**文档6**



360 DNS安全网关系统

产品开发文档

­

北京鸿腾智能科技有限公司

二〇二三年二月

**版权声明**

©2021北京鸿腾智能科技有限公司保留所有权利

本文档所有内容均为北京鸿腾智能科技有限公司（以下简称：“360政企安全”）独立完成，未经360政企安全作出明确书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印或其他形状）对本文档的任何部分进行复制、修改、引入检索系统或者传播。

Revision Record 修订记录

| Date  日期 | Revision Version  修订版本 | Sec No.  章节 | Change Description  修改描述 | Author  作者 |
| --- | --- | --- | --- | --- |
| 2021/8/10 | V1.0 |  | 初版完成 | 柯强 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[1. 产品设计 3](#_Toc79755997)

[1.1产品目标 3](#_Toc79755998)

[1.2总体技术方案 3](#_Toc79755999)

[2. 子系统描述 5](#_Toc79756000)

[2.1数据处理平台 6](#_Toc79756001)

[2.1.1 数据采集引擎 6](#_Toc79756002)

[2.1.2 数据预处理引擎 7](#_Toc79756003)

[2.2数据计算平台 7](#_Toc79756004)

[2.2.1 实时检测引擎 8](#_Toc79756005)

[2.2.2 异步分析引擎 9](#_Toc79756006)

[2.3数据存储平台 10](#_Toc79756007)

[2.3.1 原始流量存储 ClickHouse 10](#_Toc79756008)

[2.3.2 结构化数据存储MongoDB 12](#_Toc79756009)

[2.4 WEB平台 12](#_Toc79756010)

[2.4.1 WEB API 13](#_Toc79756011)

[2.4.2 WEB 系统 13](#_Toc79756012)

[2.5 基础架构、监控平台 16](#_Toc79756013)

[2.5.1 基础架构 16](#_Toc79756014)

[2.5.2 监控平台 18](#_Toc79756015)

[3. 核心算法 19](#_Toc79756016)

[3.1 未知威胁检测 19](#_Toc79756017)

[3.1.1心跳域名识别 19](#_Toc79756018)

[3.1.2 NOD 域名识别 20](#_Toc79756019)

[3.1.3逆周期域名识别 20](#_Toc79756020)

[3.1.4可疑境外域名识别 21](#_Toc79756021)

[3.1.5 DNS Tunnel 识别 21](#_Toc79756022)

[3.1.6 自动化分析 22](#_Toc79756023)

[3.2 资产画像 23](#_Toc79756024)

[3.3 域名特征识别 24](#_Toc79756025)

[4. 软硬件环境 25](#_Toc79756026)

[4.1 硬件环境 25](#_Toc79756027)

[4.2 软件环境 26](#_Toc79756028)

[4.3 网络环境 26](#_Toc79756029)

[4.3.1 互联网环境 26](#_Toc79756030)

[4.3.2 内网环境 27](#_Toc79756031)

[5 产品部署 28](#_Toc79756032)

[5.1 流量镜像 28](#_Toc79756033)

[5.1 DNS服务器日志 29](#_Toc79756034)

# 产品设计

## 1.1产品目标

应对大安全时代网络威胁，越是对安全要求高的企业，面对的安全威胁越是复杂，攻击手段往往更加高级、隐蔽，威胁也更加难以发现。360DNS安全网关系统的核心目标就是帮助企业客户看见威胁，更具体讲就是看见失陷资产，连接控制服务器的行为。

360DNS安全网关系统基于DNS流量实现安全威胁识别，DNS协议作为互联网的基础和核心协议，同样是恶意软件和控制服务器之间通信的主要手段(根据Cisco 2016年度安全报告，92.3%恶意软件在连接C&C时会使用DNS协议)，因此通过DNS流量识别安全威胁，可以涵盖绝大多数恶意行为。此外DNS流量天然具有接入成本低、部署简单、可大规模扩展等优势。

客户将DNS流量接入系统后，可快速获得以下几个能力：

* 整体安全态势感知能力
* 已知威胁、未知威胁检测能力
* 威胁分析、威胁溯源能力
* 资产可视化、DNS流量可视化能力

同时为了便于定位失陷资产，实现精准威胁溯源和研判，系统缺省还要求接入DHCP流量，通过DHCP流量可以定位具体资产名，帮助识别企业网络结构。

## 1.2总体技术方案

360DNS安全网关系统的核心逻辑是通过对DNS流量的层层过滤、计算、关联、实现已知威胁和未知威胁的检测，并通过高交互WEB系统，支持对威胁的分析、研判、溯源。为了满足这一目标，系统总体分为云端、后端、前端三部分。云端负责情报赋能，对接360云端安全大脑和360 网络安全研究院的情报平台，获取实时IoC情报和各类威胁研判情报。后端本质是一个数据处理平台，包括数据采集、数据计算、数据存储等子系统，追求高效稳定，可扩展。前端是一个高交互WEB平台，支持功能强大的威胁分析和高质量可视化模块。

产品整体采用分布式系统架构，由多个子系统组成，所有子系统低耦合、高内聚，子系统之间通过Kafka消息队列和Restful API通信。通过分布式架构，平台具有水平扩展、高可用的优点，可根据不同客户规模、不同流量大小，灵活设计单机方案或集群方案。对于中小型客户，可以通过单机模式快速实现部署，成本低、接入快。对于大型、超大型企业客户，可以利用分布式设计的优势，在不对产品架构、代码做任何调整的情况下，仅通过新增硬件资源就可以实现数据处理能力、数据计算能力、数据存储能力、数据分析能力的线性提升，满足大型、超大型企业的业务需求。且分布式设计可轻易实现高可用，通过冗余备份，保证个别设备宕机的情况下，平台同样能平稳运行、数据安全不丢失。

# 子系统描述

360DNS安全网关系统由多个子系统组成，DNS流量经采集引擎进入系统后，会在多个子系统间流动，被层层解析、标注、分类、关联、检测、存储，最终输出已知威胁和未知威胁告警。根据各子系统在整个产品架构中的功能划分，可以分为五个子系统：

* 数据处理平台
* 计算平台
* 存储平台
* WEB平台
* 基础架构、监控平台

不同的子系统根据定位不同又由多个模块组成，例如计算平台包含实时检测引擎和异步分析引擎。下图为多个子系统间的整体架构设计，接下来章节将会逐一展开，分别介绍每一个子系统的功能定位，技术实现。



