HighGuard SPA

海加网络流量分析系统

技术白皮书

上海海加网络科技有限公司

2013 年 6 月

目　录

1 技术背景

随着网络的应用越来越广泛，其承载的业务越来越丰富，了解网络承载的业务，掌握网络流量特征，以便使网络带宽配置最优化，是当前网络面临的一大挑战；另一方面，网络蠕虫病毒、DoS/DDoS 攻击等在网络中越来越流行，对网络正常业务的负面危害也越来越大，因此检测威胁网络安全的异常行为是当前网络面临的另一大挑战。如何更好地对网络进行监控、维护，如何减少网络故障的发生，保证业务的正常开展，及时发现通信中断或访问速度降低，基于事实的容量规划、对网络资源有效的使用，是一个非常现实的问题。

海加网络流量分析系统（简称 SPA）能够接收 Netflow/sFlow/SNMP 格式的流量数据，并对接收到的流量数据进行统一的统计分析，实时显示并将分析结果进行存储。可对链路利用率、广播包、组播包、CRC 错误、指定应用的利用率、应用响应时间、应用的可用性等发出告警。能够对链路层和网络层的数据流量监控，具有 2-7 层流量分析能力，支持网络流量和性能可视化系统支持旁路和分布式部署，能够对多台设备统一管理，统一呈现各种报文。能够对关键业务系统、应用服务进行分析，支持监测应到可性、 延迟、执行正确性以及质量。能够实时监控路由器、交换机、防火墙、服务器等基础硬件设备。

