

爱奇艺网络流量安全 检测能力建设实践

卢明樊

高级总监

InfoQ官网 全新改版上线

促进软件开发领域知识与创新的传播



关注InfoQ网站
第一时间浏览原创IT新闻资讯

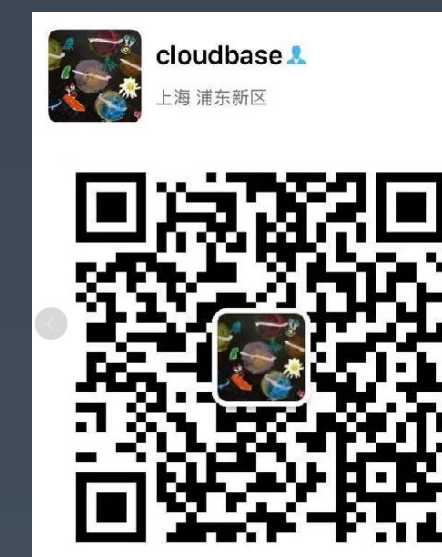


免费下载迷你书
阅读一线开发者的技术干货

自我介绍

卢明樊

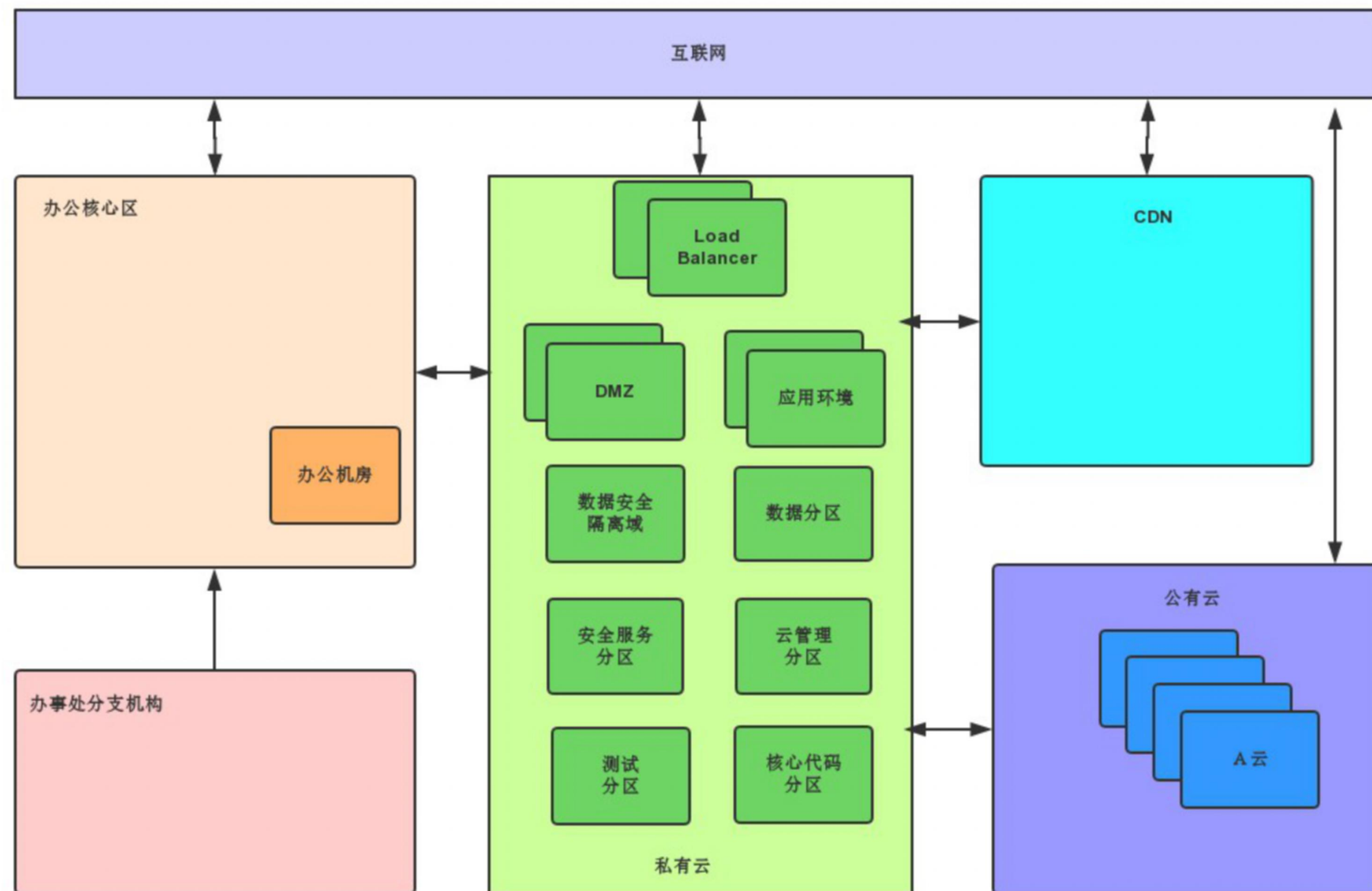
负责爱奇艺 安全·风控·大数据·数据库·中间件·服务治理
作为安全负责人，日常主导云安全, 数据安全, 网络安全,
应用和移动安全, 安全攻防和业务风控等安全领域的技术
创新和项目实施



