神州灵云
DCLINGCLOUD

NetSensor 网络应用智能分析系统

技术白皮书

目录

1 前言

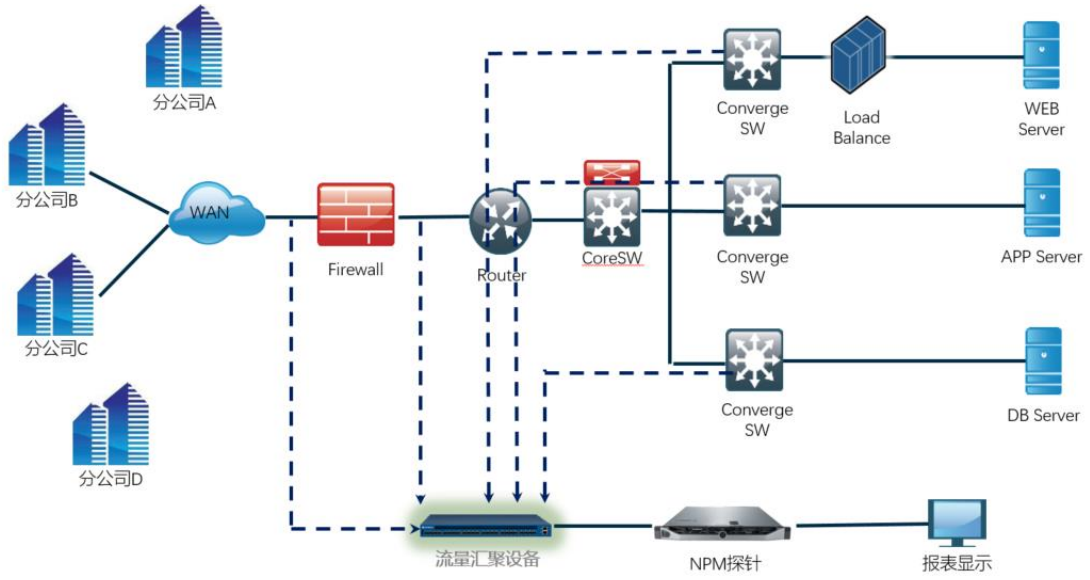
当今企业的 IT 运行环境正面临着一系列的重大变化，随着云计算时代的到来，企业的 IT 主管们都将注意力放到了服务器虚拟化、数据中心整合和基于 Web 的应用这些新技术的运用上；同时这些新兴的 IT 技术也在不断改变着企业的 IT 环境。

一个企业数据中心的核心交换机的流量上可能包含了成百上千个应用，而且每种应用所采用的协议格式也不尽相同。对于数目庞大，交互复杂的应用，IT 运维实际上无法做到对每一个应用都进行具体关注。通常 IT 的做法是从网络流量的视角去监控所有应用的整体性能，或者是重点关注某些关键应用服务器的流量，这种基于流量的分析在绝大部分情况下是无法反应出应用的运行状况。例如，防火墙的上的连接数到达上限，新建连接将被重置，造成客户端有时连接不上的故障。如果从流量的角度去看这个问题，应用的流量不会出现明显的增加，所以问题无法得到及时发现和定位。

NetSensor 网络智能分析系统将端到端应用程序交付相关性方面的可见性与网络行为分析相结合，来解决这一管理方面的差距。NetSensor 网络智能分析系统可以分析应用每一跳路径上 TCP 层的行为或者是某个核心节点上的所有基于 TCP 的应用的行为，并且在出现故障的时候及时发现问题和定位问题，从而为 IT 的运维保障提供手段。

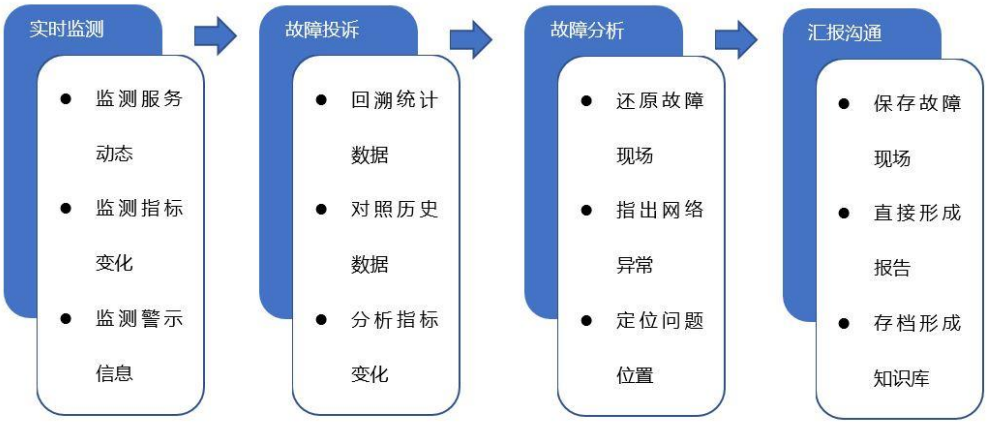
2 部署示意

NPM“网络探针”工作原理是对网络中的“真实生产数据”进行分析，从交换机的镜像端口获取原始流量。对复杂网路系统的监测，需要在业务路径上的多个重要节点进行监测分析，因此可能引入 TAP，将各节点的数据进行合并以后，统一送到监测探针进行分析。 通常的情况下，NPM 监测分析系统的部署方式如下图：



其中网络探针负责对原始流量进行分析 客户可通过 WEB 客户端报表服务器查看数据。旁路监控不会影响生产环境，一台探针可以监控多个网段，部署方便灵活，成为网络应用性能监控的首选方案。

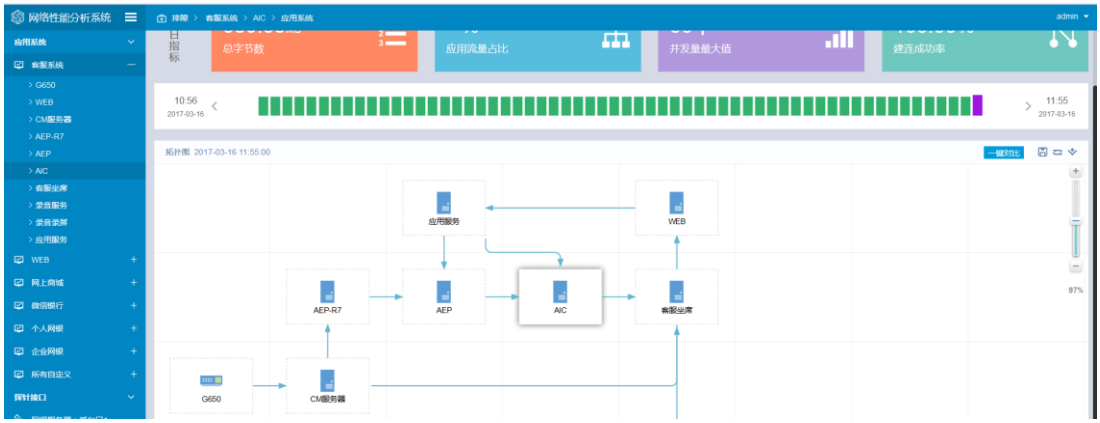
3 核心功能



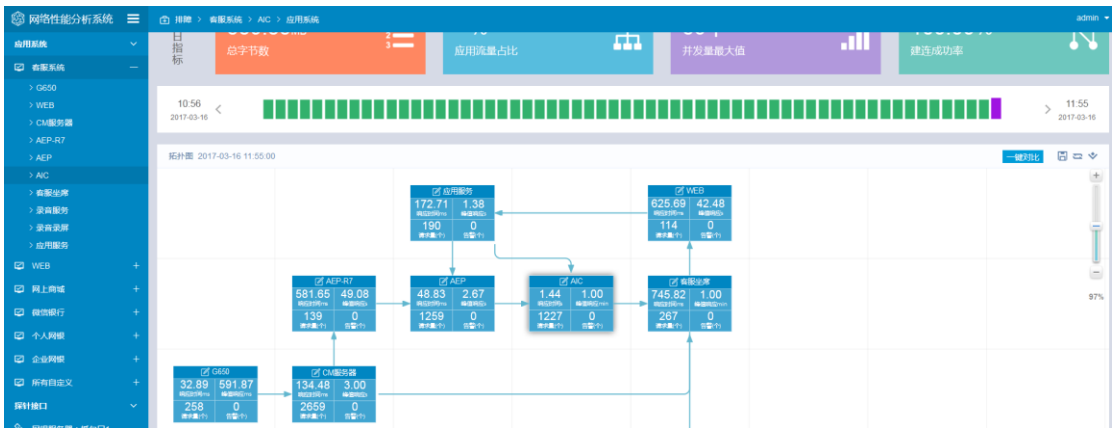
3.1 实时监控

实时监控关键业务群的网络性能指标，一旦业务出现告警，出现告警的那个时间段马上变红，用户可以点击告警发生的时间点，进行深入分析。

根据用户的网络情况自定义网络拓扑图。例如，下图是一个企业网银应用的逻辑拓扑结构，通过对多个交换机（一般是大核心和区域核心）的镜像流量分析，可以实现内部网络端到端的实时监控。



用户定义完拓扑以后，可以在界面上看到该拓扑的实时网络性能指标。



3.2 故障排查

我们遵循从 KPI 到单个会话，再到原始数据包的“三步走”故障排查思路，化繁为简，快速定位问题。

3.2.1 KPI

我们将主要的参考 KPI 分为网络负载，性能和可用性三大类。

- **负载量分析**

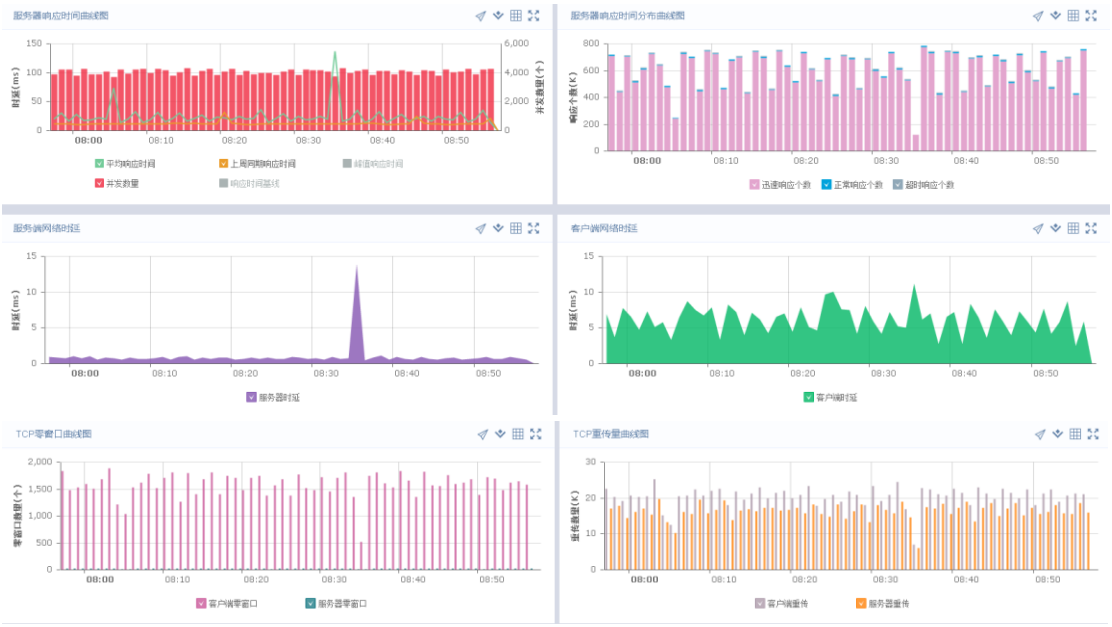
通过流量曲线图、客户端数量曲线图、并发量曲线图和包总数曲线图来刻画该分析点的网络负载情况。特别地，客户端数量和并发量 KPI 对于分析防火墙相关问题非常有意义。

