徽标

描述已自动生成

**多源数据汇聚分流**

**与安全审计分析**

**技术方案**

**北京派网科技有限公司**

**2022年3月9日**

##### 文档约定

###### 版权声明

文中关于**多源数据汇聚分流与安全审计分析技术方案**的资料、说明等相关内容归北京派网软件有限公司所有。

本文中的任何部分未经北京派网软件有限公司（以下简称“派网”）许可，不得转印、影印或复印、发行。

###### 版本修订

派网保留不预先通知客户而修改本文档所含内容的权利。

###### 责任限定

派网对于您的使用或不能使用本产品而发生的任何损害不负任何赔偿责任，包括但不限于直接的、间接的、附加的个人损害或商业损失或任何其它损失。

###### 意见反馈

我们非常欢迎和珍惜您的意见和建议，请通过下列方式反馈您对产品及文档的意见和建议。

* 通过电子邮件反馈，请发送至support@panabit.com。
* 通过http://forum.panabit.com/forum.php网站在线反馈。
* 通过客户服务电话4008981066热线电话反馈。

##### 修订记录

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **编号** | **版本** | **修订日期** | **修订人** | **备注** |
| 1 | V1.0 | 2022-04-01 | 马海业 | 创建文档 |

**目录**

[一、 项目背景 1](#_Toc22742)

[1.1 用户背景 1](#_Toc23291)

[1.2 项目背景 1](#_Toc31193)

[二、 需求分析 2](#_Toc9866)

[2.1 问题描述 2](#_Toc22792)

[2.2 实现目的 2](#_Toc23181)

[三、 解决方案 3](#_Toc757)

[3.1 派网具体解决方案 3](#_Toc23300)

[3.2.1 精细化流量镜像 3](#_Toc5746)

[3.2.2 网络性能分析（NPM） 4](#_Toc13064)

[四、 方案设计 7](#_Toc25493)

[五、 方案优势 8](#_Toc9774)

[5.1 全网流量可视化管理 8](#_Toc27668)

[5.2 业务网大数据生成 8](#_Toc4610)

[5.3 NPM动态监控大屏 9](#_Toc5963)

[5.4 一键断网（快速关停） 9](#_Toc18532)

# 项目背景

## 用户背景

GDCERT

## 项目背景

网络安全态势感知平台建设。

# 需求分析

## 问题描述

为满足XXXX态势感知平台项目的建设的多源数据汇聚与多安全分析引擎数据采集需求，现阶段都以多源汇聚交换机提供镜像接口给予安全分析引擎为主，其中存在问题有：

1. 物理接口上，一般汇聚交换机接口有限，无法满足多路多组的流量镜像需求；
2. 同时镜像多路多组流量出去对于一般交换机的性能存在压力，所有需要旁路部署获取流量的设备，策略改动均需要在核心交换机上面做变更，对于汇聚交换机的运维存在难度以及未知风险。
3. 一般汇聚交换机无法实现按需过滤流量，仅支持简单的接口镜像，且镜像资源有限，在原始流量较大但安全分析引擎性能不足的时候，根据所需协议类型进行定制化镜像分析，既可以减小分析引擎压力，仅分析关键协议流量，也充分提现分析引擎能力。
4. 缺少全流量会话审计系统；
5. 缺少关键业务流量报文留存能力。

