



API 平台 V3.2.2.0

产品白皮书

上海派拉软件股份有限公司

目 录

第 1 章 引言.....	5
1.1. 编写目的.....	5
第 2 章 产品概述.....	5
2.1. 产品背景.....	5
2.2. 产品功能架构.....	5
2.3. 产品逻辑架构.....	6
第 3 章 产品应用场景.....	7
3.1. 企业级数据互联互通.....	7
3.2. 企业级的 API 安全保护.....	7
3.3. 企业级的 API 开放能力.....	8
3.4. 跨网络的分布式网关集群代理.....	8
第 4 章 产品功能.....	9
4.1. API 智能安全网关.....	9
4.1.1. 运行引擎功能.....	9
4.1.2. 基础功能插件.....	9
4.1.3. 集成扩展插件.....	9
4.1.4. 增值开发插件.....	错误! 未定义书签。
4.2. API 管理平台.....	11
4.2.1. API 管理.....	11
4.2.2. API 监控.....	12
4.3. API 门户.....	12
4.3.1. 门户主页.....	12
4.3.2. API 中心.....	12
4.3.3. API 文档.....	12
4.3.4. 开发者中心.....	13
4.3.5. 多租户自助申请.....	13
第 5 章 产品特性.....	13
5.1. 完善的 API 生命周期管理.....	13
5.2. 强大的 API 安全防护能力.....	14
5.3. 支撑高并发、高流量场景.....	14
5.4. 服务智能熔断降级.....	15
第 6 章 产品支持系统列表.....	15

6.1. 操作系统.....	15
6.2. 浏览器.....	15
6.3. 数据库.....	16
第 7 章 产品业务价值.....	16
7.1. 制定管理和规范体系.....	16
7.2. 敏捷响应客户需求.....	16
7.3. 数字化安全价值.....	16
7.4. 及时的智能监报告警.....	16

版本记录

版本	日期	作者	修订内容
V1.1.0.0	2019-05-8	郭利民	文件创建
V2.1.0.0	2020-07-28	郭利民	添加 API 管理平台、API 门户
V3.1.1.0	2020-10-28	陈招英	添加产品优势、分布式集群管理
V3.1.2.0	2021-01-28	郭利民	更新 API 智能安全网关、API 门户、API 管理平台
V3.1.3.0	2021-03-22	郭利民	将 API 监控和 API 管理整合
V3.1.3.0	2021-05-31	陈招英	新增 ES 插件、告警历史以及审计日志的改造
V3.2.2.0	2021-06-30	郭利民	增加了 API Mock、渗透测试防护、基于 ABAC 的访问控制、日志链集成