目录

- ☆ 云时代互联网企业边界复杂性
- ☆ 爱奇艺安全边界管控防护
- ☆ 全流量安全分析技术
- ☆ QNSM 爱奇艺全流量安全分析的基石
- ☆ QNSM 开源
- ☆ 未来计划

云时代互联网企业边界复杂性



- 内网 vs. 外网
- 办公 vs. 业务
- 测试 vs. 生产
- 特殊隔离区
- 多云混合
- 核心-CDN-边缘
- 新边界

你能清楚的勾勒出你们企业的边界么？

趋势

- 防御边界呈现
 - 支离破碎
 - 更加层次化
- 单边界流量巨大，可能超过100Gbps
 - 流量检测要求高性能和扩展能力
- 威胁依旧严峻
 - 流量型、漏洞型、边界突破渗透、内部威胁
- 演进: 边界防御、纵深防御、零信任或者假设失陷
 - 不代表边界消失，边界防御依然基础一环
 - 边界间流量是安全分析和检测重要数据来源

威胁无处不在

异常流量 - DDoS/CC/爬虫

内部泄露、破坏、控制

OWASP TOP 10

边界突破和渗透 - ATT&CK

爬虫、爆破、撞库 ..

爱奇艺的网络边界安全管控体系

- 分区隔离管控和端口收敛

- 防火墙&交换机
- L4-LB黑名单
- 集中ACL管控 和 端口收敛
- ...

- DDOS/CC/爬虫攻击检测

- 边控 - 自建流量型攻击检测
- 三位一体的清洗能力
 - 高防清洗中心
 - 运营商黑洞和清洗
 - 第三方云清洗
- 云WAF
- 风控
- 验证中心 - 人机校验
- ...

你的防御武器足够么？

- 防入侵检测

- 云WAF
- IDPS
- 威胁情报
- ...

- 数据流动管控

- 绿盾
- 用户行为管理
- DLP
- ...