- **性能分析**

TCP 的重传数量和 TCP 零窗口数量是表征网络性能的最具代表性的 KPI。超时重传是 TCP 协议保证数据可靠性的另一个重要机制，其原理是在发送某一个数据以后就开启一个

计时器，在一定时间内如果没有得到发送的数据报的 ACK 报文，那么就重新发送数据，直到发送成功为止。通常情况下，重传的严重情况反映了网络的拥塞状况。如果网络中有大量的重传，会导致应用响应慢甚至超时。

滑动窗口协议，是 TCP 使用的一种流量控制方法。该协议允许发送方在停止并等待确认前可以连续发送多个分组。由于发送方不必每发一个分组就停下来等待确认，因此该协议可以加速数据的传输。一旦 TCP 的通告窗口下降到 0（即，零窗口事件出现），则表示出现零窗口方（客户端或者是服务器）无法进一步接收数据，需要等待一段时间后继续接收。这意味着网络的传输效率的下降，同时也意味着出现零窗口方的处理能力跟不上对方的发送速率。



- **可用性分析**

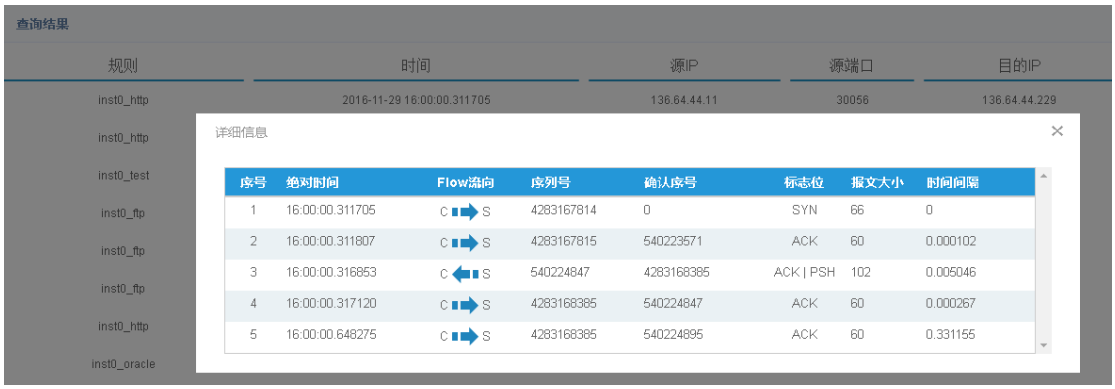
通过 TCP SYN 包数量（区分客户端 SYN 和服务器 SYN), TCP FIN 包数量, TCP Rest 包数和 TCP 建连成功失败次数来刻画该分析点的网络可用性情况。尤其是 TCP 建连的成功和失败对比，可以非常有效直观的反应网络是否存在问题。一旦发现建连失败比率很高，可以通过 NetSensor 特有的建连分析功能，快速定位到出问题的服务器或者是客户端。

3.2.2 详单分析

当在 KPI 的图表中发现指标异常，就可以进一步深入钻取，找到出问题的哪几个会话。在会话详单中，我们保留了客户端 IP，客户端端口，服务器 IP 和服务器端口以及针对这个特定会话的所有 KPI 指标。从而使得问题能够进一步缩小范围到一个或少量几个会话。

全选

应用	时间	源地址	目的地址	目的端口	服务器响应时间(ms)	服务器峰值响应时间(ms)
inst0_9080	2016-11-29 16:00:00	136.64.44.252	136.74.100.60	9080	0.000	0.000
inst0_9080	2016-11-29 16:00:00	136.64.44.253	136.74.100.59	9080	0.000	0.000
inst0_9080	2016-11-29 16:00:00	136.64.44.253	136.74.100.60	9080	0.000	0.000
inst0_9080	2016-11-29 16:00:00	136.64.44.252	136.74.100.59	9080	0.000	0.000
inst0_test	2016-11-29 16:00:00	192.168.1.12	192.168.1.11	61021	3588.034	3987.638



3.2.3 原始数据包

通过详单分析我们已经可以定位出问题的客户端、服务器以及问题发生的具体时间点。一般通过多段的 KPI 对比就可以定位问题出在哪个设备上。要进一步揭示问题的根本原因，或者再深入分析问题的本质，那么对原始数据包进行提取并进行解码分析。NetSensor 提

供了丰富易用的过滤器，可供用户快速提出故障证据—原始数据包。

支持各种过滤条件以及过滤条件的组合

3.3 智能预警

NetSensor 网络性能分析系统可以针对主要的 KPI 进行告警设置，一旦超过阀值或者基线就会产生告警，同时实时监控的拓扑图中该指标的颜色也会变红，以提醒用户注意。告警可以通过邮件、SNMP Trap 或者是 Syslog 形式发送给管理员。

传统的基于阈值的告警并不能够准确地反映网络中的异常，特别当网络环境发生变化时（并非恶化），阈值告警通常会产生大量的误报，造成管理成本的上升。针对这一问题，NetSensor 采用了独特的智能基线告警算法，可以更加准确地对应用和网络异常进行预警。NetSensor 的基线计算采用周期性基线算法和非周期性基线算法：

周期性基线对比的是同一业务时间过去四周的表现，适用于 KPI 随着业务时间不同而不同的情况，例如：交易量，流量。

非周期性基线是所有历史数据的平均，适用于 KPI 稳定的情况，例如：响应时间，重传率。

例如：在上图中，周期性告警指标有流量和请求量，选择后一般在算法 b 中设置 5 分钟内 4 次超过基线阈值则告警；另外还有触发阈值，可以依照经验设置。只有当算法和触

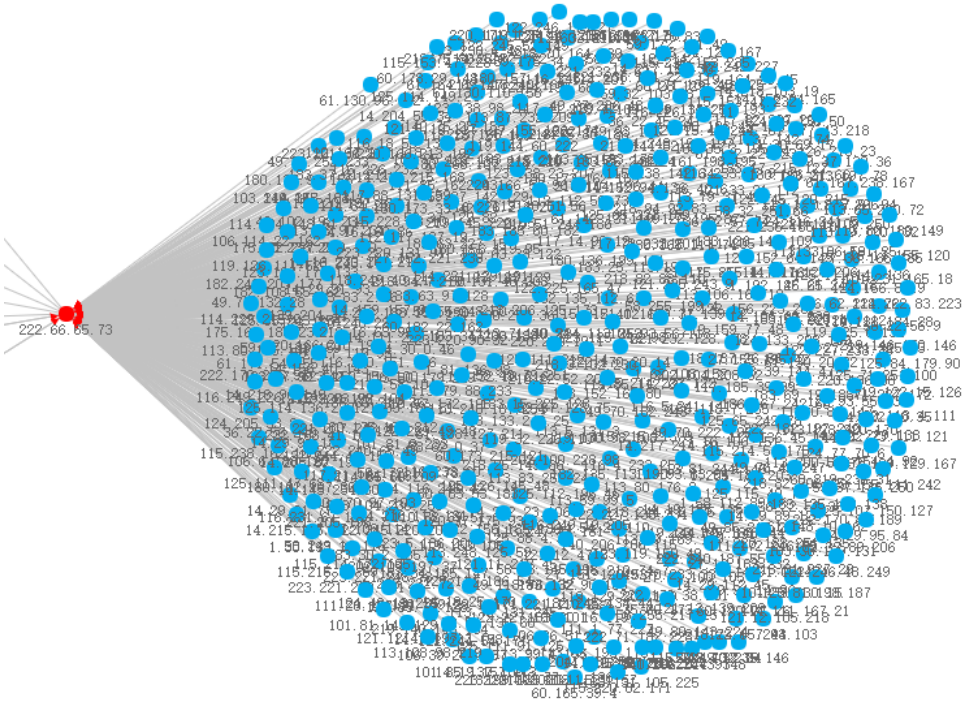
发两项都满足时，才会进行告警，可以有效避免误报的情况。

此外，NetSensor 的告警模拟功能，可以使得原本需要不断调优的告警阈值配置过程，变成了非常轻松的几次鼠标点击。通过告警模拟，可以快速配置合理的告警阈值。

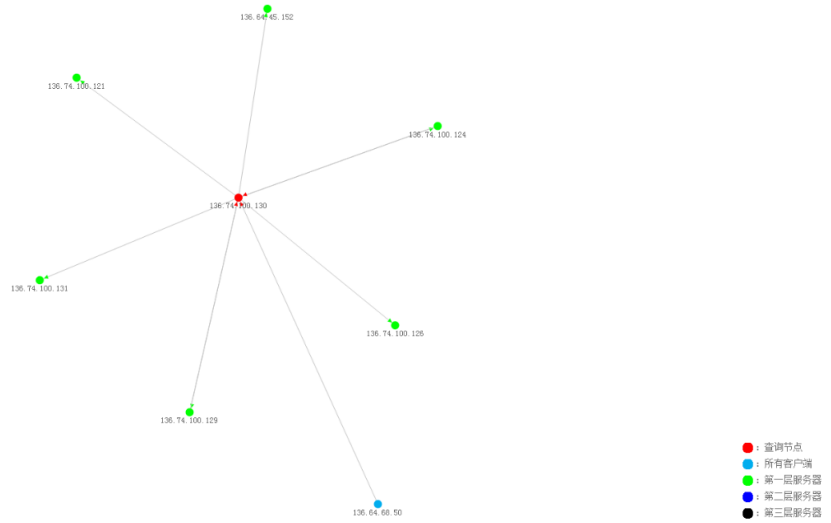
3.4 应用梳理

NetSensor 网络性能分析系统对于缺少拓扑图或者网络信息不完整的情况，提供应用梳理功能，发现不同 IP 之间的连接关系，找到核心站点和典型的拓扑结构。进入访问关系的界面，在界面中选择抓包口，填入 IP 或网段，选择需要查看的层数

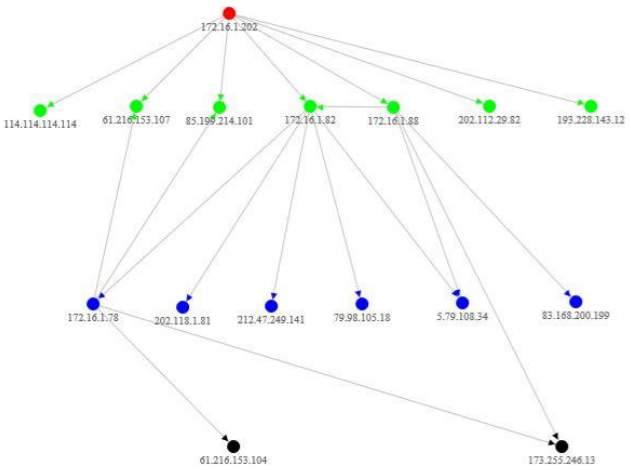
展示所有的客户端：



如果选择一层，如下图所示，用绿点表示第一层的服务器



如果选择三层，如下图所示，分别用不同颜色表示不同层级发现的服务器



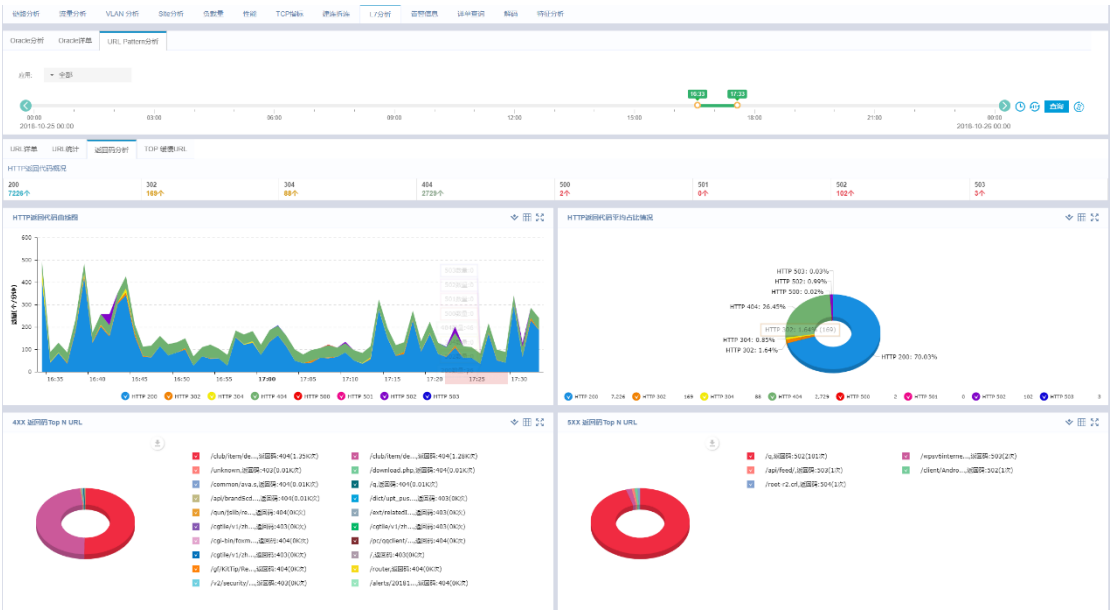
通过访问关系可以梳理出哪些 IP 站点处于访问关系的中心位置，以及不同 IP 之间的访问关联，帮助用户更深入地了解网络 IP 层面的结构，在随后的网络拓扑图添加时，能够抓住重点节点，准确无误地还原出网络拓扑图解。