第 1 章 引言

1.1. 编写目的

本文档编写的主要目的是介绍派拉软件 API 平台，帮客户迅速了解派拉软件 API 平台的产品功能、产品优势、产品使用场景以及产品价值。

第 2 章 产品概述

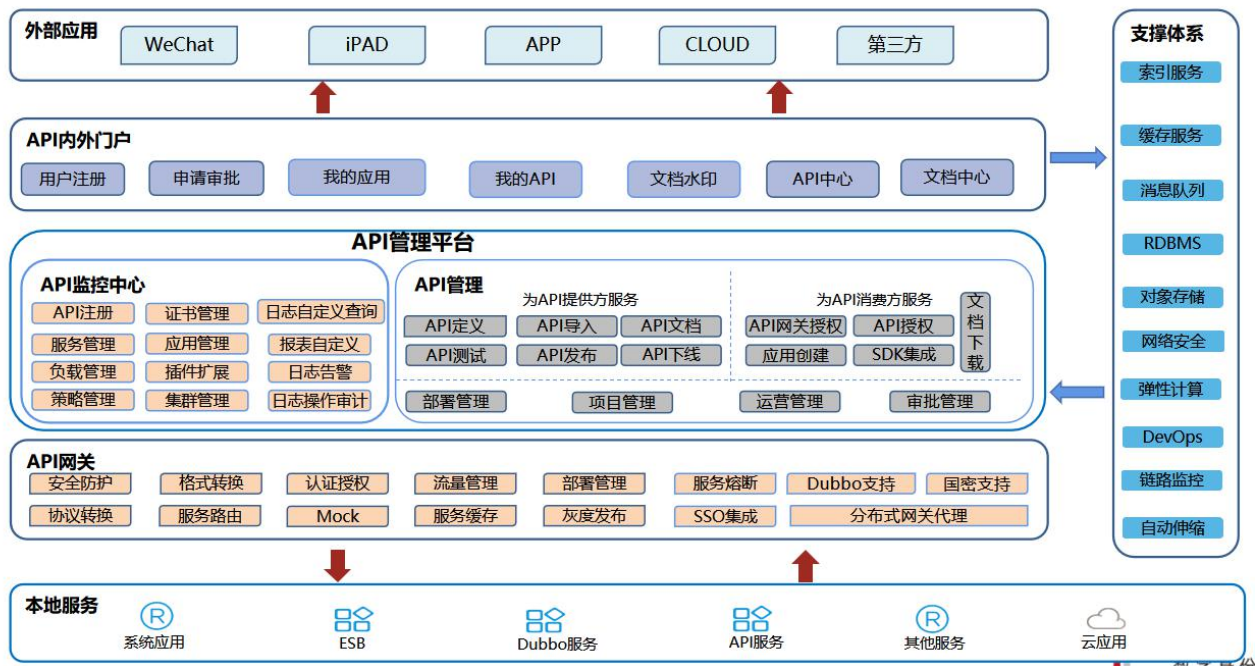
派拉 API 平台是一款安全高效准确传输的应用集成和数据交换平台，基于云原生、多租户、自主研发的新一代 API 平台商业产品。它包含了 API 智能安全网关、API 管理平台、API 门户，可以为业务中台和技术中台提供底层支撑的一体化平台。其主要特点是高可靠、高性能、强大的安全防护和扩展能力，是敏捷响应业务需求和企业数字化转型的保障。

2.1. 产品背景

随着微服务架构的普及，越来越多的企业系统都转向了微服务架构，微服务是对业务系统进行服务的拆分，导致 API 数量会成指数级的增长，企业内部的服务能力化不仅仅需要满足企业内部需求，而且企业的外部调用需求也是越来越多，微信小程序、移动 APP、物联网、云端应用、第三方合作伙伴等这些外部的触点越来越多，外部调用内部的服务就不可避免，但是这些触点都是第三方的应用，他们的安全性如何保障？流量的控制如何应对？高效的接口集成如何进行？是对企业 IT 部门非常大的挑战，API 平台就是解决这一系列问题的利器。