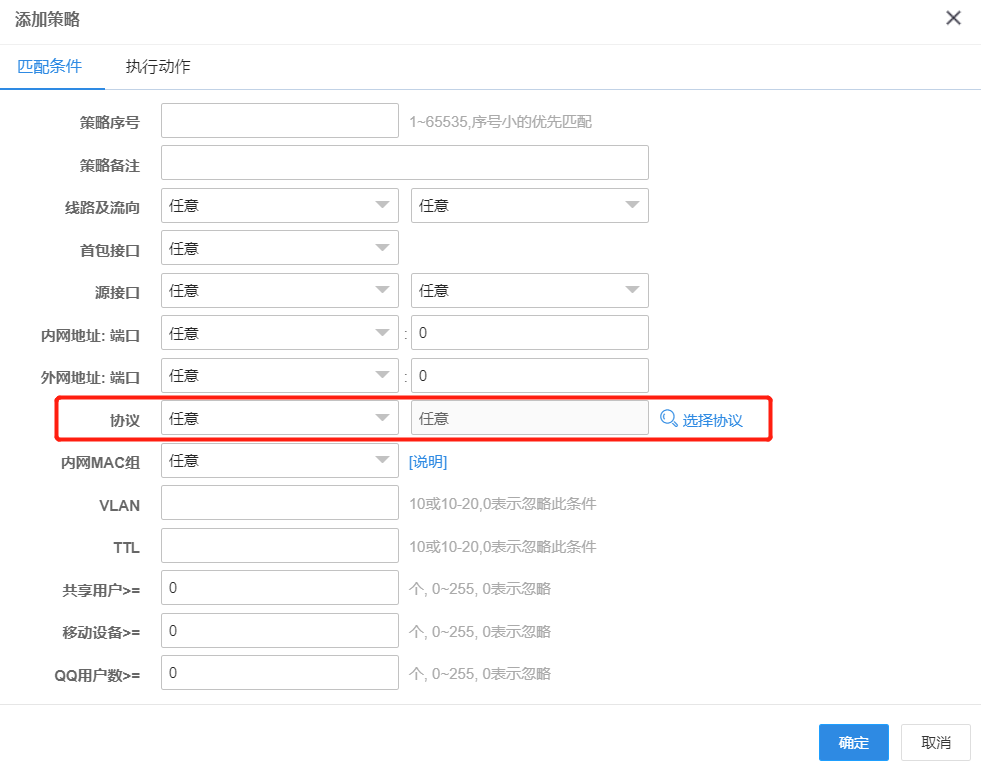
## 实现目的

根据上述多源流量采集与镜像的需求，在多源数据汇聚交换机上，旁路部署精细化汇聚分流设备，可基于应用协议与类型进行精细化镜像，且该设备作为安全分析引擎之一，提供全会话采集送到对应日志审计的能力；再部署增强型TAP镜像分流器，提供基于IP与协议类型等条件的多源多组流量镜像的功能做镜像能力升级；同时部署全流量审计日志与全流量报文设计系统，对采集的原始流量进行全会话审计与指定报文的留存。

# 解决方案

### 精细化汇聚分流

依托于强大的七层应用识别能力与对应用的管控能力，Panabit在汇聚分流的解决方案上，不仅仅是基于端口到端口的简单流量复制，更能基于IP、端口甚至应用协议、协议类型等条件进行精细化的汇聚分流，将指定协议流量镜像给对应的安全分析设备，既提高了安全设备的分析效率，还减少了大量无意义流量的分析，大大减少了安全分析设备的性能要求。在大带宽的分析场景，既满足等保要求的安全能力建设要求，还能更好的提高运维工作的效率。



### 上网行为分析/审计

**满足“151号令”和《网络安全法》需求一会话日志**

政企网内部人员非常多，用户上网访问的内容也难免会有一-些不符合国家相关规定或者涉及到“黄、赌、毒”内容。作为政务网网络总出口，必须留存相关人员上网记录，以便发生网络安全事件后进行追查。例如：某人上网攻击了政府的某个部门的网站，需要通过政务网出口NAT日志来定位到攻击来源自那个学校的那台计算机，再根据当时的时间，定位到人。Panabit提供全网统一用户认证日志+NAT日志+URL日志，同时提供1:1的日志输出,在一张表里面可以体现访问时间、源地址、目标地址、NAT地址、账号信息、域名、协议类型、7层协议名称、流量等元素完整保留网络中的相关信息。当发生相关网关安全事件时候， 通过NAT日志、帐号的登录信息以及URL访问等记录信息，可以对外到具体上网用户满足《网络安全法》和“151号令”相关要求。

**满足“151号令”和《网络安全法》需求一虚拟身份日志**

微信、QQ等聊天工具的发展,增加了人们的沟通方式。但如果某人通过QQ群,微信群发表不良言论(尤其是涉及到发动、危害民族团结言论)网监有可能要求政务网出口通过QQ号码或者微信ID来对应于上网人员。Panabit还提供这个功能通过QQ号码微信ID、邮箱地址或者论坛用户名查询到到底这些虚拟身份对应是谁。

**对外访问TOP域名分析**

域名日志的访问频率和吞吐的变化,经常会伴随着网络上一些关键事件的发生。观察域名排名变化，是追踪分析这些事件的有效手段。例如一个不熟悉的域名，突然访问量急剧上升，一般都伴随着病毒或者网站挂马的发生。一些互联网营销手段也会推动域名的急剧变化，比如360推送微软升级，会引起微软升级服务器访问频率急剧上升。同时观察某个域名的流量上下行比例，也可推测它提供的服务是否存在问题。