2 产品架构

系统架构在逻辑上可分为网元层、监控层、处理层和管理层。

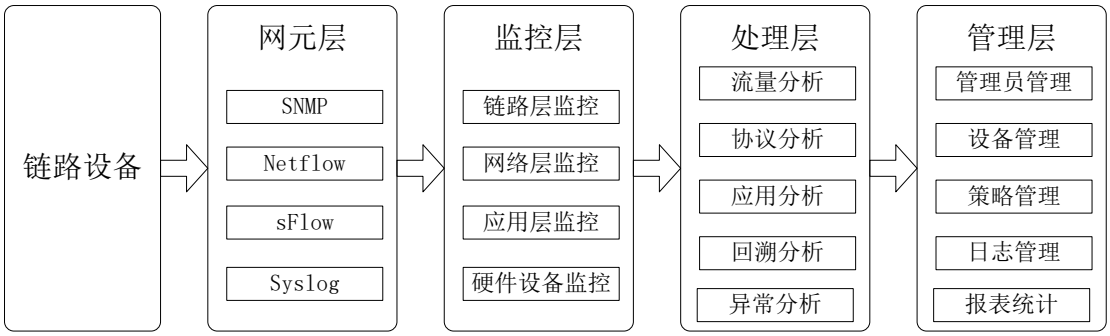

图 1 系统架构

网元层主要用来采集链路设备上的数据，支持采集 SNMP、Netflow、sFlow 和 syslog，将采集到的数据经过格式化处理后进行存储；

监控层主要对链路进行监控，可监控链路层和网络层的流量、应用层协议和链路上的硬件设备；

处理层主要对网元层采集到的数据进行统计分析，可以实现流量分析、协议分析、应用分析、回溯分析和异常分析；

管理层主要为管理员提供系统管理功能和分析统计功能，支持管理员管理、设备管理、策略管理、日志管理和各种报表输出。

系统在硬件上由采集器和分析器组成。采集器工作在网元层和监控层，分析器工作在处理层和管理层。

3 部署方式

3.1 局域网出口流量监控部署

对于大多数的局域网，都会连接到互联网中，通过对互联网出口流量的监控，不仅能分析各种应用占用出口带宽的情况，还能监视一些非工作需要的互联网访问，提高工作效率。

网络拓扑

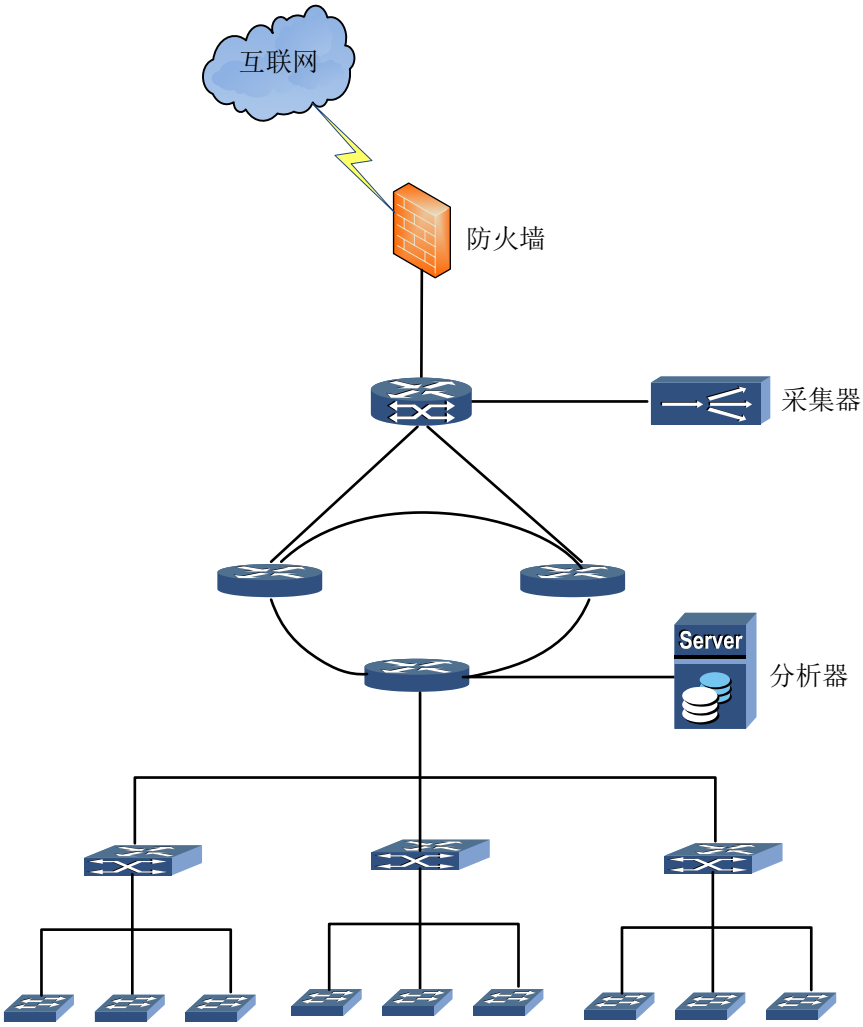

图 2 局域网出口流量监控网络拓扑

在互联网出口的路由器或交换机上部署采集器，并启动对连接互联网的流量

统计功能，并在网络中部署一套分析器，实现对互联网出口的应用的流量和个人IP 地址的流量进行分析和监视。

可实现的功能

◆ 网络流量异常监测

网络管理员通过系统提供的某段时间内的流量、应用趋势分析，可非常直观的看到网络流量是否有突然增长或突然下降的现象，并进一步分析出是哪些用户产生了最多的流量，使用了哪些应用以至于网络运转出现性能问题。并根据最终分析结果，网络管理员可快速的解决网络异常问题，保证网络正常的运行。

◆ 网络规划参考

利用日志以及系统长期监控网络带宽而形成的各类趋势报表，有助于网络管理员跟踪和预测网络链路流量的增长，从而能有效的规则网络升级（如增加路由服务、端口或使用更高带宽的接口）。