2.2. 产品功能架构

API 平台软件主要包含：API 智能安全网关、API 管理平台、API 门户三大模块。整体功能架构如下图：

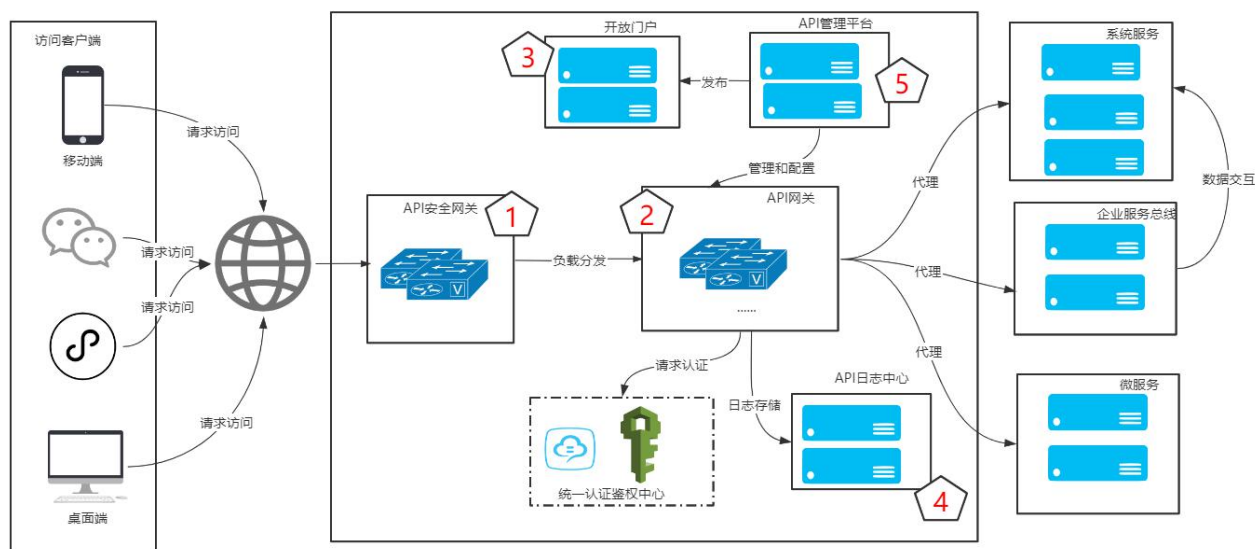


API 智能安全网关是最核心的模块，它是整个产品的主要底层组件，功能包括：路由转发、安全、认证、格式转换、流控、微服务等。

API 管理平台主要包括：实现了以项目为视角的 API 设计、API 定义、API 开发、API 测试、API 发布、API 上线、API 下线的全生命周期管理，以及服务注册中心集成管理、部署环境管理、应用管理、API 网关授权、API 授权、运营管理、审批管理、日志查询、异常告警、自定义 BI 报表以及集群扩展等功能。

2.3. 产品逻辑架构

外部业务系统通过 F5 或 SLB 负载分发到 API 智能安全网关，通过 API 智能安全网关代理到后端业务服务（传统的系统服务、遗留的企业服务总线，以及微服务）。



第 3 章 产品应用场景

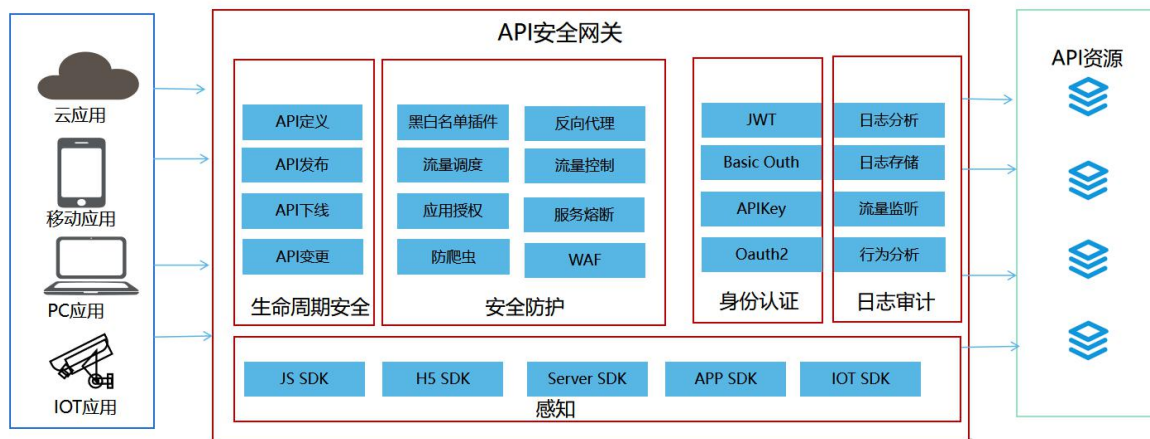
3.1. 企业级数据互联互通

API 智能安全网关是企业业务数据传输的关键枢纽，主要适用的传输场景如下：

1. 集团内部系统的业务数据交互；
2. 私有云、公有云、传统办公的不同网络区域的数据交互；
3. 第三方合作伙伴、公有云、移动端和内部业务系统的数据交互；
4. 内部到外部的公有云或者第三合作伙伴数据交互；