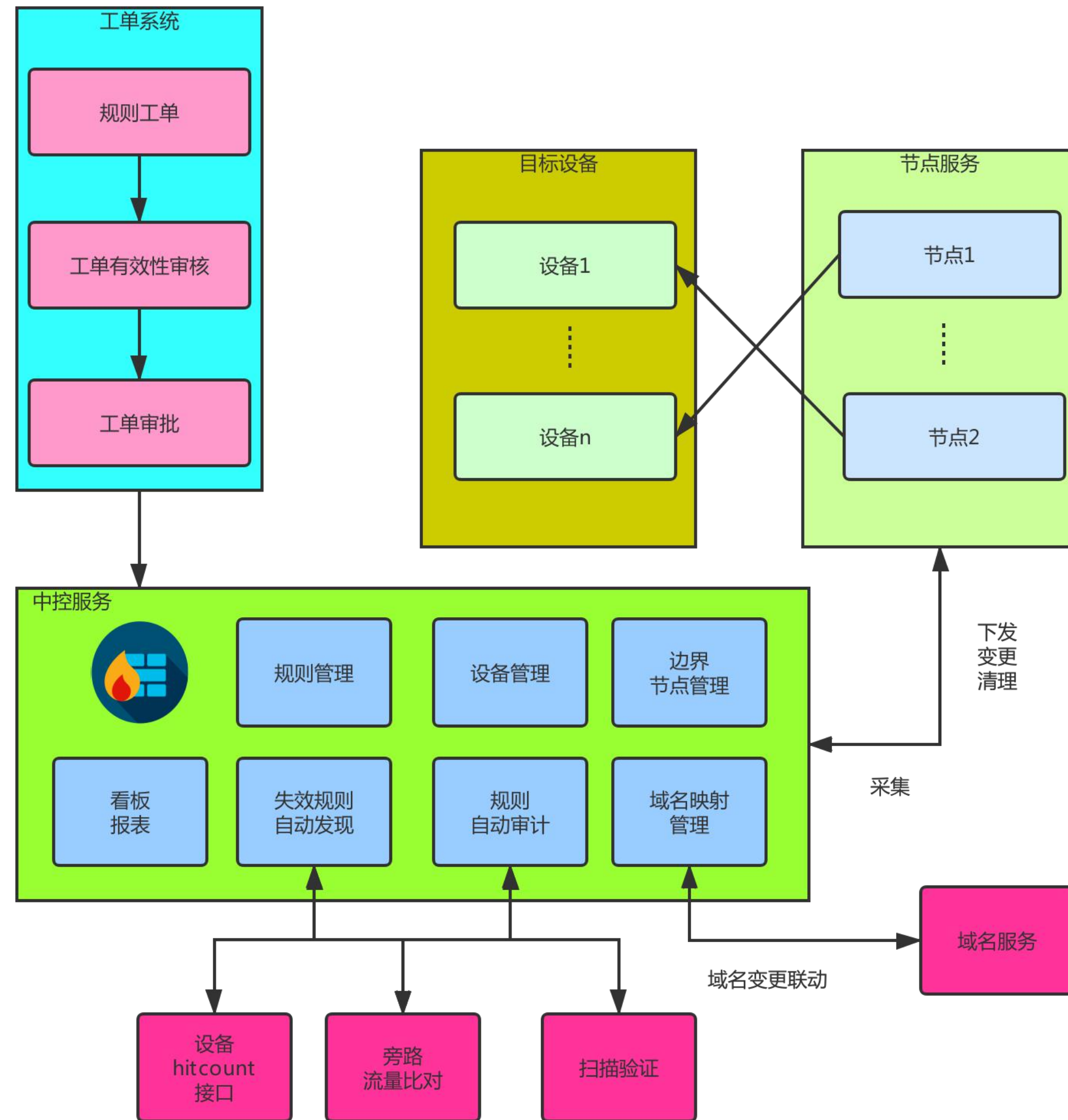
爱奇艺ACL管控服务

- 防火墙和交换机型号很多！
- ACL策略的管理难度大
 - ACL策略是否采集齐全
 - ACL策略是否有效？
 - ACL策略是否准确？
 - ACL策略是否可以下线？



- 服务A需要跨区访问服务 B
 - 服务 B 是多地部署和弹性扩容的
 - 服务 B的IP可能发生变化, 例如Failover
- 基于IP的ACL => 基于域名的ACL
 - 业务申请策略时为基于域名的ACL
 - 域名解析变化应立即更新基于IP的ACL

爱奇艺ACL管控服务



- 集中式管理
- 支持多种可交互设备(交换机、防火墙 ...)
- 支持可下发变更清理或只审计两种工作模式
- 规则生命周期管理: 新建、审计校对、失效
- 支持基于的域名规则

