智维数据
Intelligent Analytics Platform

网络流量分析平台

产品白皮书

北京智维盈讯网络科技有限公司

第一章 运维管理挑战

时至今日，各个企业 IT 建设的规模与复杂度与日俱增，信息化标准水涨船高，IT 应用模式日新月异，基础架构及应用模式的革命性变化给 IT 管理带来了巨大的挑战。如何对这些复杂的业务系统进行有效监控和风险防范，保障关键业务的高性能和高可用性，以及如何对现有的运维流程进行优化，不断提升管理和运维水平已经成为目前数据中心急需探索和解决的重要问题。

第二章 产品介绍

nCompass 网络流量分析平台，通过自动采集网络中传输的数据包，提炼加工出网络和应用性能类的指标数据。不仅具备数据回溯、定位故障、告警、分析报告等基础 NPM 功能；同时支持主动拨测、接入日志类数据并实现数据关联。以数据库的方式存储各类统计数据，提供灵活的数据消费手段。内置可自定义配置的 Dashboard、简单灵活的数据表格、以及开放的数据对接功能，能够将 nCompass 网络流量分析平台中的任何指标或事件通过内置的消息队列功能传输到第三方平台，配合开放的 Restful API 为第三方提供数据，实现为用户量身定做的大数据自服务平台。从而做到降低运维复杂度，提升业务系统可靠性。

平台主要具备以下功能：

nCompass 平台通过网络数据及日志数据，对数据中心数据流进行智能分析。

数据梳理

nCompass基于真实业务调用访问数据，自动生成各应用系统的真实、准确的应用拓扑图。并且当应用出现变更，如新增应用节点或访问关系发生变化时系统可自动更新拓扑。

智能监控

nCompass借助网络承载应用、业务及用户访问的特性，通过用户的真实访问数据，来监控数据中心关键应用系统的运行状态，当真实用户访问出现异常时，运维人员可以及时的感知到，可以及时处理，降低故障的影响。

数据可视

nCompass提供全面的数据可视化能力，既可集中呈现用户访问数据中心的用户体验状态，也可基于应用梳理结果定制出应用端到端可视化监控，实时监控、呈现各关键应用系统的实时运行状态。

数据报告

nCompass平台支持自定制的数据报告功能，同时内置常用模板以及灵活的自定义报表系统，可以按照不同客户、不同人员、不同场景实现灵活多样化的报表，同时支持按计划自动生成可归档的短期、中期、长期报告（日报、周报、月报）。

数据巡检

nCompass提供自动化的数据巡检能力，基于采集的数据，定期对数据中心进行全方位的数据巡检服务，主动发现数据中心的异常流量及隐患问题。

平台联动

nCompass平台脚本化的多平台联动能力，当数据中心出现异常事件时，可远程调用相关设备或系统，实现故障的自愈。

【nCompass 网络流量分析平台产品架构】

nCompass 系列产品以硬件内置软件的形式或单独软件部署的方式进行交付。

单独部署软件产品时，需客户提供服务器设备。

硬件设备包含 NC 系列服务器和流量探针节点设备，软件产品包含全套 nCompass 网络流量分析平台。

第三章 产品系列

智维数据的 nCompass 流量分析探针,用于实时采集分析网络流量数据包,用于数据回溯、网络故障诊断、网络质量分析、应用质量分析、趋势分析等。

- 流量分析探针具备大流量捕获能力，同时提供大容量数据存储能力。
- 最高支持 40Gbps 无损采集与实时分析，分析统计数据存入本地数据库。
- 流量分析探针具备水平扩展能力,一个集中管理端最多同时管理 20 台探针。

基于不同的用户规模，可选择不同系列的产品:

3.1 NC1000 系列

NC1000 系列面向网络流量较小的中小型用户，提供多个千兆采集接口。包括 NC1000、NC1020、NC1040 三个型号。

各型号的技术规格参数如下：

型号	数据采集能力	采集接口	储存大小
NC1000	500Mbps	2个千兆电口	4TB
NC1020	1Gbps	2个千兆电口	8TB
NC1040	2Gbps	4个千兆电口	16TB

NC1000系列服务器硬件技术规格：

类型	指标	数值
硬件规格	外形规格	1U机架式服务器
	尺寸	高42.8mm*宽482mm*长728.2mm
	重量	17.6kg
电源参数	电源	两个550W电源
	电压/频率	100～240V/50～60Hz
网络接口	管理接口	2 个千兆电口
环境参数	运行时环境温度	10° C至35° C
	非运行时环境温度	-40° C至65° C
	运行时相对湿度	10%至80%（最大露点29° C）
	非运行时相对湿度	5%至95%（最大露点33° C）

3.2 NC2000 系列

NC2000 系列面向中等规模的用户数据中心或者大规模用户的分支机构。

NC2000 系列包括 NC2040、NC2021、NC2041、NC2041-ES、NC2041-ES2 五个型号，各型号的技术规格参数如下：

型号	数据采集能力	采集接口	储存大小
NC2040	4Gbps	4个千兆电口	24TB
NC2021	6Gbps	2个万兆光口	24TB
NC2041	10Gbps	4个万兆光口	48TB
NC2041-ES	10Gbps	4个万兆光口	96TB
NC2041-ES2	10Gbps	4个万兆光口	384TB

NC2000系列服务器硬件技术规格：

类型	指标	数值
硬件规格	外形规格	2U机架式服务器
	尺寸	高86.8mm*宽434mm*长725mm 高86.8mm*宽448mm*长844.826mm (NC2041-ES、NC2041-ES2)
	重量	33.1kg，40kg(ES/ES2)
电源参数	电源	冗余双电源，1100W * 2
	电压/频率	100~240V/50~60Hz
网络接口	管理接口	2 个千兆电口
环境参数	运行时环境温度	10°C至35°C
	非运行时环境温度	-40°C至65°C
	运行时相对湿度	10%至80%（最大露点29°C）
	非运行时相对湿度	5%至95%（最大露点33°C）

3.3 NC4000 系列

NC4000 系列面向大规模用户的数据中心。NC4000 系列包括 NC4041、NC4041-ES 两个型号。

各型号技术规格参数如下：

型号	数据采集能力	采集接口	储存大小
NC4041	20Gbps	4个万兆光口	96TB
NC4041-ES	20Gbps	4个万兆光口	192TB

NC4000系列服务器硬件技术规格：

类型	指标	数值
硬件规格	外形规格	2U机架式服务器
	尺寸	高86.8mm*宽434mm*长725mm
	重量	40kg
电源参数	电源	冗余双电源，1100W * 2
	电压/频率	100～240V/50～60Hz
网络接口	管理接口	2 个千兆电口
环境参数	运行时环境温度	10°C至35°C
	非运行时环境温度	-40°C至65°C
	运行时相对湿度	10%至80%（最大露点29°C）
	非运行时相对湿度	5%至95%（最大露点33°C）

3.4 NC6000 系列

NC6000 系列面向大规模用户的数据中心核心区域、流量超过 30Gbps 的网络环境。

NC6000 系列包括 NC6041、NC6041-ES 两个型号。

各型号技术规格参数如下：

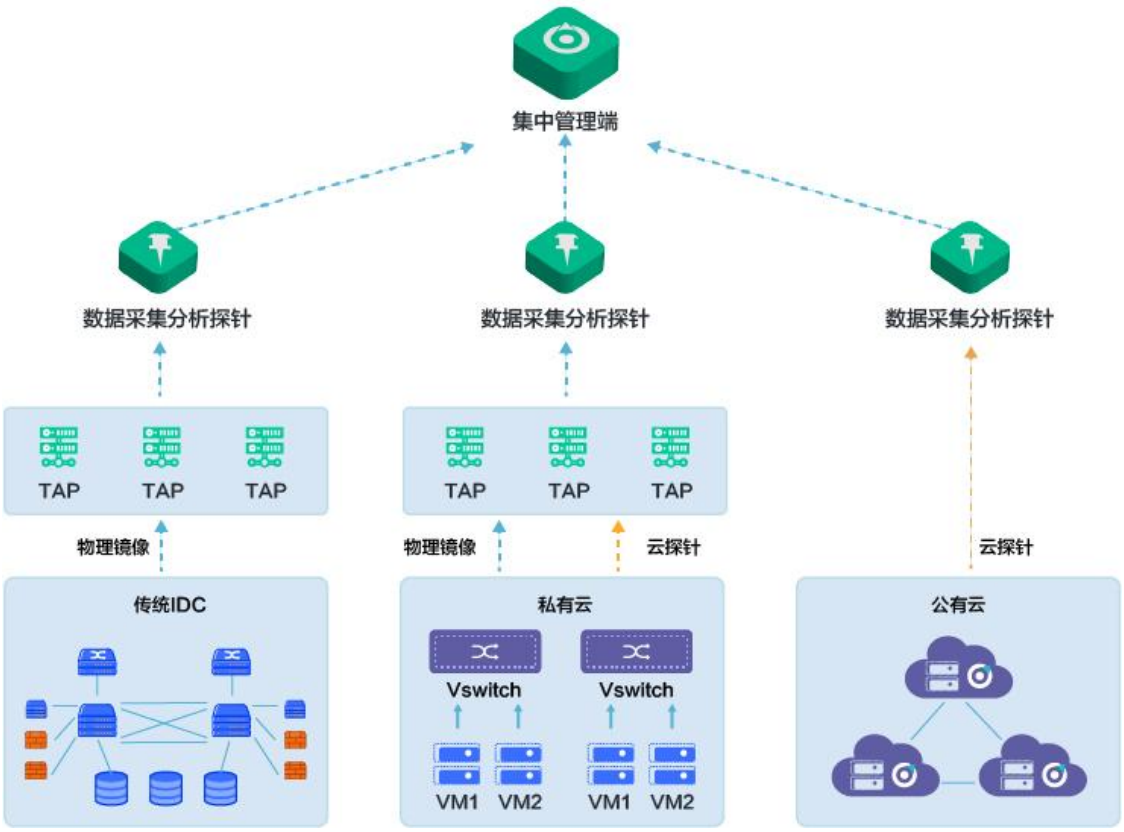
型号	数据采集能力	采集接口	储存大小
NC6041	40Gbps	2个40G MPO光口	96TB
NC6041-ES	40Gbps	2个40G MPO光口	192TB

