取长补短、并充分发挥多种技术的复合优势，**ICA**®为此提供了集中化的逻辑实现。

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，从而在 **L2~L7** 各协议层之间、流量图式与网元状态之间进行灵活的检测作业分配，并自动完成异常事件检测与反向抑制指令之间的策略驱动。**ICA**®复合技术的引入，不仅能够促进“面<->线<->点”各层面之间分阶

段逐级检测思路的实现，保持高带宽流量分析性能和应用级检测深度的高度统一，同时还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。

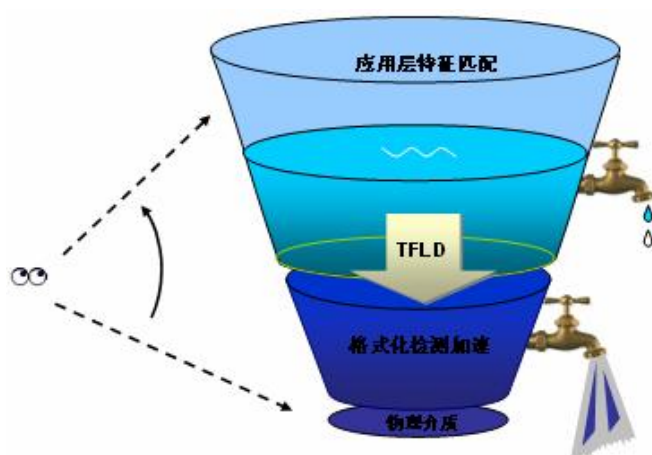


如同大海中的浪与涌一样，在网络环境中也存在着相似的流量变化现象：“浪”型流量一般具备相对稳定的“平均水位”和较为清晰的波峰波谷界定，其对网络整体服务质量的影响是短暂的，比较适合固定基线和传统动态基线的工作；然而，“涌”型流量却呈现长周期、慢增长、低曲率、大振幅等特点，无法通过固定基线及传统动态基线予以识别，却能够对网络服务质量造成长期、广泛的危害。

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

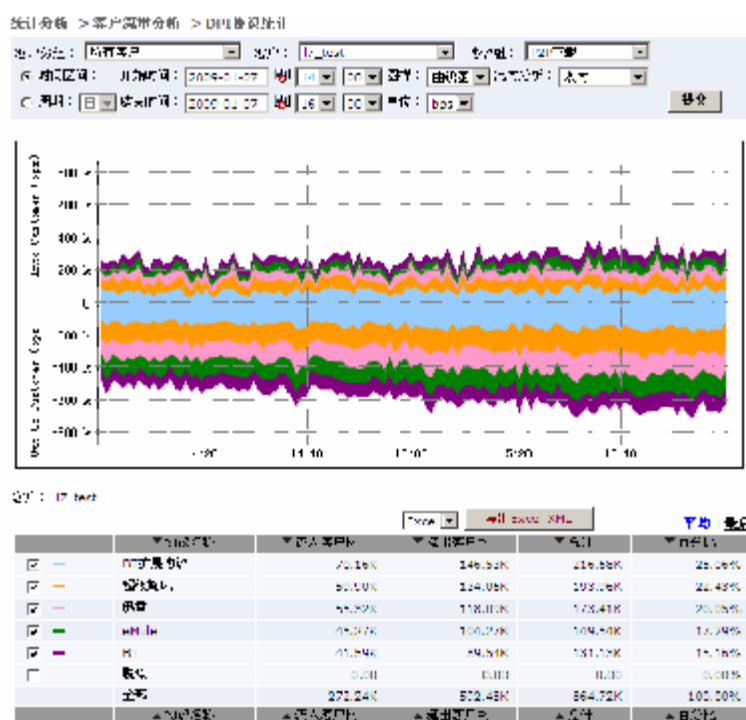


NTARS 系统的工作层面可简化为“链路层、网络层、传输层、应用层”四部分，其中传输层以下层面的检测速度是最快的，系统扩容能力也是相对平滑、便利的，而应用层的异常识别则需涉及高 **CPU** 消耗的逐比特匹配检测。在保证系统处理性能的前提下，如何有效提高检测深度，是 **NTARS** 及其同类产品都必须面对的技术课题。前文所述的 **ICA**©复合技术所实现的分阶段逐级检测思路显然是一种有效的解决方式，但 **NTARS** 系统对此提供的解决方式却并不单单如此。