在多云协同和分区隔离非常重要

安全和网络运维
需要密切合作发挥各自专业能力

边控中心

基于商用DDoS检测系统

边控基于流量阈值DDoS检测

三位一体清洗中心上线

2019

2017

自研QNSM流量分析系统
研发边控中心

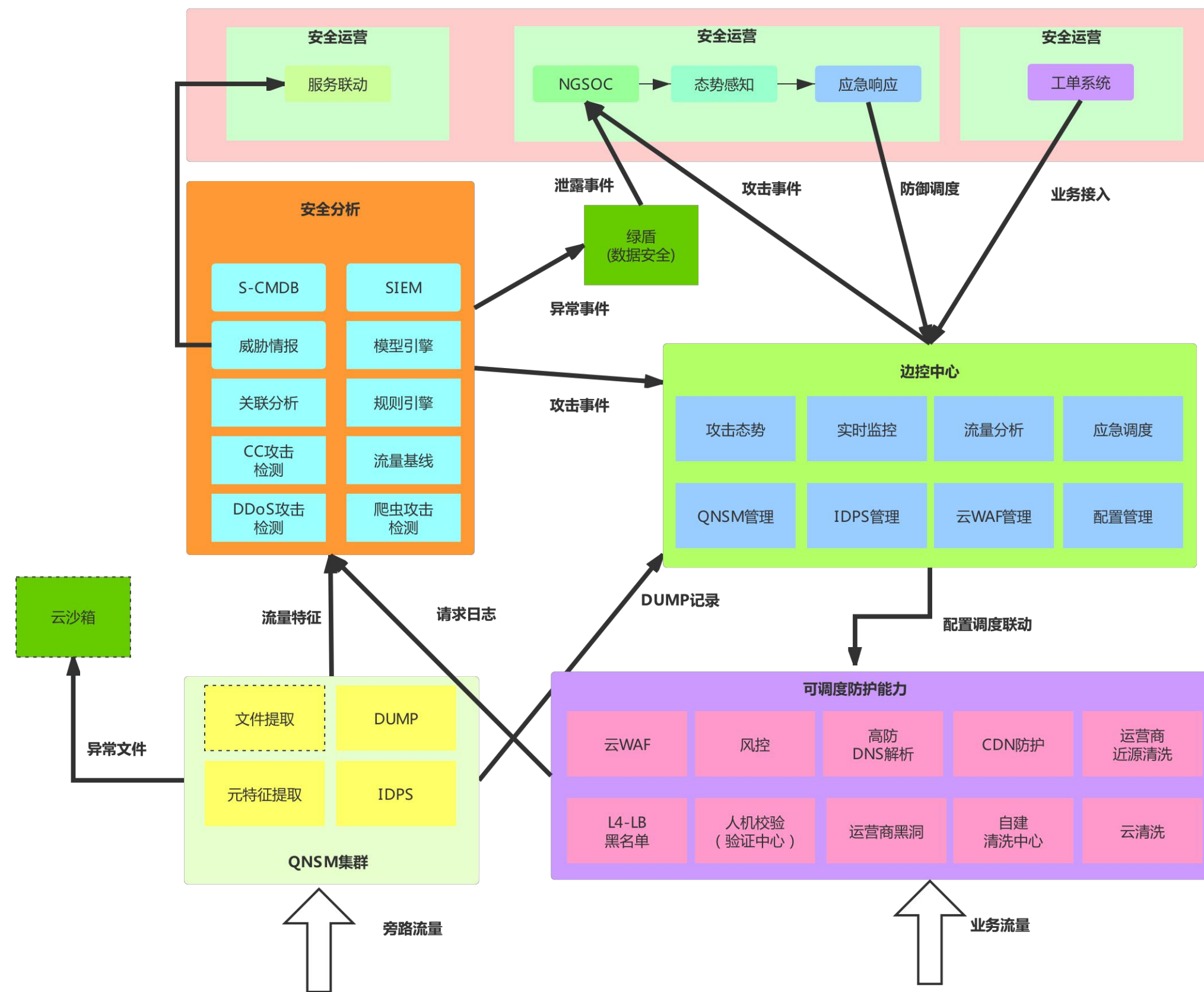
边控基于流量模型DDoS检测

持续运行

为什么自研

- 机房多，互联网接入点多，接入带宽大
- 商用检测系统扩展成本高，功能单一，无法灵活定制
- 现有开源检测系统能力不足，社区规划方向匹配度不一致
- 除了互联网流量，还希望能分析各种边界间的流量
- 不易和内部安全运营体系、智能分析体系和威胁情报联动