3.5 七层分析

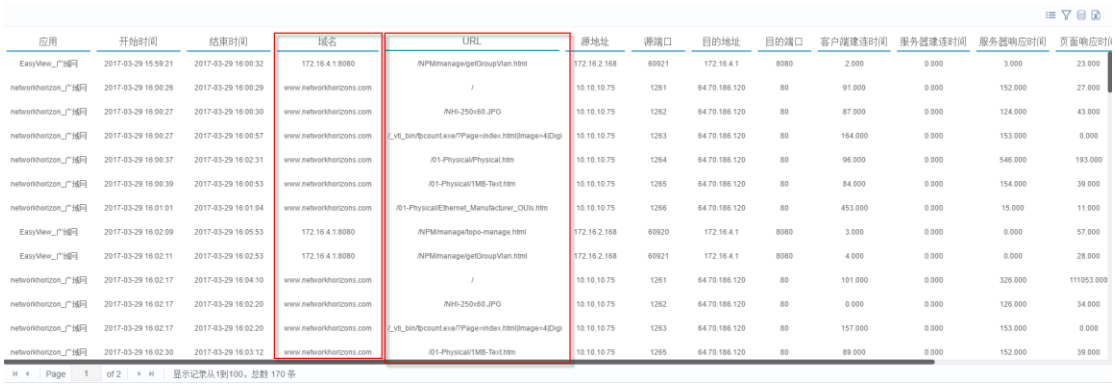
在企业数据中心的网络中，有大量的业务是基于 Web 的，而且绝大部分基于 Web 的业务都会采用 Multi-Tier（多级）架构，即 Web -> App （中间件） -> DB（数据库）的架构。针对这种情况，当我们发现业务响应慢的时候，NetSensor 可以帮助定位慢的 URL 或者是 SQL 查询语句。同时对 HTTP 错误返回码，例如客户端错误 4XX、服务器错误 5XX 也进行了精确地统计和分析。另外，也记录了缓慢的 TOP URL 的访问次数，以便运维开发人员针对异常 URL 进行深度解析。

3.5.1 HTTP URL 分析

分析 HTTP 的 URL 及错误返回码，点击相应错误返回码的 URL 可以跳转到 URL 详单查看会话详情。



HTTP URL 详单里记录下了 HTTP 请求体里的域名和 URL，并且可以根据域名和 URL 进行查询。同时，提供整个页面的传输时间。



应用	开始时间	结束时间	域名	URL	源地址	源端口	目的地址	目的端口	客户端建连时间	服务器建连时间	服务器响应时间	页面响应时间
EasyView_广域网	2017-03-29 15:59:21	2017-03-29 16:00:32	172.16.4.1:8080	/NPM/manage/getGroupVlan.html	172.16.2.168	60921	172.16.4.1	8080	2.000	0.000	3.000	23.000
networkhorizon_广域网	2017-03-29 16:00:26	2017-03-29 16:00:29	www.networkhorizons.com	/	10.10.10.75	1261	64.70.186.120	80	91.000	0.000	152.000	27.000
networkhorizon_广域网	2017-03-29 16:00:27	2017-03-29 16:00:30	www.networkhorizons.com	/NHI-250x60.JPG	10.10.10.75	1262	64.70.186.120	80	87.000	0.000	124.000	43.000
networkhorizon_广域网	2017-03-29 16:00:27	2017-03-29 16:00:57	www.networkhorizons.com	/_vti_bin/fpcount.exe/?Page=index.html|Image=4|Digi	10.10.10.75	1263	64.70.186.120	80	164.000	0.000	153.000	0.000
networkhorizon_广域网	2017-03-29 16:00:37	2017-03-29 16:02:31	www.networkhorizons.com	/01-Physical/Physical.htm	10.10.10.75	1264	64.70.186.120	80	96.000	0.000	546.000	193.000
networkhorizon_广域网	2017-03-29 16:00:39	2017-03-29 16:00:53	www.networkhorizons.com	/01-Physical/1MB-Text.htm	10.10.10.75	1265	64.70.186.120	80	84.000	0.000	154.000	39.000
networkhorizon_广域网	2017-03-29 16:01:01	2017-03-29 16:01:04	www.networkhorizons.com	/01-Physical/Ethernet_Manufacturer_OUIs.htm	10.10.10.75	1266	64.70.186.120	80	453.000	0.000	15.000	11.000
EasyView_广域网	2017-03-29 16:02:09	2017-03-29 16:05:53	172.16.4.1:8080	/NPM/manage/topo-manage.html	172.16.2.168	60920	172.16.4.1	8080	3.000	0.000	0.000	57.000
EasyView_广域网	2017-03-29 16:02:11	2017-03-29 16:02:53	172.16.4.1:8080	/NPM/manage/getGroupVlan.html	172.16.2.168	60921	172.16.4.1	8080	4.000	0.000	0.000	28.000
networkhorizon_广域网	2017-03-29 16:02:17	2017-03-29 16:04:10	www.networkhorizons.com	/	10.10.10.75	1261	64.70.186.120	80	101.000	0.000	326.000	111053.000
networkhorizon_广域网	2017-03-29 16:02:17	2017-03-29 16:02:20	www.networkhorizons.com	/NHI-250x60.JPG	10.10.10.75	1262	64.70.186.120	80	0.000	0.000	126.000	34.000
networkhorizon_广域网	2017-03-29 16:02:17	2017-03-29 16:02:20	www.networkhorizons.com	/_vti_bin/fpcount.exe/?Page=index.html|Image=4|Digi	10.10.10.75	1263	64.70.186.120	80	157.000	0.000	153.000	0.000
networkhorizon_广域网	2017-03-29 16:02:30	2017-03-29 16:03:12	www.networkhorizons.com	/01-Physical/1MB-Text.htm	10.10.10.75	1265	64.70.186.120	80	89.000	0.000	152.000	39.000

Page 1 of 2 显示记录从1到100，总数 170 条

3.5.2 数据库分析

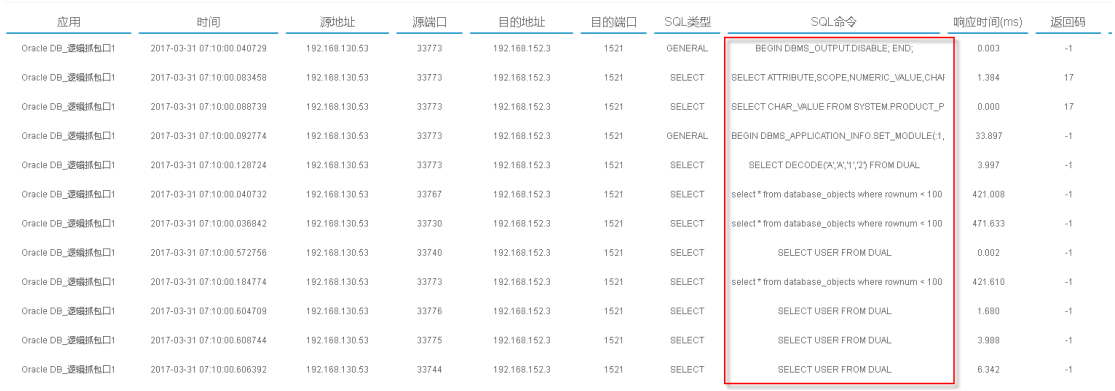
NetSensor 支持几乎所有主流企业级数据库包括大数据平台的 7 层解码分析，可以定位到响应慢的数据库语句。

- Oracle
- DB2
- Microsoft SQL Server
- Informix
- MySQL
- Redis
- MongoDB
- Kafka
- HBase

每种类型的数据库，NetSensor 可以统计 SQL 语句的类型和执行效率，同时记录下每一个 SQL 查询的操作。

以 Oracle 数据库为例: Oracle 分析可以统计针对不同类型的 SQL 语句进行分类统计，支持的类型有：insert，select，update，delete，commit，fetch，rollback，begin

在详单界面可以看到每一笔 SQL 语句，快速精准定位问题。



支持的 Oracle 错误代码：

1	unique constraint violated
54	resource busy and acquire with NOWAIT specified or timeout expired
257	archiver error. Connect internal only, until freed
600	internal error code
603	Oracle server session terminated by fatal error
604	Oracle error occurred at recursive SQL level 3
918	column ambiguously defined
942	table or view does not exist
984	column not allowed here
1000	maximum open cursors exeeded
1008	not all variables bound
1017	invalid username/password, logon denied
1031	insufficient privileges
1033	Oracle initialization or shutdown in progress
1034	Oracle not available
1089	immediate shutdown in progress - no operations are permitted
1110	data file string: string
1403	No Data Returned
1422	exact fetch returns more than requested number of rows
1461	can bind a LONG value only for insert into a LONG column

1555	snapshot too old
1653	unable to extend table in tablespace
1830	date format picture ends before converting entire input string
2330	datatype specification not allowed
3113	end-of-file on communication channel
3114	Not connected to ORACLE
3135	connection lost contact
4030	out of process memory
4031	unable to allocate string bytes of shared memory
4063	string has errors
6508	could not find program unit being called
6550	ORACLE SQL: PL/SQL: Statement Ignored
9817	Write to audit file failed
12154	TNS:could not resolve the connect identifier specified
12170	TNS:Connect timeout occurred
12203	TNS:unable to connect to destination
12500	TNS:listener failed to start a dedicated server process
12514	TNS:listener does not currently know of service
12528	TNS:listener: all appropriate instances are blocking new connections
12545	Connect failed because target host or object does not exist
12560	TNS:protocol adapter error
19511	Error received from media manager layer
20001	SQL_PLSQL ERROR: N, Routine
25228	timeout or end-of-fetch during message dequeue
27101	shared memory realm does not exist
27301	OS failure message
65534	Error Oracle

3.5.3 TLS/SSL 分析

在互联网中 HTTP 本身是明文传输的，没有经过任何安全处理。目前许多知名的互联网 Web 应用已跳转成 HTTPS 协议进行传输。 HTTPS 可以认为是 HTTP+SSL（TLS），SSL 或 TLS 是传输层加密协议，对上层 HTTP 数据加密后进行传输。一旦 HTTP 数据包被加密后，而且没有秘钥解密的话， 那么包内容中的域名+URL 将无法正常显示。NetSensor 通过自身 DPI 技术对 TLS/SSL 报文进行深度解析，生成 SSL 详单及关键域名分析。同时针对域名访问次数及相对应域名的 Web 应用性能指标进行关联。