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 深度协议分析及攻击检测

ICA[®]复合技术的实现使 NTARS 能够提供较高效率的 DPI 深度检测,快速识别应用协议、检测攻击类型,并可生成详细的图文分析报表,直观展现特定用户、特定攻击出/入流量统计及所占比例。



NTARS 可识别的协议包括 11 大类、100 余种：

- Ö 传统协议，HTTP，FTP，POP3 等
- Ö 流媒体协议，RTSP，Web 视频等
- Ö P2P 协议，eMule，迅雷，Bittorrent 等
- Ö IM 协议，MSN，QQ，IRC 等

- Ö 网络电话，H.323，SIP，H.248 等
- Ö 网络电视，PPLive，迅雷看看等
- Ö 网络游戏，WOW，QQGame 等
- Ö 股票交易，招商证券，同花顺等
- Ö 数据库，MSSQL，MySQL 等
- Ö 加密协议，SSH，GRE 等
- Ö 其他，RRS 阅读，IP fragment 等

东软安全实验室实时跟踪国内外最新出现的攻击方法，识别其特征，并及时应用到产品中，保持产品最新的检测分析能力。



4.8 细粒度的异常溯源定位

借助于 ICA[®]复合技术所带来的丰富的数据资源，NTARS 系统可在异常检测命中之后，提供细粒度的溯源定位功能，从而为管理员采取后续的处理措施提供准确的位置信息。

IP地址	MAC地址	交换机IP	交换机接口	VLAN交换机	VLAN号	发现时间
10.1.3.100	0002B3A2AE4B	10.1.3.254	23	10.1.3.254	26	2006-03-11 16:23:06
10.1.3.154	000B4688E340	10.1.3.254	21	10.1.3.254	26	2006-03-11 16:23:06
10.1.3.10	0002B3A2EB61	10.1.3.254	1	10.1.3.254	26	2006-03-11 16:23:06
10.1.3.211	000423C49933	10.1.3.254	9	10.1.3.254	26	2006-03-11 16:23:06
10.1.3.110	0002B3A2F0FB	10.1.3.254	1	10.1.3.254	26	2006-03-11 16:23:06

NTARS 系统可在两个层面中提供异常溯源定位：

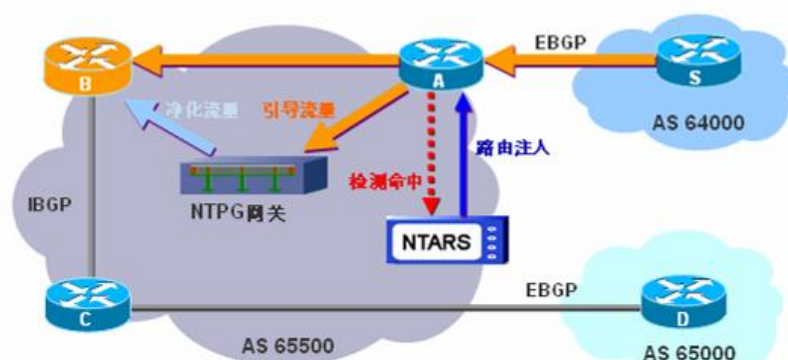
- Ö 网络层：在其监控的网络范围之内，**NTARS** 能够将异常流量来源直接回溯至最接近攻击源的路由设备接口；
- Ö 链路层：在其监控的网络范围之内，**NTARS** 能够将异常流量来源直接定位于最接近攻击源的交换设备端口。

4.9 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” (**response**) 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：