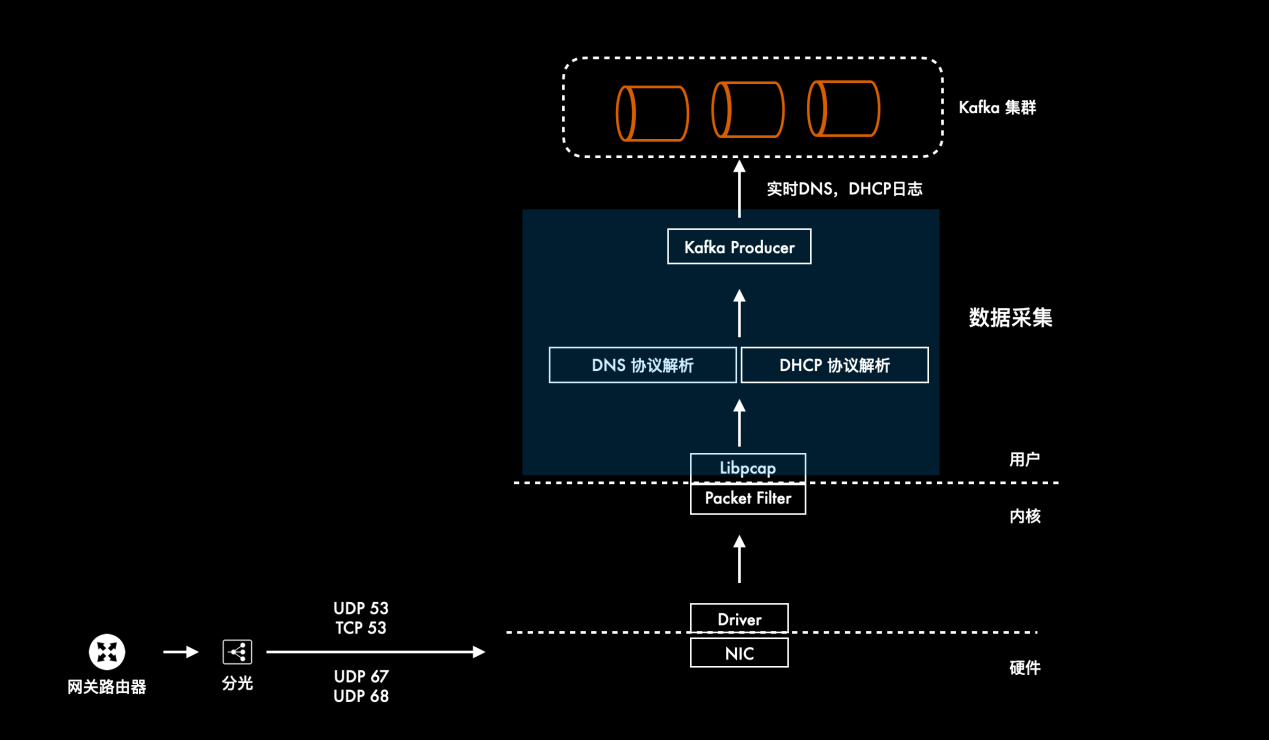
## 2.1数据处理平台

数据处理平台主要负责数据采集、数据预处理、数据标注、数据入库等工作。根据他们负责的功能不同、技术实现不同、开发语言不同，可以分为数据采集引擎和数据预处理引擎。

### 数据采集引擎

360DNS安全网关系统的数据接入方式有两种：分光镜像和syslog日志。分光镜像的场景下，数据采集引擎负责DNS和DHCP分光流量的抓包、报文重组、协议还原等工作，解析完成的DNS流量和DHCP流量，会以文本的形式发送到Kafka队列，交由下游数据处理引擎继续处理。syslog场景下，数据采集引擎负责接收syslog发来的DNS服务器日志，并发送到Kafka队列。

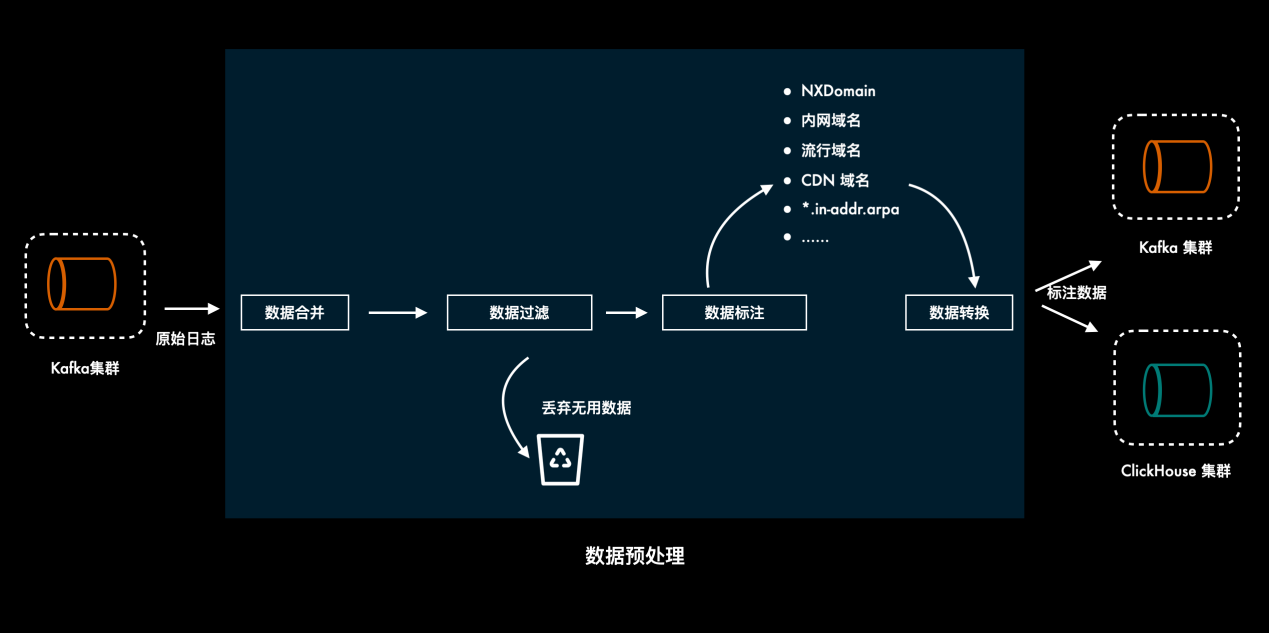
分光镜像是我们的主要数据接入场景，因此接下来以分光镜像场景为例，介绍数据采集引擎的整体设计实现。



数据采集引擎为C语言实现，流量抓包部分包含两个版本：Libpcap和Netmap，默认使用libpcap版本，优点是工作在用户态，对硬件和操作系统无依赖，简单灵活，但性能不如Netmap。Netmap支持更大流量抓包解析，但需要重新编译网卡驱动，对硬件和操作系统有依赖，只有在DNS流量超过600M bps才会考虑启用这一方案。不过相对于IPS、全流量检测等设备，DNS流量通常仅占企业流量的1% - 1‰，因此缺省的libpcap就可以满足绝大多数场景的需求。

### 数据预处理引擎

数据预处理引擎本质是一个流式数据处理程序，实时DNS流量经采集引擎解析成文本格式之后进入Kafka，数据预处理引擎会实时从kafka里面将数据消费出来，并实时对数据进行合并、过滤、标注、转换等ETL操作。预处理后的数据会分成两路，一路重新回到kafka，由后续的实时检测引擎消费处理。另一路由数据入库程序，将数据批量写入Clickhouse数据库集群。