关键域名	访问次数 ↓	平均响应时间	峰值响应时间	平均页面时间	峰值页面时间
Others	340652	2394.573 ms	2321717.353 ms	50606.318 ms	8684617.113 ms
Google	73586	7230.906 ms	1680384.281 ms	132747.579 ms	7442124.818 ms
Apple	63211	419.456 ms	299968.092 ms	22457.895 ms	4502951.299 ms
Baidu	23725	802.225 ms	85175.836 ms	29125.379 ms	3602075.840 ms
Instagram	18872	116.515 ms	185056.533 ms	37760.831 ms	2115215.247 ms
GoogleVideo	14968	194.394 ms	239996.475 ms	37432.713 ms	3649956.854 ms
Facebook	9645	921.464 ms	300839.968 ms	78004.766 ms	7623492.676 ms
Microsoft	8751	190.965 ms	70248.070 ms	10794.665 ms	3880916.166 ms
Alipay	6501	224.197 ms	299966.630 ms	12020.350 ms	1891125.142 ms

3.5.4 基础服务协议分析

针对常用的提供基础网络服务的协议，例如 :DHCP ,DNS ,FTP 和 Tetlnet ,NetSensor 提供了 7 层详单的功能。当基础服务出现问题时，通过 7 层详单可以定位到出问题的 DNS 查询，FTP 命令，Telnet 命令等。

3.5.5 邮件协议分析

NetSensor 能够分析 SMTP，POP3 和 IMAP 协议，可以解析邮件发送方，接收方，邮件主题等主要字段。

3.5.6 AAA 协议分析

NetSensor 提供对 LDAP，Radius，TACACS 协议的 7 层解析

3.5.7 IBM-MQ 协议分析

MQ 是搭建企业服务总线的基础传输层 ,为 SOA 架构提供可靠的消息传递。NetSensor 可以对 IBM-MQ 协议进行 7 层解析。

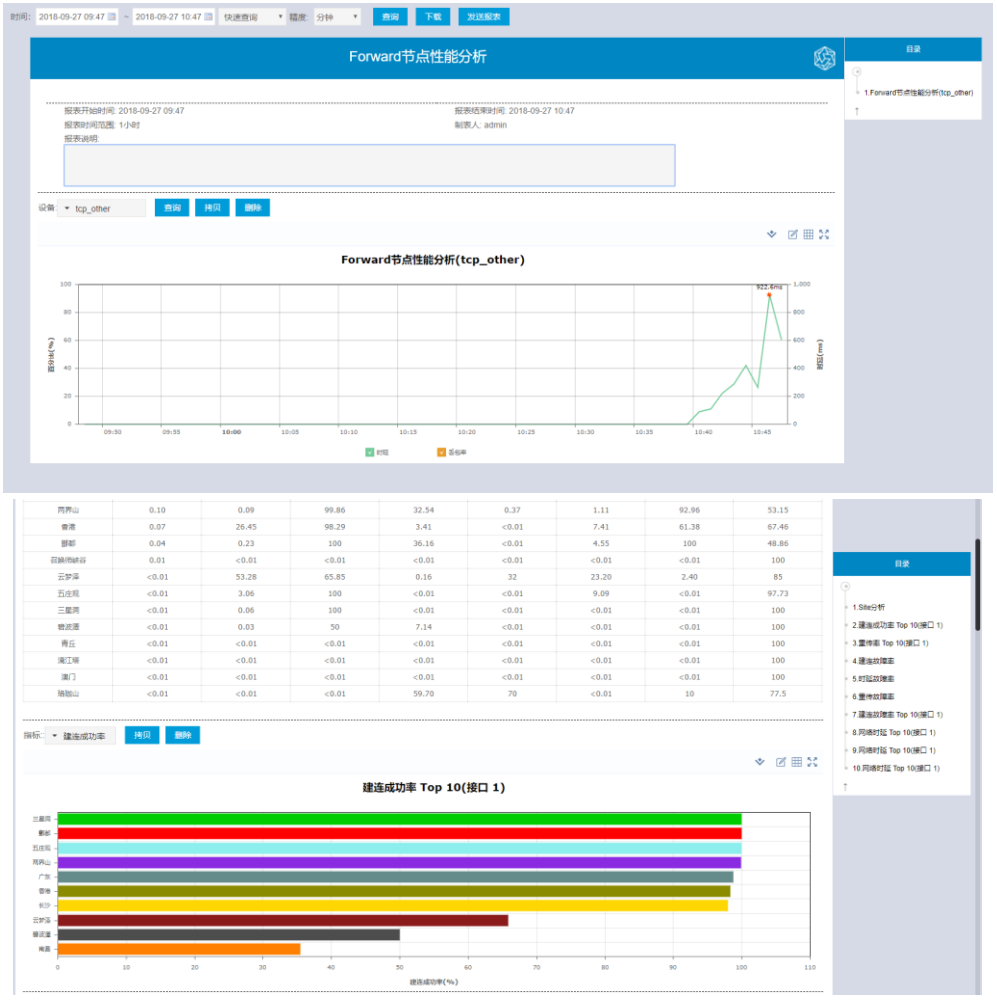
3.6 所见即所得的报表

NetSesnor 支持所见即所得的报表定义，可以选取任意应用和 KPI 的组合生成各种类型的报表，并且生成日报、周报、月报，定时发送。

此外，针对一个业务系统 NetSensor 特有的一键对比功能，可以在两秒钟内生成各个应用子系统的某个 KPI 对比报表，快速比对子系统的流量、响应时间等重要 KPI。

NetSensor 不仅支持定制化报表，而且还提供以下模板组方便客户迅速针对网络流量、关键业务及监控站点性能指标生成报表。

- 流量报表组
- 业务系统报表组
- 站点报表组



3.7 智能健康度打分模型

随着被监控的业务不断增加，如何快速发现出存在问题的业务系统并且快速定位到出故障的业务组件一直是企业级监控的难点。NetSensor 特有的智能健康度打分模型，可以针对应用系统每个组件的网络健康度和业务健康度进行打分，然后汇总成整个业务系统的健康度得分，使用户对业务系统的网络和业务的表现一目了然。

当发生业务系统得分偏低时，可以通过查看每个业务组件的得分，定位到具体某个或者某几个组件。

继续深入到组件级别进行分析，就可以定位到出问题的 KPI 指标。

健康度模型采用机器学习算法，根据历史基线数据或者阈值自动计算分数，定义指标减值分值：

网络响应时延减值（Nts）

服务响应时延减值（Sts）

建连成功率减值（Scs）

网络重传率减值（Rns）

零窗口数减值（Zns）

服务集网络健康值（Ans）

服务集应用健康值（Aas）

业务系统的网络健康值（Ns）

服务健康值（Ss）

分值计算方式：

服务集网络健康值：

Ans = 100 - （Nts + Scs + Rns + Zns）

服务集业务健康值：

Aas = 100 - （Sts + Rns + Zns）

网络健康值：

Ns = min(Ans1,Ans2,Ans3,Ans4)

服务健康值：

Ss = min(Aas1,Aas2,Aas3,Aas4)

4 应用场景

4.1 流量分析

流量分析是网络性能管理软件的基础功能，有别于纷繁复杂的流量分析工具，NetSensor 把对传统的流量分析做了创新，主要体现为：“一图一表看数据 “、“流量性能一起看”。

通过流量分析图，我们可以解决这些基本问题：“我的网络中的流量组成？” 、“哪些主机流量最大？”、“哪些通讯对流量最大？”。

而通过流量分析表，我们可以对流量进行五个不同维度的分析，并且 NetSensor 不但能提供流量的 KPI，还能提供一般流量分析软件提供不了的性能 KPI。

按应用	快速定位某个应用的某个服务器/客户端/通讯对的情况
按端口	获取服务器侦听端口的情况，快速识别
按主机	找出网络中（流量，重传，响应时间，零窗口，并发连接数）最

	大的问题主机
按通讯对	找出网络中（流量，重传，响应时间，零窗口，并发连接数）最大的问题通讯对
主机查找	对问题主机进行全面分析

下图展示的是从应用->服务器->端口的层层深入分析，通过各项 KPI 指标，在一张表里，就可以进行问题排查，定位“表现”的应用/服务器/客户端/通讯对。

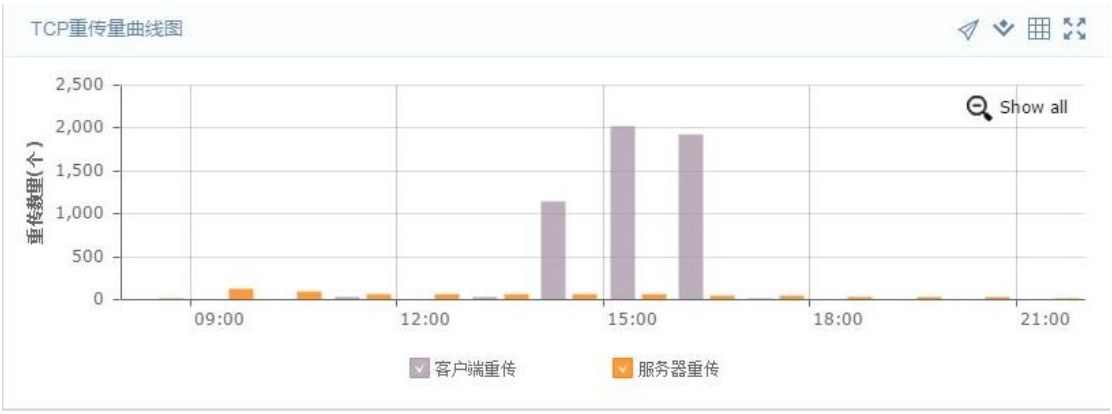
应用名称	总流量 ↓	客户端流量	服务器流量	并发数连接	重传数量	零窗口数量	响应时间
inst0_CRM_port5559	14545.21MB	3022.60MB	11522.61MB	25706个	11035192个	243370个	708.70ms
服务器(1)							
183.195.157.211	7272.61MB	1511.30MB	5761.31MB	25706个	3475344个	119959个	707.24ms
Port 5559	7272.61MB	1511.30MB	5761.31MB	25706个	3475344个	119959个	707.24ms
客户端(1)							
通讯对(1)							
inst0_222.66.65.72:5559	10559.90MB	2220.82MB	8339.08MB	20042个	8096062个	170174个	845.97ms
inst0_tcp_other	4470.96MB	2055.84MB	2415.12MB	52748个	6414592个	156308个	783.57ms
inst0_http	104.49MB	15.97MB	88.52MB	241个	9776个	208个	103.97ms
inst0_https	56.37MB	10.27MB	46.10MB	434个	22718个	0个	845.65ms
inst0_主机search	19.69MB	1.19MB	18.50MB	21个	1154个	0个	128.70ms
inst0_udp_other	3.54MB	3.00MB	0.54MB	89个	0个	0个	N/A
inst0_EasyView	3.29MB	0.29MB	3.00MB	2个	0个	0个	18.90ms
inst0_rdp	1.97MB	0.66MB	1.31MB	4个	3116个	0个	3520.60ms
inst0_iscsi	0.55MB	0.32MB	0.23MB	2个	612个	0个	3434.81ms

4.2 长期趋势分析

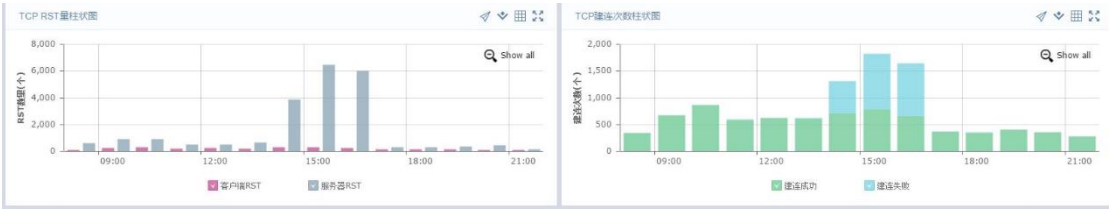
对于网络流量的长期监测可以很容易地辨识出变化的周期性，从而得到一条周期性参数的基线，通过基线对当前值做出比较，查找出可能的问题来。