3.2 分布式流量监控部署

适用于有一个总部、多个区域网络的情况。通过租用运营商的线路相连，构建一个庞大的广域网结构。

网络拓扑

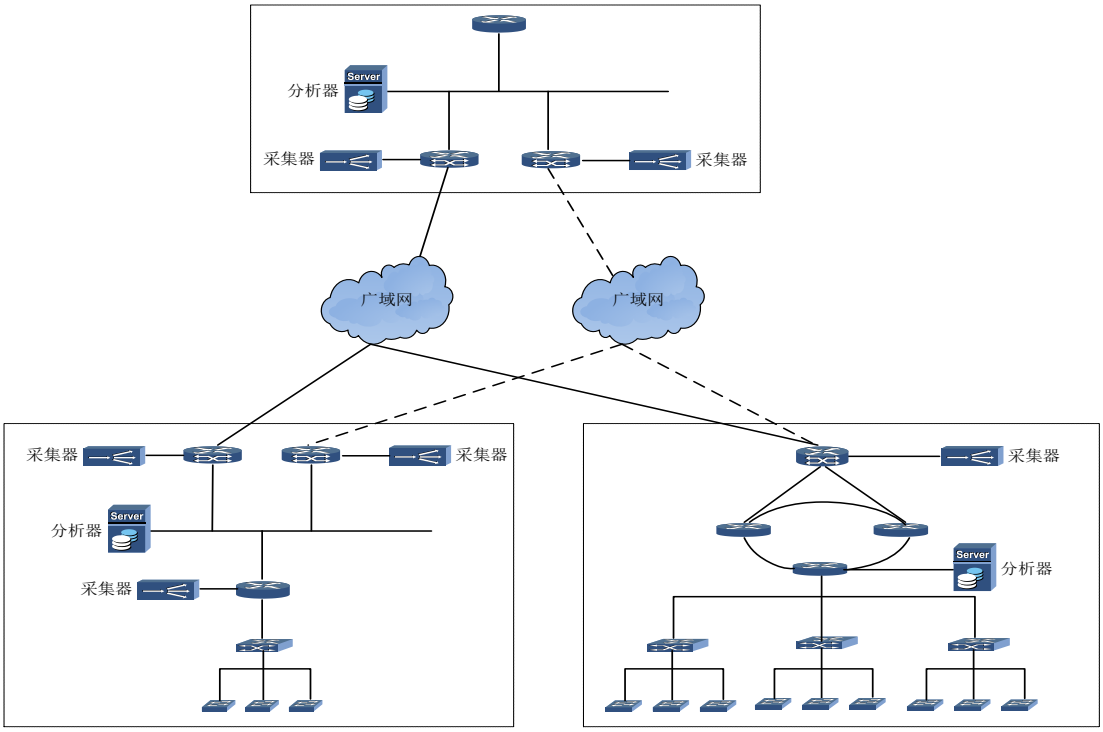

图 3 广域网分布式流量监控网络拓扑

各分支机构部署一套流量分析系统，实现分布式流量接收和分析处理。总部部署一套流量分析系统作为流量分析中心，实现统一的 Web 流量分析。通过多台服务器分布式安装建立区域化、层次化的流量分析系统，分散了大规模网络的流量分析压力。

可实现的功能

◆ 分布式流量检测

针对一个总部多个分支、跨广域网的大型网络，提供了分布式流量检测能力。通过在核心出口部署流量检测点，实现对企业各分支之间、分支到总部应用流量的统计分析；通过在各分支部署流量检测点实现各分支网络内部应用流量的监控。并以统一的 Web 界面展示全网总部和分支所有流量，实现层次化的分级流量监控解决方案。

◆ 广域网链路流量检测

对于一个企业来说，WAN 带宽通常是有限的，如果 WAN 链路上的流量增大，通常企业的做法就是进行投资以升级 WAN 链路。但如果企业能掌握 WAN 流量的特征，制定相应的策略（比如 QoS 和针对源或目的 IP 地址作流限制），就能使 WAN 带宽得到最合理最充分的使用，避免进行不必要的升级投资。

系统通过流量、应用、会话、节点等几大类预定义报表，提供准实时的流量监控和详尽流量分析结果，帮助网络管理员洞察 WAN 链路的流量特征、承载的应用、用户使用状况，从而针对是否应投资升级带宽快速的做出响应。

◆ 网络优化

通过系统可使网络管理员及时掌握网络负载状况，网内应用资源使用情况，尽早发现网络结构的不合理 ,或是网络性能瓶颈 ,尽快做出网络优化方面的决断，使网络带宽分配最优化，为用户提供高品质的网络服务，并且避免了网络带宽和服务器瓶颈问题。