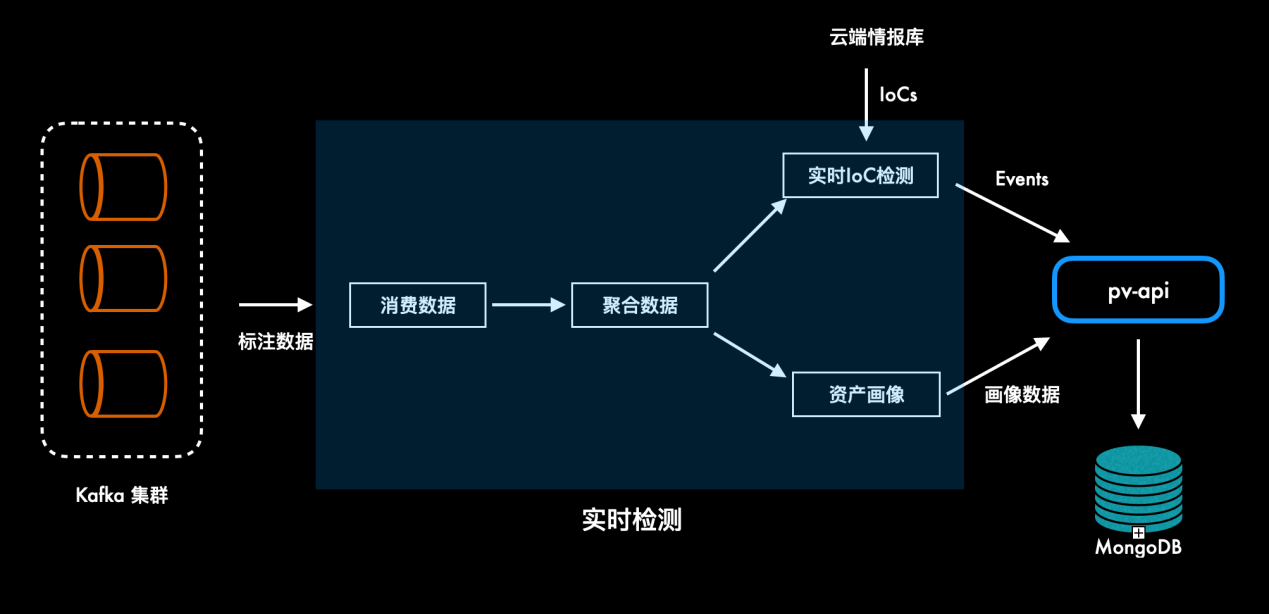
数据预处理引擎由GO语言开发，GO语言的并发编程、编译执行、自动内存回收等特性，非常符合数据预处理引擎对运行性能高、开发高效、流式处理模型的需求。

## 2.2数据计算平台

计算平台是整个产品的核心系统，标注数据进入Kafka和ClickHouse后，计算平台会对客户的DNS流量进行各种维度的计算分析、情报关联、跑算法模型等，并实现威胁告警、用户行为分析、特征分析、资产识别等核心功能。计算平台根据功能不同，分为实时检测引擎和异步分析引擎，他们的功能定位不同，实现技术也完全不同。

### 2.2.1 实时检测引擎

实时检测引擎最主要的功能是已知威胁检测，用Go开发，本质也是一个流式数据处理程序，程序实时从Kafka消费DNS数据，经过数据聚合后，再和云端准实时同步的IoC情报库匹配，识别已知威胁。



已知威胁检测依赖IoC情报库的质量，而360作为国内最大的网络安全公司，拥有业内绝对领先的IoC情报资源。除了情报质量本身之外，理解和用好威胁情报同样重要，用不好最典型的例子就是大量误报，以及告警空洞缺乏威胁研判的上下文。本产品的研发团队 360 网络安全研究院(netlab)，作为国内最早开始研究和建立威胁情报库的团队，在威胁情报应用和分析领域有着多年积累和经验，而这些经验也都融入到了实时检测引擎的系统逻辑中。

实时检测支持多类已知威胁，包括：

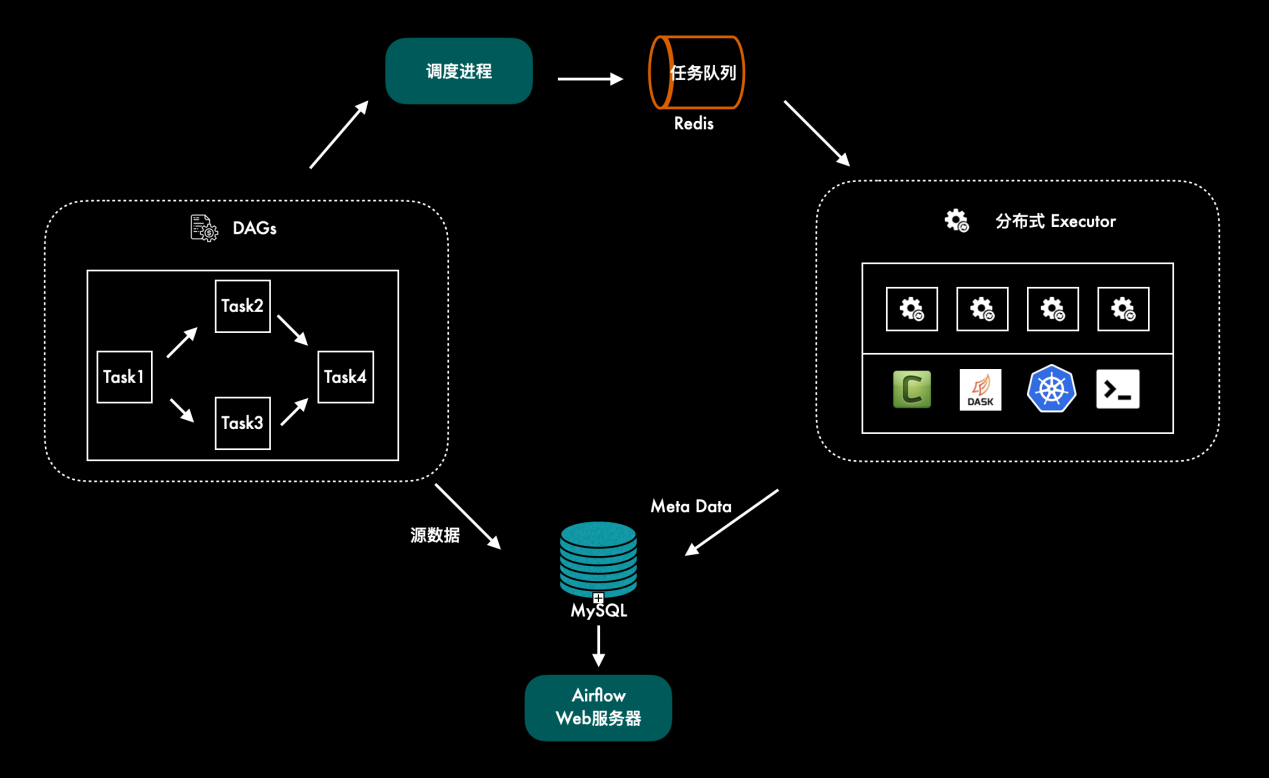
* 远控木马
* 勒索软件
* 后门程序
* 挖矿木马
* DDoS僵尸网络
* 数据窃取软件
* 恶意程序下载
* DGA域名检测