NC6000系列服务器硬件技术规格：

类型	指标	数值
硬件规格	外形规格	2U机架式服务器
	尺寸	高86.8mm*宽448mm*长844.826mm
	重量	40kg
电源参数	电源	冗余双电源，1100W * 2
	电压/频率	100～240V/50～60Hz
网络接口	管理接口	2 个千兆电口
环境参数	运行时环境温度	10°C至35°C
	非运行时环境温度	-40°C至65°C
	运行时相对湿度	10%至80%（最大露点29°C）
	非运行时相对湿度	5%至95%（最大露点33°C）

第四章 产品部署

当 nCompass 网络流量分析平台以硬件+软件的形态部署在用户的数据中心时，基于用户数据中心环境不同，主要分为以下几种部署方式：



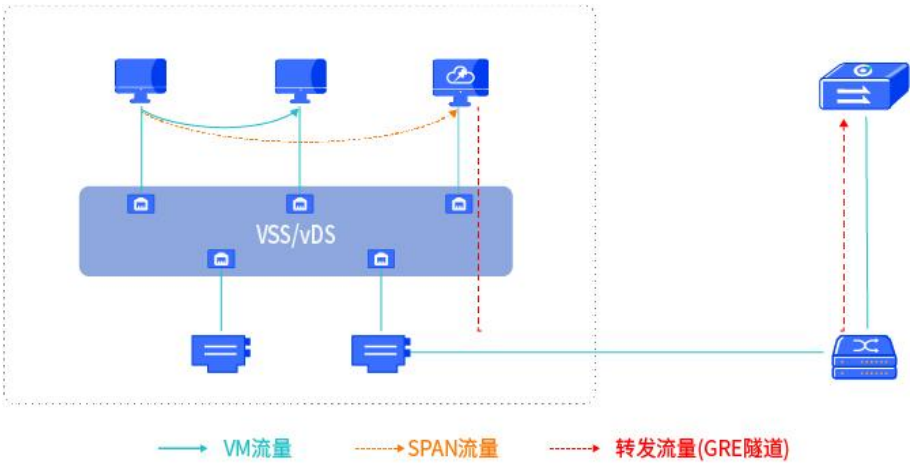
【nCompass 网络流量分析平台产品架构】

4.1 数据中心物理环境部署

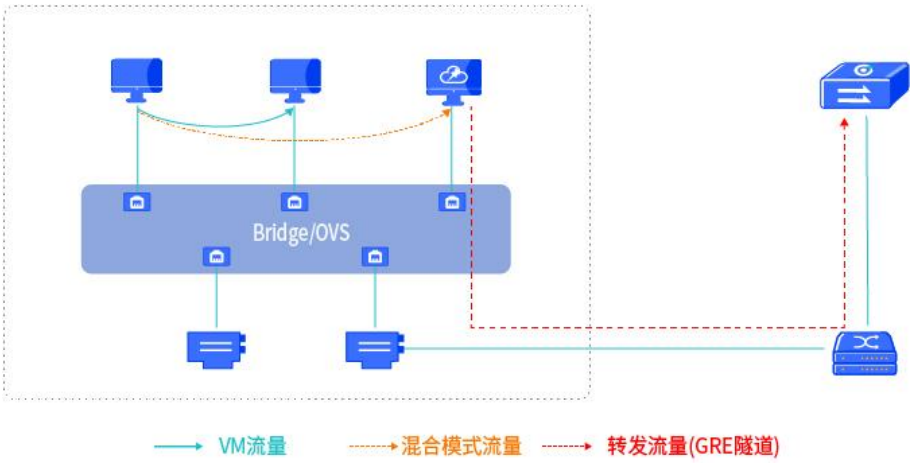
在非云化数据中心， 可以用软硬一体化设备的方式部署，通过从物理交换机获取网络流量数据并对流量进行实时分析，用于发现及分析网络中出现的异常事件。

4.2 私有云环境部署

在非云化数据中心， 可以用软硬一体化设备的方式部署，通过从物理 交换机获取网络流量数据并对流量进行实时分析，用于发现及分析网络中出现的异常事件。



【nCompass VMware 私有云环境部署架构】

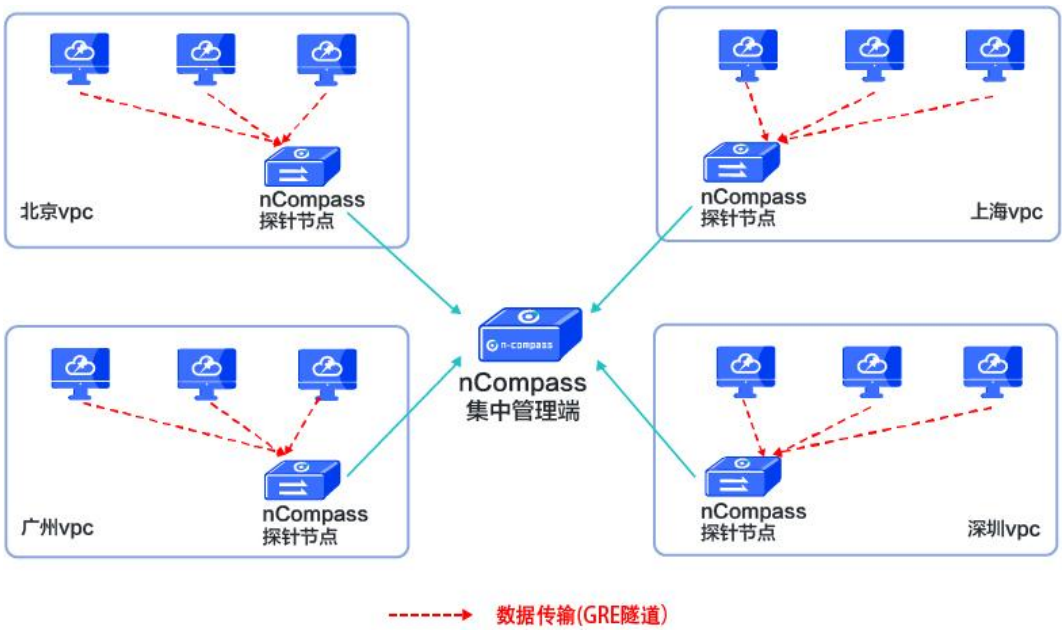


【nCompass OpenStack 私有云环境部署架构】

可部署在用户的私有云环境，不论是 VMware 还是 KVM 等私有云环境，还是 Kubernetes 容器云环境，均可通过轻量级探针或虚拟交换机采集流量数据。

4.3 公有云环境部署

当前阿里、腾讯和百度的公有云目前暂不支持流量镜像，所以公有云部署需要在每个公有云 VPC 中安装一套管理端，并在每个 VM 中安装 Agent 用于采集 VM 的流量。



【nCompass 公有云环境部署架构】

4.4 所支持的数据类型

支持网络镜像流量、Netflow、主动拨测、网络设备的访问日志、第三方平台 API 接口的时序、告警或配置数据等。

第五章 功能场景

nCompass 网络流量分析平台支持镜像流量，以及自研的 NLC 数据接入平台获取其他外部数据，比如 F5、NGINX、Zabbix、CMDB 等各种数据源，用于关联分析。核心数据源是平台采集的 NPM 数据，NPM 数据不仅可用于分析网络层指标，也支持对常用的 HTTP、HTTPS、DNS、Oracle 等提供应用层分析结果。

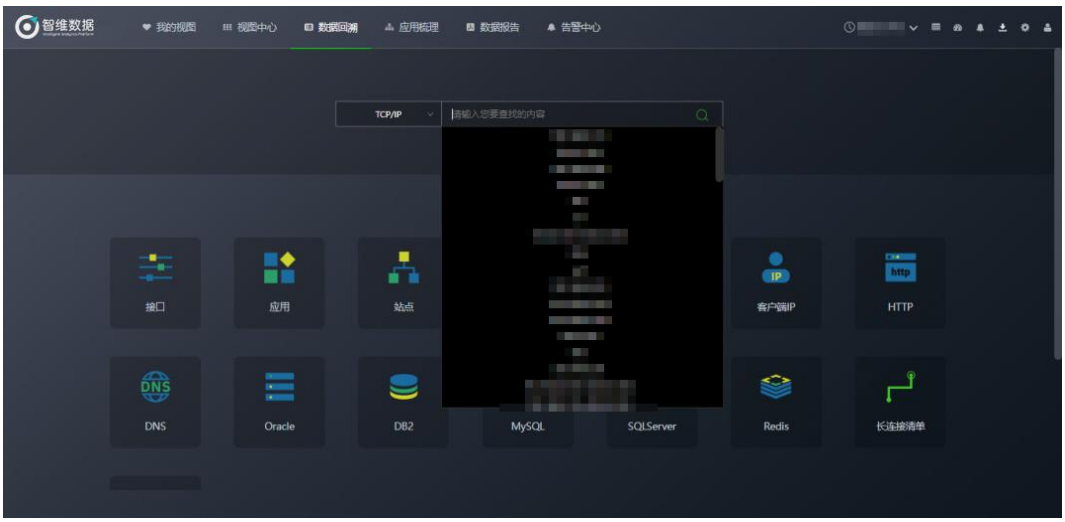
以下为 nCompass 网络流量分析平台场景功能介绍：

5.1 数据回溯

网络流量分析平台具备全面的数据回溯功能，可以对IP、通讯对、应用、站点等数据进行快速回溯分析与查看，能够回溯数据的原始数据包和解析的指标数据，平台中的数据表格能够满足用户对数据进行灵活的筛选以及快速过滤的需求，提供、编辑、下钻、筛选、排序等多种功能组件。