例如：在 7 天的监测中发现 11 月 23 日有很大的客户端重传，放大这一天的图像

可以发现重传率高峰出现在 14-16 点的这段时间

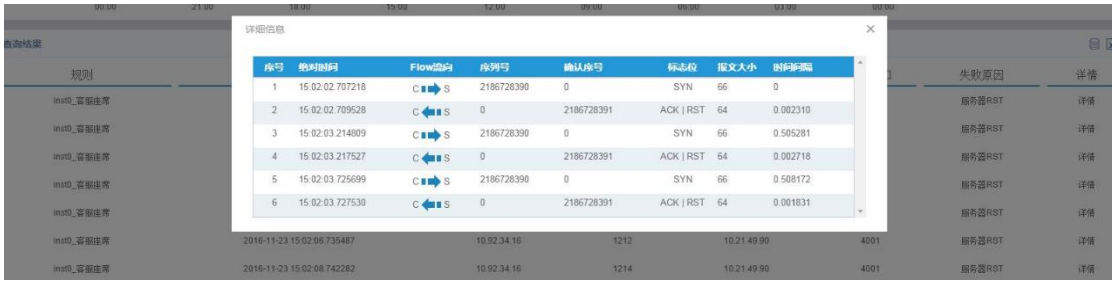


同时可以看到这个时间段的服务器 RST 和建连失败都有明显的提升



那么我们跳转到建连分析的界面，对这段时间的建连情况进行观察，发现有大量的服务器 RST 故障导致建连失败

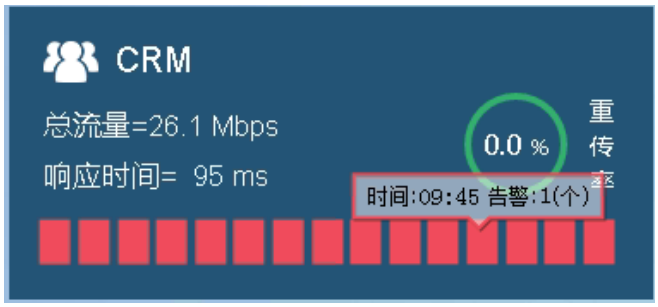
如果点击查看详情，可以进一步看到服务器收到来自客户端的 SYN 包后，回应直接 RST，可能是服务器端口不可用或者中间有防火墙策略阻挡了。



4.3 两分钟定位慢响应问题

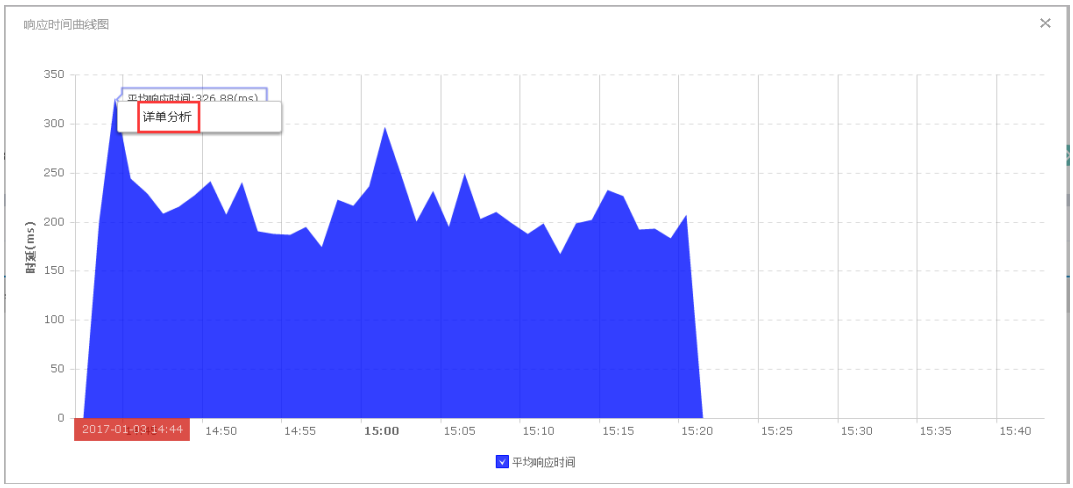
NetSensor 实时处理能力业界领先，特有的全量详单，为高效排障奠定了基础。在业界“ KPI->Flow->Packet“的排障方法学的基础上 ,我们进行了创新 ,发展为“告警-> KPI-> 详单 -> 请求响应分析-> 数据包” 的排障方法，可以缩短 80%的问题处理时间。具体示例如下：

1. CRM 系统产生告警，点击产生告警的红色柱子，可以进行深入分析。

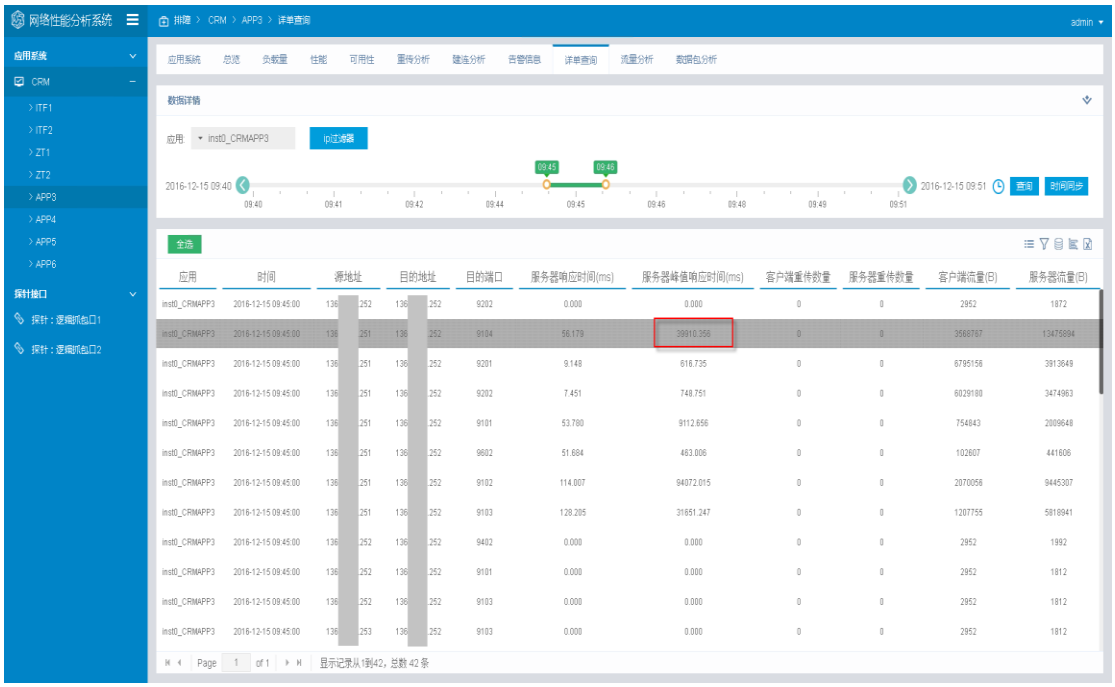


2. 界面自动跳转到告警列表界面，在告警列表中看到平均响应时间超过基线值 100%。

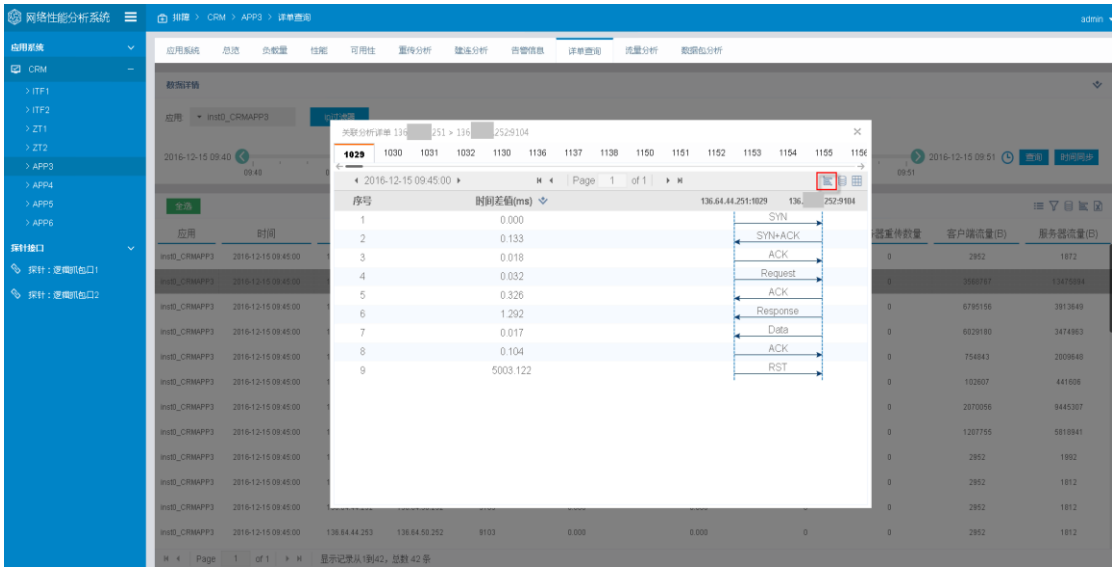
3. 在弹出的响应时间曲线图中，可以查看了告警发生时间节点前后的告警 KPI 的曲线图。选中响应时间较长的时间点单击右键进行详单分析。



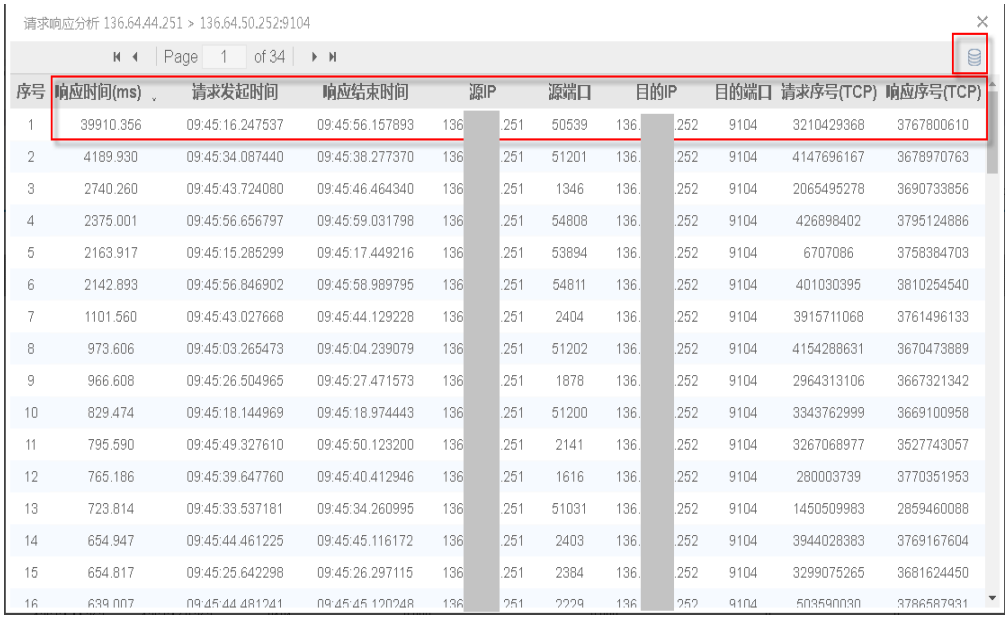
4. 在弹出的详单界面，查看这个应用在这一分钟内的所有的通讯对以及相关的指标。至此可以定位到出问题的通讯对了。选中响应时间最大的通讯对，单击右上角关联分析。



5. 可以看到，关联分析详单中列出了这个通讯对之前所有的 TCP session，并且对每一个 session 的数据包进行了请求和响应的识别。单击右上角的请求响应分析继续深入分析。