检测到的已知威胁告警最终通过API，存入MongoDB数据库。

### 2.2.2 异步分析引擎

异步分析引擎是360DNS安全网关系统最为复杂的子系统之一，基于Airbnb开源的Airflow (https://airflow.apache.org/)开发，实现未知威胁检测、恶意行为分析、威胁情报关联、网络异常识别、数字资产识别等诸多功能。这些功能的实现通常都较为复杂，涉及大规模数据计算，需要运行复杂算法模型，并由多个子流程配合完成。由于未知威胁检测等程序过于复杂，难于实现、难于调试，在异步分析引擎中通常将复杂的程序拆解成多个相对简单可控的子任务，然后对各类计算、分析、算法模型等子任务，进行调度、串联、编排，形成一个个灵活的workflow，通过workflow实现各种复杂业务逻辑。在Airflow的概念中，一个负责的业务逻辑被定义为一个DAG (Directed acyclic graph 有向无环图，也就是一个workflow)，这个DAG包含多个Task（子任务）， 这些Task完成具体的业务功能。而执行这些Task的载体被定义为Executor，Executor可以是本地进程，也可以是分布式程序，例如Celery或Dask，分布式Executor的好处是可以将一个负责的DAG调度到多台机器上共同完成计算。由于360DNS安全网关系统多是一些CPU 密集型的计算任务，因此我们使用Dask作为我们的Executor，好处是对于复杂的算法模型，可以利用多台设备的CPU和内存共同完成计算任务。

下图简单描述了异步分析引擎如何基于Airflow实现了一个功能完整、健壮、可扩展的分布式任务调度和工作流引擎



有别于实时检测，异步分析任务通常都是定时运行，由Airflow负责调度，根据我们的业务定义，这些任务每分钟、每小时或每天运行一次，运行状态和日志由Airflow进行监控和管理，并对运行失败的任务进行重试以及告警。根据业务需要，当前产品的异步分析引擎实现了十几个DAG，这些DAG对实时性要求不高，但通常有几个特点：

* 处理的数据量大。很多特征统计和算法类的任务，必须基于一定时间窗口的数据来计算才可能准确，例如恶意行为分析、未知威胁监测等。
* 算法复杂。以未知威胁检测为例，要实现准确的未知威胁检测，需要运行多个算法模型，需要进行多维威胁情报关联，还要辅助多个特征识别。
* 系统资源占用高。因为涉及的数据量大，使用的模型复杂，任务被调度执行时，对系统的CPU和内存通常有比较大的挑战。为了应对超大规模客户单机可能有瓶颈的挑战，我们选择Dask作为分布式Executor保证批处理引擎的可扩展
* 涉及流程多。一个功能通常涉及多个子任务，需要Airflow对这些子任务进行串联、编排完成复杂的业务逻辑。

## 2.3数据存储平台

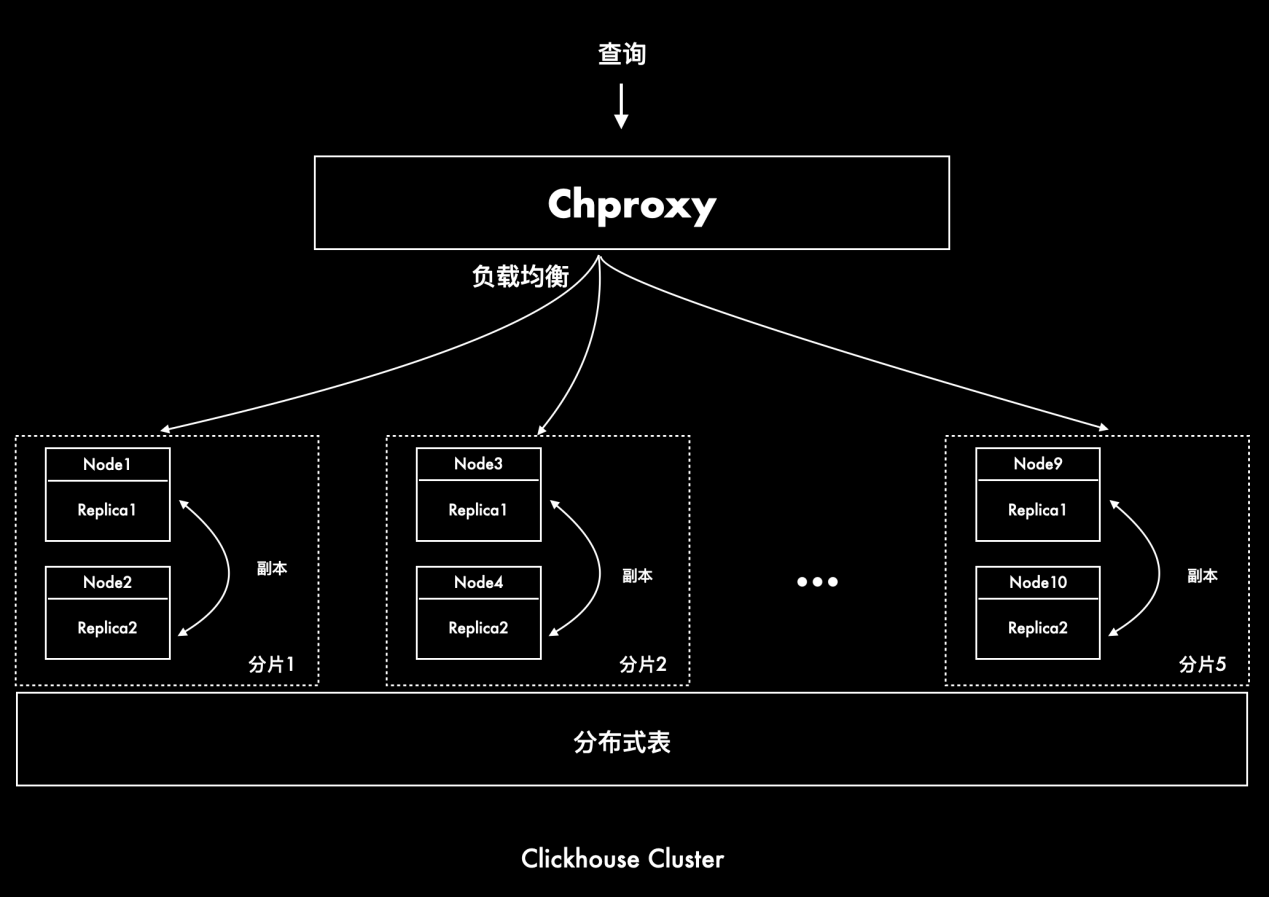
360DNS安全网关系统有两个主存储数据库，ClickHouse和MongoDB。 ClickHouse负责存储DNS原始日志和聚合后的视图数据，MongoDB负责存储告警、账号等结构化数据。ClickHouse中的数据量大，数据结构相对固定简单，可以支持海量数据的OLTP、OLAP查询。MongoDB中存储的数据量相对少，但结构灵活多样，可以支持相对复杂的关联查询。

### 2.3.1 原始流量存储 ClickHouse

区别于大多数流量检测类产品只存储告警流量，360DNS安全网关系统会存储全量DNS数据，并最少保存一年历史数据。这是本产品实现精准告警、未知威胁检测、用户行为分析、威胁溯源等诸多重要功能的基础。且全量数据存储，可以让用户快速评估1-day，N-day漏洞在客户网络中的感染情况。例如近期披露的SolarWinds供应链攻击，有了全量数据存储，客户就可以在攻击刚披露，而所有安全设备还没来得及跟进时，就可以通过IoC域名排查自己网络中是否有资产感染威胁。但全流量存储对于数据库的性能、成本等是巨大挑战，我们在衡量多个数据库产品后，最终选择了查询性能高、写入速度快、数据压缩比高的ClickHouse作为我们的主存储数据库。

