蓝海卓越日志系统

技术白皮书

修订记录

版本号	作者	修订日期	描述
1.0.0	杨	2020-06-04	初稿
1.1.0	刘	2022-03-06	修订

版权声明

免责条款

根据适用法律的许可范围，成都星锐蓝海网络科技有限公司按“原样”提供本文档而不承担任何形式的担保，包括（但不限于）任何隐含的适销性、特殊目的适用性或无侵害性。在任何情况下，成都星锐蓝海网络科技有限公司都不对对最终用户或任何第三方因使用本文档造成的直接损失或间接损失负责。

文档更新

本文档仅用于为相关技术和管理人员提供信息，并且随时可由成都星锐蓝海网络科技有限公司更改或撤回。

责任限定

蓝海卓越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。

联系我们

如您对本文档有任何问题，可联系我们进一步了解。

目录

1. 引言

1.1. 日志管理现状

随着计算机技术、自动控制技术等相关应用技术在各行业中的广泛应用，信息系统在企业经营管理和社会经济生活中所起的作用越来越重要。信息化、数字化的概念不断深入到各行业的技术应用中，大量网络设备、安全设备（防火墙、IDS 系统、防病毒软件等）、操作系统（包括Windows 和 Unix）、应用服务（Email， www ，DNS）在各行各业得到广泛应用。这些 IT 信息系统以及相关网络设备，在各行业的业务应用、过程控制、企业管理以及战略决策等领域起到了至关重要的作用。但是在信息高速发展的前提下，我们的大数据信息安全保障面临了严峻的问题，数据信息留存不及时，数据采集方面不够全面立体，对整体网络的状态了解不够详细，对用户上网的行为没有审计，对网络安全的威胁没有防御，对网络设备的资源没有整合，缺乏溯源工作技术手段支撑等等。

1.2. 国家政策

自2007年网络安全等级保护制度实施至今，已从等保1.0时代进入等保2.0时代，再加之2017年6月《中华人民共和国网络安全法》颁布实施，中国的网络安全发生了突破性进展，不仅体系发生了大升级，而且网络安全标准也从制度上升为法律，变得空前重要。这套制度标准的实施为信息系统安全开辟了一条可落地可操作的道路，不仅为各信息系统提供体系化的指导，根据各自责任落实相应技术措施；同时为落实信息系统安全工作提供方向和依据，明确法律法规要求，让安全工作有法可依；还致力于落实保障个人信息、资金等安全，为个人隐私提供保护伞。

全面贯彻党的精神，深入贯彻习近平总书记系列重要讲话精神，认真落实党中央、国务院决策部署，按照“五位一体”总体布局和“四个全面”战略布局，牢固树立创新、协调、绿色、开放、共享的发展理念，着力补齐核心技术短板，全面增强信息化发展能力。

根据《网络安全法》第二十一条（三）项：采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；第五十九条之规定，决定给予该公司警告处罚，并责令限期十五日内进行整改。

针对网络安全法规定的日志留存要求，蓝海卓越已经推出了成熟的适用与运营商、大型企业、中型企业、中小企业的完整日志安全合规解决方案。

2. 产品特色与定位

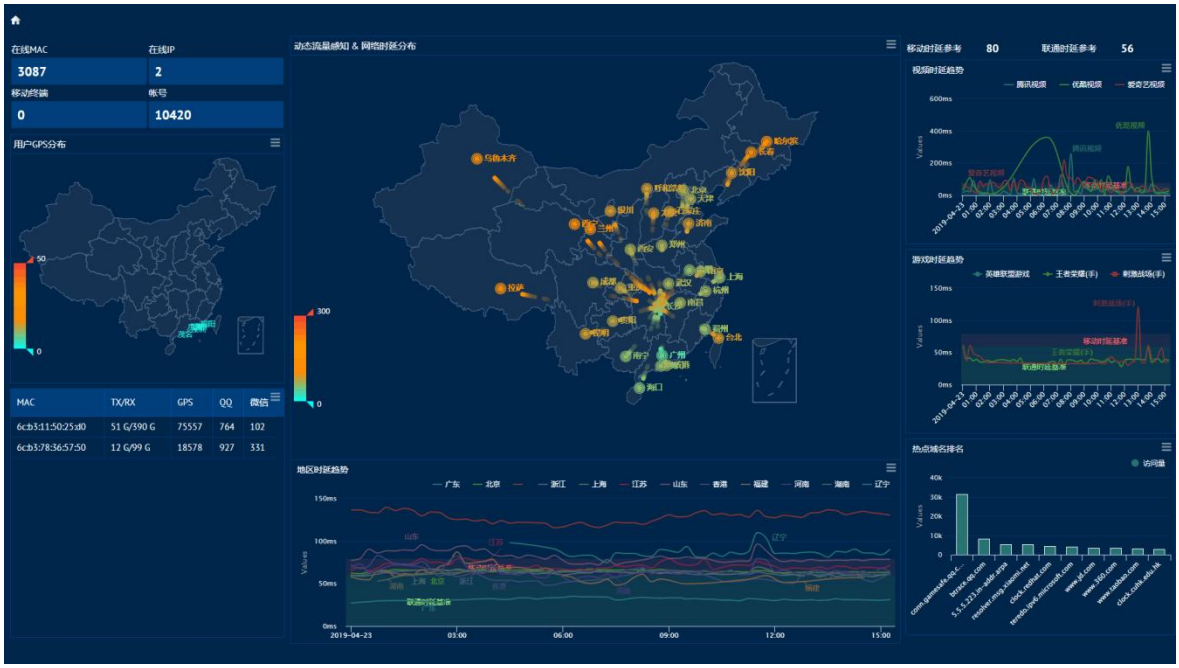
1. **运维健康辅助，**通过日志手段对网络设备进行实时健康度监控，有效补充网管软件的不足；