- à **BGP: v4**，可实现流量牵引、黑洞注入等操作；
- à **SNMP: v1/v2c/v3**，可通过对特定 **OID** 写操作以改变设备状态、配置；
- à **CLI**：可针对设备进行 **ACL**、**SPAN**、**QoS**、路由配置等策略调整；
- à **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。

4.10 契合业务的客户访问界面

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；
- 集中身份鉴权和粒度化的功能划分，便于向客户提供定向、定量的增值业务销售；
- 为每个客户提供可定制的安全防护能力，客户可根据己方业务特点自行设置安全策略；
- 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，客户可在访问权限范围内获得对各类分析数据的直接读写控制，保证数据的真实性和透明度。

4.1.1 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：

- à 链路帧捕捉及逐字节解码分析
- à IP 地址全球地理位置定位
- à IP 地址归属快速查询
- à 主机端口服务探测
- à 主机漏洞扫描评估
- à **NTARS** 设备系统状态监控

4.1.2 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与定向发送；
- 流量数据自动备份与空间维护能力；
- 流量抑制指令的 **ICA** 智能加载与撤销；
- 应用层深度分析的 **ICA** 智能调度；
- 外挂协同设备的 **ICA** 智能联动与回馈；
- 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	实时检测因泛滥式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、蠕虫病毒等异常流量
流量图式基线	支持固定基线、动态基线两种类型
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

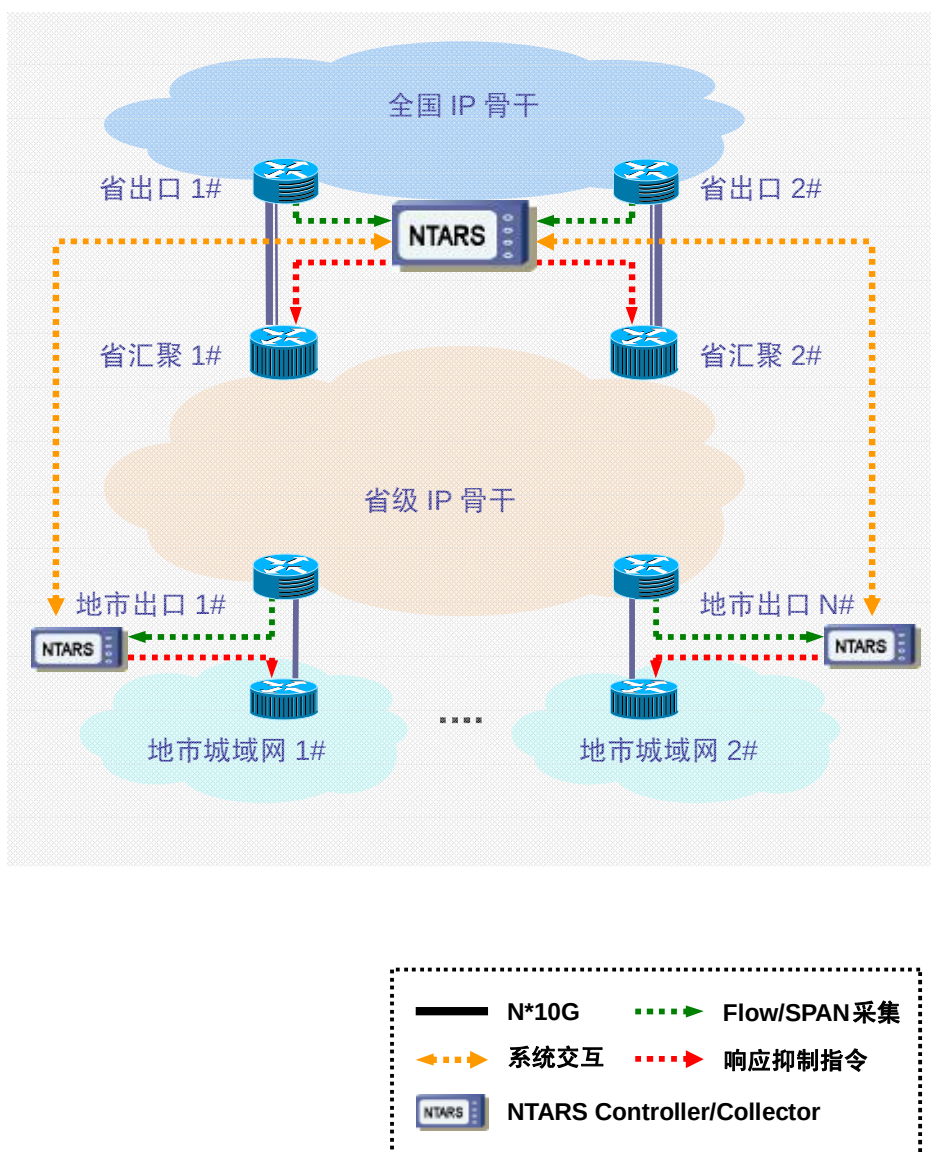
异常流量溯源能力	可对异常流量相关 IP 地址进行路由转发路径的追溯并可直接定位到交换机物理端口，便于管理员进行快速的人工干预
异常流量自动响应	可在正确检测异常流量发生的前提下，自动作出响应抑制动作，包括黑洞路由、ACL 过滤、可疑流量牵引、QoS 区别化质量保证等措施
联动响应兼容性	可通过 CLI、BGP、NAP 等方式支持主流路由器、交换机、防火墙、NTPG 流量净化网关、IPS 等设备联动
深度协议分析	通过流量模型匹配、特征检测、协议分析等多种检测方法的结合，深度分析原始数据包，从而检测出网络中的各种攻击行为并提供完备的统计分析报表。
支持协议类别	支持多种常见应用，识别为分析其所用协议，如： - Ö 传统协议，HTTP，FTP，POP3 等 - Ö 流媒体协议，RTSP，Web 视频等 - Ö P2P 协议，eMule，迅雷，Bittorrent 等 - Ö IM 协议，MSN，QQ，IRC 等 - Ö 网络电话，H.323，SIP，H.248 等 - Ö 网络电视，PPLive，迅雷看看等 - Ö 网络游戏，WOW，QQGame 等 - Ö 股票交易，招商证券，同花顺等 - Ö 数据库，MSSQL，MySQL 等 - Ö 加密协议，SSH，GRE 等 - Ö 其他，RRS 阅读，IP fragment 等