数据回查

网络流量分析平台可快速灵活的对数据进行检索，如 IP、应用、站点、URL 等数据，帮助用户快速查看相关对象的详细数据，并能在数据表格中进行多维扩展及下钻分析。

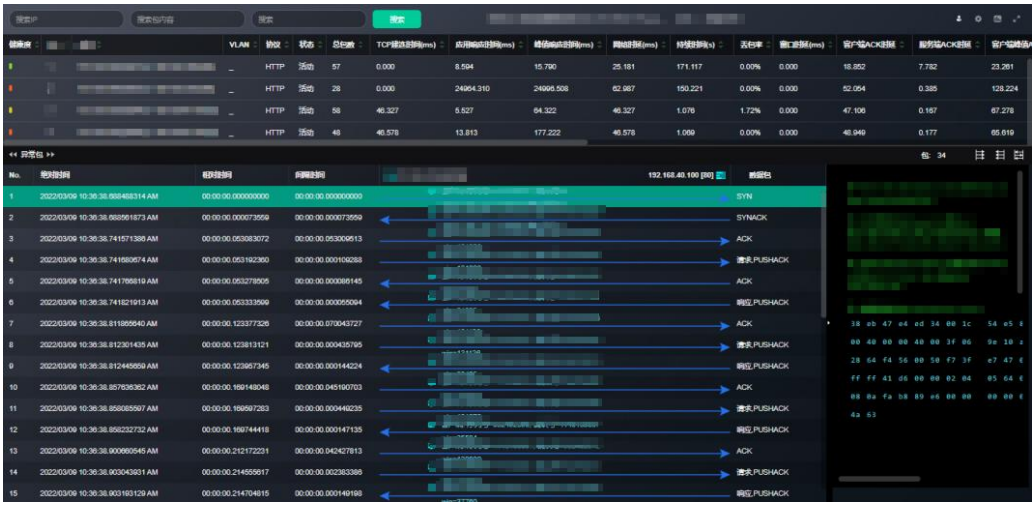


数据灵活筛选

网络流量分析平台可对数据进行灵活筛选，包括维度、指标的过滤等，并可对用户需求的复杂的条件过滤，使用维度表达式的方式进行编辑筛选，快速筛选出用户想要查看的数据信息。

数据包分析

网络流量分析平台还提供了一套在线网络数据包分析工具，用户不仅可以针对统计数据进行数据分析，也可以对原始网络数据包进行解码分析。用户可在该界面中，基于数据包 payload 中的关键词，快速找到所需分析的网络会话，如基于交易流水号、交易订单号等。



5.2 流量统计

网络流量分析平台能对获取到的流量数据进行统计分析，帮用户对数据进行筛选过滤及分析，如跨区域访问流量分析、外联防火墙前后会话关联分析、不合理的跨数据中心访问、接入层流量模型评估以及内网 CDN 可视化等。

- **跨区域访问流量分析**

数据中心中总是会出现跨网络区域的大流量访问现象，这种现象我们很难主动的发现它，如何及时主动发现并快速定位消除异常数据成为很大的难题。

网络流量分析平台通过接入数据中心流量，对 IP 地址以及网段进行配置划分，明确定义各个网络区域，最后由区域访问分析视图清晰展示不同区域访问的流量数据，清晰展示不同网络区域是否存在互访的情况，以及查看是哪些业务交互引起的、流量最大的 IP 有哪些，快速定位排查异常互访根源。

● 异常跨区域流量访问

数据中心内网本不该出现不允许的跨区域访问，如何识别这类事件，并及时验证是否是安全事件；

网络流量分析平台通过监控跨区域访问的流量数据，结合维度和指标的过滤，筛选出异常以及安全隐患事件，帮助用户对以上数据进行快速检索。

● 不合理的跨数据中心访问

用户在多个数据中心建立了多个私有云，有些业务在申请资源时申请不规范，导致很多可以在一个数据中心交互的数据跑在多个数据中心，如何发现这种情况；

网络流量分析平台通过数据表格以灵活的过滤条件，将不合理的跨数据中心访问展现出来，如某个业务在两个以上的数据中心都有流量的情况。

接入层流量模型评估

用户要实现内网 SDN，我们需要精准评估接入设备的流量情况，才好及时调整我们的 SDN 方案；

接入层通常是指网络中直接面向用户连接或访问的部分。在一般的网络结构内，接入层的流量是最多的，通常不能通过镜像的方式来采集流量。网络流量分析根据行业经验通过 NETFLOW 功能，采集对端设备的流量，可以将流量以 1:10，1:100 的比例采集接入层流量。

IPv4/IPv6 数据分析

户有众多业务上了 IPv6，上线后 IPv6 承载业务的质量和 IPv4 有无明显差异？转化率情况如何？如何建设更好的 IPv6 网络？

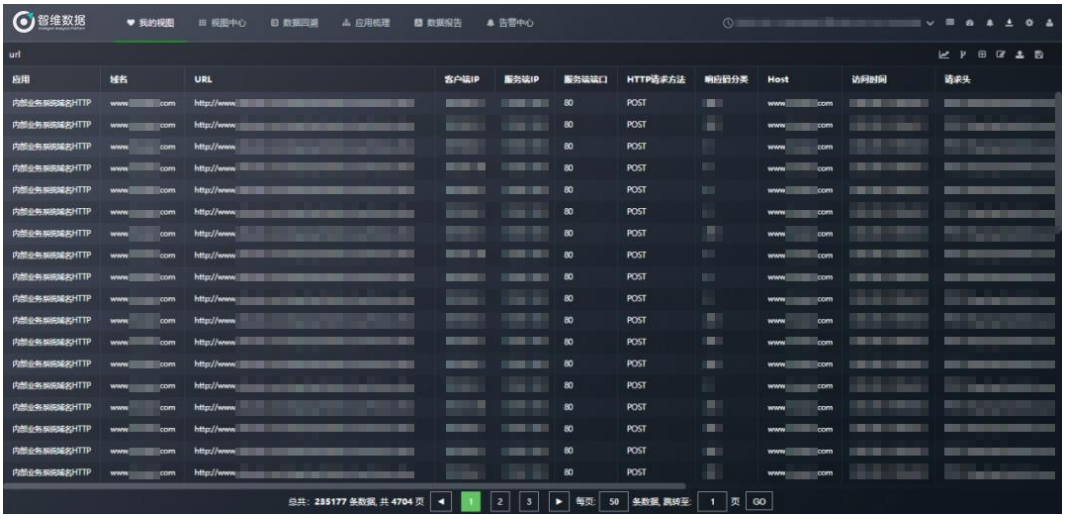
网络流量分析平台通过接入镜像流量，自动识别 IPv4 网络流量及 IPv6 网络流量，并且通过视图清晰展现出：哪些业务上线了 IPv6，哪些没上线；业务上线 IPv6 后的质量如何，以及不同省份、城市运营商业务占比情况。同时还能展现出 IPv6 网络与 IPv4 网络对比情况，帮助用户实时了解转化率情况。当发

现监控项异常时可以右键点击界面进行下钻分析，实现问题故障的快速回溯取证。

- **关键 URL 进行统计**

需要针对重要目录进行统计，例如用户登录、管理进后台、文件上传等目录。主动发现暴露在互联网的高危端口，服务目录，域名等资产；

管理流量分析平台通过监控网络流量数据，对 HTTP 数据进行解析，将业务系统按照访问行为分类，过滤出如用户登录、上传文件、暴露互联网的高危端口等行为（例如：过滤 URL 里包含 login、upload 等），最终以数据表格形式进行展示。



- **内网域名化改造**

用户部门要求内网服务器全部通过域名进行互访，如何快速找出仍然使用 IP 访问的设备？

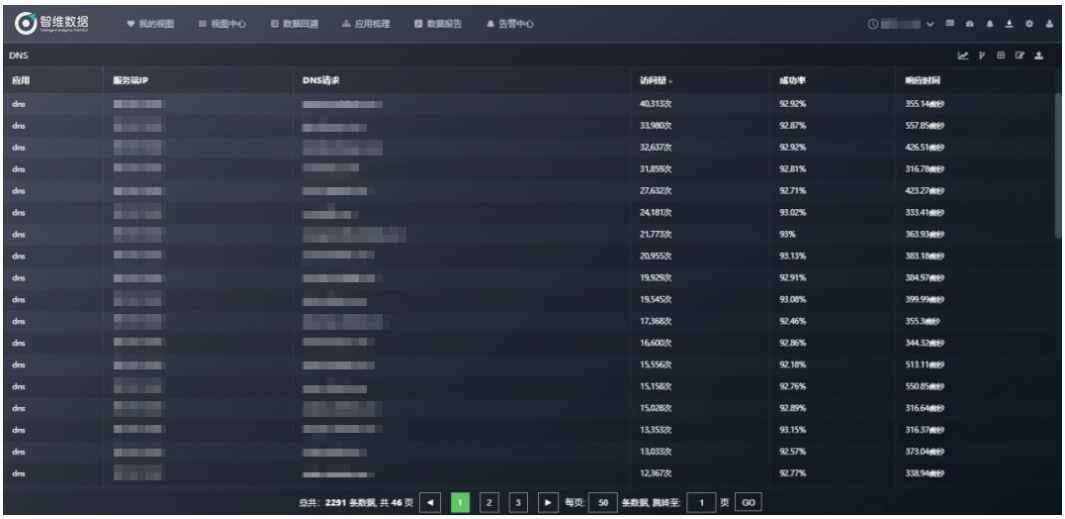
网络流量分析平台通过识别访问的 URL 中带有 IP 地址的数据，筛选出仍然使用 IP 访问的设备。

- **DNS 访问记录回溯**

用户需要记录所有用户访问 DNS 的信息，以便回溯、审计需要；

网络流量分析平台可提供全流量 DNS 访问的数据回溯，帮助用户具备了弱特征的防护能力，以及在安全事件定性过程中提供数据回溯能力，帮助用户更精

准、更高效的分析安全事件。通过数据回溯，可以查看 DNS 历史访问数据，为安全审计提供数据支撑。数据表格功能可以进行 DNS 数据回溯，可以对所有 DNS 域名访问记录进行回溯查询。