4 技术优势

4.1 功能描述

系统功能模块可以分为网元层、监控层、处理层和管理层四个部分。

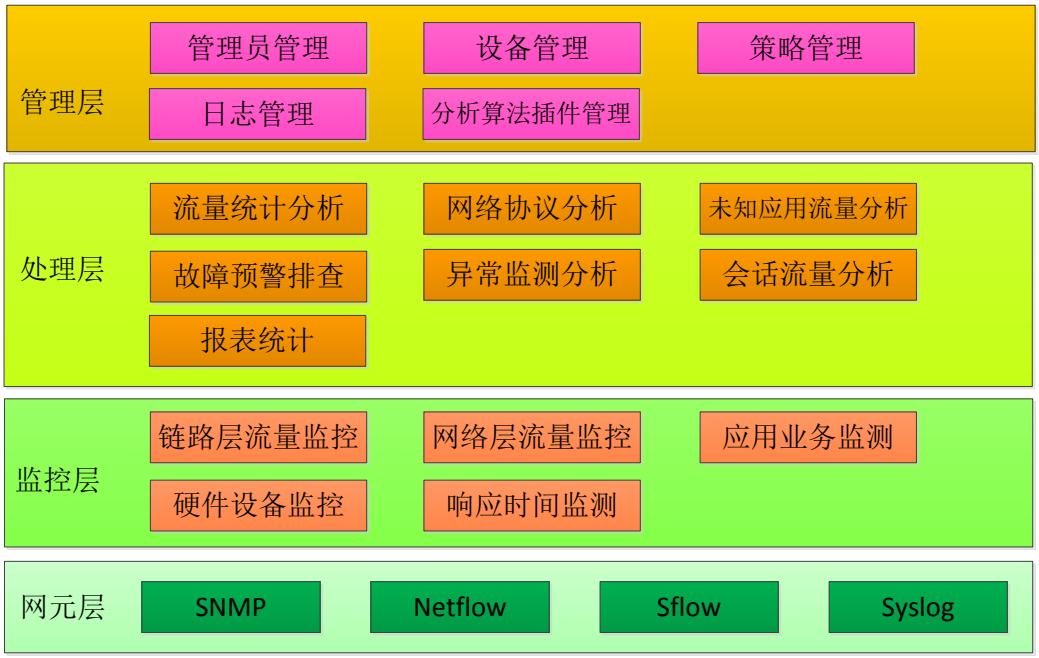

图 4 功能模块组成

4.2 功能模块

4.2.1 系统管理

系统配置

配置系统的参数，如操作员最大闲置时长、报表 TopN 取值、报表自动刷新间隔时长、网络日志保存时长、磁盘使用阈值等。采集器和分析器的端口配置。以及查询采集器和分析器的状态，如启动状态、内存的使用率、网络的使用率等。

系统支持多种分析算法，管理员可根据单位实际情况选择不同的分析算法插件，以实现最优化的方式对单位网络流量情况进行分析。

用户管理

支持用户的新增、修改、删除功能。用户可自行调整定义不同角色的权限，也可增加角色。不同的用户拥有不用的权限。最高级别的系统管理员可以为其他人员配置密码和权限。设置的权限包含系统的配置、统计和分析、告警、报表等。

不同的管理员或者用户登陆系统后，看到的可能是完全不同的菜单内容，可以对系统的操作权限也是不相同的，这样可以做到权责分明，也可以增加系统运行的安全性和信息的保密性，使得系统管理更加规范化。

日志管理

日志管理记录了系统的主要操作和事件。方便管理员进行系统的维护和故障的查询。日志管理员可以根据时间段、关键字等方式灵活的查询信息。

日志管理主要包括所有用户的操作、访问记录等各类信息，异常流量、数据流特征值等告警日志信息。

应用业务配置

系统可以自定义业务，比如可以将一个具体的业务的名称、地址、端口定义为一个对象。可以根据这个对象去查询该业务的流量，方便管理人员进行分析。也可以自定义 IP 组，比如将某个单位下面的所有的用户的 IP 定义成为一个 IP 组，可以根据这个 IP 组去查询该单位的流量并进行分析。

4.2.2 网络流量监控

链路层监控

系统通过管理人员预先配置好利用率阈值，对链路利用率情况进行监控。利用率阈值可分别设置最大值和最小值，如果利用率超过了最大值或者低于最小值，系统都会自动向管理人员发出告警，提醒查看链路流量信息。系统会自动记录当前告警信息，并通过对得到的链路层数据包大小、分类、吞吐量等进行分析，识别误码率，对误码进行分类。对当前流量情况进行统计，形成报表。

流量实时统计

系统能够实时显示当前网络流量，以直观的趋势图来展示当前网络流量的趋势。系统支持自定义间隔时间（比如 2s 或 5s）为单位来显示网络流量统计结果，可统计当前总流量、流出总流量、注入总流量、总数据包数、流出数据包数、注入数据包数、带宽总利用率、进网带宽利用率和出网带宽利用率。

网络流量统计

可使用采集器对网络层数据包进行监听，也可从网络设备的 SNMP/MIB2、交换机的 SNMP/RMON/MIB 中获取网络运行数据，收集报文并实时显示和进行历史分析。能够提供可视化的网络流量和性能可视化的分析，支持流量回溯及会话还原分析。