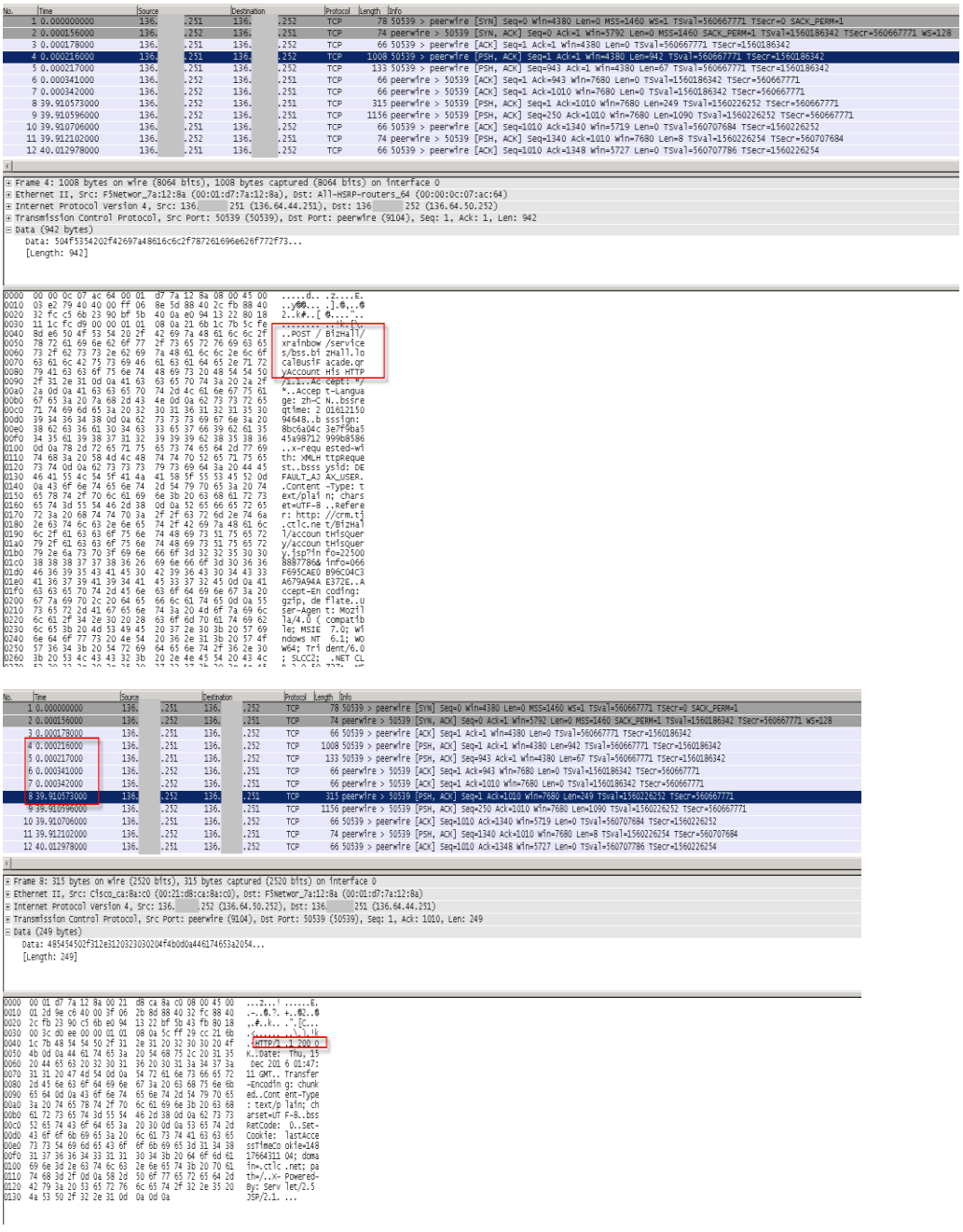


6. NetSensor 列出了每一笔请求和响应的具体数据，包括源 IP、源端口、目的 IP、目的端口，请求报文的序号，响应报文的序号。至此通过对响应时间的排序，可以清楚地分析到哪笔响应慢。选择所要解码的数据，单击右上角解码。



序号	响应时间(ms)	请求发起时间	响应结束时间	源IP	源端口	目的IP	目的端口	请求序号(TCP)	响应序号(TCP)
1	39910.356	09:45:16.247537	09:45:56.157893	136.[redacted].251	50539	136.[redacted].252	9104	3210429368	3767800610
2	4189.930	09:45:34.087440	09:45:38.277370	136.[redacted].251	51201	136.[redacted].252	9104	4147696167	3678970763
3	2740.260	09:45:43.724080	09:45:46.464340	136.[redacted].251	1346	136.[redacted].252	9104	2065495278	3690733856
4	2375.001	09:45:56.656797	09:45:59.031798	136.[redacted].251	54808	136.[redacted].252	9104	426898402	3795124886
5	2163.917	09:45:15.285299	09:45:17.449216	136.[redacted].251	53894	136.[redacted].252	9104	6707086	3758384703
6	2142.893	09:45:56.846902	09:45:58.989795	136.[redacted].251	54811	136.[redacted].252	9104	401030395	3810254540
7	1101.560	09:45:43.027668	09:45:44.129228	136.[redacted].251	2404	136.[redacted].252	9104	3915711068	3761496133
8	973.606	09:45:03.265473	09:45:04.239079	136.[redacted].251	51202	136.[redacted].252	9104	4154288631	3670473889
9	966.608	09:45:26.504965	09:45:27.471573	136.[redacted].251	1878	136.[redacted].252	9104	2964313106	3667321342
10	829.474	09:45:18.144969	09:45:18.974443	136.[redacted].251	51200	136.[redacted].252	9104	3343762999	3669100958
11	795.590	09:45:49.327610	09:45:50.123200	136.[redacted].251	2141	136.[redacted].252	9104	3267068977	3527743057
12	765.186	09:45:39.647760	09:45:40.412946	136.[redacted].251	1616	136.[redacted].252	9104	280003739	3770351953
13	723.814	09:45:33.537181	09:45:34.260995	136.[redacted].251	51031	136.[redacted].252	9104	1450509983	2859460088
14	654.947	09:45:44.461225	09:45:45.116172	136.[redacted].251	2403	136.[redacted].252	9104	3944028383	3769167604
15	654.817	09:45:25.642298	09:45:26.297115	136.[redacted].251	2384	136.[redacted].252	9104	3299075265	3681624450
16	639.007	09:45:44.481241	09:45:45.120248	136.[redacted].251	2229	136.[redacted].252	9104	5035900030	3786587931

7. 打开数据包文件，可以定位到出问题的原始数据包。



在这个案例中，我们看到响应慢是由于 localBusiFacade.qryAccountHis 这个查询账号明细的 API 调用慢造成的。

4.4 主机画像

针对某台服务器的分析是运维人员经常面临的一个任务，当拿到目标主机的 IP 后，通常运维人员需要知道：

这台主机的流量在哪些区域被监控了？

这台主机是否已经在应用系统里已经定义了？是否可以直接在应用拓扑图上呈现？

这台主机对外提供了哪些服务？服务端口是哪些？

这台主机访问了哪些服务器？那些服务器的端口又是哪些？

这些信息构成了一个主机在网络上的画像，我们可以在全局搜索里查找这个主机的 IP 来获得这些信息。

可以显示出所有和该主机相关的流量，包括多台探针的不同接口。

4.5 站点上下行流量可视化

广域网线路承载着企业所有的业务通讯，而且一般线路的租用费用价格高昂。针对广域网线路的监控是网络运维部门的重点工作之一。NetSensor 可以通过 IP 地址段来区分同一个广域网线路中的不同远程站点（营业厅/分行/分支机构）的流量，并以站点为单位进行流量的可视化分析。

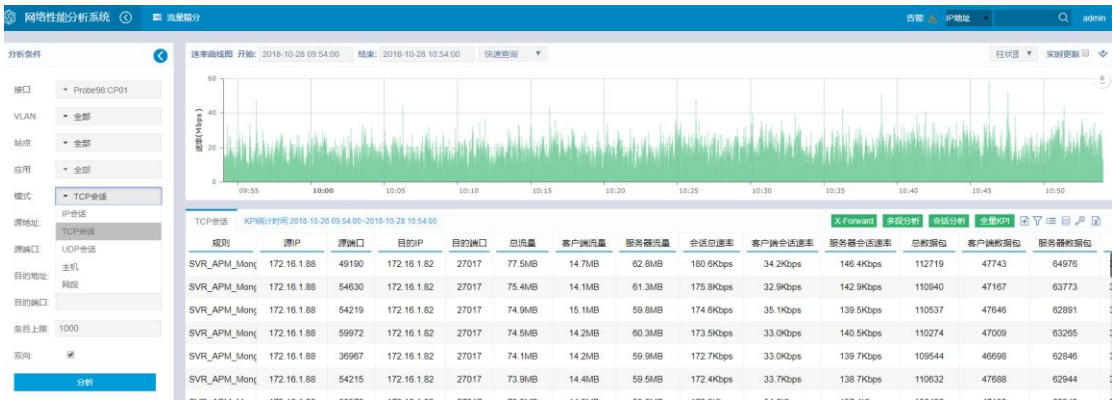
此外，NetSensor 特有的多维度站点流量精分功能，可以从多个不同的视角来详尽分析站点的流量：

- 站点上行（再以主机，通讯对，应用或者端口做为第二维度）
- 站点下行（再以主机，通讯对，应用或者端口做为第二维度）
- 站点发起
- 站点接入

当广域网专线出现拥塞的时候，可视化呈现可以第一时间告警，通过站点流量精分可以快速定位大流量主机/应用/通讯对/端口。

4.6 流量精分

流量精分也叫全流量分析，是对接口上所有的会话进行各类汇总统计的界面。在精分流量中，可以对流量进行各种维度，例如可以基于 IP 会话、TCP 会话、UDP 会话、主机和网段，甚至也可以基于采集接口下关联的不同 VLAN、站点、应用的统计分析。选择单个会话，支持‘全量 KPI’、‘会话分析’、‘多段分析’和 HTTP 的‘X-Forward’关联分析。另外，在精分界面中也提供了链路秒级的实时更新。



5 技术指标

5.1 推荐运行环境

CPU：2 颗 Intel 6 核 2.4GHz 及以上 （支持超线程）

内存：64GB 及以上

存储：本地 RAID-5 磁盘整列

浏览器：Firefox 或 Chrome

操作系统：CentOS 7.0

千兆专用采集卡

10G 专用采集卡

5.2 数据精度及保存时间

数据精度

NO.	各类数据	精度（粒度）
1	采集的数据包时间戳	1 微妙（千兆），10 纳秒（万兆）
2	各项 KPI 指标	1 分钟精度（提供 1 毫秒级别的高精度流量曲线）
3	重传、建连分析详单	1 分钟精度
4	通信对的详单	1 分钟精度