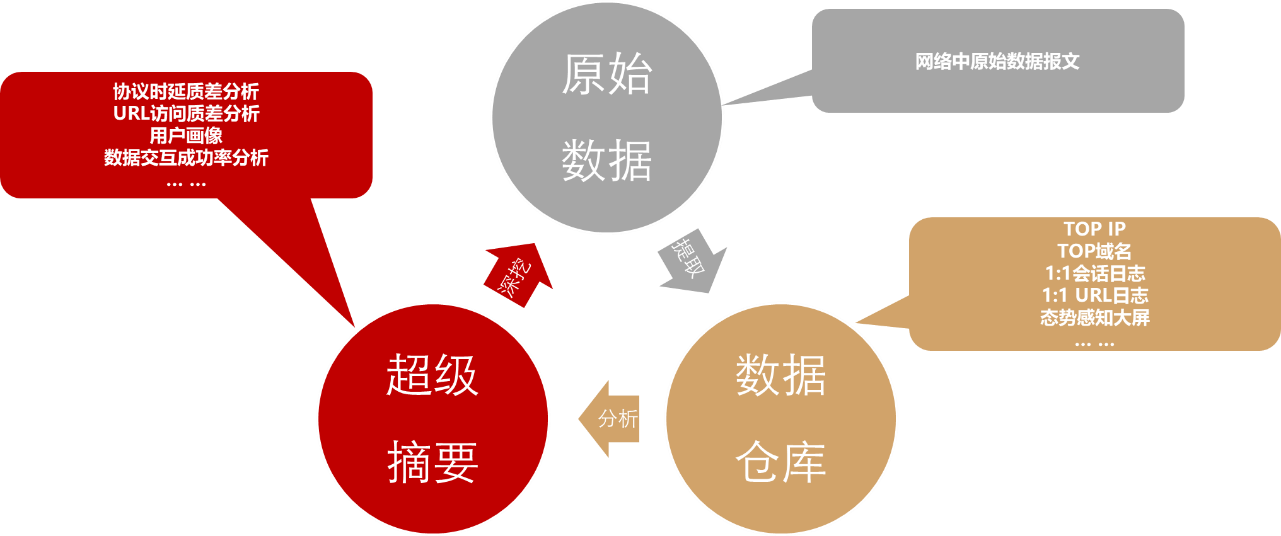
### 全流量报文分析

Panabit NTM（Network Trace&Monitor）是一种全新的，基于超级摘要的全流量分析产品。专门为运营商、教育、政府、集团企业等客户提供高性能、高可用性、功能丰富的全流量分析解决方案。能够满足用户对网络故障定位、网络未知威胁发现、原始数据包溯源等全方位需求，赋予用户最细粒度的可视能力。

通过上面的分析，我们可以看到，在多数场景中，仅针对部分流量进行分析和存储是远远不够的，真正的全流量分析不仅限于关注某些安全分析关心的流量，而是全部的流量，并将原始数据包保存下来。NTM正是这样一款存储全部数据包的全流量分析产品。

当然，在做到全流量的采集和储存之后，面对可能出现的大量无分析价值的数据，NTM还具备快速定位异常的能力，也就是全流量分析的重点——超级摘要。

超级摘要是对全部原始数据包的提炼与分析结果展示，包含例如域名差量，异常诊断，性能异常分析，异常会话提取等运维及安全人员关注的关键信息。超级摘要与原始数据包的关系如下：

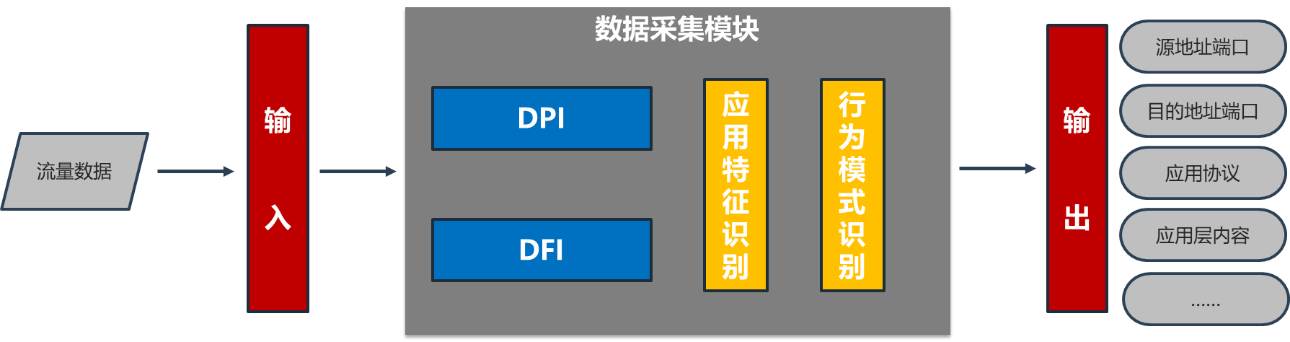


NTM首先实现的是对原始数据的储存。其后，在原始数据包的基础之上提取关键字段，生成数据仓库，其中包含1:1会话日志、URL日志，TOP IP及域名等信息。最后，NTM进一步对生成的数据仓库进行分析，将分析结果进行展示，形成超级摘要。