ClickHouse 是一款由俄罗斯 Yandex 公司开发的 C++ 开源高性能 OLAP 列式数据库，ClickHouse属于比较新的数据库技术，以性能卓越著称。在我们这个产品中，ClickHouse主要存储原始DNS日志和DHCP日志，以及根据不同业务场景设计的聚合视图，例如月、周、天、小时、分钟等不同时间维度的聚合视图。视图是Clickhouse一个重要特性，可以在数据入库时按照业务设计的维度对数据自动进行聚合存储。有了不同时间维度的视图，当前端页面选择了不同时间窗口时，后端就可以灵活使用不同视图数据进行响应。例如分析一天的流量数据时，可以使用原始表数据，这样能得到精度到秒级别的数据。分析一周数据时就可以使用按小时聚合的数据，虽然时间精度只能到小时级别，但小时视图极大压缩了数据量，可以显著提升查询响应速度，而且时间窗口为一周时，精确到小时的数据一般足够满足我们的分析需求。

ClickHouse也是一个优秀的分布式数据库，根据客户规模和客户流量大小，可以进行集群化部署。集群模式下可以获得更好的性能，更高的可用性，这也是我们推荐的部署方式。下图示例了一个十台节点组成的CH集群架构，十台机器划分为5个分片，数据均衡存储在这5个分片中，每个分片又由2台设备组成，互为备份。查询请求通过CHproxy实现负载均衡，将查询请求均衡分散到集群的各个设备。



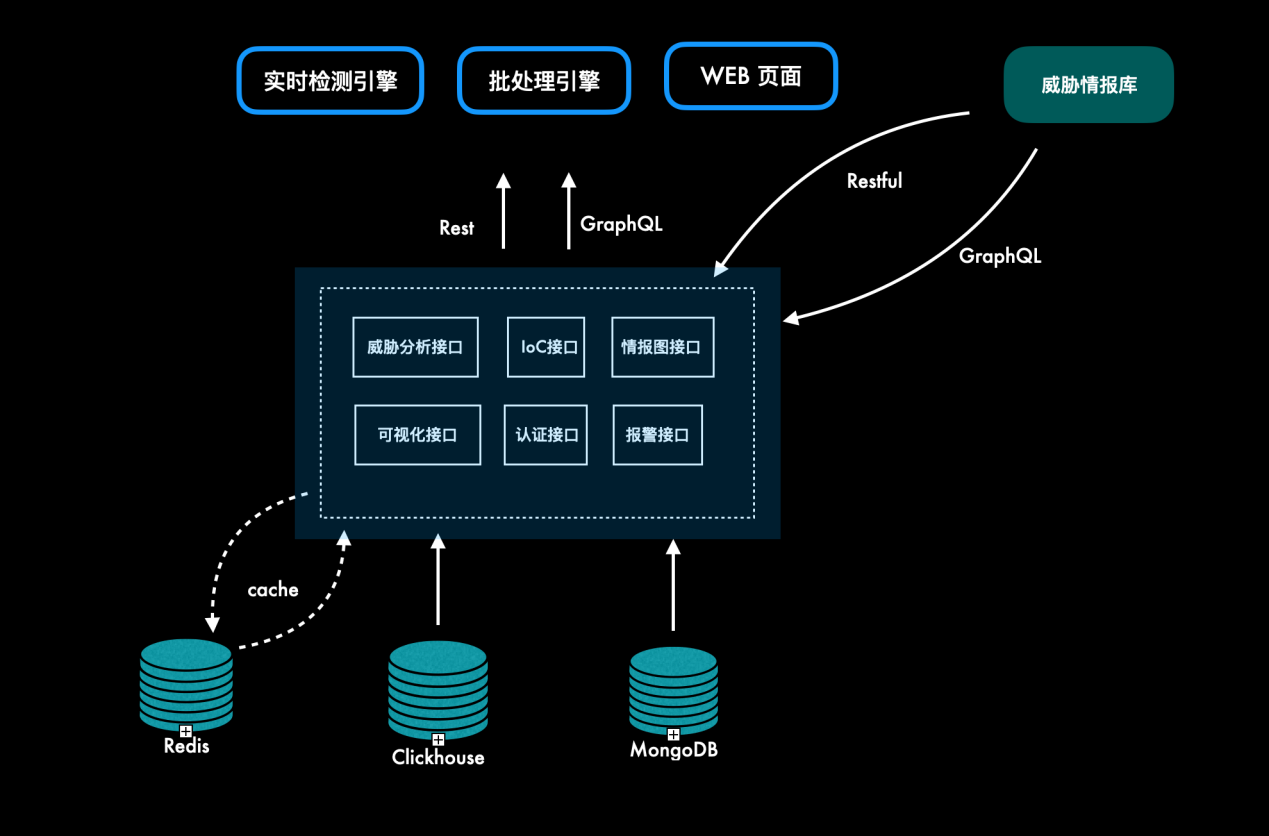
### 2.3.2 结构化数据存储MongoDB

MongoDB相对来说是一个成熟得多的数据库产品，早已在多个领域有非常多成功的应用案例，本文就不对MongoDB做过多介绍。360DNS安全网关系统主要利用MongoDB存储告警、配置等schema较为灵活的数据，同时使用MongoDB代替MySQL等关系型数据，存储账号、标签等数据，通过数据结构设计，实现join查询。

## 2.4 WEB平台

相较于传统安全产品WEB仅仅是告警和数据展示，本产品开发了一个高质量WEB系统来支持威胁分析工作，安全工程师可以在WEB系统上对各种已知威胁、未知威胁高效分析，精准研判。WEB平台分为WEB API和WEB页面两部分，WEB API负责数据计算和各种业务逻辑处理，WEB 页面是前端高交互页面的实现。