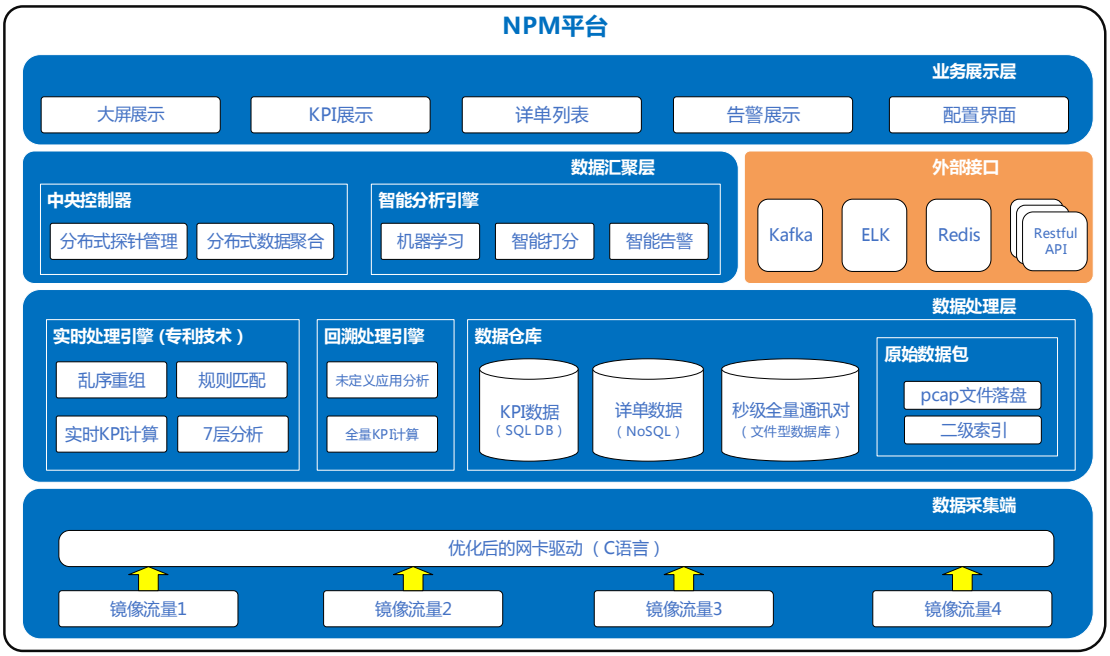
数据保存时间

NO.	各类数据	保存时间
1	KPI 指标	默认：1 年（可配置）
2	重传、建连分析详单	默认：7 天（可配置）
3	通信对的详单	默认：7 天（可配置）
4	业务详单	默认：31 天（可配置）
5	采集数据包的回溯时间	以 1Gbps 采集接口总流量计算 8T 容量，11 小时，只存头部，70 小时 16T 容量，24 小时，只存头部，144 小时 24T 容量，35 小时，只存头部，210 小时 48T 容量，75 小时，只存头部，450 小时

		64T 容量，100 小时，只存头部，600 小时
6	基线	设置完可以回溯查看设置当天零点开始的基线， 一直保存直到下次更改。

6 技术架构

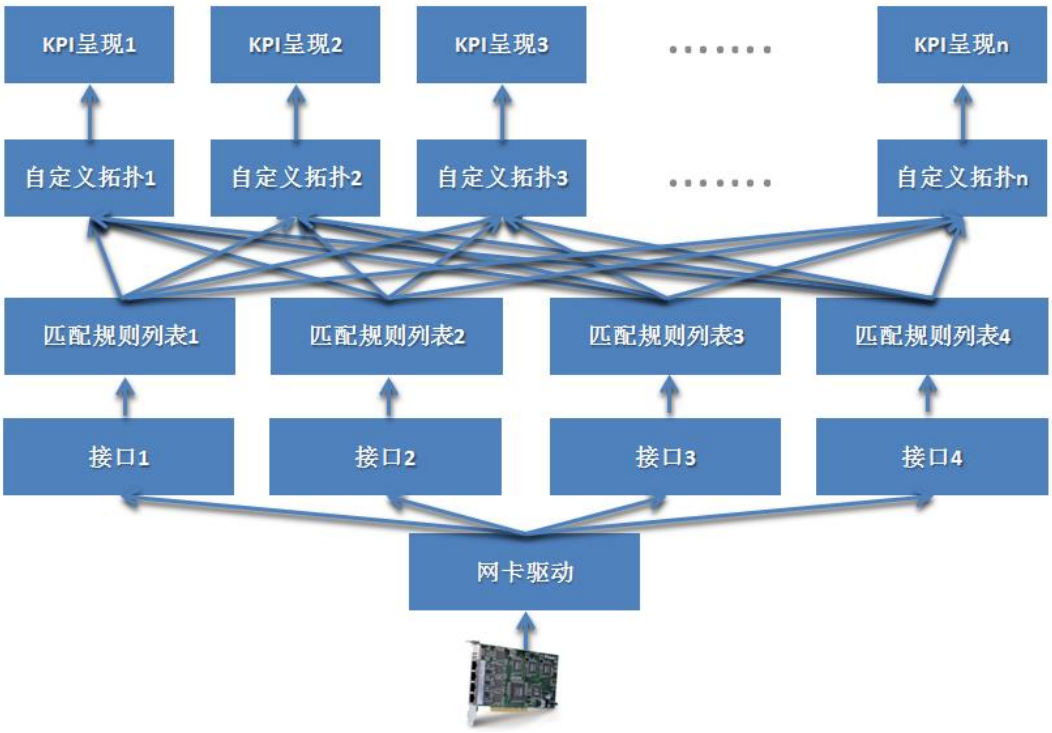
NetSensor 网络智能分析系统在单台服务器上集成数据采集和分析的功能，同时，对于多点部署的情况，也支持分布式方案。总体的架构图如下：



6.1 系统架构

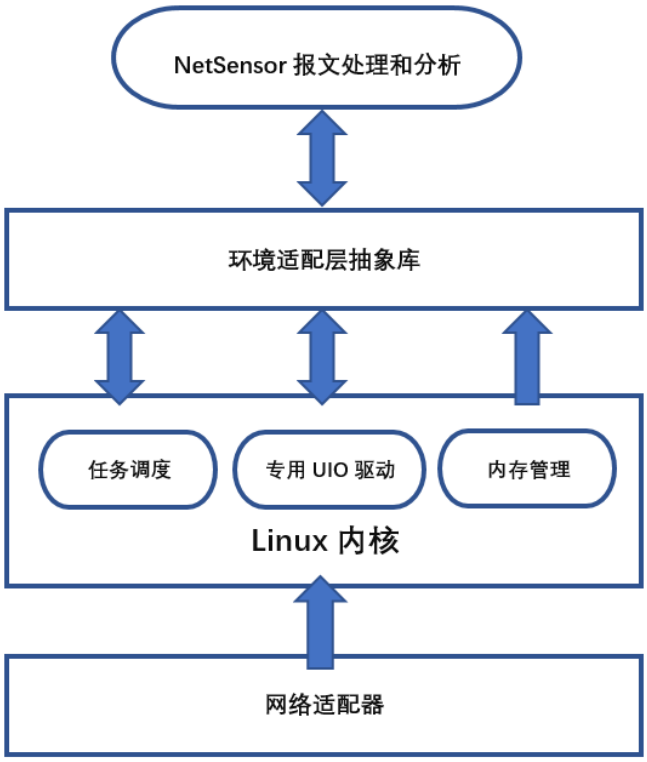
NetSensor 网络智能分析系统从网卡采集数据后，送到不同的接口。一块网卡可以有四个物理接口，同时监控 4 路数据源。用户可以为每个物理接口定义不同的过滤规则列表。而每个用户自定的拓扑又可以指定不同物理接口上的不同的过滤规则。这样最大程度的保证了用户拓扑定义的灵活性。NetSensor 网络智能分析系统的高性能解析引擎会根据匹配规

则列表，对接口上捕获的每个数据报文进行匹配，对满足匹配条件的报文进行处理，生成各类 KPI 指标，最后呈现在界面上。

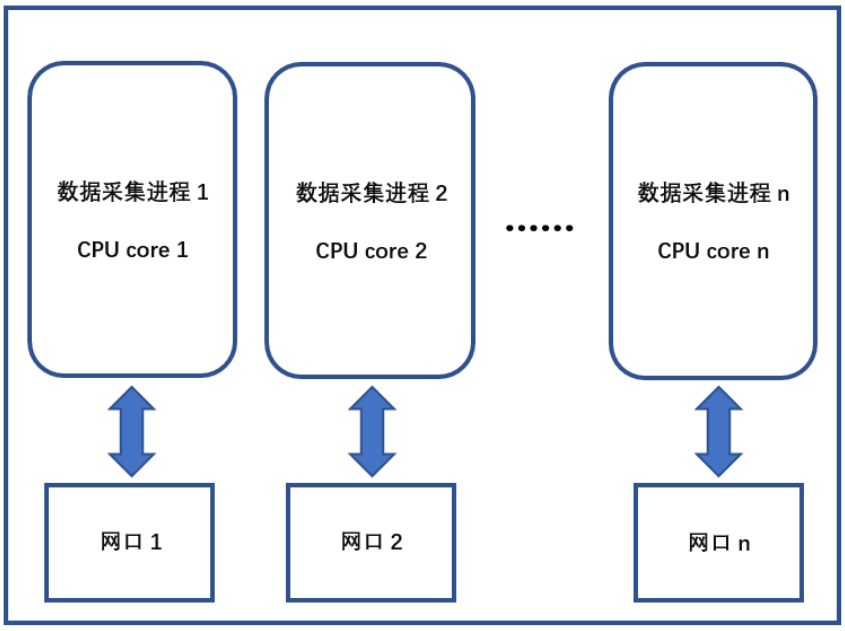


6.2 数据采集

数据包采集的关键是效率，NetSensor 网络性能分析系统在内核层通过特殊的驱动以及充分利用 CPU、数据总线以及网卡的优化特性，以最快的速度读取采集到的数据包并进行过滤和分析。

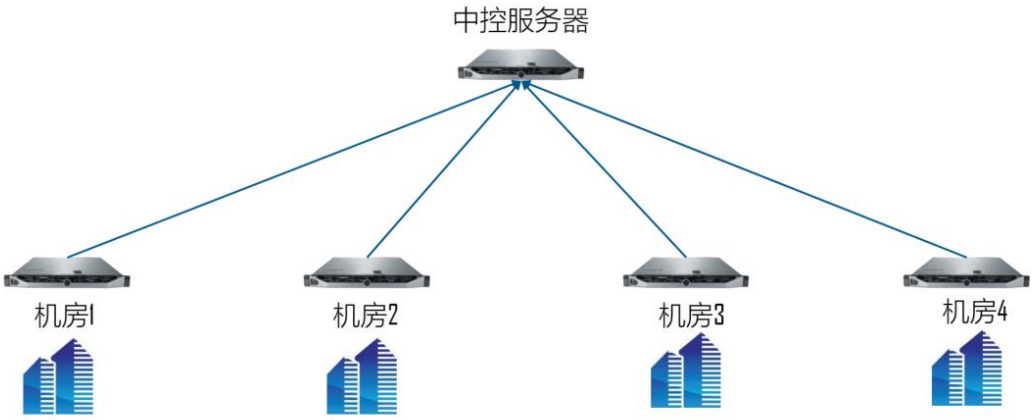


同时，通过中间的环境适配层，实现了多核 CPU 并行处理多网口数据采集的特性，使得采集数据的性能达到网卡线速的水平。



6.3 分布式部署

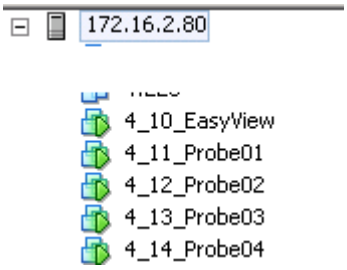
对于有多个机房的需求，NetSensor 支持探针的分布式部署，在中控服务器上集中管理，KPI 数据也可以集中呈现。一台中控服务器最多可以管理 10 台探针。



6.4 虚拟化支持

NetSensor 探针支持虚机部署，全面支持 VMWare，KVM 和 OpenStack 的虚拟化环境。

虚拟化部署：一台中控服务器（EasyView），四台探针。



附录 A

参数释义

pkt 负载量	速率	总速率	trafficRate	单位时间内的总速率，单位 bps
		上行速率	trafficRate_uplink	上行速率
		下行速率	trafficRate_downlink	下行速率
	流量	总流量	totalBytes	单位时间内所有的数据包的总字节数
		上行流量	totalBytes_uplink	单位时间内所有上行的数据包的总字节数
		下行流量	totalBytes_downlink	单位时间内所有的下行数据包的总字节数
	利用率	总利用率	utilization	速率除以线路带宽
		上行利用率	utilization_uplink	速率除以线路上行带宽
		下行利用率	utilization_downlink	速率除以线路下行带宽
	包率	总包率	pktRate	单位时间内发送数据包的速度，单位：pps
		上行包率	pktRate_uplink	单位时间内发送上行数据包的速度
		下行包率	pktRate_downlink	单位时间内发送下行数据包的速度
	包大小	平均包大小	avgPktSize	数据包的平均大小
	TCP 连接	最大并发量	concurrentConn	单位时间内 TCP 的最大的连接数量
		新建连接数	newConn	单位时间内新建 TCP 连接数量
		客户端数量	numClients	单位时间内独立客户端 IP 的数量
网络性能	延迟	建连时间/网络延迟/RTT	connTime	TCP 三次握手的时间，也叫往返时间
		服务器延迟	serverConnTime	通过 TCP 三次握手来计算，表示客户端到抓包点的网络延迟。计算方式：服务器端收到客户端 SYN 和发送 SYN+ACK 之间的时间