3.2. 企业级的 API 安全保护

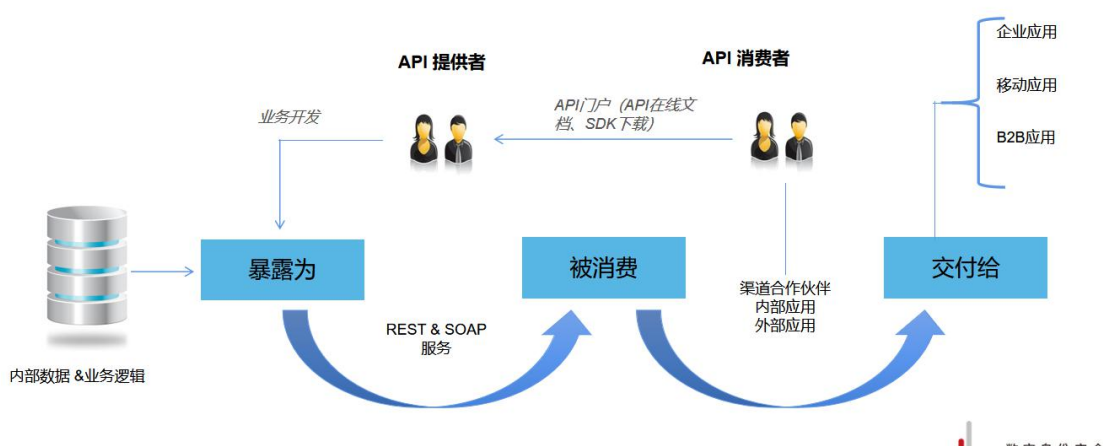
企业沉淀了很多的业务能力需要发布到外网，将 API 开放给合作伙伴或者第三方，通过 API 生命周期安全、身份认证、安全防护、日志审计、SDK 动态感知等手段对 API 进行安全防护，防止造成 API 被非法调用和数据泄露。



3.3. 企业级的 API 开放能力

企业会将很多业务能力开放到互联网，通过企业内部业务能力、合作伙伴能力、第三方云端服务能力进行快速整合，敏捷响应客户需求，API 门户帮助第三方合作伙伴实现自助注册以及自动化对接，可以在很大程度上降低沟通成本。第三方合作伙伴快速集成的主要步骤如下：

1. API 提供者进行服务的发布上线；
2. API 消费者在 API 门户上进行账号注册，并进行 API 申请，申请授权。
3. 授权通过后，下载 SDK，并根据 API 文档进行业务开发测试联调。



3.4. 跨网络的分布式网关集群代理

企业需要多个区域网络（混合云）的部署分布式网关，派拉 API 安全网关实现分布式网

关集群代理能力，实现 API 安全网关的幂等性，也就是在任何一个网络区域客户端访问本地的安全网关都可以访问其他网络区域的 API,并可以提高网络区域交互的安全性。

第 4 章 产品功能

4.1. API 智能安全网关

4.1.1. 运行引擎功能

API 安全网关功能主要包括负载均衡、反向代理、负载健康检查、缓存支持的功能，安全网关支持的传输协议包括：HTTP/HTTPS、TCP/IP、Websocket、GRPC、Dubbo、MQTT、Websocket。

4.1.2. 基础功能插件

基础功能插件主要分为基础插件、安全、认证、流量控制、格式转换共 5 类插件

- 基础插件：
包括：Session 保持、全局交易流水号、日志记录。
- 安全插件
包括：IP 黑白名单、跨域支持、MD5 验签等安全方式。
- 认证插件：
包括：APIKey、Basic 验证、ACL 认证、Oauth2 插件、Ldap 等认证方式。
- 流量控制：
包括：请求限流、交易限流、请求报文大小限制、请求终止、响应报文限制、响应报文大小限制。
- 格式转换：
包括：JSON 格式转换、XML2JSON 格式转换、模板格式转换。

4.1.3. 扩展功能插件

集成扩展插件功能包括：ElasticSearch 日志插件、应用授权插件、跨域插件、防重放、加

验签（国际算法）、加解密（国际算法）、Hmac、灰度发布、全局流量控制、Mock 功能。

企业级版本会增加如下扩展插件，他们功能包括：

- Kafka 日志集成

很多的客户需要将流量日志打到 Kafka，然后从 Kafka 在抽取到大数据日志存储中心，日志中心在统一进行展现。

- 服务熔断降级

当服务器压力剧增的时候,API 智能安全网关对一些服务进行有策略的降级，如果有大量超时或者异常，则会熔断该服务。

- 智能安全防护

通过集成 WAF 插件，实现防御 SQL 注入、XSS、CSRF 等 WEB 攻击，并可以根据 AI 算法识别大流量中的安全威胁。

- 渗透测试安全防护

通过集成 API 网关可以实现暴力破解、权限失效等常用的渗透测试的防护

- 服务注册中心集成 (Nacos/Eureka/Zookeeper)