### 2.4.1 WEB API

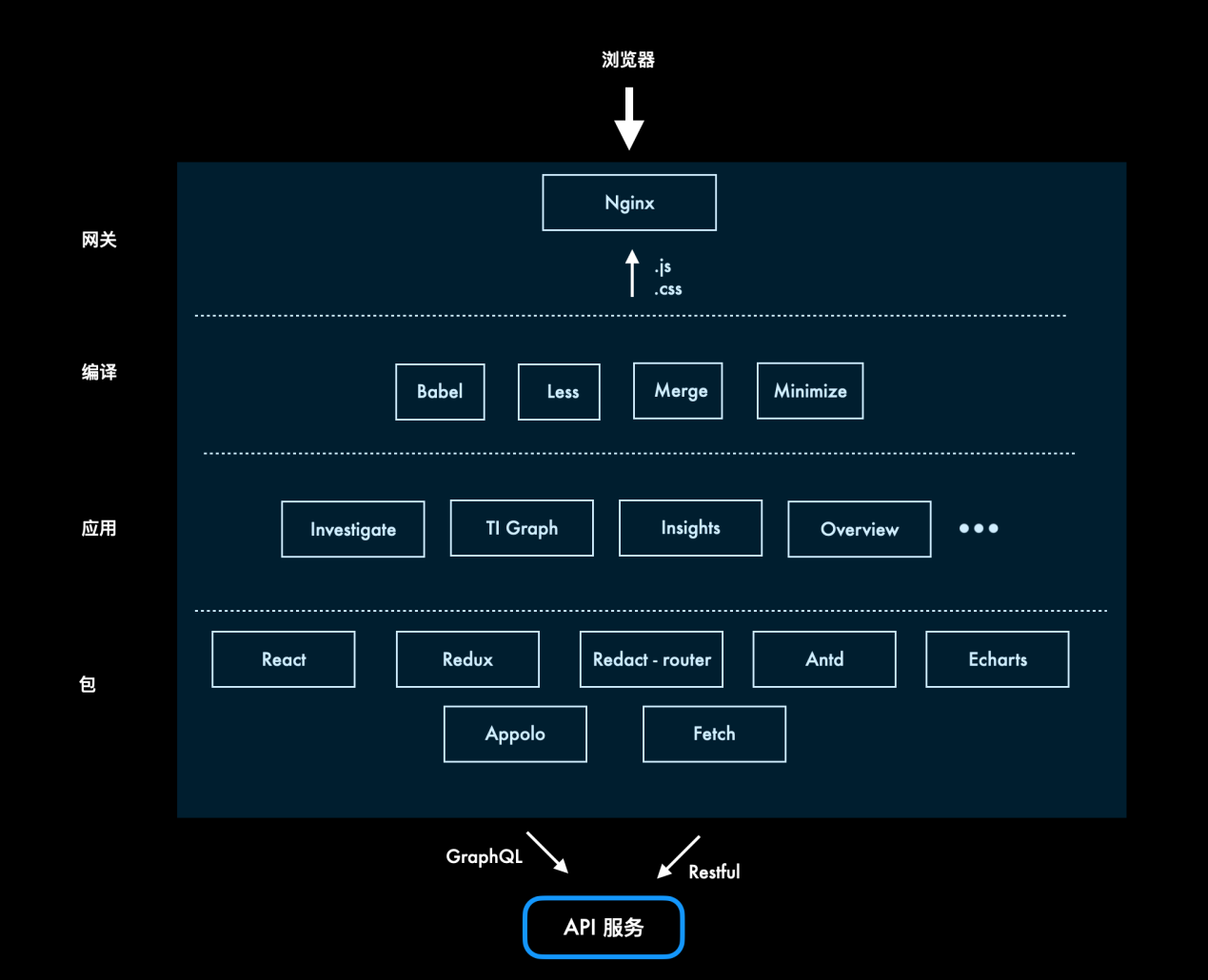
WEB API 是整个系统的中间业务逻辑层，原则上对数据库的所有操作均由API服务实现，其它子系统要查询、更新数据库，均通过调用API的相应接口来完成。API 实现了一系列标准Restful接口，使用Python开发，Flask作为后端WEB框架，Gunicorn作为API进程的容器来支持高并发请求。由于产品还实现了一个高交互的威胁情报图，针对图数据库的数据结构特点和前端页面的请求特点，图相关的API则使用了当前较为创新的GraphQL作为API协议。

除了本地数据，API还会将云端情报数据和本地数据深度融合，为威胁分析提供需要的上下文和情报信息。

### 2.4.2 WEB 系统

WEB系统使用当前流行的前端技术React + Type Script开发，实现了一个功能强大，交互丰富的WEB系统。该WEB系统可以高效完成威胁分析、告警管理等功能，同时在流量可视化、资产可视化、威胁分析可视化方面，本产品有非常多创新和高质量的实现。