- **DNS 运营商解析不一致**

数据中心每条链路有与其对应的运营商，但有时会出现跨运营商之间进行访问的情况，这样就会造成 DNS 运营商解析不一致的错误发生。

网络流量分析平台可以通过视图的方式来展示跨运营商之间的访问，使用运营商客户端和运营商服务端等维度来展示运营商不同时，每条线路所使用的运营商，并且对链路状态等信息进行监控和数据展示。

DNS 流量调度优化

DNS 负责跨数据中心的流量调度，依赖于 DNS 设备内置的 IP 地址库，用户的 DNS 设备信息不完全准确，导致跨运营商的访问，我们需要找出这类问题，并持续优化 DNS 设备的调度策略；

当网络中存在跨运营商访问的现象，部分 DNS 服务器解析的服务端 IP 地址与真实客户端地址的运营商不一致，会导致部分跨运营商访问的用户体验较差，网络流量分析平台通过对流量数据进行 DNS 协议解码或者对于 DNS 日志信息的采集，帮助用户收集整理展示跨运营商访问的数据，可以展示跨运营商访问的总数、跨运营商解析占比、跨运营商解析的详细信息。

● 外联防火墙前后会话关联

用户有几千家商户通过外联链路接入数据中心进行业务交易，经常收到商户的投诉业务办理失败或者非常缓慢，我们需要一种手段可以自动追踪商户的交易路径并进行自动化的端到端分析，快速定位故障节点。

网络流量分析平台可以通过解析防火墙日志、缝合流量等方式对防火墙前后的会话进行关联，实现了 NAT 前后会话的动态关联，帮助用户快速查看分析防火墙前后数据。

- **内网 CDN 可视化**

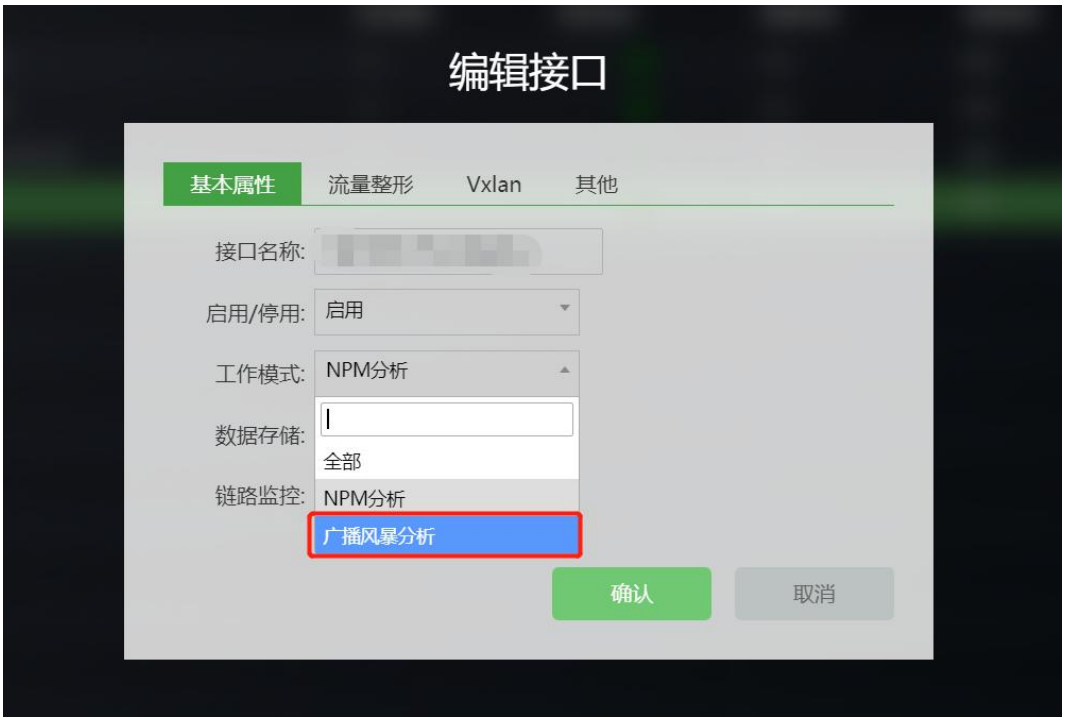
公司用了 CDN，如何评估 CDN 效果？使用了内网 CDN 站点，如何验证内网 CDN 效果？

用户增加内网 CDN 站点，变更前职场员工通过本地互联线路访问视频，变更后职场员工直接通过本地访问 CDN 获取视频。通过网络流量分析平台实时监控变更前后的用户体验和带宽的变化情况。

- **广播风暴分析**

用户网络偶发性会出现广播风暴，这种故障影响极大，如何及时识别，并能自动化解决故障，恢复业务；

网络流量分析平台根据行业经验通过设定区间指标对网络进行监控，对网络上的单播、组播、广播的包数以及广域网传输协议的各种形式的包数进行分析展示，根据展示的数据进行快速分析、及时识别异常现象，并进行快速告警通知。



5.3 网络链路质量及用量分析

网络流量分析平台对于网络链路的监控可以通过镜像流量、拨测以及 NETFLOW 的方式进行。镜像流量可进行全流量、高精度的监控，主动拨测可以监控流量时延抖动、丢包率；NETFLOW 是网络设备自带的功能，可解决远程站点监控问题，网络流量分析平台支持 NETFLOW 的版本包括：NetFlow V5、

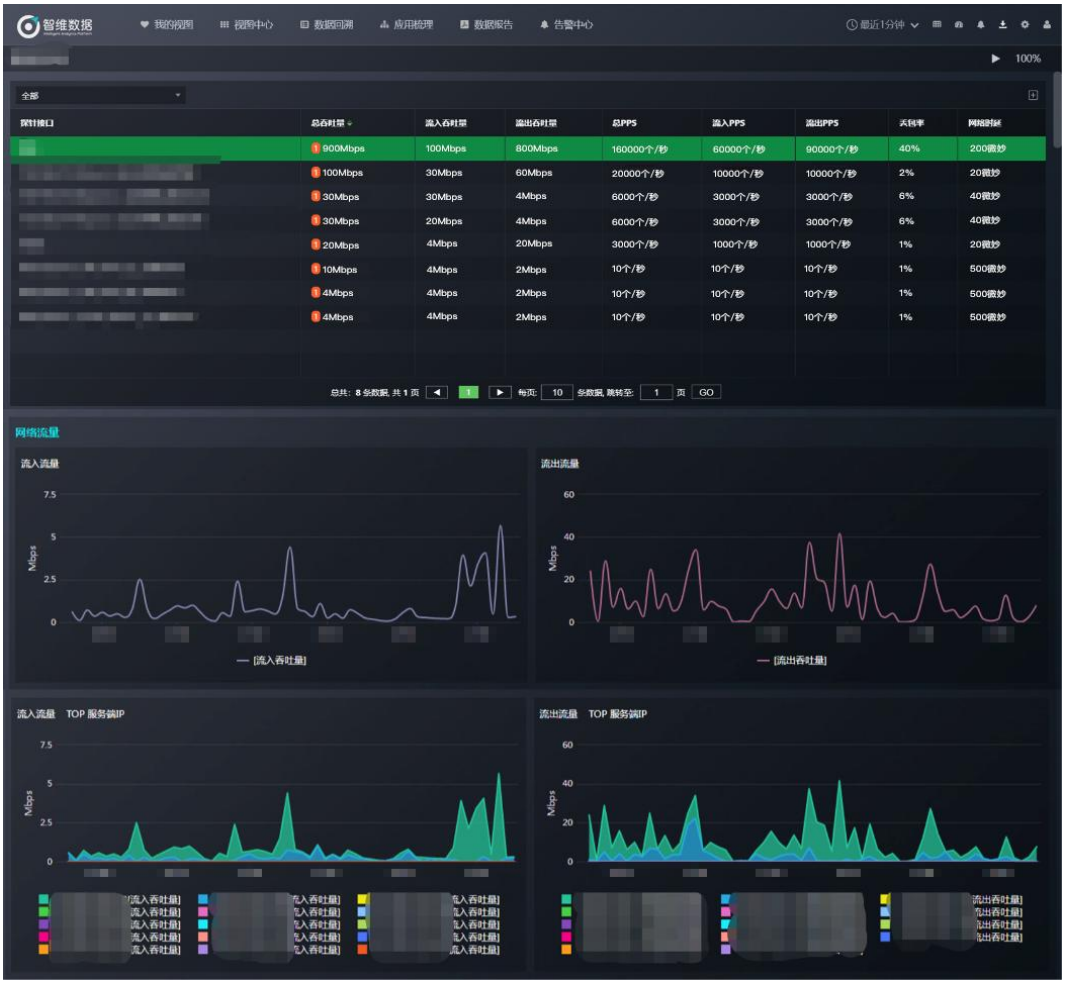
NetFlow V9、SFlow、NetStream V5、NetStream V9 版本。

- **链路用量质量监控与分析**

在实际用户环境中会出现因为业务促销、上线新业务等事件导致带宽跑满的情况，能通过网管平台得到流量突发告警，但是难以快速定位是哪个业务、哪个IP、哪个 URL 导致；通过网络流量分析平台可以快速通过视图来进行查看分析，快速查看互联网链路流量突发是由于哪个会话、访问哪个业务、哪个 URL 异常导致。

在发生因为链路严重丢包导致业务不可用的问题，如何快速定位是运营商线路问题还是数据中心设备的问题导致；在网络流量分析平台中能够通过“客户侧丢包率”、“服务侧丢包率”两个指标结合网络分析模板快速定位是数据中心内部还是运营商线路发生了严重丢包。并且结合阈值和基线也可快速告警出链路丢包问题。