作为一款基于超级摘要的全流量分析产品，NTM能够集中推送与展示需要关注的信息，大大提高运维人员的工作效率。首先，通过超级摘要，运维人员能够快速定位网络中存在的异常；另一方面，运维人员可以根据超级摘要的提示，有目的地深挖相应的原始数据，实现进一步的深入分析。

**数据采集模块**

基于精准的应用识别能力，数据采集模块实现流量的采集与识别分类。在应用识别中使用了DPI引擎，将传统DPI技术中的基于“特征字”的识别技术、应用层网关识别技术、行为模式识别技术有机的整合起来，有效的灵活的识别网络上的各类应用。



数据采集模块目前支持1400多种协议和应用的自动识别，从而为用户提供全面的、有效的、灵活的大数据处理基石。

**数据管理模块**

数据管理模块实现原始数据包，以及流量日志数据的存储与管理。Panabit的全流量探针NTM产品具备一套完整的智能文件管理系统，以达到稳定快速的数据包存盘，以及数据包快速检索的目的。该系统具备以下三种特性：

1）时序存储：对采集的数据进行时序存储，并采用固定块大小，固定文件个数，轮循覆盖最老文件，减少硬盘存储碎片。

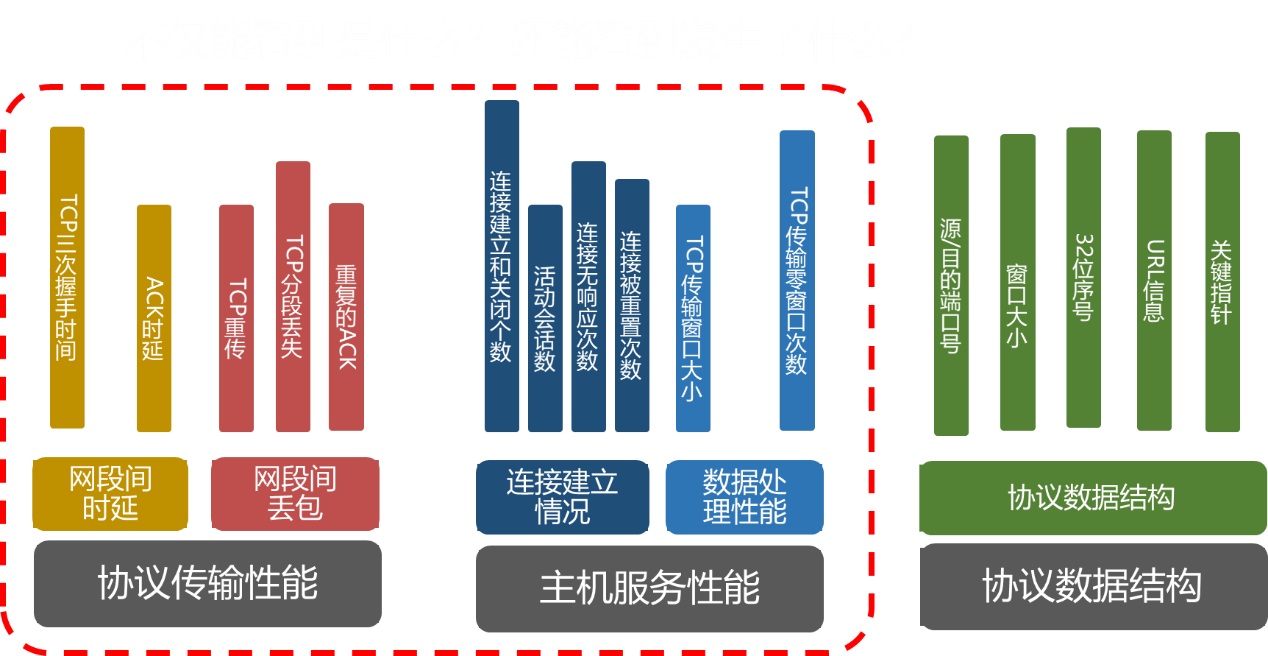
2）数据压缩：通过内存进行原始数据压缩，减少硬盘存储文件的数量，以达到存储性能提升的目的。并且由于内存擅长文件的压缩，使用内存进行数据压缩并不会消耗太多性能。

3）分级存储：智能文件管理系统支持元数据与原始数据包的分级存储，元数据存在SSD中，原始数据包存在机械硬盘中。以此保证索引信息的快速查询，又不会因为原始数据包过多，造成用户硬盘存储成本的增加。