在和微服务网关进行集成的时候, 通常需要同步 Nacos 或者 Eureka 中心的服务, 实现 API 网关和服务注册中心的联动。

- 全链路监控日志

当客户端需要通过 API 安全网关访问后端服务的时候，派拉 API 网关产品通过埋点可以实现端到端、端到云、云到端、以及微服务内部的调用的全链路监控。

- 高级服务路由

实现统一服务请求入口，提供基于 HTTP 请求头的高级服务路由功能。

- 灰度发布

通过请求头、请求体实现流量灰度切换、在服务路由中设置灰度标识，实现接口的灰度发布。

4.1.4. 增值开发插件

- 国密支持

支持国密算法 SM2/SM3/SM4 的加验签、加解密，也支持 360 浏览器端的国密证书。

- 高级格式转换

主要支持 Restful 到 Dubbo，以及 Restful 到 GRPC 的格式转换功能。

- 基于 ABAC 集成

实现了基于用户、请求参数、服务、路由的访问控制权限。

4.2. API 管理平台

4.2.1. API 生命周期管理

- 项目管理

项目管理具有多租户功能，一个项目经理可以创建项目，并可以管理项目内的人员。

- API 生命周期管理

通过 API 设计、API 定义、API 测试、API 发布、API 运维、API 消费实现 API 的生命周期管理。

- API 文档管理

可以通过 Swagger 导入也可以单独进行 API 的字段定义，在 API 发布后会同步到 API 门户上。

- API 部署环境管理

实现 API 多个部署环境的管理配置。

- 服务管理

配置 Eureka 或者 Nacos 的注册中心，以及对服务中心的服务进行定时同步。

- 应用管理

管理员可以在后台添加应用，也可以在门户上进行自助申请，管理员添加应用包括应用 ID 应用名称、认证方式、用户、状态等参数。添加应用后还可以实现配置应用的访问认证方式，目前主要包括 APIKEY、Basic Auth、Hmac、Oauth2 这四种方式。还需要针对网关授权和 API 授权进行申请，有运维人员进行审批，审批通过后，才可以访问 API.实现消费端的应用配置管理，并对应用实现 API 网关授权和 API 授权。

- API 权限管理

针对 API 网关授权给应用的权限主要包括：APIkey 、Basic Auth、No Auth、Hmac、Oauth2

- API 授权

实现某个应用的 API 授权。

- 审批管理

实现对 API 发布、API 上线、API 下线、应用网关授权、应用 API 授权流程审批。

- 运营管理

通过后台实现门户的 API 产品、API 文档、个人申请的相关管理，并可以发布到门户上。

- 在线扩展和部署

可以自定义开发网关插件，通过管理平台上传并发布到网关。

- 插件策略配置

当定制化一些插件，需要在插件策略里面进行统一配置。

- 分布式集群管理

实现多个 API 网关集群节点的管理，可以快速切换集群节点，并进行权限控制，以及可以进行多个集群节点的状态监控。

4.2.2. API 监控平台

主要包括：日志查询、日志审计、BI 报表、异常告警、用户权限管理。

4.3. API 门户

4.3.1. 门户主页

API 门户是展示企业所有的业务能力，实现应用集成的一体化自动流程，门户主页包括热门 API、消息通知、轮播图、自助集成流程等功能模块。

4.3.2. API 中心

集中展示企业服务能力，根据项目为视角展示 API，API 可以进行在线申请，单个 API 可以展示具体详情，包括请求报文、响应报文、响应码、集成接入文档等

4.3.3. API 文档

可以实现 API 的文档管理，主要文档分为：帮助文档、集成文档、集成规范、SDK 文档下载。

4.3.4. 开发者中心

服务消费方实现需要进行自动注册, 通过实名认证或者法人实名后才可以进行应用申请、API 申请调用、API 的查询、用户的基本信息等功能。

我的应用: 用户可以通过企业开放出来的 API 进行应用申请、API 申请和调用, 先通过沙箱环境的应用创建和 API 申请, 测试通过之后可以申请正式环境的 API, 运维管理员可以对 API 申请进行审批, 保证开发者的应用访问 API。