视图：


智维数据
我的视图
视图中心
数据回溯
应用梳理
数据报告
告警中心
最近1分钟
100%
全部
监针接口
总吞吐量
流入吞吐量
流出吞吐量
总PPS
流入PPS
流出PPS
丢包率
网络时延
900Mbps 100Mbps 800Mbps 160000个/秒 60000个/秒 90000个/秒 40% 200微妙
100Mbps 30Mbps 60Mbps 20000个/秒 10000个/秒 10000个/秒 2% 20微妙
30Mbps 30Mbps 4Mbps 6000个/秒 3000个/秒 3000个/秒 6% 40微妙
30Mbps 20Mbps 4Mbps 6000个/秒 3000个/秒 3000个/秒 6% 40微妙
20Mbps 4Mbps 20Mbps 3000个/秒 1000个/秒 1000个/秒 1% 20微妙
10Mbps 4Mbps 2Mbps 10个/秒 10个/秒 10个/秒 1% 500微妙
4Mbps 4Mbps 2Mbps 10个/秒 10个/秒 10个/秒 1% 500微妙
4Mbps 4Mbps 2Mbps 10个/秒 10个/秒 10个/秒 1% 500微妙
总共：8 条数据, 共 1 页
每页: 10 条数据, 跳转至: 1 页 GO
网络流量
流入流量
Mbps
[流入吞吐量]
流出流量
[流出吞吐量]
流入流量 TOP 服务端IP
流出流量 TOP 服务端IP

告警：

链路-用量监控	TCP/IP	是	站点	站点流出利用率 阈值 >90% 并且 流出吞吐量 基线 上偏离 200%	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59
链路-质量监控	TCP/IP	是	站点	丢包率 阈值 >3% 并且 网络时延 阈值 >200毫秒	发送	星期一,星期二,星期三,星期四,星期五,星期六,星期日	00:00-23:59

- **链路承载业务分布与趋势变化**

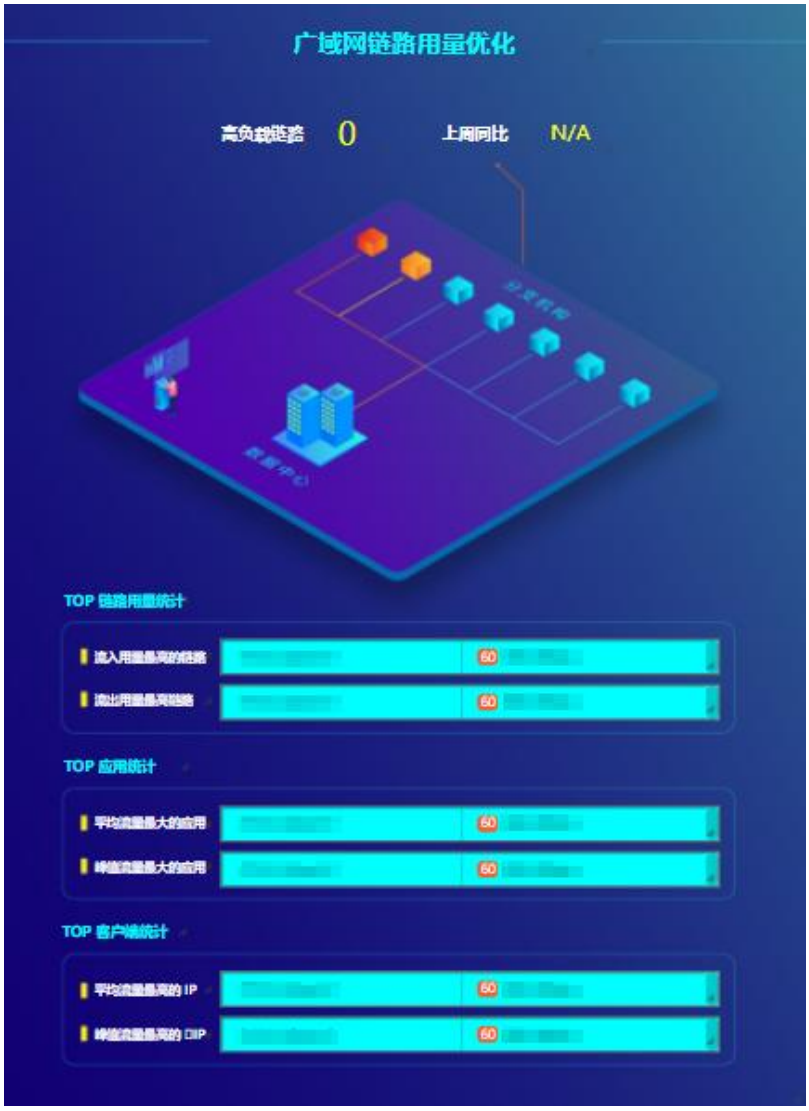
用户在链路用量报表中可以看到带宽用量持续上涨，原本 1G 的出口 3 个约上升到 1.5G。是哪个业务导致的？增长的流量是否合理？是否可以上 CDN

以节省带宽投资？通过网络流量分析平台基于流量、NETFLOW 等数据源，结合趋势变化算法及应用层分析能力，自动统计流量上涨的业务、URL、文件等关键信息。

链路带宽投资合理性规划

用户有众多的专线链路，每年带宽投入巨大，如何合理做出带宽评估及合理的投资预算？是否可以通过数据分析节省带宽投入？

网络流量分析平台能够定期统计广域网链路的带宽容量，定期进行数据报告的推送，帮助用户定期统计哪些链路的带宽长期处于跑满的状态，需要进行扩容，哪些链路的带宽长期处于闲置的状态，可以进行缩减，为广域网链路的容量规划提供数据支撑。



主动拨测+NETFLOW 实现链路监测

网络流量分析平台解决方案提供“主动+被动式”的链路质量实时监控能力。被动式监控及基于镜像链路的网络流量或 NETFLOW 的方式实现，主动式的监控则可通过网络流量分析平台主动发起拨测，来监控链路质量。两种方式相辅相成，且互相补充，可以全面的监控链路的运行状态，当链路出现拥塞、高延迟、高丢包等问题时，可第一时间发出告警通知。

- **SDWAN 链路可视化分析**

用户使用 SDWAN，但是线路数据没有手段获取，比如某些大流量的网络区域，我们不清楚流量有多大，有没有手段能获取？SDWAN 上线后，如何通过真实数据评估效果？如何保障 SDWAN 网络平稳运行；网络流量分析平台通过解码 GRE 封装，能够追溯到真实的会话，呈现实际的数据传输过程。

5.4 应用质量分析

网络流量分析平台能够对应用进行实时监控，监控应用流量的变化情况以及应用性能的状态，通过对应用层协议进行协议解析，实时分析各个协议的应用层的维度和指标，给出这些关键应用的具体指标数据，并通过监控视图和数据表格等形式一目了然的将这些数据展示出来（支持 HTTP、DNS、HTTPS、ICMP、Oracle、My Sql、SQL Server 等应用协议的解析）。

- **应用质量优化**

F5 等应用交付设备作为承载业务系统重要关卡，但是内部信息完全是不可见的，尤其是重要的业务数据以及数据内容，如果出现业务系统故障或者业务质量异常会很难判断原因；

网络流量分析平台通过获取相关业务系统的 HSL 日志配置信息。通过产品界面可以直观展示业务系统的整体运行状态以及业务系统的具体数据内容。Web 层协议系统如 http 响应码信息、http 页面大小，响应时间等；整体应用系统如 Apdex 评分，错误页面占比，大页面占比等，通过以上方式对业务系统运行在 F5 上的情况进行一个评价，清晰直观感受业务系统运行状态。

HTTP 500错误页面统计

HTTP 500错误统计，通过新增、减少、相同三个方法统计应用存在的HTTP 500错误页面。新增即上周没有，本周出现的错误页面，减少即上周有，本周没有的错误页面。相同即上周有本周也有的错误页面。

TOP 5 本周新增500错误页面

应用	HTTP响应码	URL	访问量
	500-服务器内部错误	http://*	297次
	500-服务器内部错误	http:/	6次
	500-服务器内部错误	http:/	6次
	500-服务器内部错误	http:/	5次
	500-服务器内部错误	http。	5次

*统计Top 5 本周新增的HTTP 500错误页面

HTTP 400错误页面统计

HTTP 400错误统计，通过新增、减少、相同三个方法统计应用存在的HTTP 400错误页面。新增即上周没有，本周出现的错误页面，减少即上周有，本周没有的错误页面。相同即上周有本周也有的错误页面。

TOP 新增400错误页面

应用	HTTP响应码	URL	访问量
	404-资源未找到	http:	15次
	404-资源未找到	http:/	6次
	404-资源未找到	http:/	6次
	404-资源未找到	http:/	5次
	404-资源未找到	http:/	5次

*统计Top 5 本周新增的HTTP 400错误页面

超过5秒慢页面统计

超过5秒的慢页面统计，通过新增、减少、相同三个方法统计应用存在的慢页面。新增即上周没有，本周出现的错误页面，减少即上周有，本周没有的错误页面。相同即上周有本周也有的错误页面。

TOP 新增>5秒慢页面

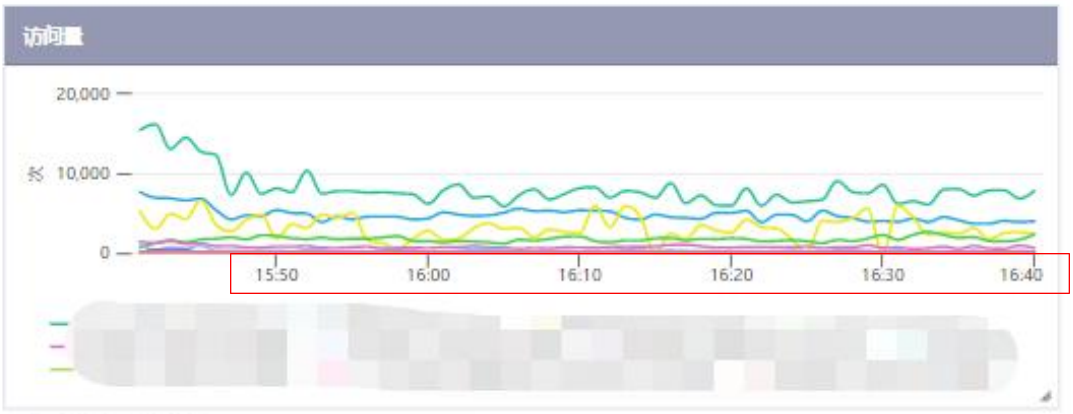
应用	URL	响应时间(>5s)次数
	http:	0次
	http:/	0次
	http:/	0次
	http://	0次
	http:/	0次