**数据分析模块**

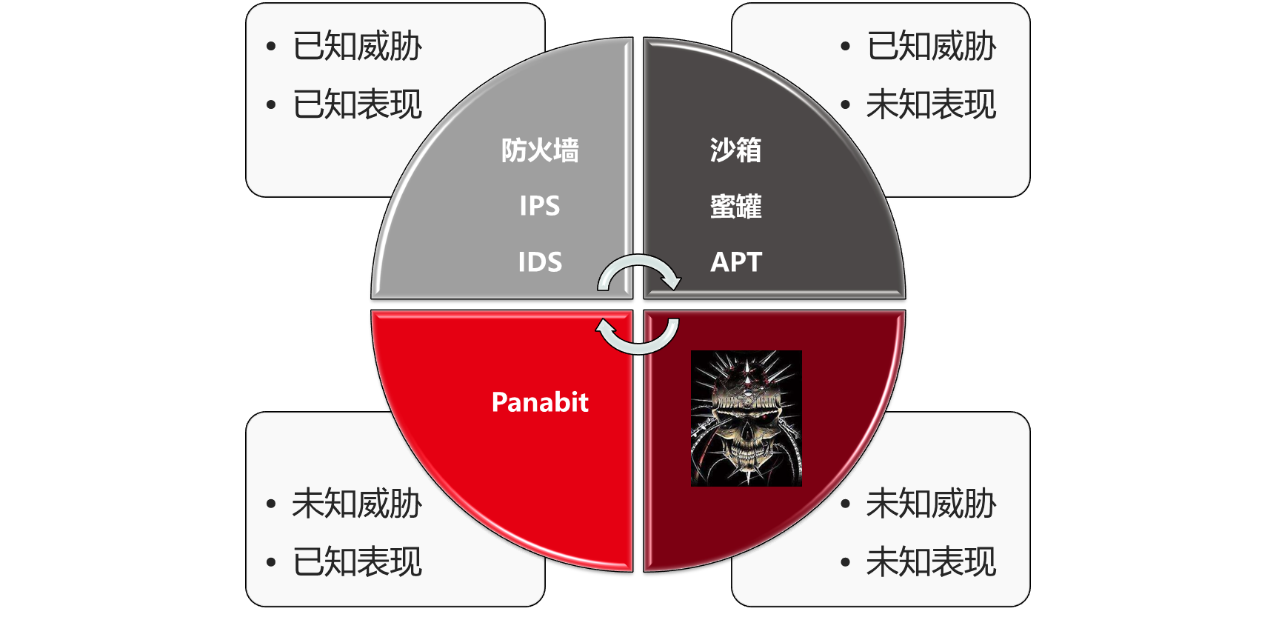
数据分析模块实现对原始数据包，以及流量日志数据的分析工作。除了浏览查询等基本操作，NTM还提供了针对网络数据的性能分析与安全分析。