2. **网络优化辅助，**通过日志系统精准的数据采集平台，将数据集中分析，对用户运营中存在网络、应用等问题集中汇总，为应用和网络的优化提供参考依据，最大限度的提升用户的使用体验和网络的利用率。

3. **信息安全响应，**满足国家等级保护要求，对网络设备，安全设备日志进行集中收集和存储。

4. **网络安全保障，**通过对设备日志分析，有效实现用户日志和溯源分析，加强网络安全管理，提高网络安全等级。

5. **网络态势感知，**蓝海卓越大数据态势感知系统让运维管理进入3.0时代，网络故障、异常报文、异常网络时延等实现主动告警，并可在控制台上实时展示。



以此同时，公安机关在办案过程中发现，大量互联网信息安全隐患，和基于此的违法犯罪行为，都是因为访问日志留存规范不健全，违法犯罪分子趁虚而入，最终对用户合法权益造成危害。违法犯罪行为还会利用日志留存的漏洞，逃脱公安机关的循线追缉，导致网络违法犯罪案件的嫌疑人逃脱法律制裁，给公民和企业的合法权益带来损害。同时，遵守“日志留存”的相关规定，对运营者本身也有着极其重要的安全防护作用，不仅能够留存历史数据，更为未来可能发生的安全威胁消除了隐患。

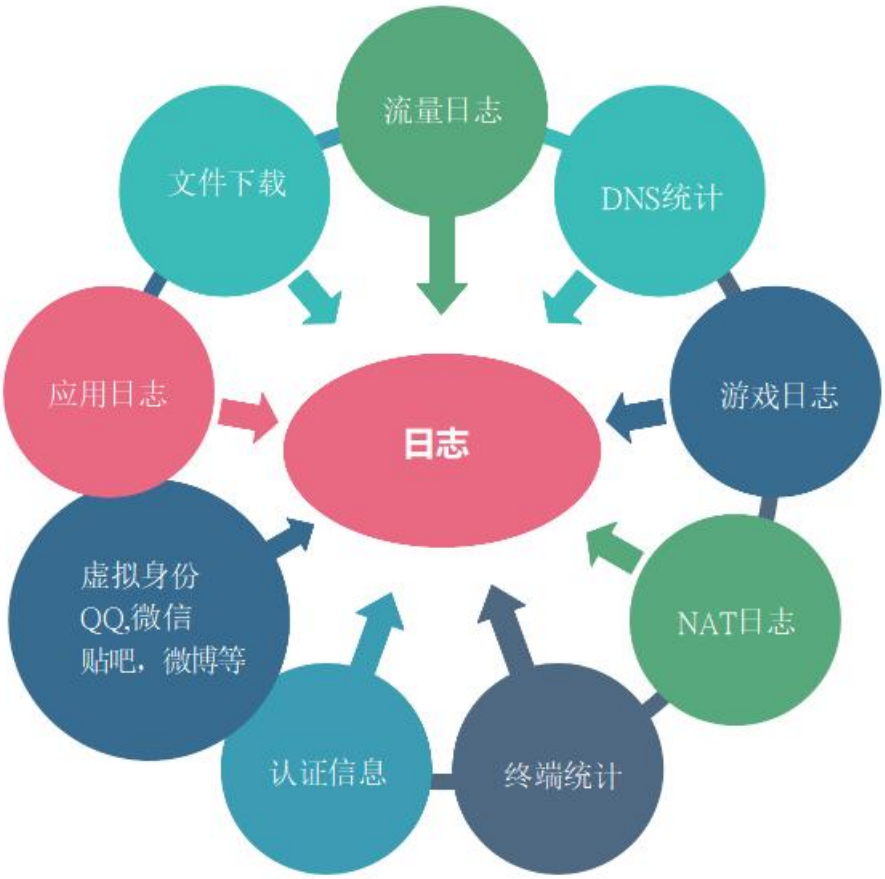
所以该产品是高校、公安、政企、医疗、金融、能源等行业之中是必不可少的，针对网络流量的信息进行日志留存，对用户上网行为进行审计，逐渐形成大数据采集、大数据分析、大数据整合的工作模式。