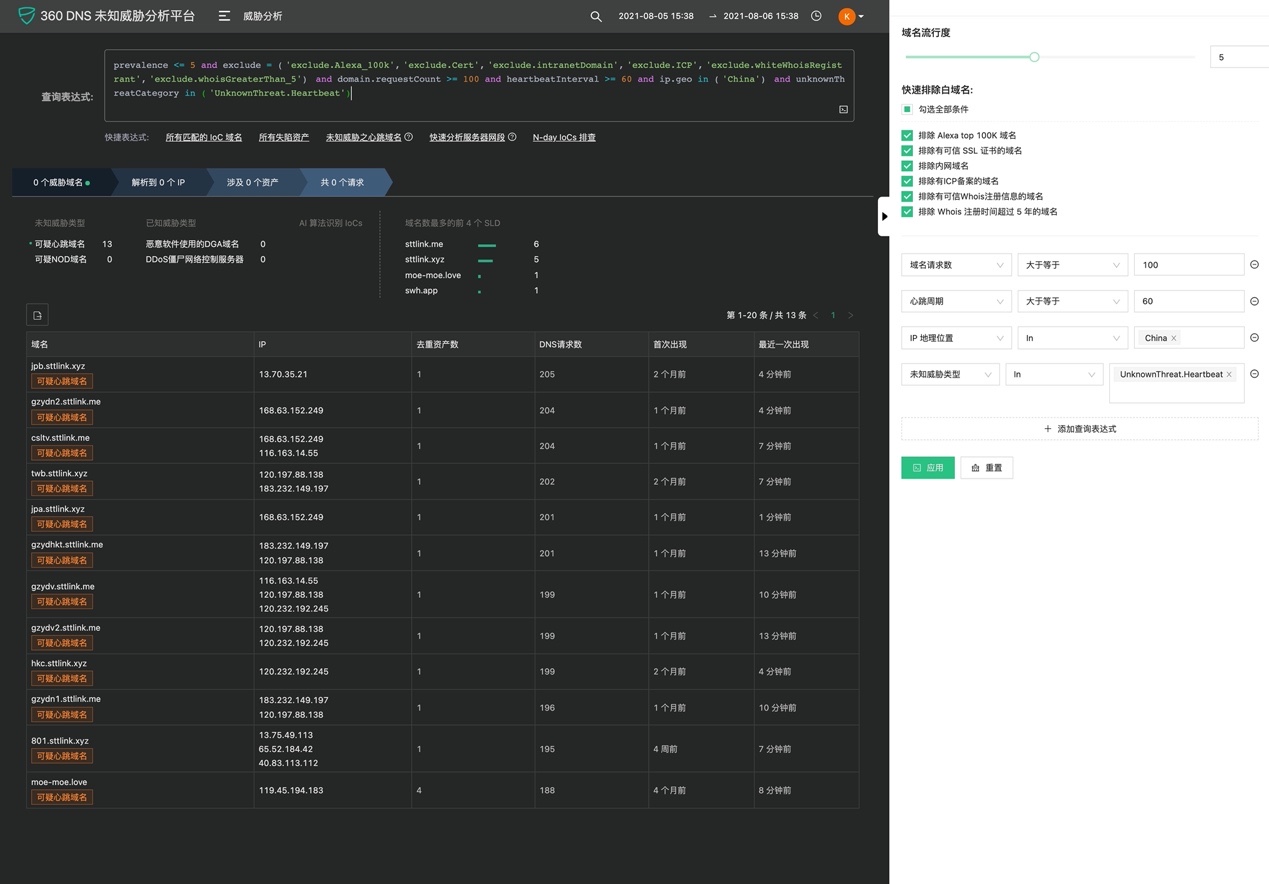
下图为WEB系统具体前端技术栈：



接下来以两个页面为例，重点说明本产品的WEB系统在前端交互和数据可视化方面的高质量实现。

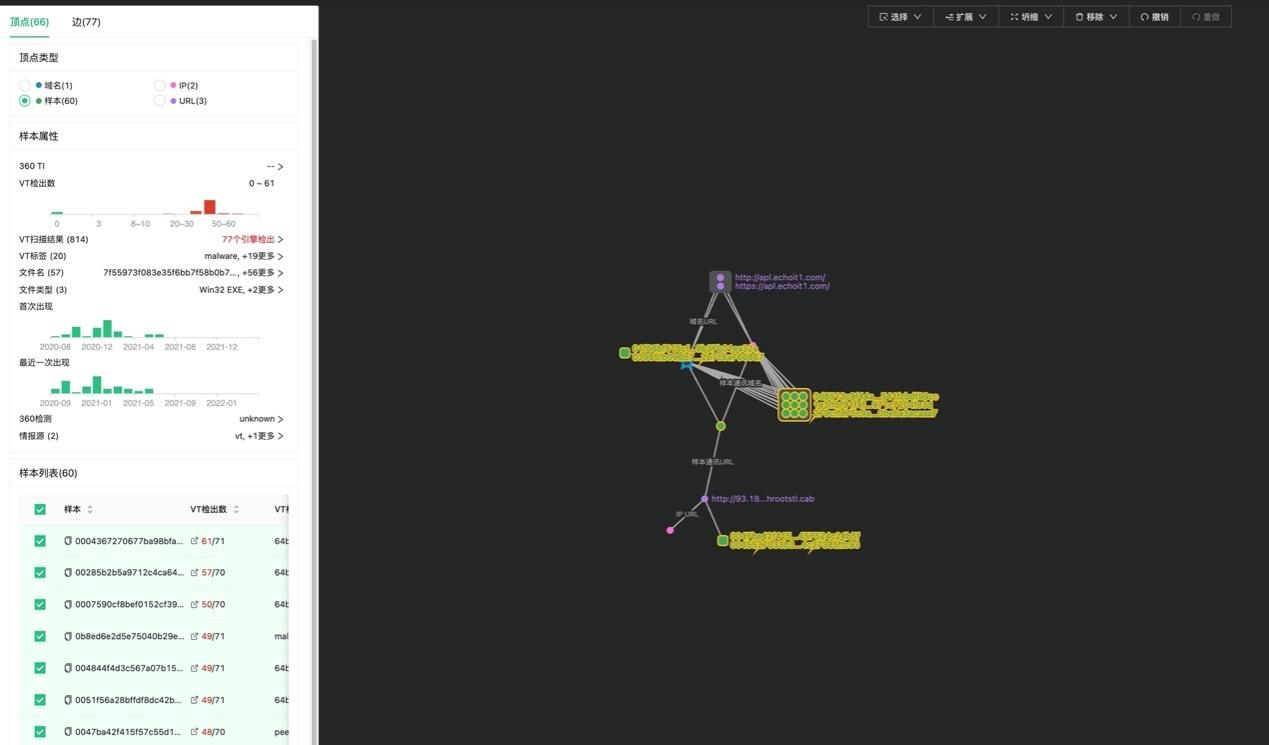
* 高级威胁分析

      对于安全分析专家，可利用在线威胁分析系统提供的自定义查询语言，以及系统自动标注的数据和提供的各种线索，主动分析APT等高级威胁。



* 威胁情报图

     本地数据与云端情报深度融合，利用系统强大的交互分析能力，快速拓展线索，了解威胁相关情报。



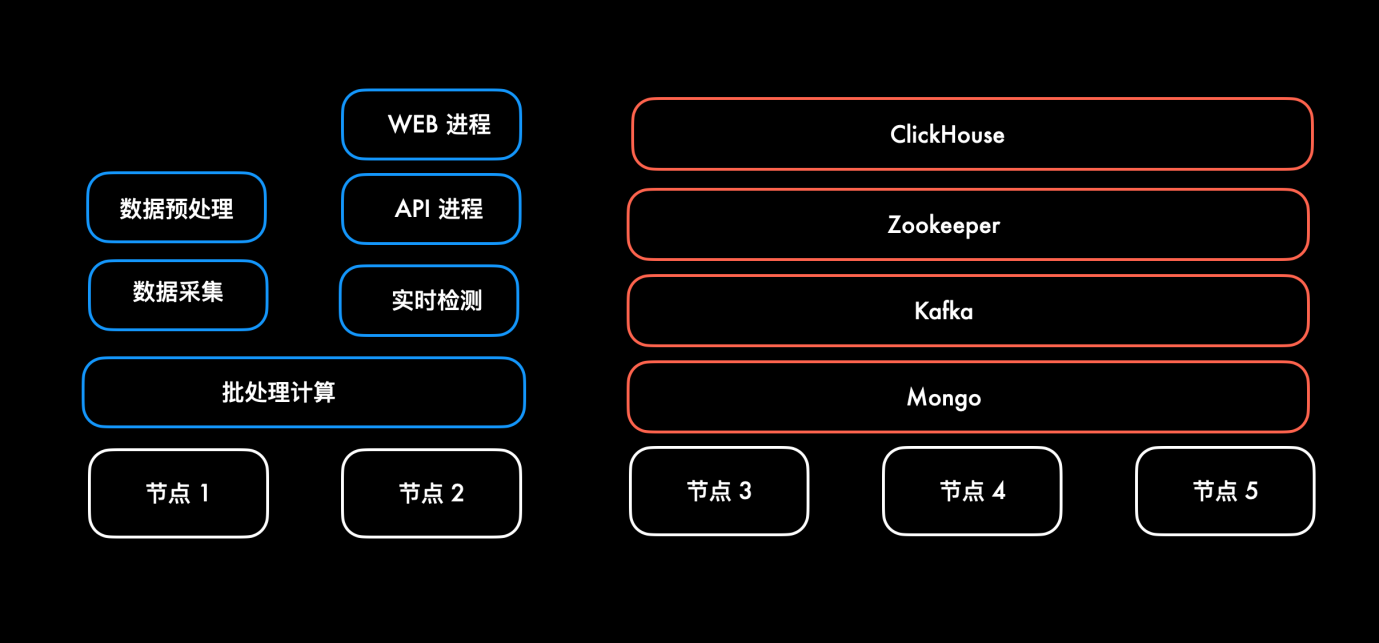
## 2.5 基础架构、监控平台

### 2.5.1 基础架构

通过前面章节描述可知，360DNS安全网关系统是一个子系统众多，结构复杂，实现技术多样的大型系统。众多子系统根据业务需求不同，采用不同的开发语言、不同的技术方案实现。除了自己开发的业务子系统，产品还依赖多个开源的存储、消息队列、分布式一致性系统，包括ClickHouse, MongoDB, Redis, Kafka, Zookeeper, CHProxy。无论是自己开发的业务子系统，还是采用的开源系统，如何让这么多复杂的程序在同一个或多个节点下稳定运行，对产品的基础架构是一个不小的挑战。特别是产品支持分布式集群，在集群方案下，众多业务进程，开源系统运行于多个节点，程序之间又需要跨节点互相协作， 更进一步增加了基础架构的复杂度。继续介绍前先解释一下节点的定义，本文提到的节点是指运行程序的设备，360DNS安全网关系统支持的节点可以是物理裸机、虚拟机，或公有云、私有云平台上的云主机等，整个系统不依赖具体硬件平台或型号，可以稳定运行在多类硬件或虚拟设备上。

单节点的架构相对比较简单，所有子系统都在同一台设备上运行，无论是自己开发的应用程序还是各类开源存储、消息队列都工作在单机模式下，不用考虑负载均衡和高可用，只需要做好系统资源隔离，稳定运行即可。