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 地理定位、归属查询、主机端口服务探测及漏洞评估、系统状态监控、链路帧逐比特解码等辅助功能
安全增值业务接口	面向运营商增值业务提供专用访问接口，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、策略配置等权限
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
	提供网络连接、应用审计、网络管理、安全日志等分类，记录网路访问详细信息，为事后追踪提供数据基础
	可按照日志类型、时间等条件进行数据备份、删除和导入导出操作
	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、年报等报表并按照报表内容自动发送给对口负责人
	可按照时间周期和基于流量、数据包、IP、设备、接口等排序条件进行报表生成
	可针对用户（组）、IP 地址、流向、时间段、具体应用名称等条件统计并生成协议分析报表。

升级管理	针对新出现的应用协议的分析方法，提供增量式的升级手段，保证产品具备针对最新应用的协议分析能力。
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详细的授权控制
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

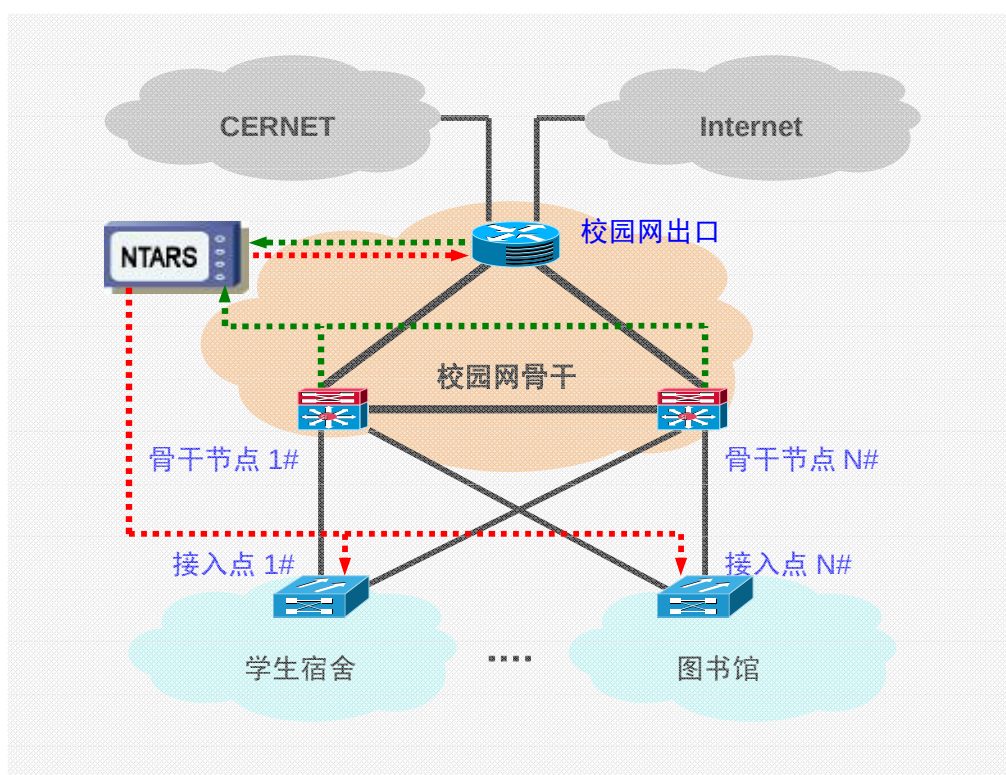
六、典型应用场景

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。

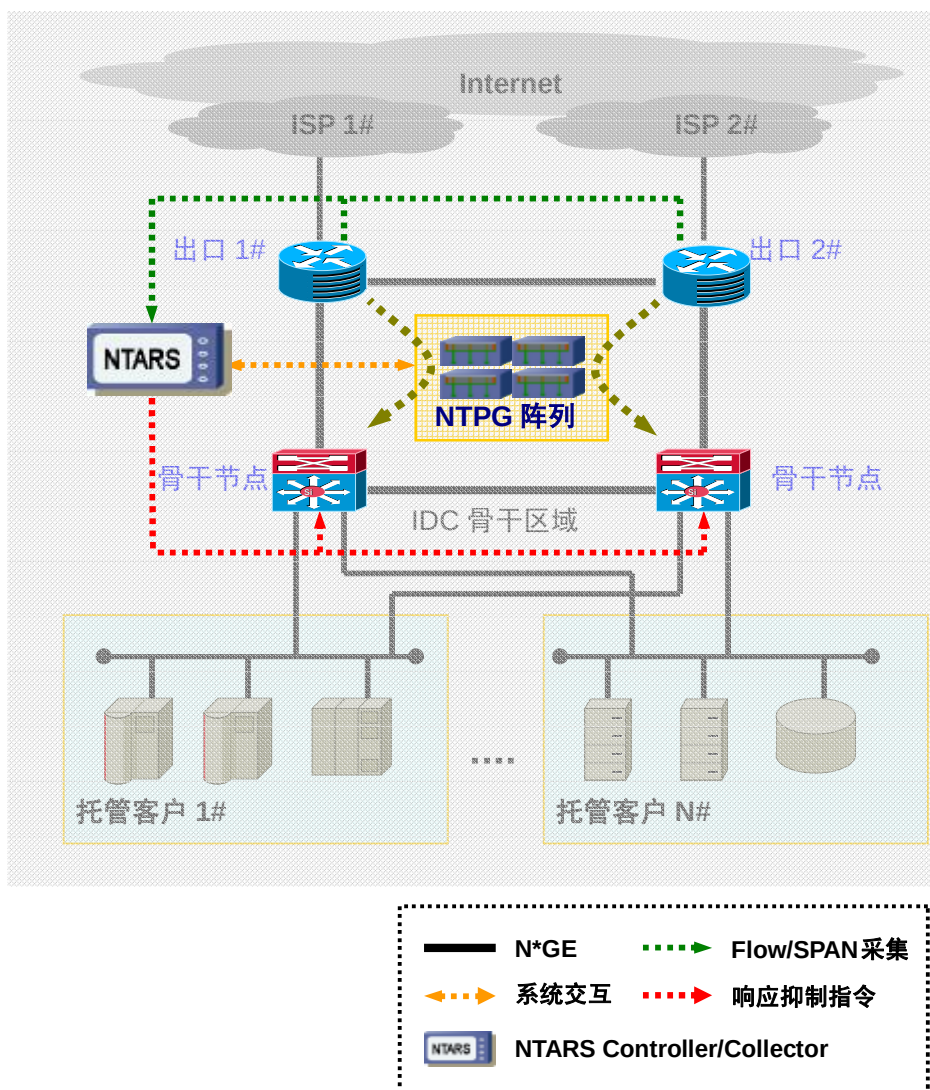
6.2 园区网络骨干区域



✚ 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、应用层深度检测。
- ✦ 方案简述：采用单机模式，监控多个采集点的流量图式分布，并根据总出口链路资源占用情况动态调整各接入区域的带宽分配，并能够通过 **ICA** 机制驱动骨干交换机 **SPAN** 而完成针对可以流量的应用层深度检测分析。

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。

七、产品型号及标称参数

7.1 NTARS 12800