3. 特色功能

- 支持大屏自定义面板，支持实时告警
- 支持用户流量根据协议展示和排名以及详细信息记录
- 支持用户流量根据用户地址和目的地址进行展示和排名以及详细信息记录
- 支持用户流量根据地域进行展示
- 支持用户流量图片实时展示
- 支持用户DNS信息记录和统计信息以及展示
- 支持用户认证信息记录和展示
- 支持用户QQ以及QQ图片和QQ视频信息记录和展示
- 支持用户微信以及微信图片和微信视频信息记录和展示
- 支持用户贴吧信息记录和展示
- 支持用户NAT信息记录和展示
- 支持游戏节点和视频节点信息展示
- 支持用户虚拟身份信息记录和展示
- 支持用户游戏信息记录和展示
- 支持用户HTTP请求的信息记录和展示
- 支持用户文件下载信息记录和展示
- 支持网贷信息记录和展示
- 支持用户图片信息记录和展示
- 支持数据根据记录的信息进行查询
- 支持查询数据一键导出功能
- 支持系统数据盘挂载后台一键操作，不需要登录系统
- 支持数据存储和展示的时间自定义
- 支持系统运行状态异常短信告警
- 支持日志系统分布式部署，避免数据丢失的可能

4. 产品构架

蓝海卓越日志是基于大数据架构的日志审计系统，针对客户部署的蓝海卓越路由流控设备实现日志数据的高效采集、统一管理、集中存储、统计分析。如针对排名、分布、趋势和相似性分析，提供IP 轨迹、TOP域名、应用流量流向图、URL 地图、TOP 用户、连接可视化分析和DNS 可视化分析等为代表的分析工具，并可协助运营商高效统一管理网络日志并为安全事件的事后取证提供依据。



系统基于SOA架构设计，采用B/S 管理模式。系统由日志采集、日志处理、日志管理、事件监测、日志存储、统计分析、告警响应以及系统管理八个子系统构成。各子系统相互耦合、协作，保证整个系统稳定、高效。

5. 功能简介

5.1. 常规日志输出功能

源IP目的IP NAT日志、URL查询、DNS查询、微信日志、QQ日志、虚拟身份、游戏日志、移动终端、网贷情况、节点日志、图片浏览、文件下载、用户认证、百度贴吧、GPS记录等。

5.2. 流量监控分析

实现对网络进行流量可视化和应用精细化，将每一个连接的具体应用呈现出来，便于网

络管理者进行分析、定位、处理和优化，通过流量可视化管理，可以看到学校上行、下行流量趋势以及各种协议占用带宽的百分百等信息。

对网络出口的TOP IP 流量、TOP 并发 IP 数、TOP 应用均可实现统计分析呈现。从流量大小、连接数多少、应用的访问量等多维度呈现网络现状，记录网络大趋势。