*统计Top 5 本周新增的响应时间大于5秒的慢页面

- **应用优化分析**

网络流量分析平台通过数据统计分析报表功能，可以帮助用户掌握应用的运行细节，帮助用户通过历史数据，持续的发现应用存在的隐患、为优化应用提供数据指引。Web 应用优化统计报表就是内置报表中的一种，该报表默认设置为周报，每周统计数据中心内关键 Web 应用系统的服务质量评分以及找出应用运行过程中出现的问题。

应用服务运行统计



*应用服务集群访问量趋势图

*应用服务集群成功率趋势图

*应用服务集群成功率趋势图

HTTP 业务性能优化

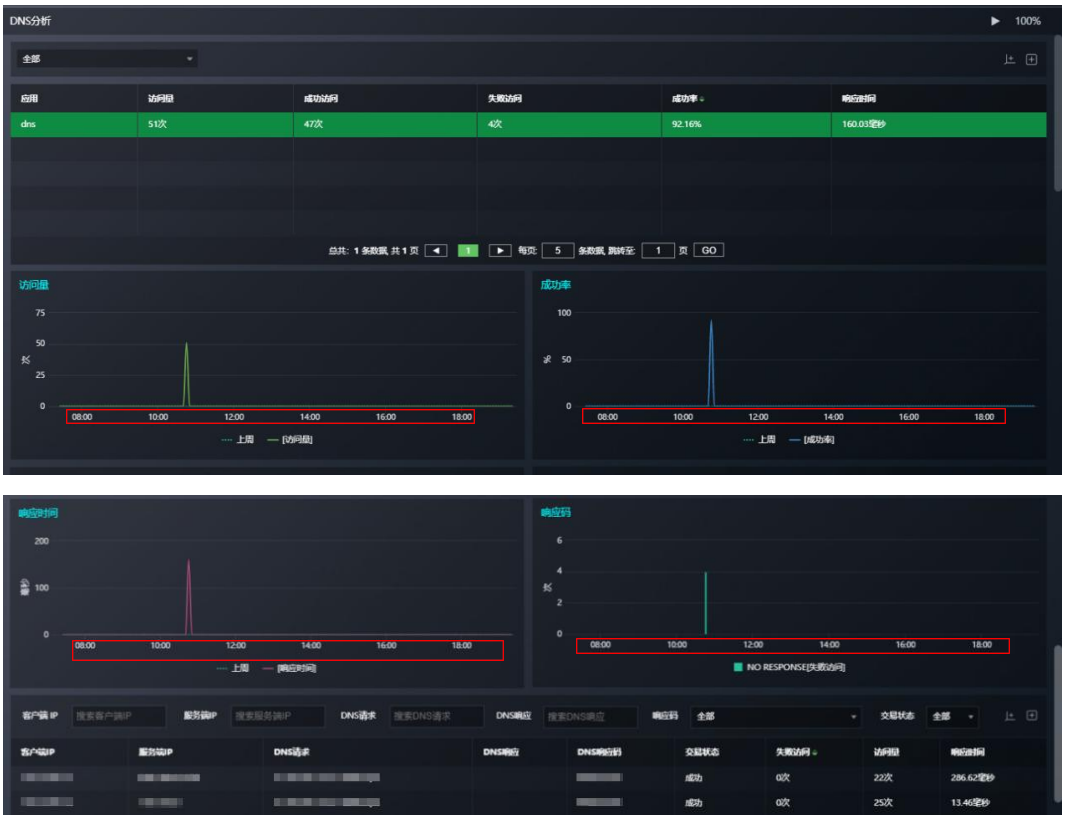
用户需要对业务进行优化，对业务了如指掌。不知道网站 QPS、以及用户分布情况等；

网络流量分析平台中有内制 HTTP 监控视图，用户可在 HTTP 分析视图中对各个应用的访问情况、客户端数量、响应时间等一些指标进行查看。同时可以对客户端数据进行数据检索、回溯，也可对其 URL 进行查看，包括访问 WEB 无法进行连接后，显示的响应码、页面文件内容的平均大小对其进行了解。用户可根据 HTTP 视图，对业务进行其优化，提高流程运行质量，满足顾客的需求。

DNS 监控分析

DNS 异常事件一直是 DNS 设备负责人关注的重要工作内容，企业每年都要投入大量的资金用于 DNS 事件排查，但是往往缺少有效的手段进行分析；

网络流量分析平台根据自己独有的算法及指标，可以统计每一条 DNS 的 DNS_TYPE、响应码、四层协议类型、成功率、访问量、访问事件等指标从而可以更更为合理的做出分析排查。



● 路由差错分析

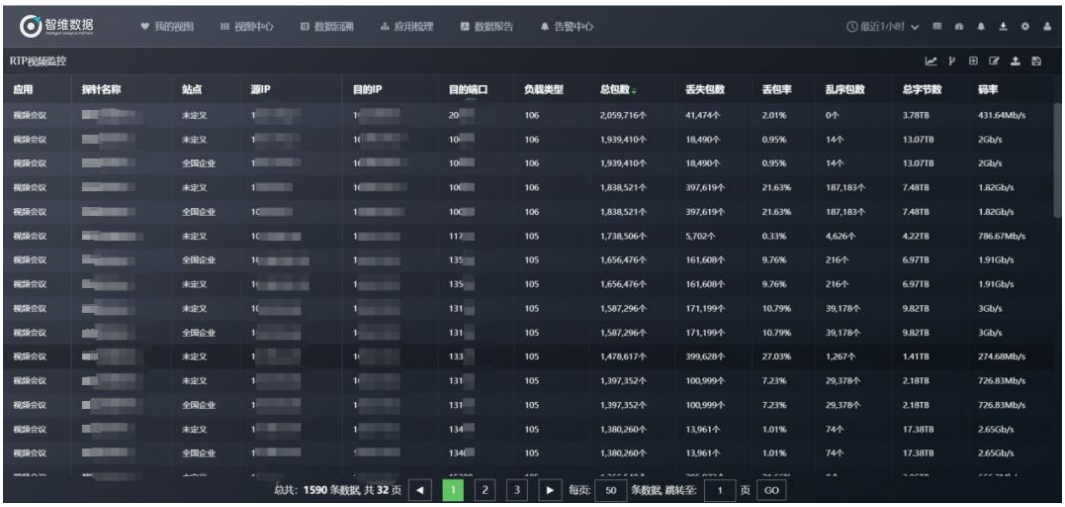
网络不通是网络运维人员经常遇到的问题，有时一个新的业务上线都会伴随着许多策略的开通。但是在变更之后经常会出现网络不通的问题，这种问题往往是由于路由问题导致的，如何快速定位路由导致网络不通的问题是运维人员非常关注的重点。

网络流量分析平台通过解析 ICMP 协议，可在视图中查看 ICMP 实时/历史运行数据，包括通告源 IP、通告源端口、通告目的 IP、通告目的端口、通告码和通告次数等。可通过通告码来快速查看时什么路由原因导致的网络不通，还可以对通告事件进行实时的告警，快速感知网络异常。

● 视频流量分析

视频会议经常遇到视频卡顿、黑屏等问题。作为网络部门，如何快速定位是否是网络传输相关原因导致的视频会议异常？

网络流量分析平台基于视频会议流量，通过完善的视频解码能力，实时监控视频会议的质量。针对视频会议异常，进行问题的分析和排查。



5.5 辅助故障定位

- **关键网络设备前后对比监控**

随着业务的不断增长，原本简单的访问关系变得越来越复杂，很多情况下故障的发生可能是由于网络设备异常导致，如何清晰的了解关键网络设备的状态，进行实时监控？

网络流量分析平台通过可视化的视图的方式，实时监控关键网络设备前后的指标变化情况，当发生异常时可以通过视图进行分析查看，并能及时发出告警通知。

- **异常事件分析模板**

网络流量分析平台内置多种分析模板，可对常见问题快速分析，将常见问题归类总结，形成根因指标；分类统计，提高趋势图，会话详单，快速洞察问题；提供排查建议，易于解决定位问题。


智维数据
我的视图
视图中心
数据回溯
应用梳理
数据报告
告警中心
最近1小时
拨测
地址
发包数
收包数
最快RTT
平均RTT
最慢RTT
丢包率
参考值
偏离度
超时次数
106,138,356,840个
117,168,156,420个
480个
480个
480个
0个
480个
下载数据包
添加维度
分析模板
复制文本
(系统)建连分析模板
(系统)SSL握手分析模板
(系统)应用分析模板
(系统)网络分析模板


7,000个
建连请求数
20%
建连失败率
700毫秒
TCP建连时间
1个
建连客户端失败
1个
建连服务端失败
0个
建连异常-SYN
0个
建连异常-SYNACK
建连客户端失败 --- 客户端引起的TCP建连失败
端口复用
0个
说明：TCP建连过程中，服务端不回SYNACK，导致建连失败
原因：1.客户端复用前面的源端口，而服务端对应的上个连接还没有断开
建议：1.检查设备连接超时配置，调整相关参数
客户端重试次数不足
0个
说明：握手不成功，需要重试3-6次，但是客户端只重试了1次
原因：客户端TCP参数配置不合理
建议：修改客户端TCP建连重试次数
建连客户端无响应
0个
说明：服务端正常回复，客户端未回应，最终建连失败
原因：1.SYNFlood 攻击 2.端口扫描
建议：检查客户端行为，屏蔽有问题的外网客户端
建连探测
0个
说明：客户端发出建连请求，服务端响应，客户端终端连接
原因：用于探测端口是否可以正常建连
建议：可以忽略
建连客户端失败-其他
1个
说明：建连过程，客户端重置了连接，但不属于已知的建连失败类型
原因：原因未明
建议：下载数据包分析