表格 1 NTARS 12800 产品参数标称值

产品型号	NTARS 12800-Bundle
产品形态	ATCA 软硬一体化设计，14 插槽
构成单元	2*Controller(Redundancy) + 5*Collector
管理界面	B/S、SSH
端口配置	5*10/100/1000Base_Tx Flow 采集端口 5*10/100/1000Base_Tx 应用层深度检测端口 2*10/100/1000Base_Tx 管理端口
系统扩展能力	7*NTARS 12800-CLCT 插板(可提供 840,000 records/s 的性能↑) 安全存储增强模块(数据容灾、容量扩展)
可选接口板卡	千兆以太电/多模/单模接口板卡
存储	内置 5*300G，外置磁盘阵列
内存	7*4G
Flow 分析	600,000 Records/s
Flow 转发	5,000,000 Records/s
深度检测能力	100%线速
最大并发会话	10,000,000
功能特征	流量流向分析模块 应用层深度检测模块

	SNMP 网元监控模块
	ICA 复合机制单元
	合同用户自助模块
	NTPG/IPS/FW 外挂协同模块
	Collector 扩展模块
机箱规格	12U, 19"机架式
供电模块	1 + 1 冗余, 直流 48V, 2800W(Max.)
重量	35Kg
线缆配件	1*串口线 2*电源线 1*直连网线 1*交叉网线

7.2 NTARS 8800

表格 2 NTARS 8800 产品参数标称值

产品型号	NTARS 8800-Bundle
产品形态	ATCA 软硬一体化设计, 6 插槽
构成单元	1*Controller + 2*Collector
管理界面	B/S、SSH
端口配置	2*10/100/1000Base_Tx Flow 采集端口 2*10/100/1000Base_Tx 应用层深度检测端口 2*10/100/1000Base_Tx 管理端口
系统扩展能力	3*NTARS 8800-CLCT 插板(可提供 300,000 records/s 的性能↑) 安全存储增强模块(数据容灾、容量扩展)
可选接口板卡	千兆以太网/多模/单模接口板卡
存储	3*300G
内存	3*4G
Flow 分析	200,000 Records/s
Flow 转发	2,000,000 Records/s
深度检测能力	100%线速
最大并发会话	4,000,000
功能特征	流量流向分析模块