多节点的分布式集群下，架构相对复杂很多，要根据不同子系统的业务特点，资源占用情况，将子系统合理分配在不同节点运行。对于存储系统，还要考虑数据水平分布，数据高可用，读写负载均衡等问题。不同客户大小，需要的集群规模不一样，采用的集群架构也不完全一样。下图以一个5节点的小型集群为例，介绍分布式集群下的基础架构。



5个节点简单分为了两组，一组运行我们自己开发的各类应用程序，一组运行存储、消息队列等基础系统。有一些子系统跨多节点运行，例如批处理计算系统、MongoDB、Kafka、ClickHouse等，有一些只运行在单个节点上，具体是单节点运行还是多节点运行依赖于该子模块对系统资源的需求。例如ClickHouse作为主数据存储系统，需要消耗大量CPU资源、磁盘存储资源，因此将它部署在三台设备上组成一个分布式集群，这样就可以将数据分散存储在三台设备上，读写操作也均衡分布到三台设备上，从而增强ClickHouse的整体性能。还有批处理计算在运行一些复杂检测任务时需要消耗大量CPU和内存资源，因此将他们分布在两台设备，同时利用两台设备的CPU和内存资源，以增加检测能力。而数据采集、数据预处理、API等子系统，出于实际性能需求和成本考虑，在5节点的集群上运行于单个节点就能满足业务需求。对于超大规模客户，当这些子系统，单机有瓶颈时，也都支持分布式部署在多个节点上，从而线性扩展整个平台的威胁检测、威胁分析能力。

除了单节点架构、分布式多节点架构，产品还将支持云原生架构，让整个系统运行于Kubernetes的容器云上。

### 2.5.2 监控平台

对于一个复杂的系统，对整个系统的运行状态进行监控同样至关重要。360DNS安全网关系统的监控分三部分：

* 对集群的整体监控，例如集群健康状况，各节点状态等。
* 对具体节点的系统监控，例如CPU使用率、内存占用、磁盘剩余空间、网卡带宽等
* 对业务关键指标的监控，例如关键进程状态、数据采集统计、数据库空闲存储、消息队列生产消费速度等

监控系统基于当前流行的Promethues和Grafna实现，Promethues负责收集和存储各类Metrics数据，Grafana 对数据进行分析和展示。还有多个开源和自研的Exporter负责导出各类关键指标数据，例如系统的CPU、内存信息，数据库的存储空间信息等。基于这套开源技术栈，我们实现了一个非常专业监控系统，对产品的各类关键指标进行实时监控和可视化展示。



# 软硬件环境

360DNS安全网关系统对于硬件平台、型号没有强制要求，推荐是360提供的标准软硬一体设备，但也可以使用客户提供的硬件设备或是虚拟机设备，亦或是私有云、公有云主机。操作系统则必须是标准CentOS 7.2.X版本。

## 4.1 硬件环境

通过前面的介绍可知360DNS安全网关系统是一个前后台很复杂的产品，包含数据处理引擎、数据计算引擎、数据存储平台、系统监控平台、WEB平台等诸多组件和程序，不同组件和程序对于系统的硬件资源都有一定的要求。而不同客户规模、流量大小又会对硬件资源的要求带来一定的差异性。这里以我们生产的标准软硬一体设备为例，介绍系统推荐的硬件环境。

标准软硬一体设备综合考虑所有系统组件、运行程序对于CPU、内存、磁盘、网卡的资源消耗，设计了一个标准的硬件环境。

## 4.2 软件环境

软件环境只有操作系统要求，无论标准软硬一体设备还是由客户提供的服务器设备，均安装标准版的CentOS 7.9系统。

## 4.3 网络环境

### 4.3.1 互联网环境

360DNS安全网关系统在威胁检测和威胁分析过程中大量依赖360安全大脑的实时云端情报，因此产品必须能连接互联网才能正常工作。虽然很多安全产品为了实现不连接互联网也能使用情报库，通过将IoC库离线保存在本地，然后通过离线包更新的方式来使用威胁情报。但这种方式下，威胁情报真正为产品赋能的效果是非常有限的。

首先，威胁情报绝不仅是IoCs，还有PassiveDNS、Whois数据、证书数据、IP数据、样本数据、沙箱数据、漏洞数据、大网蜜罐数据、大网测绘数据等等，所有这些数据对于综合检测、分析威胁，精准报警都至关重要，360DNS安全网关系统大量使用这些数据进行多维情报关联和威胁研判。而从硬件成本、维护成本考虑，这些情报都是没有办法离线存储在客户本地网络的。以PassiveDNS数据为例，360云端仅存储这个数据就用了几十台硬件服务器，沙箱分析的硬件设备则超过上百台，要把这些情报数据都离线在客户本地网络显然不现实。

其次，在当前网络攻防环境下，情报的时效性要求非常高，只有实时更新才能发挥它的价值，一旦情报没有及时更新，就可能引起漏报、误报。而离线存储，需要人不定期来手动升级情报，这种方式天然就决定了情报的更新不可能非常及时。而360DNS安全网关系统在联网的环境下，几乎实时都在和情报库通信，获取各类最新的情报。

基于上述两点考虑，我们认为只有联网才能发挥情报的真正价值，因此在设计之初就确定了360DNS安全网关系统必须联网才能工作的设计。而对于连接互联网有安全顾虑的客户，可以在防火墙添加ACL规则，让360DNS安全网关系统仅能通过互联网连接我们的云端情报服务和升级服务对应的域名，并阻断所有其它连接。情报服务和升级服务对应的域名为：

* api.netlab.360.com (情报服务)
* update.netlab.360.com (升级服务)

### 内网环境

产品对内网环境有两个要求：

* 通过流量分光的方式接入数据时，产品需要和分光设备在同一个机房，并能将流量接入到设备的镜像口。
* 集群模式下，集群各个设备之间处于相同子网络，可以互相连通。

# 5 产品部署

360DNS安全网关系统支持旁路、串行两种部署模式，下面对两种部署模式详细介绍。

## 串行部署

串行部署是指将360DNS安全网关系统串行到企业内网DNS请求转发路径中，采用此方式，当360DNS安全网关系统识别到恶意域名时，可以实时阻断。串行部署一般分为本地有DNS递归服务器和无递归DNS服务器两种情况进行部署，当企业内网有DNS递归服务器时，一般通过修改DNS递归服务器配置，将上游主DNS服务器配置为360DNS安全网关系统，由360DNS安全网关系统代替本地递归服务器发起递归请求，当企业内网没有递归服务器时，一般通过DHCP下发的方式将360DNS安全网关系统配置下发到终端，完成配置后，终端将DNS请求直接转发到360DNS安全网关系统。

## 旁路部署

旁路部署是指将360DNS安全网关系统旁路在DNS请求的转发路径下，仅对DNS数据进行检测、分析，无法实时拦截恶意域名的访问，通常旁路部署分为两种：

* 流量镜像：通过镜像交换机流量采集DNS请求和响应包。
* Syslog日志转发：通常情况下，本地DNS递归服务器会记录所有的递归请求和响应，并支持通过Syslog的方式转发到第三方平台，因此，通过采集DNS服务器的访问日志也可达到检测和分析内网DNS流量的目的。

客户需要将企业网络的DNS请求和DHCP请求接入360DNS安全网关系统，这是实现威胁检测和威胁分析的基础。目前360DNS安全网关系统支持两种数据接入方式：流量镜像的方式和DNS服务器日志通过Syslog接入的方式。