1）性能分析：对比传统的网络性能检测系统，数据分析模块能够提供业务级别的性能感知，看得更深、更广。



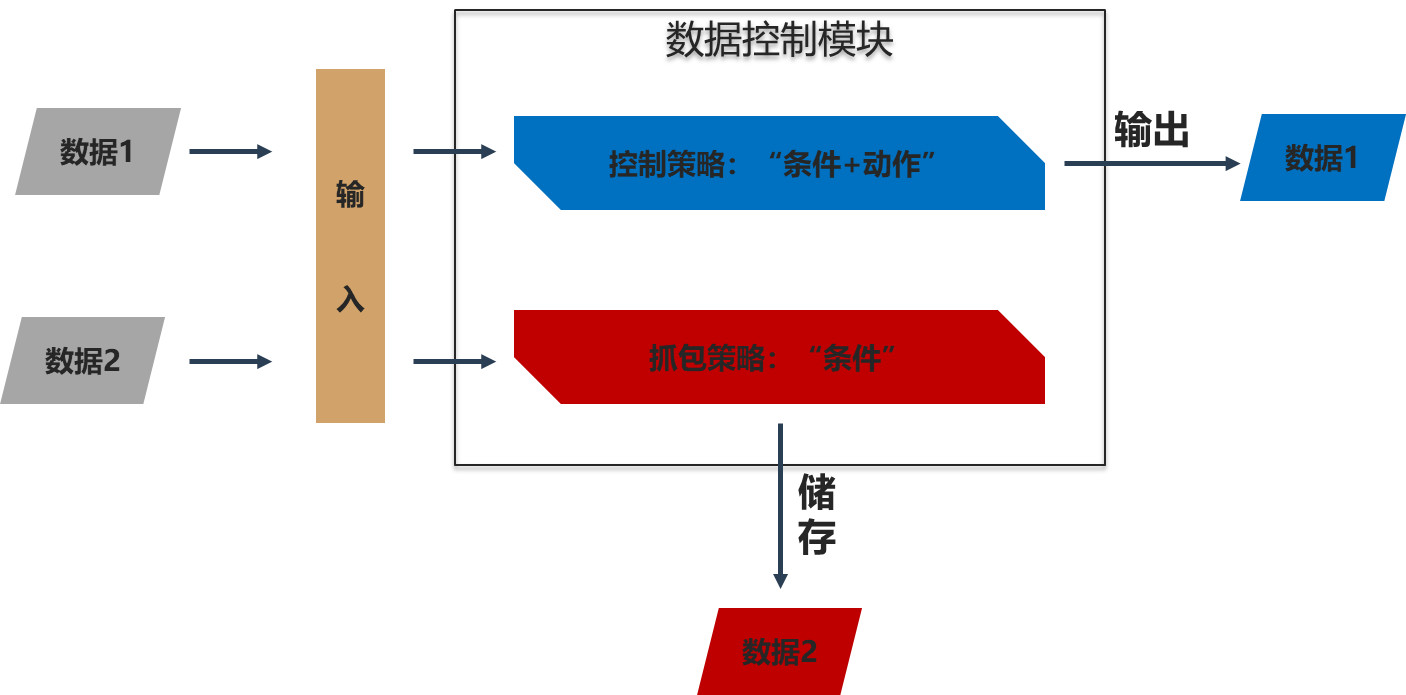
除了可以识别出应用协议数据结构，NTM还能看到应用协议的交互流程，以及业务的传输服务性能。既可以实现业务性能指标的实时查看，在出了问题后，也可以按需追溯，找到问题所在。

2）安全分析：对于传统的安全设备而言，由于其所秉承的“黑名单”理念，它们更关注于已知威胁的表现。但是，全流量分析中相当重要的一部分是对未知威胁的探索，因为无论是操作系统、应用软件或是网络设备均普遍有可能存在未知的漏洞。NTM能够根据威胁情报系统检测已知威胁，并通过对异常网络行为的分析，发现未知威胁。