系统能够对 ISO 2-7 层的网络流量进行监控分析，采用深度数据分析技术，能够对当前网络的访问质量及业务性能进行监控，可同时查看多个端口或链路的带宽占用、协议占用、网络通讯对的分布情况，分析影响网络性能的原因。

流量查询

系统支持对历史流量数据进行检索，检索条件可包括起始/终止时间、源 IP 地址（单个 IP 地址、地址范围、子网）、源端口（单个端口、端口范围）、目的 IP 地址（单个 IP 地址、地址范围、子网）、目的端口（单个端口、端口范围）、

协议等。

4.2.3 应用业务监测

应用业务分析

用户配置完自定义业务和 IP 组以后，可针对自己关心的 IP 组、业务等不同的对象自定义一个查询方式，将统计结果显示在一个图表中，减少日常监控的工作量。统计数据可以使用图标加上数据列表的方式显示。应用业务监测的统计时间跨度可以是当天、本周和当月，也可以选择具体的时间段去统计。

响应时间监测

延时是网络的固有属性之一也是评价网络性能的基本指标。延时测量在网络性能监测、网络行为分析、网络应用设计等领域有着广泛的应用。同时，也是测量延时抖动、网络带宽等性能指标的基础。

利用业务模拟测量方式，在不影响客户网络应用的情况下，能方便的测量各种应用的响应时间。

4.2.4 报表统计

系统提供丰富的报表功能。支持默认报表的统计及自定义报表。系统提供的默认报表包含链路分析报告、链路预测报告、网络层分析报告、TopN 统计报告、应用层协议分布、应用响应分析报告、网络应用流量基准报告、网络故障统计报告、汇总分析报告等。

各种报表按照统计周期的不同，可以分为年报表、月报表、周报表、日报表。可以将统计结果输出成 PDF、HTML、EXCEL、WORD 等格式的文档。

4.2.5 回溯分析

网络的持续、高效和安全运行是用户业务正常运行的基础。这就要求网络管理员能够随时掌握业务应用运行的关键指标，及时发现异常并预警，实现主动运维、主动管理；当故障发生时，能够快速有效地定位问题点、分清责任并分析原因，从而减少故障时间；一旦网络收到攻击或发生安全事件，需要有手段有依据，实现有效地定位、分析和取证。

系统根据实际需要提供对历史数据回溯功能，主要有以下特点：

长期数据存储

系统具备长时间、大容量数据存储能力，能实时捕获原始数据包、数据流、网络会话、应用日志等各种统计数据并长期保存，提供针对用户重要网络流量的线速分析处理能力。

回溯取证能力

系统具备对所存储的海量数据进行快速回溯的能力。在存储容量允许的情况下，具备对过去长达半年内（取决于单位的流量大小和存储空间的大小）已发生的网络行为、应用数据和主机通讯数据进行回溯分析，为用户提供网络问题的追踪和取证。

大数据挖掘能力

系统提供任意时段内的海量数据进行快速检索和挖掘能力，让用户可以在复杂的海量数据里，采用数据关联，筛选过滤、挖掘分析等手段进行大数据分析。系统自带强大的过滤条件，可最大限度的帮助用户挖掘问题并提取相关内容，为迅速定位问题发生原因提供了更全面的分析手段。

七层协议解码

系统提供目前互联网常见的各种网络通讯协议的解码分析能力，帮助用户透视网络各个层次的通讯状况。

4.2.6 异常告警与预警

异常流量告警

系统对网络流量进行实时监控，能够及时发现网络中出现故障或异常，通过告警预处理将非关注的告警过滤，压缩重复的告警并重定义相关告警后，将真正有用的告警信息以列表、视图、声音等形式呈现给运维人员，并将重要告警信息通过邮件、短信等方式及时告知相关运维人员。此外，系统还提供了功能强大、设置灵活的查询功能，包括对活跃告警和历史告警的查询。

数据流特征值告警

系统具有对数据包特征值告警功能。管理员可预先定义需告警的特征值，系统会对捕获到的数据包进行过滤，如果在特定位置搜索到与特征值相一致的内容，则会触发数据流特征值警报。

流量趋势预警

系统具有对流量的预测及预警功能，根据网络流量的历史数据，结合实际序列的多种预测算法和预先设置的预警阈值，能准确高效地预测出用户所关心的 IP 及设备未来流量的变化趋势。根据预测结果，对流量可能超过阈值的 IP 及设备进行预警，方便用户提前做好准备，避免网络故障的发生。同时有助于网络运维人员更好地解决某些网络流量长期低于设定阈值的区域所带来的通信设备资源配置浪费，以及流量长期高于设定的阈值的区域所引起的通信资源配置不足的问题，从而达到网络设备资源配置合理化、最优化的目的。