5.3. 流量区域流向分析

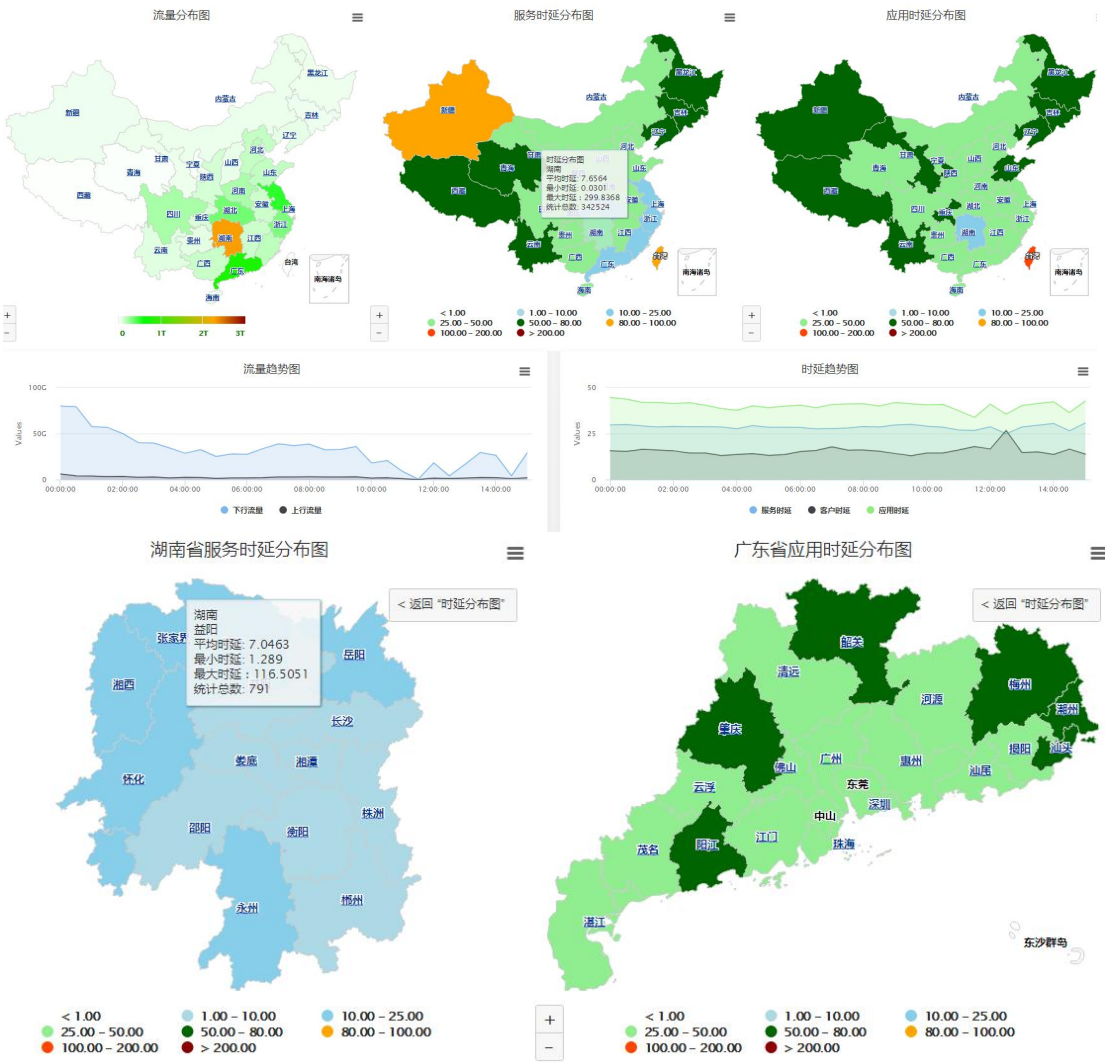
实现了可视化的流量流向信息，大屏模式下可以呈现整个网络中用户访问流量的最终落地节点，记录分析全网的TOP 目标IP、同时记录GPS信息，精确到市级单位。通过运营商流量情况、地址流量排名、协议排名、目的地址流量等数据综合展示，可对网络流量调度和内网优化起到关键性作用。