**数据控制模块**

数据控制模块实现针对流量的控制，以及数据包的按需采集。数据控制模块的逻辑如下图所示。

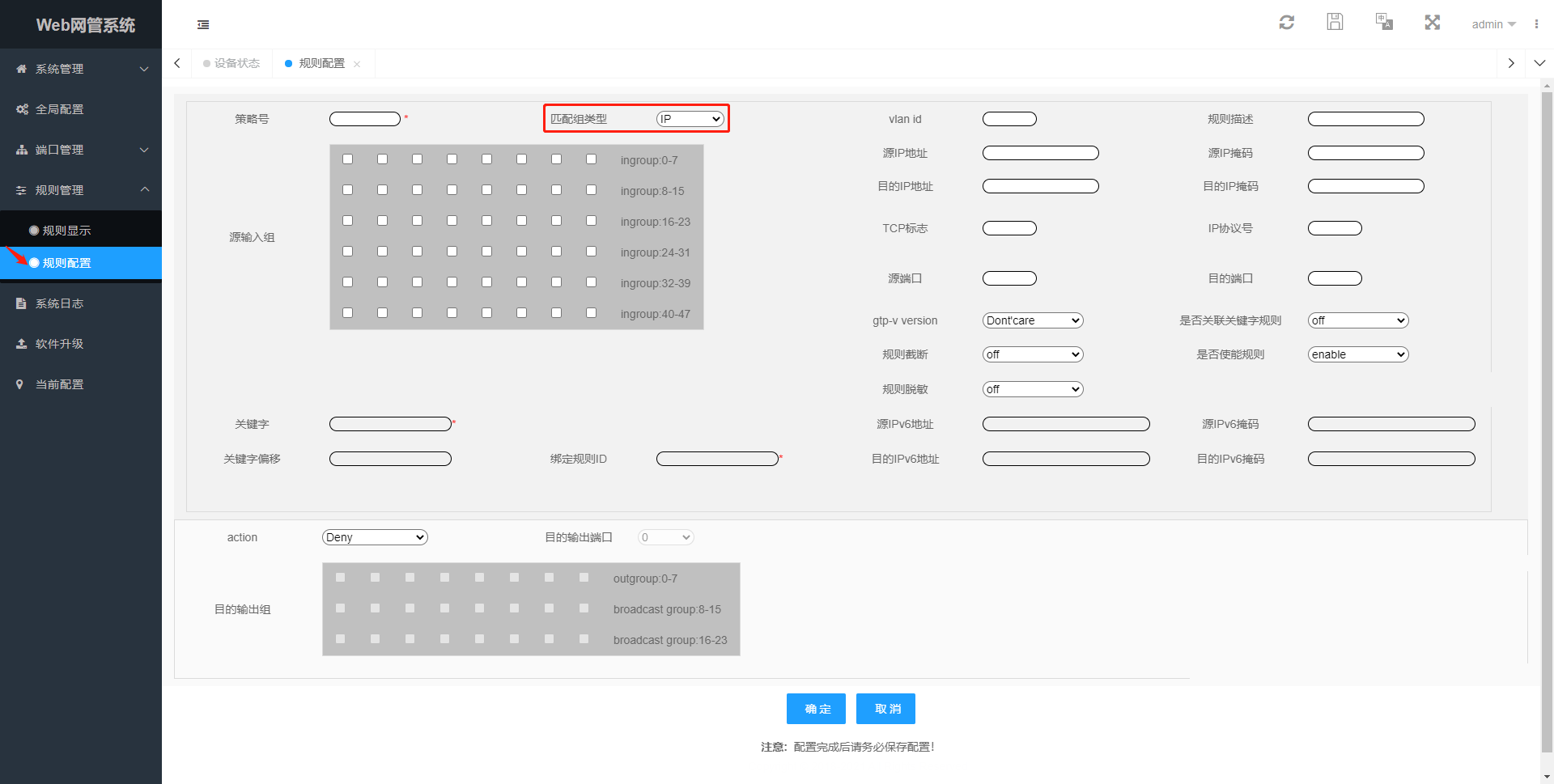


数据控制模块分为流量控制与抓包控制两个子模块。与其他全流量分析设备不同，NTM支持串接部署，并在串接的基础之上对流量进行管控。NTM在串接部署时，数据从内网接口进外网接口出，或者从外网接口进内网接口出，在这个过程中，NTM默认不会对数据做任何干预。如果要对数据进行干预，则可以配置控制策略来实现，解决了分析设备缺乏反制干预能力的问题。

此外，在对流量精确识别的基础上，NTM的数据采集模块可以做到数据包的按需采集。例如基于应用协议抓包（只抓HTTP的数据包）；或者基于策略抓包（对于HTTPS的应用，只抓前100个包，其他应用则全部抓）等。这样可以合理采集所需的流量，有针对性地进行储存分析，更加有效的利用磁盘空间。

### 高性能流量镜像

PA\_TAP支持基于源接口、源/目的地址端口等条件进行流量镜像，过滤安全分析引擎不需要的流量，仅对引擎需要的流量进行镜像。有效减少汇聚交换机的镜像压力，大幅度降低网络拓扑的单点故障隐患。通过，经过有效流量筛选分流，对于安全设备WAF，DLP，IPS等按需分配流量，对于安全设备的性能压力能够大幅度下降。