4.2.7 安全分析

蠕虫病毒分析

根据蠕虫病毒在网络上的传播及发作机制，使用蠕虫病毒特征库，过滤评判出可疑数据信息，并显示在图形界面上。蠕虫病毒特征库备有常用蠕虫病毒单位端口、协议、字节数等特征信息，对符合条件的数据流量进行敏感文件类型 dll、dot、数据等匹配检测，并将疑似蠕虫病毒的信息在界面呈现。

DDoS 攻击分析

DDoS 攻击包括 SYN flood、ICMP flood、UDP flood 等。DDoS 较传统的 Dos 攻击，危害更广泛。可以使用 DDoS 特征库对数据流量进行匹配，分析 DDos 攻击的存在。DDos 特征库会统计一段时间内 SYN 数据包、ICMP 包百分比、UDP 报文数量，以及向同一主机的请求数等特征数据。在实用环境下，利用相应的 DDoS 攻击识别规则，分析出可疑的攻击信息。

对可疑的 DDoS 攻击信息及对网络设备资源占用率的情况给出警告，并显示在图形界面上。

ARP 攻击分析

APR 攻击是攻击者通过发送大量的 ARP 请求数据包，占用网络通道资源，引起网络的拥堵及瘫痪。或者利用伪造的 ARP 应答报文，来骗取 ARP 请求者的通讯。ARP 攻击分析会统计链路的 ARP 报文百分比及趋势变化，关联主机并设置筛选条件，将异常的 ARP 行为信息可视化警告并展现。

统计分析真实环境中的 IP 及 MAC 地址信息的关联情况及变动频率，设置过滤条件，对疑似伪造 APR 应答的行为信息显示在 ARP 攻击图形界面上。

P2P 下载

根据 P2P 下载技术原理，得知 P2P 下载流量具有相关特征。通常某些地址之间的通讯流量占比大，并发连接数趋势变化大。可以对这些参数设置基准值，去分析判断 P2P 下载行为。并将符合过滤条件的主机信息在界面上展示。

用户自定义异常

用户可以自己设定一些流量特征作为异常行为 ,如对 23 端口的 telnet 服务或 53 端口 DNS 的访问，以及大于数据包长度阈值的流量。对这些用户感兴趣的流量信息，给出警告并显示在异常行为界面。

4.2.8 硬件设备实时监控

系统支持集中管理硬件设备功能，主要功能有：

- 客户端可通过 Web 远程管理系统
- 支持分布式的管理，统一管理系统内所有设备
- 支持管理员分级分权管理
- 可远程监测各设备的运行状态
- 可远程控制、管理采集器
- 支持实时监控路由器、交换机、防火墙、服务器等基础硬件设备

采集器具有一个专用管理端口，支持外部管理功能。分析器可对采集器进行远程管理、控制，实现远程监控分析、数据包捕获等工作，远程进行网络故障检测。

5 分析中心

5.1 多角度的网络流量分析

系统可以统计设备接口、接口组、IP 地址组、多链路接口的实时流量信息，包括流入、流出速率以及当前速率相对于链路最大速率的比例。

系统可以从多个角度对网络流量进行分析，并生成报表，包括基于接口的总体流量趋势分析报表、应用流量分析报表、节点（包括源、目的 IP）流量报表、会话流量报表等几大类报表。