5.4. 时延区域分析

新版蓝海卓越路由采用三段式时延展示方案，清晰明了的展现出网络时延的动态情况。

蓝海卓越大数据系统可以实现单个协议时延、抖动等性能指标在时间维度的查询。可以实现多个协议和用户的交叉查询，监测异常情况，上报告警。可以实现对业务指标自定义的实

时查看，全局实时掌握每种网络资源的区域分布和区域时延情况，针对出现的问题，可视化的展现在我们面前，让我们更快速合理的配置资源，提升用户上网体验。



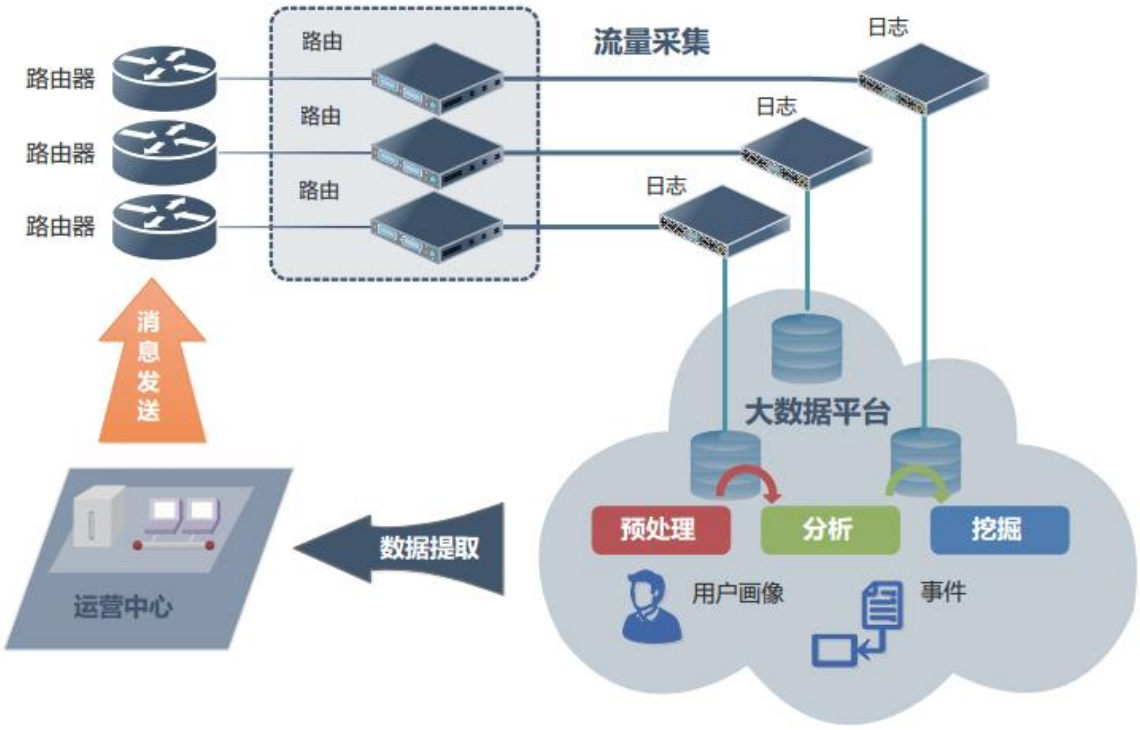
5.5. 大数据分析

蓝海卓越路由具备计算机领域内先进的数据包处理技术，能识别95%以上的应用，实现精准流量分析，生成详细的日志数据。结合蓝海卓越日志可以实现海量PB级别的数据存储分析。帮助