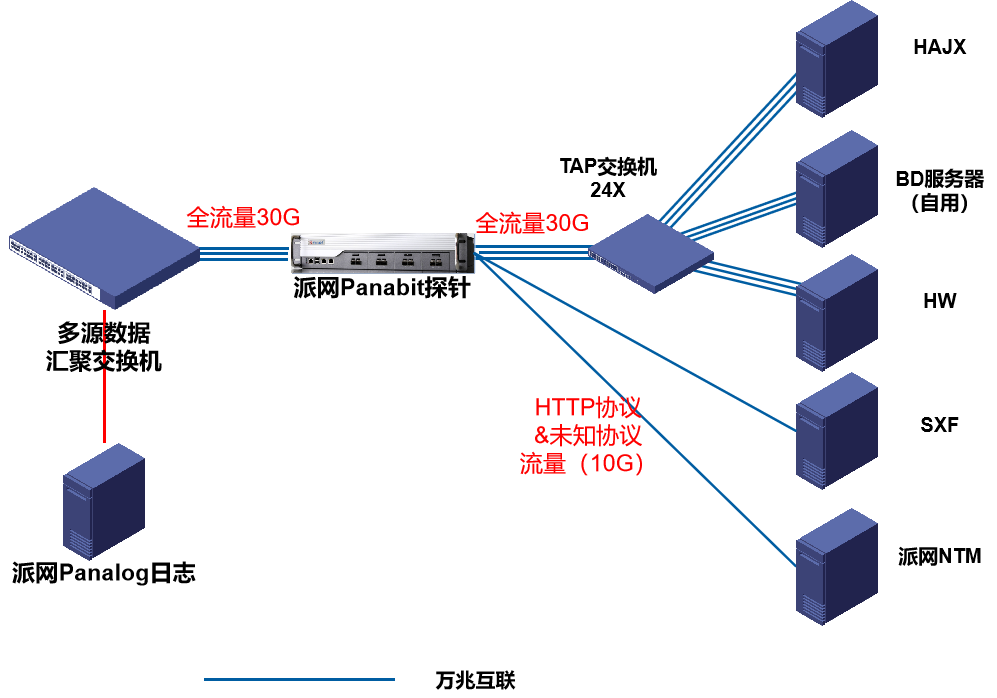


# 方案设计

为满足上述需求，且本次流量镜像速率达30Gbps，具体部署方案如下：

1. 新增一台Panabit探针旁路部署在多源汇聚交换机上，由汇聚交换机将多源数据从3个万兆光纤路镜像到Panabit探针上，在Panabit上实现流量清洗过滤后镜像给TAP交换机，同时将本机日志通过IP+端口方式将SYSLOG留存到Panabit日志系统上；
2. 新增一台PATAP交换机旁路部署在Panabit探针上，通过3个口Panabit探针镜像过来的流量，基于本TAP交换机的多口多组端口流量复制能力，将接收口的流量按需复制到指定的物理接口上，镜像给对应的态势感知引擎设备，如需全量复制，则所有引擎均通过3根万兆光纤路接收TAP交换机镜像的流量。
3. 新增一台Panabit日志系统旁路部署于数据中心服务器上（支持虚拟化），对接Panabit探针设备的流量做日志分析与留存。对派网探针提供的数据进行整理分析，最后将分析的结果分级呈现。最终实现对网络进行监控管理、网络态势感知，完成网络虚拟身份信息、故障快速排查，网络管理审查工作迈向高效、智能、可监管、可审计的新阶段。

方案部署的拓扑示意图如下：



# 方案优势

## 全网流量可视化管理

实现流量异常随时发现，便于随时管控。通过长期记录多个协议的TOP排行情况，可以实时发现网络出现的异常和突发情况。当遇到异常和突发情况时，来追溯网络中真实发生的情况，对网络可能出现的危险进行预判和告警，从而防患于未然。

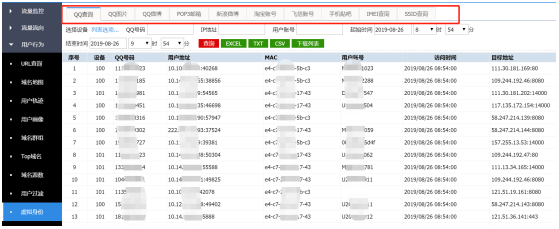
## 业务网大数据生成

**精确识别应用**

派网Panabit通过14年的积累，应用识别能力方面无人出其右。通过对DPI、DFI、节点跟踪、主动探测等方面的技术积累和研究，可精确识别网络中的14大类数千种应用协议，识别率在95%以上。也许Panabit应用识别只比别人强5%，但影响用户体验的往往就是那5%，占用带宽的往往就是那5%，出现安全问题也往往就是那5%。

**全量1:1的日志留存**

Panabit具备日志输出功能，配套提供专用的Panalog大数据日志集群系统，可提供IP日志、应用日志、帐号日志、事件日志；其中事件日志主要包含：URL访问日志、QQ登陆登出日志、POP3登陆日志、DNS查询事件、微博帐号日志、淘宝、飞信等日志。例如URL日志，它的访问频率和吞吐的变化，协助判断、分析企业网的一些关键事件的发生。



全量1:1行为日志留存，记录每时每刻每个IP的每个会话信息，提供日志审计查询、分析和回溯。充分满足《网络安全法》和公安部“151号令”的要求，确保企业网的日志信息安全。

## 超高处理性能

不同于大多数厂商使用改装过的Linux/FreeBSD等通用操作系统，Panabit使用自研的数据面操作系统PanaOS，采用虚拟化技术完成了数据面和控制面分离，从驱动、内存管理到任务调度等数据面核心任务都由PanaOS一肩承担。利用虚拟化OS技术，PanaOS赋予了系统永不宕机超高稳定性。路由、NAT、负载均衡、应用识别与控制等关键基础设施内置PanaOS之中，为用户提供一体化解决方案提供了坚实基础。

Panabit智能应用网关的高性能及高稳定性早已获得业内公认，特别是在移动、铁通、广电等多个城域网100G节点案例中用实际表现赢得用户的一致好评。 在用户群体，Panabit以技术指标100%线上可达、功能默认全开而不会导致网络延迟卡慢、配置使用灵活、设备升级扩容便捷而著称。