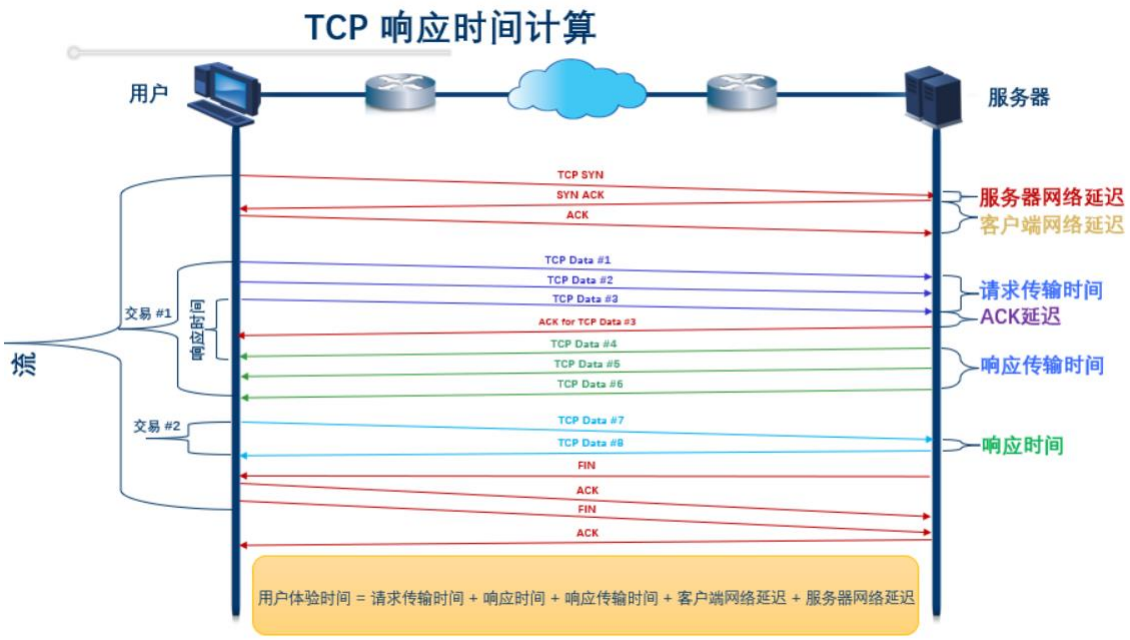
		客户端延迟	clientConnTime	通过 TCP 三次握手来计算，表示服务端到抓包点的网络延迟。计算方式：用户端收到 SYN+ACK 和发送 ACK 之间的时间
	重传	总重传	retxNum	双向重传数据包的个数
		客户端重传	clientRetxNum	客户端重传包的个数
		服务器重传	serverRetxNum	服务器重传包的个数
		重传率	totalRetxRate	重传率
		客户端重传率	clientRetxRate	客户端重传率
		服务器重传率	serverRetxRate	服务器端重传率
	丢包	总丢包数	segLos	总的丢包数量
		客户端丢包	clientseglostnum	客户端传输给服务器的丢包的数量
		服务器丢包	serverseglostnum	服务器传输给客户端的丢包的数量
		丢包率	segLosRate	总的丢包百分比
		客户端丢包率	clientSegLosRate	客户端丢包百分比
		服务器丢包率	serverSegLosRate	服务器丢包百分比
应用性能	响应时间	响应时间	tranRespTime	服务器收到客户端数据包请求后应答的第一个数据包时间，单位时间内的平均值
		请求传输时间	reqTransferTime	客户端的每个请求的平均传输时间
		响应传输时间	respTransferTime	服务器的每个响应的平均传输时间
		请求量	reqNum	采样周期内客户端发出的业务请求的数量
		响应量	respNum	采样周期内服务器发出的业务响应的数量
		正常响应时间	normalTransResp	落在正常响应区间内的服务器响应时间的个数
		慢响应时间	slowTransResp	落在正常响应区间内的服务器响应时间的个数
		超时响应	timeout	大于设置的超时响应时间的服务器响应时间的个数
		超时比率	timeoutRate	超时比率=超时响应/

				响应量
		响应率	hasRespRate	响应率=1-超时比率
	窗口	零窗口数	zeroWinNum	双向零窗口的个数
		客户端零窗口数	zeroWinClientNum	客户端的 TCP 零窗口个数
		服务器零窗口数	zeroWinServerNum	服务器的 TCP 零窗口个数
		最小窗口客户端数量	clientMinWin	客户端的最小窗口值
		最小窗口服务器	serveMinWin	服务器的最小窗口值
	拆连时间	客户端拆连时间	clinetFinTime	客户端主动发起的 FIN,直到拆连完成所花费的时间
		服务器拆连时间	serverFinTime	服务器主动发起的 FIN,直到拆连完成所花费的时间
可用性	建连指标	建连成功数	successfulTcpConnNum	成功创建 TCP 连接的个数
		建连失败数	failedTcpConnNum	TCP 连接创建失败的个数
		建连成功率	succTcpConnRate	TCP 三次握手的成功率
		建连失败率	failTcpConnRate	TCP 三次握手的失败率
	拆连指标	四次拆连数量	normalTeardown	正常拆连得数量
		FIN+Reset	finRst	FIN+Reset 拆连数量
		FIN 超时	finTimeout	FIN 超时数量
		RST 关闭	Rst	Reset 拆连数量
	SYN 数量	总 SYN 数量	synNum	双向 SYN 包的个数
		客户端 SYN 数量	clientSynNum	客户端发送的 SYN 包个数
		服务器 SYN 数量	serverSynNum	服务器发送的 SYN 包个数
	RST 数量	总 RST 数量	rstNum	双向 RST 包的个数
		客户端 RST 数量	clientRstNum	客户端发送的 RST 包个数
		服务器 RST 数量	serverRstNum	服务器发送的 RST 包个数
	FIN 数量	总 FIN 数量	finNum	双向 FIN 包的个数
		客户端 FIN 数量	clientfinNum	客户端发送的 FIN 包个数

		服务器 FIN 数量	serverfinNum	服务器发送的 FIN 包个数
扩展指标	ACK 数量	ACK 数量	ackNum	总共的 ACK 数量
		客户端 ACK 数量	clientAckNum	客户端 ACK 数量
		服务器 ACK 数量	serverAckNum	服务器 ACK 数量
	重复 ACK	重复 ACK	dupAck	重复 ACK 的数量
		客户端重复 ACK	clientDupAck	客户端重复的 ACK 数量
		服务器重复 ACK	serverDupAck	服务器重复的 ACK 数量
	ACK 延时	客户端 ACK 延时	clientAckDelay	客户端发送纯 ACK 数据包的延迟
		服务器 ACK 延时	serverAckDelay	服务器发送纯 ACK 数据包的延迟
	耗时	平均 ACK 等待时间	avgAckWait	ACK 数据包之间的延迟
		平均零窗等待耗时	avgZeroWinWait	从 TCP 通告零窗口开始到窗口再次不为零的间隔时间
		平均重传耗时	avgRetxTime	所有重传数据包的耗时的平均值
	建连失败原因	RST C→S	clientRstTD	客户端发送给服务器 RST，导致连接断开
		RST S→C	serverRstTD	服务器发送给客户端 RST，导致连接断开
		超时 C→S	clientTimeoutTD	服务器发送 FIN，客户端超时。
		超时 S→C	serverTimeoutTD	客户端发送 FIN，服务器超时。

附录 B

响应时间的算法

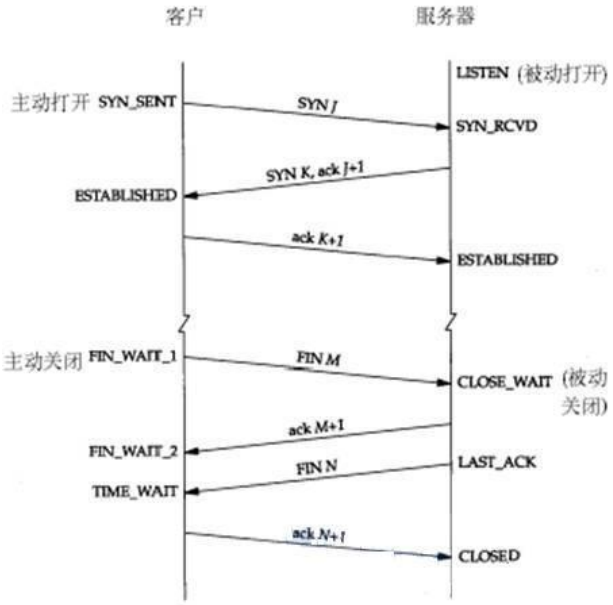


三次握手以后，客户端发送给服务器的第一个数据包（len > 0）为请求数据包，服务器返回的第一个数据包（ len > 0)为响应包，时间差作为一次响应时间。

如果没有三次握手，当判断出客户端和服务器后，使用相同算法，计算响应时间。

附录 C

TCP 建立连接的三次握手过程，以及关闭连接的四次握手过程



展示一个 telnet 建立连接和断开连接的过程，使用 wireshark 捕获的 packet 解码界面

Source	Destination	Protocol	Info
172.29.132.60	172.29.21.25	TCP	proxy-gateway > telnet [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
172.29.21.25	172.29.132.60	TCP	telnet > proxy-gateway [SYN, ACK] Seq=0 Ack=1 Win=49640 Len=0 MSS=1460 SACK_PERM=1
172.29.132.60	172.29.21.25	TCP	proxy-gateway > telnet [ACK] Seq=1 Ack=1 Win=65535 Len=0
172.29.132.60	172.29.21.25	TCP	proxy-gateway > telnet [FIN, ACK] Seq=76 Ack=80 Win=65456 Len=0
172.29.21.25	172.29.132.60	TCP	telnet > proxy-gateway [ACK] Seq=80 Ack=77 Win=49640 Len=0
172.29.21.25	172.29.132.60	TCP	telnet > proxy-gateway [FIN, ACK] Seq=80 Ack=77 Win=49640 Len=0
172.29.132.60	172.29.21.25	TCP	proxy-gateway > telnet [ACK] Seq=77 Ack=81 Win=65456 Len=0

1、建立连接协议（三次握手）

（1）客户端发送一个带 SYN 标志的 TCP 报文到服务器。这是三次握手过程中的报文 1

（2） 服务器端回应客户端的，这是三次握手中的第 2 个报文，这个报文同时带 ACK 标志和 SYN 标志。因此它表示对刚才客户端 SYN 报文的回应；同时又标志 SYN 给客户端，询问客户端是否准备好进行数据通讯

（3） 客户必须再次回应服务段一个 ACK 报文，这是报文 3

2、连接终止协议（四次握手）

由于 TCP 连接是全双工的，因此每个方向都必须单独进行关闭。当一端完成它的数据

发送任务后就发送一个 FIN 来终止这个方向的连接。收到一个 FIN 只意味着这一方向上没有数据流动，一个 TCP 连接在收到一个 FIN 后仍能发送数据。首先进行关闭的一端将执行主动关闭，而另一端执行被动关闭。

（1） TCP 客户端发送一个 FIN，用来关闭客户到服务器的数据传送（报文 4）

（2） 服务器收到这个 FIN，它发回一个 ACK，确认序号为收到的序号加 1（报文 5）和 SYN 一样，一个 FIN 将占用一个序号

（3） 服务器关闭客户端的连接，发送一个 FIN 给客户端（报文 6）

（4） 客户段发回 ACK 报文确认，并将确认序号设置为收到序号加 1（报文 7）