运营商实现精细化运营，为第三方提供特定数据源。协助运营商高效统一管理网络日志并为

安全事件的事后取证提供依据。适用于运营商、网络监管相关单位、大数据应用组织实体 拥有强大的节点、协议趋势、用户趋势、终端趋势分类汇总功能，可通过用户对需求数据

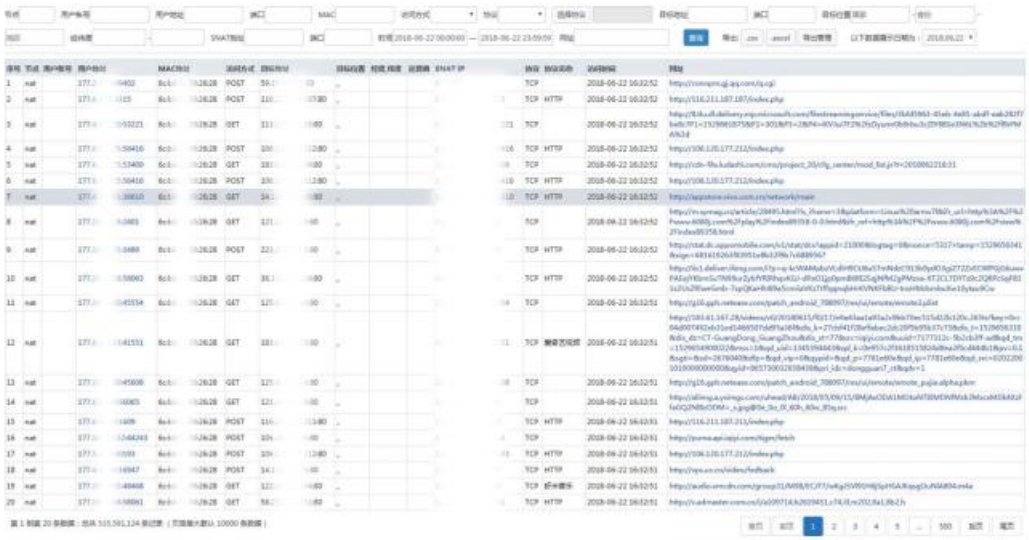
筛选最终得到此类数据画像。



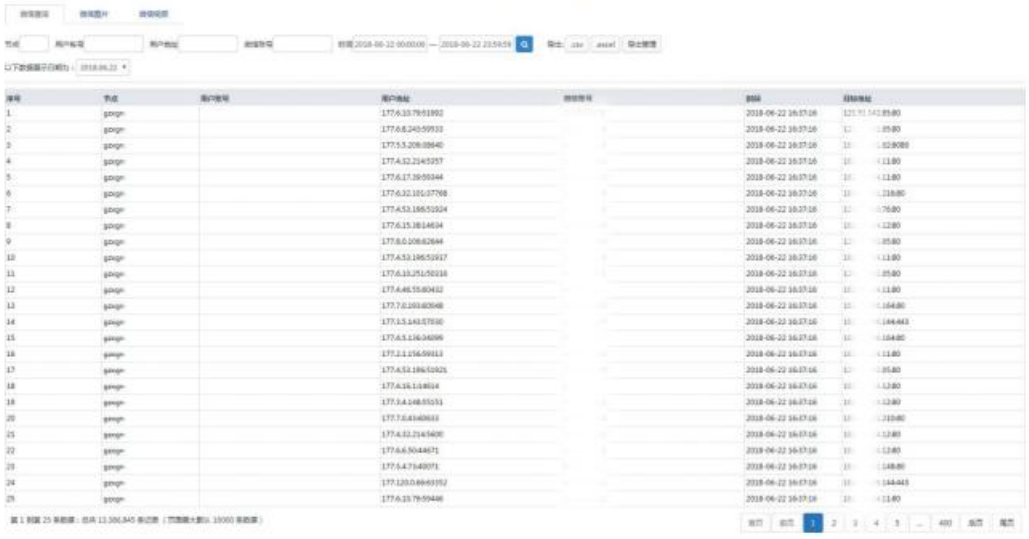
6. 产品优势与特点

1. 海量日志秒级查询，对于规模较大的运营商，每日日志量动辄几百G，而公安部82号令要求日志必须保留60天以上，这对海量日志的存储和检索都提出了严峻的挑战，传统的关系数据库存储已经完全满足不了要求，而存储为文件的方式不利于检索，蓝海卓越独有的分布式结构化存储完美的解决了这个问题，只要存储空间足够，即使PB级的数据量也能应付，10亿数量级别的检索只需要5-20秒即可获得结果。

2. 精细的日志采集粒度，对比并不具备足够DPI能力的传统网关类设备，蓝海卓越日志的突出优势在七层应用日志，如微博、微信、QQ、淘宝账户、手机贴吧、DNS请求、地理位置等。可提供网络内任意一个IP的深层信息，精确到每时每刻每IP每条连接。



URL访问日志



微信日志

3. 支持对原始安全信息数据进行全文检索，支持单一条件、多条件检索查询，查询结果即查即显，支持查询结果二次查询。实时流量监视，轻松了解系统处理速度。

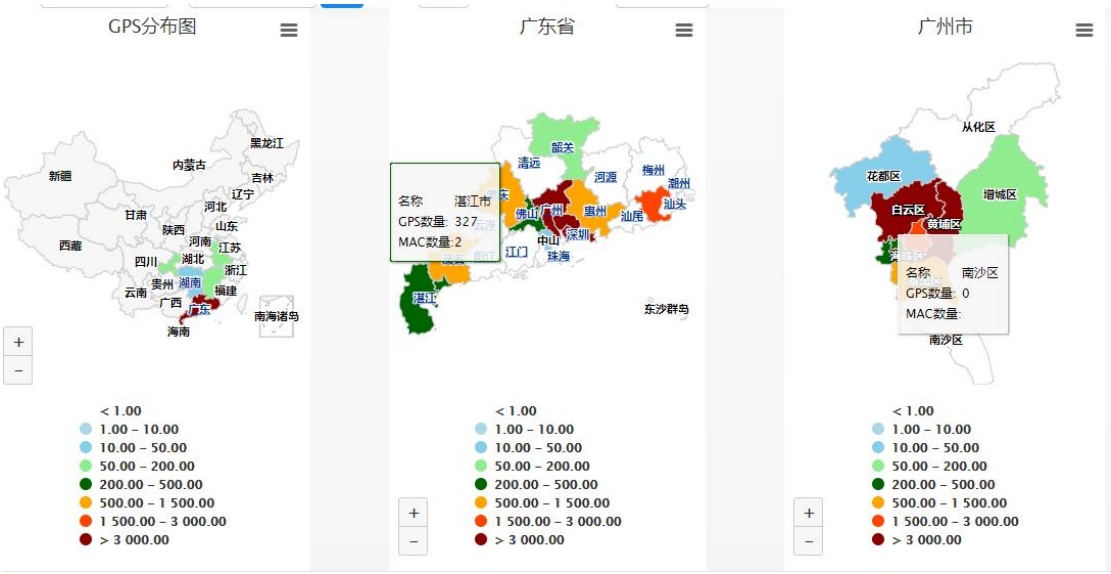
4. 支持单点部署、分布式部署，可与蓝海卓越路由器完美无缝结合。

5. 更贴近运营需求的输出图表。


运营商流量分布图
联通
电信
移动
其他
25%
40%
18%
17%
运营商流量TOP图
10KG
7.5KG
5KG
2.5KG
2.4K
3.7K
2.1K
3.2K
3.1K
6.1K
1.1K
1.7K
电信
联通
移动
其他
下行
上行