我的 API: 主要展示了用户申请的 API 详情以及 API 的申请状态, 同时也可进行 API 解绑等操作。

个人中心主要展示是用户个人信息和账号密码的修改等操作

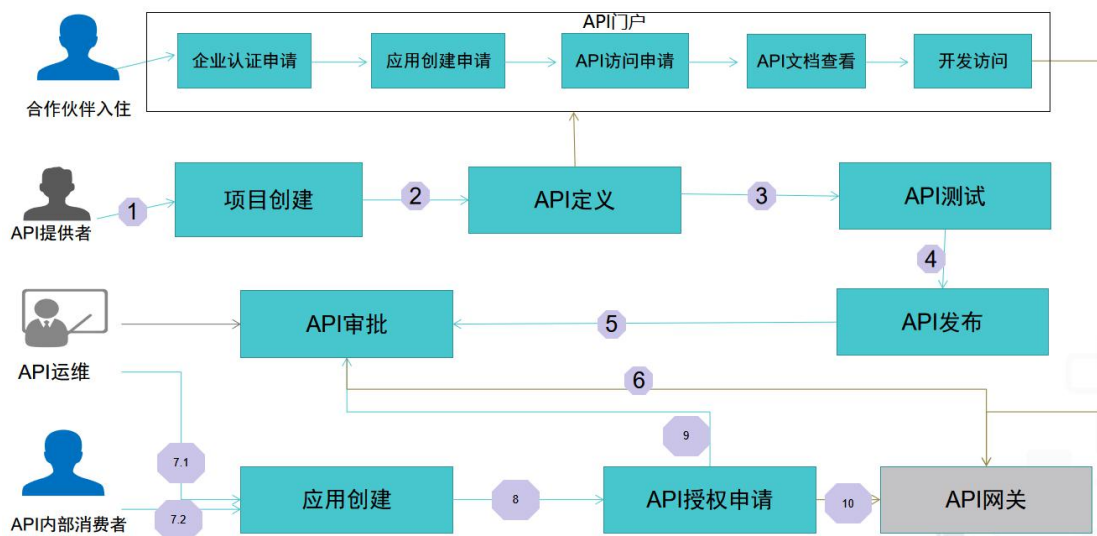
4.3.5. 多租户自助申请

实现多租户进行自助注册账号, 用户信息需要通过才可以进行注册应用, 通过应用申请 API 的权限, 通过后就可以进入联调阶段。

第 5 章 产品特性

5.1. 完善的 API 生命周期管理

结合 K8S 和 Docker 环境, 实现 API 定义、开发、测试、部署、上线、文档的生命周期管理, 实现服务提供者、服务消费者、运营管理的发布消费一体化流程。



5.2. 强大的 API 安全防护能力

- 身份认证

1. 派拉有自己的统一身份认证管理中台, 后期的安全认证中心是 API 智能安全网关的核心组成部分, 派拉的 API 智能安全网关产品和统一身份认证产品是无缝集成。
2. 派拉 API 智能安全网关支持 APIKEY、JWT、Basic Auth、Oauth2、SAML、OIDC 等安全插件, 功能丰富, 开箱即用。
3. API 鉴权插件, 通过 ABAC 或者应用的授权可以实现第三方合作伙伴、开发者等访问 API 的细粒度授权。

- 安全防护

1. 自带 WAF 产品 (可以实现防御 SQL 注入、黑客扫描、XSS/CSRF 等常用攻击、IP/ 用户的主动拦截和防护)
2. 流量调度中心 (可以根据后端服务的状态和服务器状态, 进行动态的流量权重变更。根据实际情况进行服务降级和服务熔断操作)
3. 流量控制 (可以根据用户/IP、API、服务、全局进行限流操作)
4. 自带大数据日志分析产品, 可以进行用户的异常行为调查分析。