5.2 总体流量趋势分析

总体流量趋势分析报表可反映被监控对象（如一个接口、接口组、IP 地址组）的入、出流量随时间变化的趋势。

图形化的统计一览表提供了指定时间段内总流量、采样点速度最大值、采样点速率最小值和平均速率的信息。对于设备接口，还可提供带宽资源利用率的统计。

支持按主机统计流量 TopN，显示给定时间段内的流量使用在前 N 位的主机流量统计情况，以及每个主机使用的前 N 位应用流量统计。

同时还支持流量明细报表，可提供各采样时间点上的流量和平均速率值。

5.3 应用流量分析

应用流量分析报表反映被考虑对象（如一个接口）的流入（或流出）方向上，带宽被各种网络应用占用的比例随时间变化的趋势，包含报表统计时间内该应用

的总流量、平均流速和占所有应用总流量的百分比等。

同时还支持对该应用的流量信息进一步的数据挖掘，分析使用该应用流量的最大来源和目的地址 TopN 列表。

5.4 会话流量分析

会话流量分析报表反映被考察对象（如一个接口）的注入（或流出）方向上，在指定时间范围内总流量最大的网络节点（源、目的）、以及网络节点间会话的排名。

同时还支持对节点、会话流量进行进一步的数据挖掘，分析节点流量中使用最多的应用和与该点通讯最多的节点、分析会话流量中双方节点使用应用的排名信息。

5.5 未知应用流量分析

未知应用流量分析对系统中没有定义的 TCP、UDP 应用进行了深入的分析，提供按照端口号、源 IP 和目的 IP 分组的未知应用流量信息，并可查看到某一个端口、源 IP 和目的 IP 的详细通信信息，提供按源、目的分类的流量 TopN 情况。

可以按照协议和端口将统计到的未知应用定义为已知应用。

6 报表中心

统计报表是一种事后的分析工具。统计报表按照其内容分为：

◆流量报表

◆告警报表

◆自定义报表

系统收集采集器的监控信息 ,存储到数据库中 ,并提供功能强大的分析报表。系统可提供日报、周报、月报、季报、年报等中、长期的流量报告。系统内置多个标准报表，同时支持用户自定义报表。

在生成报表之前，允许用户从界面上选择一些报表条件，如时间范围、统计周期、报表类型、报表模板等。在流量分析页面中可以选择特定监控对象和时间范围，然后把查询结果输出成 PDF、HTML、EXCEL、WORD 等格式的文档，也可以作为一种灵活定制的报表。告警监控和设备监控页面也有类似的报表导出功能。报表主要包括：

1) 链路分析报告

2) 链路预测报告

3) 网络层分析报告

4) TOP N 统计报告

5) 应用层协议分布

6) 网络应用流量基准报告

7) 网络故障统计报告

8) 汇总分析报告

通过报告，可对网络的整体性能、网络的运行状况、网络的流量趋势乃至应用的服务质量进行分析，辅助网络管理人员预先确定应用资源需求以避免出现性能问题。并根据应用的发展要求调整网络，改善网络服务质量，为中行提供容量规划、网络优化和网络扩容的依据。

7 产品型号说明

7.1 技术参数

产品型号	SPA-3000
系统管理	1.支持通过 HTTP 和 HTTPS 两种方式远程管理系统； 2.系统全中文操作界面，便于管理； 3.支持用户访问权限管理，可为不同级别管理员指定不同的权限； 4.支持对采集器统一集中管理，远程管理采集器； 5.统一集中呈现分析器和采集器审计日志和告警日志。
网络流量监控	1.支持对链路层流量进行监控； 2.支持对网络流量进行实时监控和分析； 3.支持对流量进行自定义查询。
应用业务监测	1.支持将应用业务定义为分析对象，对其进行统计分析； 2.支持对应用业务的响应时间进行监测。
回溯分析	1.支持对历史数据进行回溯分析，精细查找问题原因； 2.支持对历史数据进行各种自定义查询。
异常告警与预警	1.能够及时发现异常流量并发出告警； 2.支持通过流量特征匹配异常流量； 3.能够对未来流量趋势发出预警； 4.支持多种告警方式，包括页面、邮件、短信、声音等，提供定制化接口；

		5.支持通过 SNMP、Syslog 将告警信息发送到网管平台。
安全分析		1.能够对蠕虫病毒进行分析； 2.能够对网络层和应用层 DDoS 攻击进行分析； 3.能够对 ARP 攻击进行分析； 4.支持用户自定义异常分析。
硬件设备实时监控		1.支持统一集中管理硬件设备； 2.自动生成当前网络拓扑图，对网络拓扑进行管理； 3.支持对各硬件设备告警日志统一集中管理； 4.支持对各硬件设备性能统一集中管理。
报表统计		1.系统内置多种标准报表，分为流量报表、告警报表、日志报表等； 2.支持用户自定义报表。
部署方式		支持旁路和分布式部署
硬件规格	**分析器**	1.规格：2U 机架式 8 个热插拔硬盘位 2.处理器：2*INTEL Xeon E5-2640 v2 8C 20M 2.6GHz 3.内存：4*16GB DDR3 RECC 1600 4.存储：8*3TB SATA 7200r 5.网卡：4*INTEL 千兆网口 6.电源：2U/500W 冗余电源
	采集器	1.规格：2U 机架式 8 个热插拔硬盘位 2.处理器：2*INTEL Xeon E5-2620 v3 6C15M 2.4GHz 3.内存：2*16GB DDR3 RECC 1600