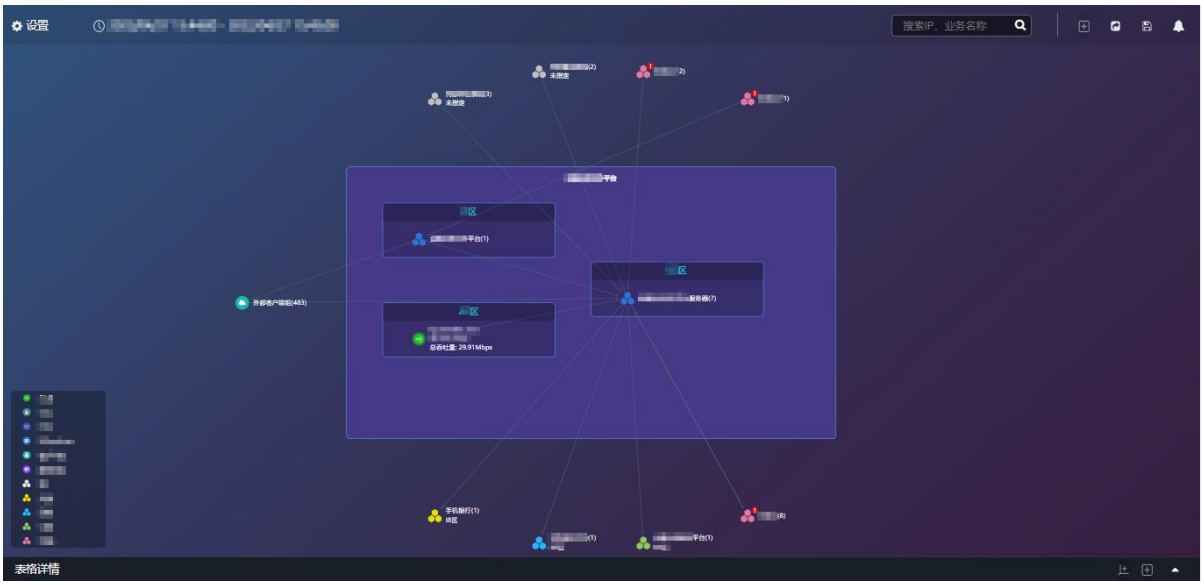

新建会话数
丢包率
TCP建连时间
应用响应时间
Client
Server
SYN
SYN ACK
ACK
Request
Data
ACK(window_size=0)
window_size update
Fin
客户端网络时延
0.843毫秒
客户端重传时延
117.684毫秒
客户端小窗口时延
4.802毫秒
服务端网络时延
40.065毫秒
网络连接时间
753.52毫秒
首包时间
151.76毫秒
应用响应时间
163.814毫秒
服务端重传时延
81.027毫秒
服务端小窗口时延
0毫秒
拆连超时次数
165个
性能时延构成图
应用负载
网络性能

5.6 业务访问关系梳理

- **业务梳理**

大部分业务人员只知道自己的业务模块依赖哪些业务模块，但很少清楚都有哪些模块是紧紧依赖我的；在版本升级、机房迁移等场景很难快速做出判断；如何确认机房迁移前后业务访问关系没有放生变化，依然能够正常工作。

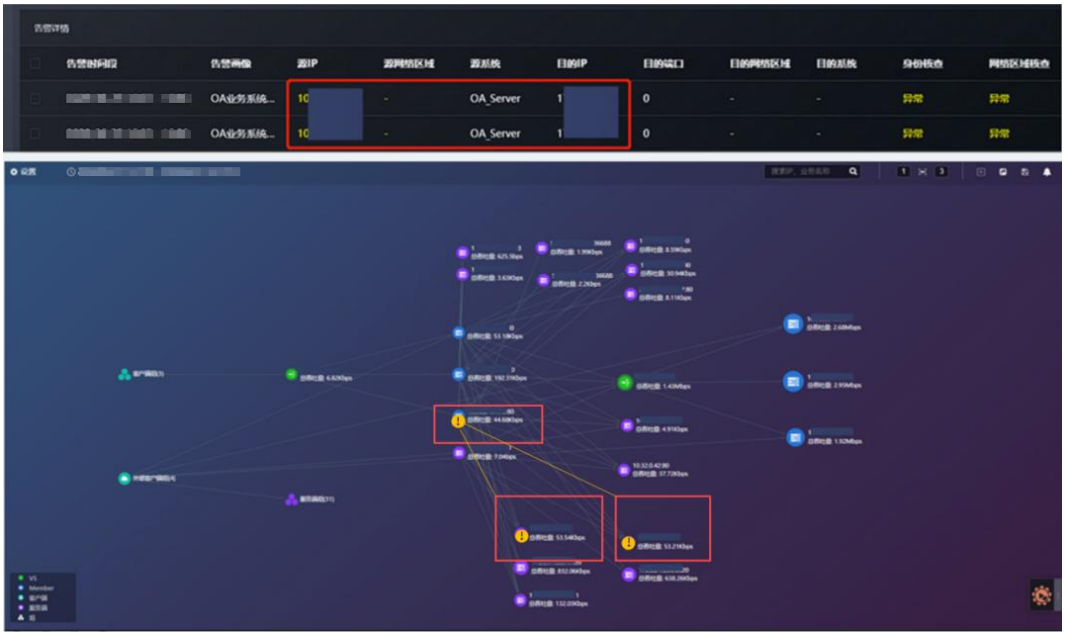
网络流量分析平台，获取到 CMDB 信息后，再结合特定的应用梳理模块，呈现出真实的业务访问关系，能够快速发现依赖自己的业务，得到该业务名称及 IP 以及所属区域，轻松解决用户需求。



● 内网异常访问识别

大部分企业重边界轻内网，边界失守，内网防护手段相对薄弱，渗透手段越来越高级，特征越来越难以识别；

网络流量分析平台可以根据自身的业务梳理功能清晰展示各个节点之间的前后访问关系，客户可以选择业务访问比较正常的时间段来作为基准画像，然后可以根据此张基准画像来定义监控策略，对来访或者是减少访问的 IP 进行身份、网络区域、服务端口和异常行为的检查。客户也可以在定义基准画像时添加白名单和黑名单，对不重要或重点关注的 IP 进行过滤，从而发出告警，帮助用户快速查找并定位异常访问 IP。

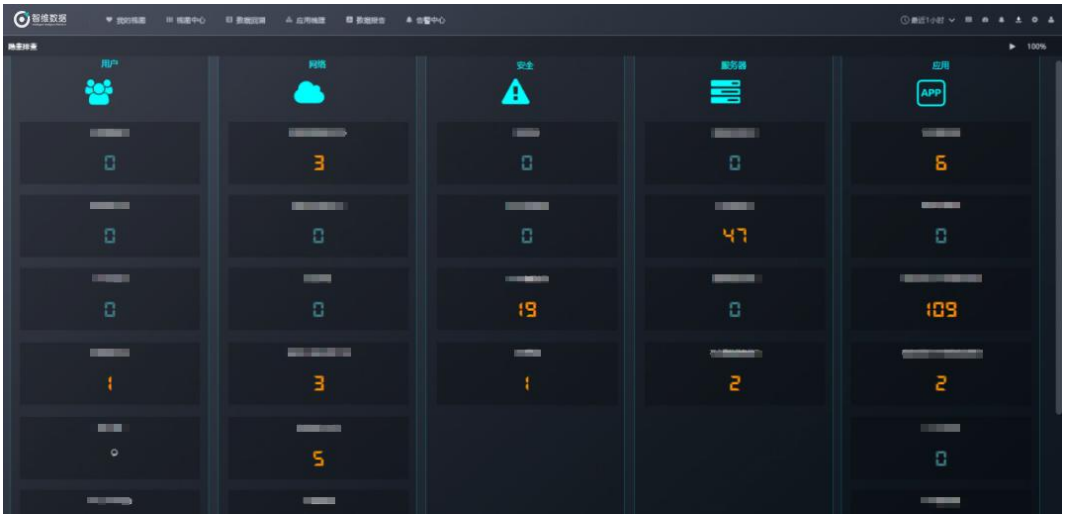


5.7 安全辅助

- **隐患分析**

公司内部有许多网络区域，每个区域的安全问题往往都是被网络运维人员重点关注的。是否可以通过流量数据帮助其发现存在的安全隐患问题？

根据行业经验提供业内独有的数据指标，从用户、网络、安全、服务器、应用五个层面出发，分别展示这 5 个层面的隐患信息。通过统计当前各个层面存在的隐患条目数，为及时知悉并做出处理提供数据支撑，从而更好的保障整体网络的安全性和可用性。



- **合规访问**

现在越来越重视合规访问，领导要求：“针对内网绕过审计，访问 22、3389 等高危端口的访问事件进行监控；

网络流量分析平台通过常用的“数据表格”功能，就能够发现访问高危端口的信息。在编辑表格时，可以确认高危端口有哪些，可以对允许访问高危端口的主机进行过滤，可以显示访问高危端口主机地址、时间点、访问次数等，通过数据表格能够灵活展现访问端口的信息。

- **未知资产梳理**

与 CMDB 集成，识别未知资产。消除隐患，提高 CMDB 资产的完善程度；

基于流量和 CMDB 资产数据，自动检测未知资产、新增和减少资产，完善资产数据内容。

- **终端违规配置 DNS**

要求所有用户使用指定内部 Local DNS 上网，所以理论上只有 Local DNS 为源地址对外部 DNS 发起 DNS 请求，有些用户会自己配公网 DNS 发起违规访问，需要排查这种违规问题，找出是哪个 IP 地址；