- 数据安全

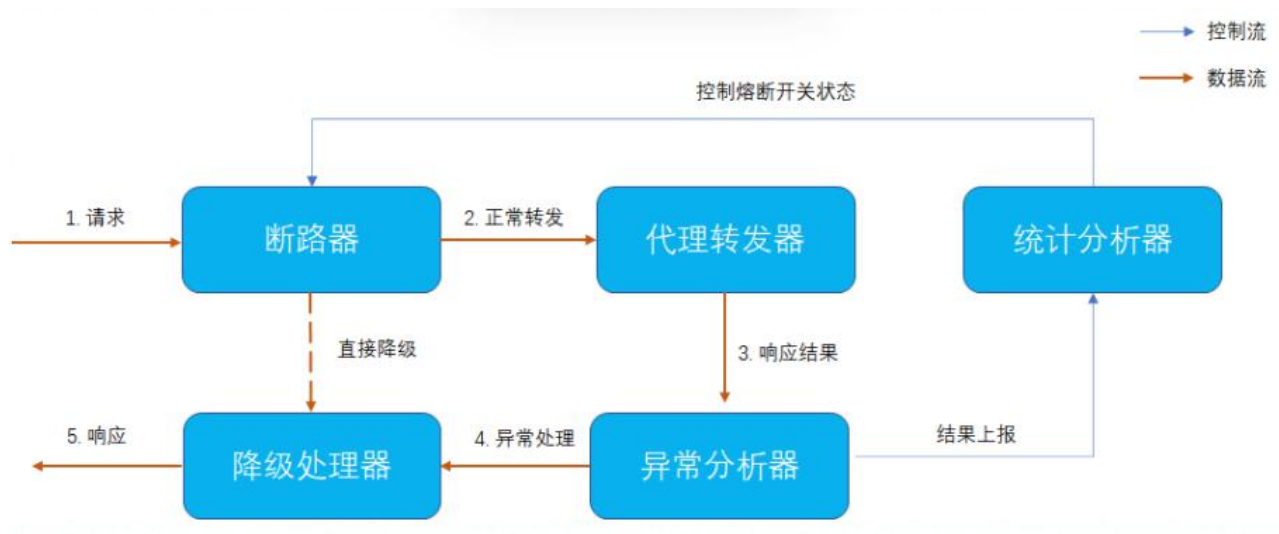
1. 自带加解密、加签验签等安全插件, 支持国密算法和国际算法。
2. 传输层支持 SSL/TLS 加密传输模式

5.3. 支撑高并发、高流量场景

1. 性能卓越, 单集群节点支持 10w 并发
2. API 智能安全网关基于 Nginx/OpenResty 开发, 2 台 8 核 8G 的集群节点可以支撑 10w 并发
3. 日志基于自研的日志分析产品, 在 5kw 条数据下, 查询时间不超过 3S。
4. 可以结合 K8S 和 docker 实现流量自动缩扩容, 满足大流量并发自动扩展。
5. 使用 Redis 的缓存, 减少 IO 操作, 支持流量高并发。

5.4. 服务智能熔断降级

当服务器压力剧增的时候,根据当前业务情况以及流量, 对一些服务有策略的降级, 以此缓解服务器资源的压力以保障核心任务的正常运行, 同时也保证了大部分客户能得到正常的响应。当某个目标服务响应超时或大量异常, 熔断该服务的调用。



第 6 章 产品支持系统列表

6.1. 操作系统

操作系统支持 Linux 或者国产麒麟操作系统, 版本如下:

1. Redhat 7.X/Redhat 8.X
2. CentOS 7.X/CentOS8.X
3. 国产麒麟操作系统 V10

6.2. 浏览器

支持的浏览器版本如下:

1. 支持 IE 内核浏览器有: IE11、360 安全浏览器 (兼容模式)
2. 支持 Firefox 内核常见的浏览器即火狐浏览器: Firefox 浏览器;

3. 支持 Chrome 内核常见的浏览器有：Chrome（最新）
4. Windows 10 自带的 Edge 浏览器

6.3. 数据库

API 安全网关支持的数据库包括：

1. PostgreSQLv9.6 以上版本
2. Mysql v5.5.X v8.0.X
3. 人大金仓 v8.0

第 7 章 产品业务价值

7.1. 制定管理和规范体系

制定企业管理集成规范，降低集成成本和运维成本；实现业务对接自助化，对接自动化，降低沟通成本

7.2. 敏捷响应客户需求

建设 API 低代码开发平台，快速响应业务需求；打通企业上下游业务，实现企业生态建设；借力服务编排平台，敏捷响应业务变化

7.3. 数字化安全价值

减少 API 数据泄露和攻击风险，提升企业信息化安全，数字化下云化、移动化、微服务化场景下提升 API 安全；保护 API 资产暴露风险和数据安全。

7.4. 及时的智能监控告警

实现端到端、端到云、云到端的全链路监控追踪体系，实现预测问题，定位问题，解决问题的一体化流程；建设应急响应体系，增强业务可用性。