用户在线热力分布图

6. 异常GPS告警输出。



序号	MAC	IP	QQ数量	微信数量	GPS数量	上行流量	下行流量	位置:GPS数量
1	6c:b[illegible]:d0	(177.1[illegible]5:196)(177.19[illegible])(177.1[illegible]0.139:188)...	827	104	8436	2.23GB	16.64GB	(白云区:8436)
2	6c:b[illegible]:d0	(177.5[illegible]173)(177.6.12.[illegible]7.5.3.11[illegible]8)...	827	104	3280	2.23GB	16.64GB	(黄埔区:3280)
3	6c:b[illegible]:d0	(177.1[illegible]:109)(177.199[illegible]77.4.14.[illegible]:62)...	827	104	2455	2.23GB	16.64GB	(天河区:2455)
4	6c:b[illegible]:d0	(177.1[illegible]6:121)(177.19[illegible])(177.1[illegible]0.133:104)...	827	104	827	2.23GB	16.64GB	(番禺区:827)
5	6c:b[illegible]:d0	(177.1[illegible]:94)(177.199.0[illegible]7.199.0.[illegible]47)...	827	104	497	2.23GB	16.64GB	(海珠区:497)
6	6c:b[illegible]:50	(120.2[illegible]109:192)(120.[illegible]8:92)(1[illegible]236.218.110:63)...	2884	1416	356	15.58GB	79.41GB	(白云区:356)
7	6c:b[illegible]:50	(120.2[illegible]109:145)(120.[illegible]8:115)([illegible].236.218.110:61)...	2884	1416	321	15.58GB	79.41GB	(天河区:321)
8	6c:b[illegible]:50	(120.2[illegible]109:117)(120.[illegible]8:98)(1[illegible]236.218.110:58)...	2884	1416	273	15.58GB	79.41GB	(海珠区:273)
9	6c:b[illegible]:d0	(177.1[illegible]:38)(177.120.0[illegible]7.199.0.[illegible]29)...	827	104	238	2.23GB	16.64GB	(越秀区:238)
10	6c:b[illegible]:d0	(177.1[illegible]:74)(177.199.0[illegible]7.199.0.[illegible]19)...	827	104	165	2.23GB	16.64GB	(荔湾区:165)
11	6c:b[illegible]:d0	(177.6[illegible]3)(177.4.4.137[illegible]5.197:2[illegible]	827	104	133	2.23GB	16.64GB	(增城区:133)
12	6c:b[illegible]:50	(120.2[illegible]108:43)(120.2[illegible]:14)(12[illegible]36.218.109:7)...	2884	1416	64	15.58GB	79.41GB	(黄埔区:64)
13	6c:b[illegible]:50	(120.2[illegible]109:41)(120.2[illegible]:11)(12[illegible]36.218.110:11)...	2884	1416	63	15.58GB	79.41GB	(荔湾区:63)
14	6c:b[illegible]:50	(120.2[illegible]108:29)(120.2[illegible]:24)(12[illegible]36.218.110:9)...	2884	1416	62	15.58GB	79.41GB	(番禺区:62)
15	6c:b[illegible]:50	(120.2[illegible]109:34)(120.2[illegible]:12)(12[illegible]36.218.110:11)...	2884	1416	57	15.58GB	79.41GB	(越秀区:57)