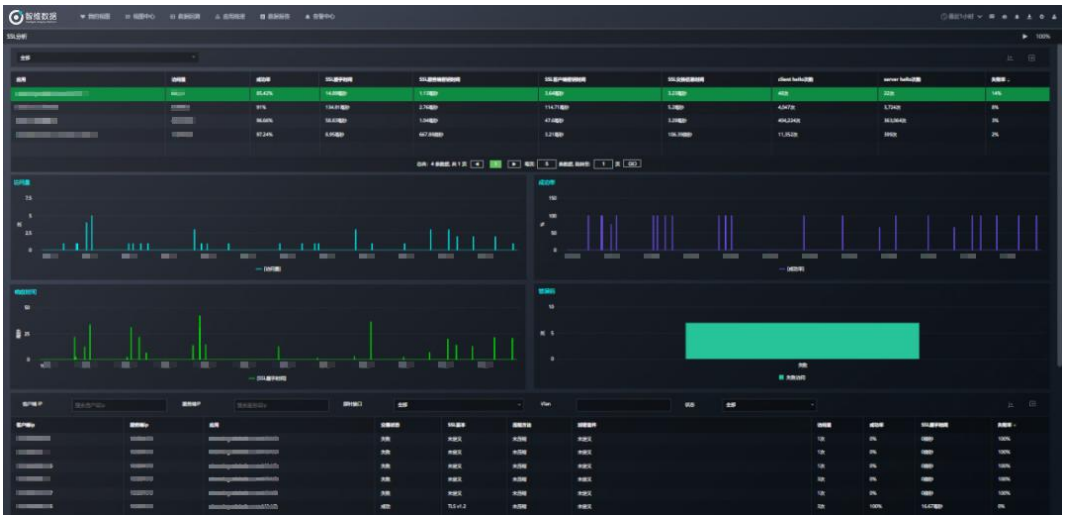
网络流量分析平台根据行业经验通过多维度、指标的灵活筛选，可以找出通过配置公网 DNS 域名服务器发起违规访问的客户端 IP 地址。实时发现违规终端和违规访问的域名。

- **加密协议识别**

网络流量分析平台能够基于流量数据，集中展示 SSL 失败比率和失败原因。结合智能基线和趋势变化算法，对异常增高的 SSL 失败率进行预警，及时发现业务故障。

网络流量分析平台能够基于配置信息和流量数据，获取并集中展示所支持的 SSL 版本和算法列表。针对风险版本和弱算法，提供安全整改建议。

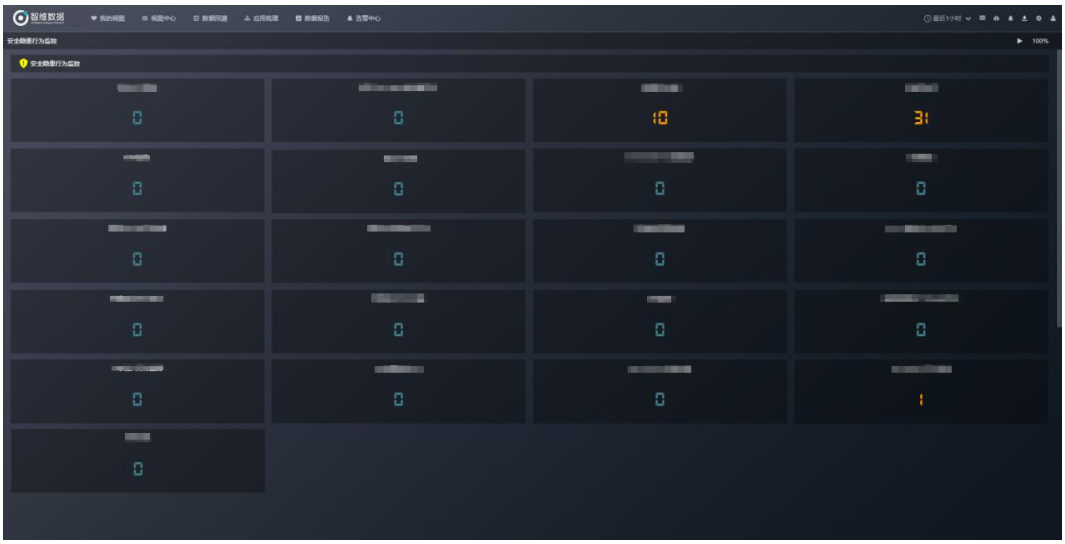
网络流量分析平台能够基于配置信息和流量数据，通过 SSL 握手交互过程，对比配置中支持算法列表与流量中握手完成的算法列表。提供安全整改建议。



- **攻击溯源取证分析**

网络流量分析平台内置的行为监测引擎及全网流量回溯能力，帮助用户具备

了弱特征的防护能力及在安全事件定性过程中，提供数据回溯能力，帮助用户更精准、更高效的分析安全事件。



第六章 产品优势与价值

nCompass 网络流量分析平台独创了流量数据采集、策略检索、AI 算法、知识图谱、可视化一体化平台，是国内率先实现全流量数据源采集分析的大数据平台。通过大量行业头部客户场景研究及模型训练，nCompass 形成了独有智能算法与知识图谱，是业界唯一能直接给出用户异常检测结果和处置方案的产品。

平台技术优势如下：

多源数据整合：支持网络流量、设备日志、应用日志、NetFlow、NetStream、sFlow数据的接入处理，为智能分析、应用画像提供丰富的元数据。也可以对接CMDB，应用性能管理（APM），自动化等运维管理平台，搭建运维数据中台。

故障快速定位：结合多种AI算法计算出的智能基线结合智能分析产品可以快速的进行故障的根因诊断，评估流量趋势、确定性能瓶颈。

多平台灵活可选：为客户提供软件或软硬一体化多种产品方案。单台处理性能从1Gbps到40Gbps的网络流量可选择。

灵活的自定义配置界面：除了内置的上百种大屏视图，也可以通过拖拽图形完成展示的视图内容，如编写PPT一样便捷高效。引以为傲的数据表格功能可以根据用户实际需求进行多维度的过滤展现，关键数据指标一目了然，便于快速分析定位问题。

应用代理前后端数据整合：通过对接设备日志以及前后端流量，网络映射关系可精确到Session级别的数据缝合，无论应用代理前后端做了NAT还是PAT，都可以快速的把前后端每个链接对应起来结合数据快速定位故障点，提升可视化能力，解决网络映射引起的管理盲点。

第七章 公司介绍

智维数据，全称是北京智维盈讯网络科技有限公司，成立于 2015 年，智维数据是一家使用全新智能分析软件技术,改变企业对网络流量数据的消费场景，提升用户在 IT 网络运维及安全上的响应能力的企业服务公司，致力于打造技术领先的智能流量数据分析平台。

核心产品 **nCompass 网络流量分析平台**可以接纳流量，Traffic log 等各种数据源，通过规则引擎进行动态数据分析与展现，通过流数据采集，策略检索，AI 智能算法，知识图谱，可视化一体化平台，帮助用户清晰了解流量中应用及业务流的不同维度的状态，将故障与隐患在从事后排障提升到了事中预警，为用户实现机器的问题机器处理，帮助用户快速提升智能运维、安全、业务数据分析的能力、效率和准确性。

该能力已经被全球领导厂商和各行业头部企业认可并完成数据对接与合作。公司从 15 年成立至今，服务于金融、电力、医疗、政企、互联网等多行业，服务客户包含中国银行 、民生银行、浦发银行、华夏银行、中信证券、中国人寿、银联商务、中金集团、中石油、中石化、国家电网、中国联通、中山医院、海尔集团、上海韵达等，累计合作头部客户超过百余家，得到客户的一致认可。


中国银行 BANK OF CHINA
招商银行 CHINA MERCHANTS BANK
中国民生银行 CHINA MINSHENG BANK
华夏银行 HUAXIA BANK
中信银行 CHINA CITIC BANK
浦发银行 SPD BANK
国家开发银行 CHINA DEVELOPMENT BANK
中原银行 ZHONGYUAN BANK
江苏银行 BANK OF JIANGSU
郑州银行 BANK OF ZHENGZHOU
大连银行 BANK OF DALIAN
厦门银行 Xiamen Bank
宁夏银行 BANK OF NINGXIA
山东城商行合作联盟 Shandong City Commercial Banks Alliance
BEA東亞銀行
银联商务 ChinaUMS
CICC 中金公司
中信证券 CITIC SECURITIES
平安证券
宏信证券 HONGXIN SECURITIES
新时代证券 New Times Securities
中国人寿财产保险股份有限公司 China Life Property & Casualty Insurance Company Limited
中国太平 CHINA TAIPING
嘉实基金 Harvest Fund
易方达
国家信息中心 国家电子政务外网管理中心
新华社 XINHUA NEWS AGENCY
人民网 people.cn
国家税务总局 State Taxation Administration
教育部考试中心 National Education Examinations Authority
中国石油
SINOPEC
国家电网 STATE GRID
中国南方电网 CHINA SOUTHERN POWER GRID
ENN 新奥
中国铁路总公司 CHINA RAILWAY
北京中科院软件中心有限公司 Software Engineering Center Chinese Academy of Sciences
郑州地铁 ZHENGZHOU METRO
市政交通一卡通
中华人民共和国福州海关 FUZHOU CUSTOMS DISTRICT P.R.CHINA
China unicom 中国联通
国美云服 gyun.com
Haier 海尔
韵达 EXPRESS
oppo
上海大众动力总成有限公司
sina 新浪
HITACHI 日立 Inspire the Next
TOYOTA

第八章 nCompass 产品系列

作为国内**率先实现全流量数据源智能分析的大数据公司，智维数据以流量数据作为切入点，结合日志、配置、CMDB、拨测、Netflow、Telemetry 等多种数据源，通过系统内置的 AI 算法库，分析海量运维数据，准确发现问题，进而从决策层面进一步提高运维效率。**从根本上改变了传统 IT 运维管理依靠工具+人工经验的模式，为服务企业提升数据挖掘及应用创新能力。

智维数据的产品系列可服务网络、安全、应用、业务等多类别场景。

nCompass 产品系列

第九章 联系我们

北京总部：

地址：北京市朝阳区八里庄西里 99 号住邦 2000 二号楼 807

电话：400-666-8216

上海办事处：

地址：上海市静安区大宁中心广场三期灵石路 718 号 A7202

电话：400-666-8216

广州办事处：

地址：广州市天河区天河北 906 号高科大厦 A 座 1906

电话：400-666-8216

深圳办事处：

地址：深圳市南山区高新科技园南十二路九洲电器大厦 B 座 3 层 F 室

电话：400-666-8216

公司网址：

www.ncmps.com

邮箱：

技术支持：support@ncmps.com

市场或合作渠道：marketing@ncmps.com