	应用层深度检测模块
	SNMP 网元监控模块
	ICA 复合机制单元
	合同用户自助模块
	NTPG/IPS/FW 外挂协同模块
	Collector 扩展模块
机箱规格	5U, 19"机架式
供电模块	1 + 1 冗余, 直流 48V, 1200W(Max.)
重量	22Kg
线缆配件	1*串口线 2*电源线 1*直连网线 1*交叉网线

7.3 NTARS 6800

表格 3 NTARS 6800 产品参数标称值

产品型号	NTARS 6800
产品形态	软硬一体化设计
构成单元	Controller + Collector
管理界面	B/S、SSH
端口配置	1*10/100/1000Base_Tx Flow 采集/管理端口 1*10/100/1000Base_Tx 应用层深度检测端口
系统扩展能力	1*GE 合同用户访问端口 1*GE 系统管理专用接口 1*GE 应用层深度检测接收端口 安全存储增强模块(数据容灾、容量扩展)
可选接口板卡	千兆以太多模/单模接口板卡
Flow 分析	100,000 Records/s
Flow 转发	1,000,000 Records/s
深度检测能力	GE 端口 100%线速
最大并发会话	2,000,000

功能特征	流量流向分析模块
	应用层深度检测模块
	SNMP 网元监控模块
	ICA 复合机制单元
	合同用户自助模块
	NTPG/IPS/FW 外挂协同模块
	Collector 扩展模块
机箱规格	2U, 19"机架式
供电模块	1 + 1 冗余, ~220V/50Hz, 400W(Max.)
环境温度	10~50℃
相对湿度	5~95%, 非冷凝
重量	22 Kg
线缆配件	1*串口线 2*电源线 2*直连网线 1*交叉网线

7.4 NTARS 6500

表格 4 NTARS 6500 产品参数标称值

产品型号	NTARS 6500
产品形态	软硬一体化设计
构成单元	Controller + Collector
管理界面	B/S、SSH
端口配置	1*10/100/1000Base_Tx Flow 采集/管理端口 1*10/100/1000Base_Tx 应用层深度检测端口
系统扩展能力	1*GE 合同用户访问端口 1*GE 系统管理专用接口 1*GE 应用层深度检测接收端口 安全存储增强模块(数据容灾、容量扩展)
可选接口板卡	千兆以太多模/单模接口板卡

Flow 分析	60,000 Records/s
Flow 转发	1,000,000 Records/s
深度检测能力	100%线速
最大并发会话	1,500,000
功能特征	流量流向分析模块
	应用层深度检测模块
	SNMP 网元监控模块
	ICA 复合机制单元
	合同用户自助模块
	NTPG/IPS/FW 外挂协同模块
	Collector 扩展模块
机箱规格	2U, 19"机架式
供电模块	1 + 1 冗余, ~220V/50Hz, 400W(Max.)
环境温度	10~50℃
相对湿度	5~95%, 非冷凝
重量	17.5 Kg
线缆配件	1*串口线 2*电源线 2*直连网线 1*交叉网线

7.5 NTARS 6000

表格 5 NTARS 6000 产品参数标称值

产品型号	NTARS 6000
产品形态	软硬一体化设计
构成单元	Controller + Collector
管理界面	B/S、SSH
端口配置	1*10/100/1000Base_Tx Flow 采集/管理端口 1*10/100/1000Base_Tx 应用层深度检测端口
系统扩展能力	1*GE 系统管理专用接口

可选接口板卡	千兆以太网模/单模接口板卡
Flow 分析	30,000 Records/s
Flow 转发	1,000,000 Records/s
深度检测能力	100%线速
最大并发会话	1,000,000
功能特征	流量流向分析模块
	应用层深度检测模块
	SNMP 网元监控模块
	ICA 复合机制单元
	合同用户自助模块
	NTPG/IPS/FW 外挂协同模块
	Collector 扩展模块
机箱规格	1U, 19"机架式
供电模块	单电源, ~220V/50Hz, 300W(Max.)
环境温度	10~50℃
相对湿度	5~95%, 非冷凝
重量	10 Kg
线缆配件	1*串口线
	1*电源线
	2*直连网线
	1*交叉网线