7. 技术参数

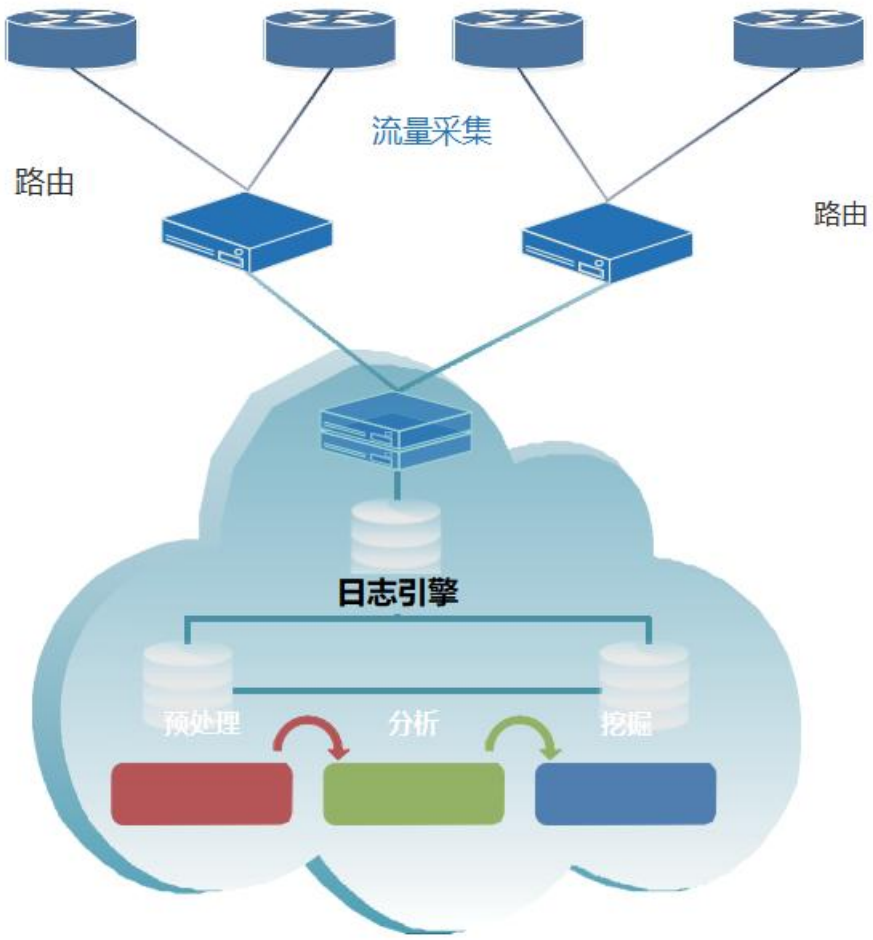
7.1. 配置参数

产品名称	蓝海卓越日志审计系统
CPU	8 核 16 线程，频率≥2.4GHz，具体性能依据流量而提升
内存	根据流量配置，内存最低 16G
硬盘	一天数据量 day:流量速率最高值*20(单位 G) 总数据大小:day*存储天数*1.3(单位 G) 例如某环境下最高流量速率最高是 17G，那么一天日志存储数据大概是 340G 左右，如果存储天数为 60 天，那么需要的磁盘大小为 340*60*1.3=26520G
性能	查询性能上很优秀，在数据量大的情况下也能很快的查询出数据，如某用户环境中一天的数据存储 356G，数据 3 亿多条，不带条件查询，大概 20s 左右出数据，带条件查询根据条件不同时间会更少，一般在 10s 左右 同时在安全性上，系统可以检测系统运行状态，当检测到系统运行不正常时提供告警信息，信息以短信的形式发送到手机上； 数据分类众多，记录数据完整

7.2. 部署方式

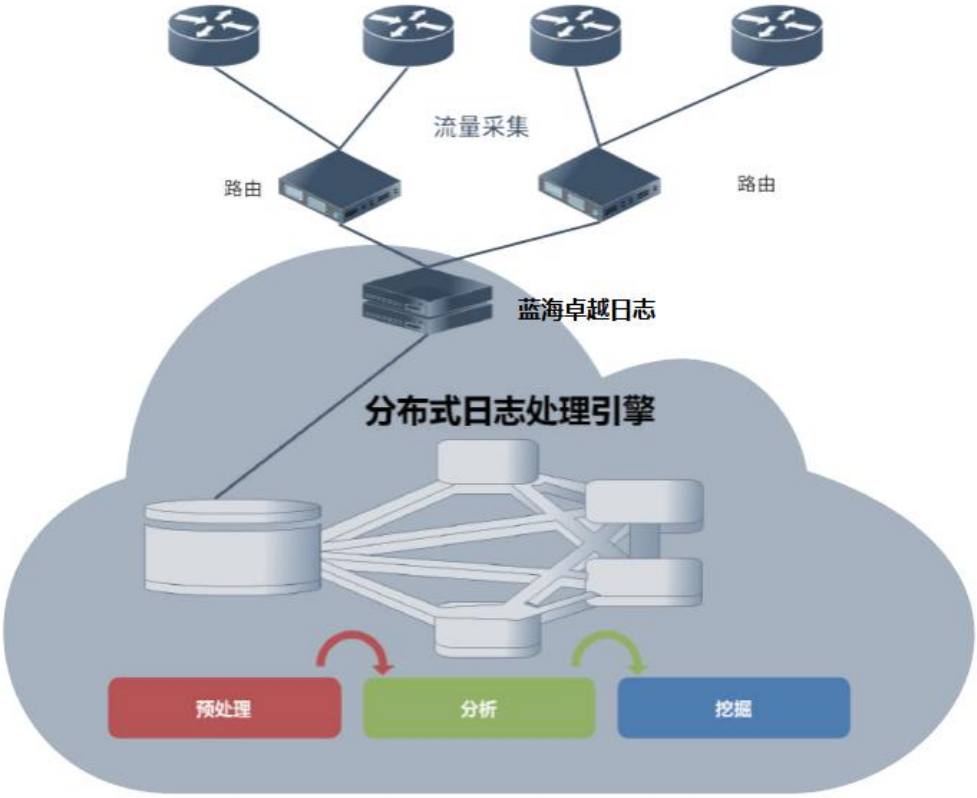
7.3. 单机模式

单机模式部署相对简单，可部署在网络任意位置，保证与路由服务器互通就可以了，它仅仅是单一存在的。



7.4. 分布式部署

相对于单机模式，分布式部署区别为日志主控和存储为分开部署。



成都星锐蓝海网络科技有限公司
成都总部
电话：028-86679789（FAX）

www.natshell.com

客户服务热线
028-86679789

版本：20220306-V1.1.0