		4.存储：2*300G SAS15000r 5.网卡：4*INTEL 千兆网口，1*万兆卡含 2 个 SPF+多模模块 6.电源：2U/500W 冗余电源
工作温度		工作环境：10℃～35℃ 运输/储存环境：-40℃～70℃
工作湿度		工作环境：8%-90%相对湿度 运输/储存环境：5%-95%相对湿度

7.2 安全性说明

安全性包括操作系统本身的安全性和应用系统的健壮性。海加网络流量分析系统的采集器和分析器的操作系统均采用最新版的 Linux，且对内核进行了裁剪，去除了不相关的功能，最大程度地对操作系统进行优化，提高了系统的性能。除 443、80、22（用于远程管理）端口外，关闭操作系统其它端口。采用的 Web 容器、数据库、第三方开发库等均采用当前的最新版本。

8 海加网络服务体系

海加网络凭借着先进的技术，秉承客户至上的服务理念，为客户提供最为完善的技术支持服务。

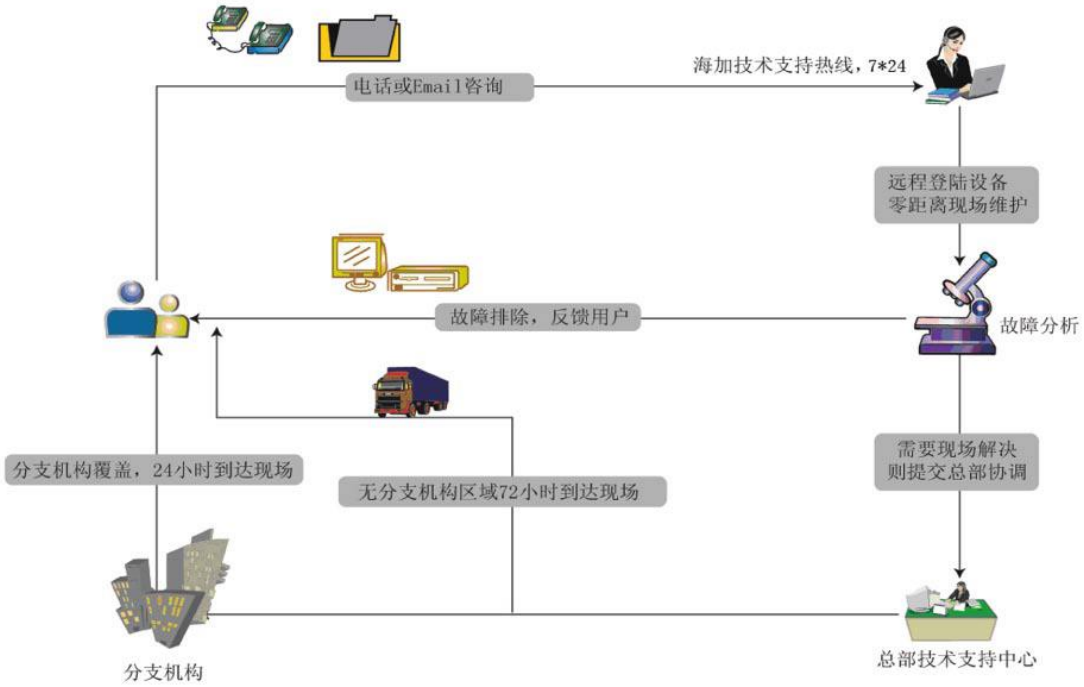

图 5 售后服务体系

- 远程支持服务

Email和电话技术支持服务

公司设有7 x 24小时的电话和Email支持服务，接收客户咨询、服务调度和投诉。

虚拟现场产品维护服务

公司技术人员通过在公司和客户间利用互联网建立SSL数据加密通道，远程登录公司设备，为用户提供零距离的虚拟现场产品维护。

- 现场服务

有办事机构覆盖区域将在24小时内到达现场为用户排除故障，无办事机构或需

总部支持则公司总部技术人员可以在72小时内到达现场解决问题。

- 备机服务

基于用户业务运行的重要性及响应时间考虑，通过公司备件更换程序，可以先将好的备用设备供用户使用，直至故障设备修复。