边控中心



业务流量和旁路流量**协同分析**

集成多种可调度防护能力**协同联动**，应对多类型和多层次攻击

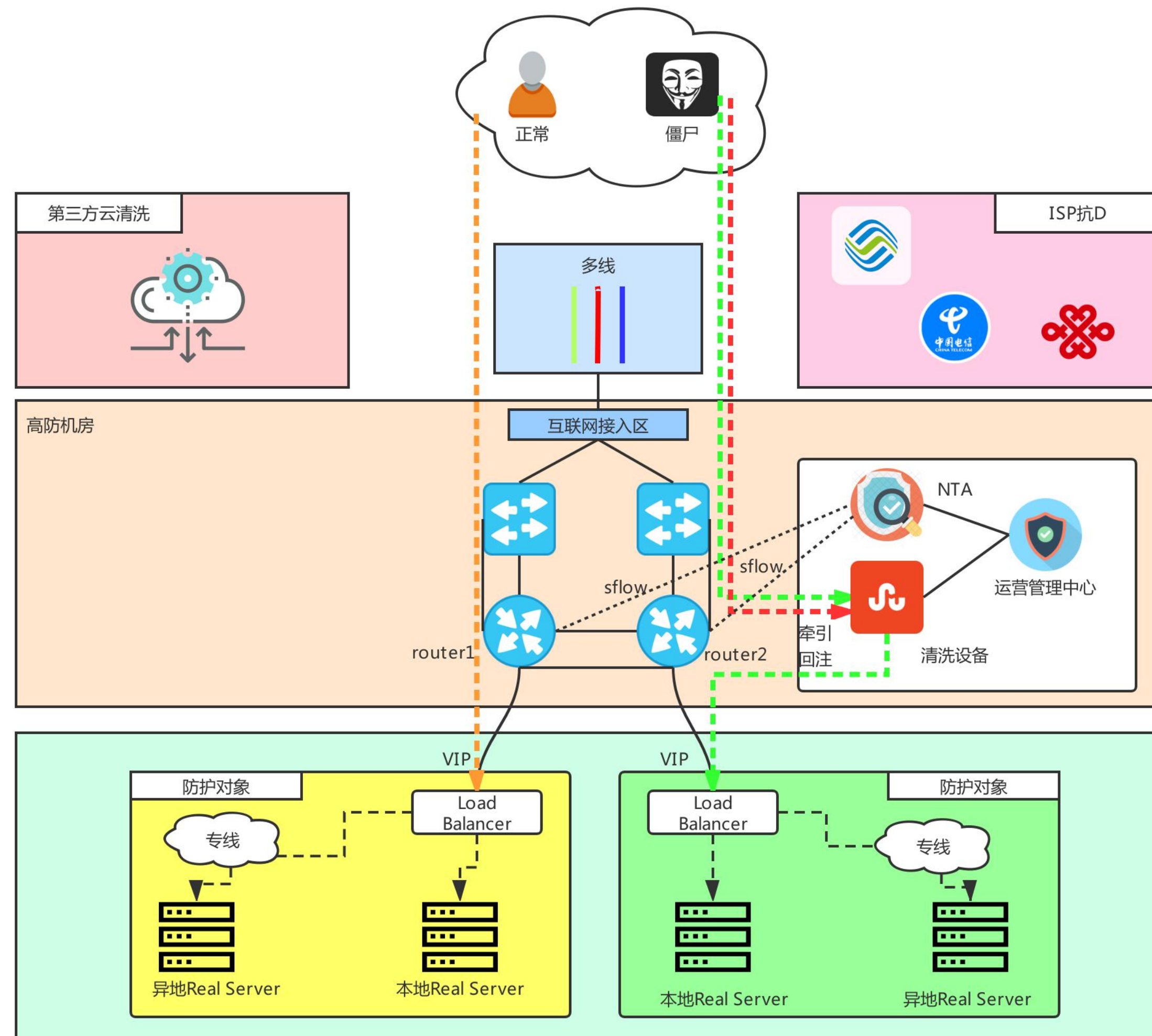
集成安全运营体系 - 不能有效运营的产品只是摆设!

核心流量分析组件: **QNSM**

The screenshot shows the ADS interface with a sidebar on the left containing navigation options: Dashboard, 实时监控 (Real-time Monitoring), 流量分析 (Traffic Analysis), 智能告警 (Smart Alerts), 应急响应 (Incident Response), WAF, IDPS, NTA, and 系统配置 (System Configuration). The main content area displays "DDoS攻击事件" (DDoS Attack Events) with a table of event details.

事件编号	攻击类型	目标IP	事件等级	状态	开始时间	结束时间	操作
116355	UDPFlooding	[REDACTED]	3	ONGOING	[REDACTED]	[REDACTED]	详情
116354	ACKFlooding	[REDACTED]	1	END	[REDACTED]	[REDACTED]	详情
116353	ACKFlooding	[REDACTED]	1	END	[REDACTED]	[REDACTED]	详情
116352	ACKFlooding	[REDACTED]	1	END	[REDACTED]	[REDACTED]	详情
116351	ACKFlooding	[REDACTED]	1	END	[REDACTED]	[REDACTED]	详情
116350	ACKFlooding	[REDACTED]	1	END	[REDACTED]	[REDACTED]	详情
116349	ACKFlooding	[REDACTED]	1	END	[REDACTED]	[REDACTED]	详情
116348	ACKFlooding	[REDACTED]	1	END	[REDACTED]	[REDACTED]	详情
116347	ACKFlooding	[REDACTED]	1	END	[REDACTED]	[REDACTED]	详情
116346	ACKFlooding	[REDACTED]	1	END	[REDACTED]	[REDACTED]	详情

清洗中心



带宽资源大的机房成为独立的清洗机房

典型的 检测 - 牵引 - 清洗 - 回注 架构

高防清洗 - 第三方清洗 - 运营商近源清洗 三位一体

业务提前接入，充分授权

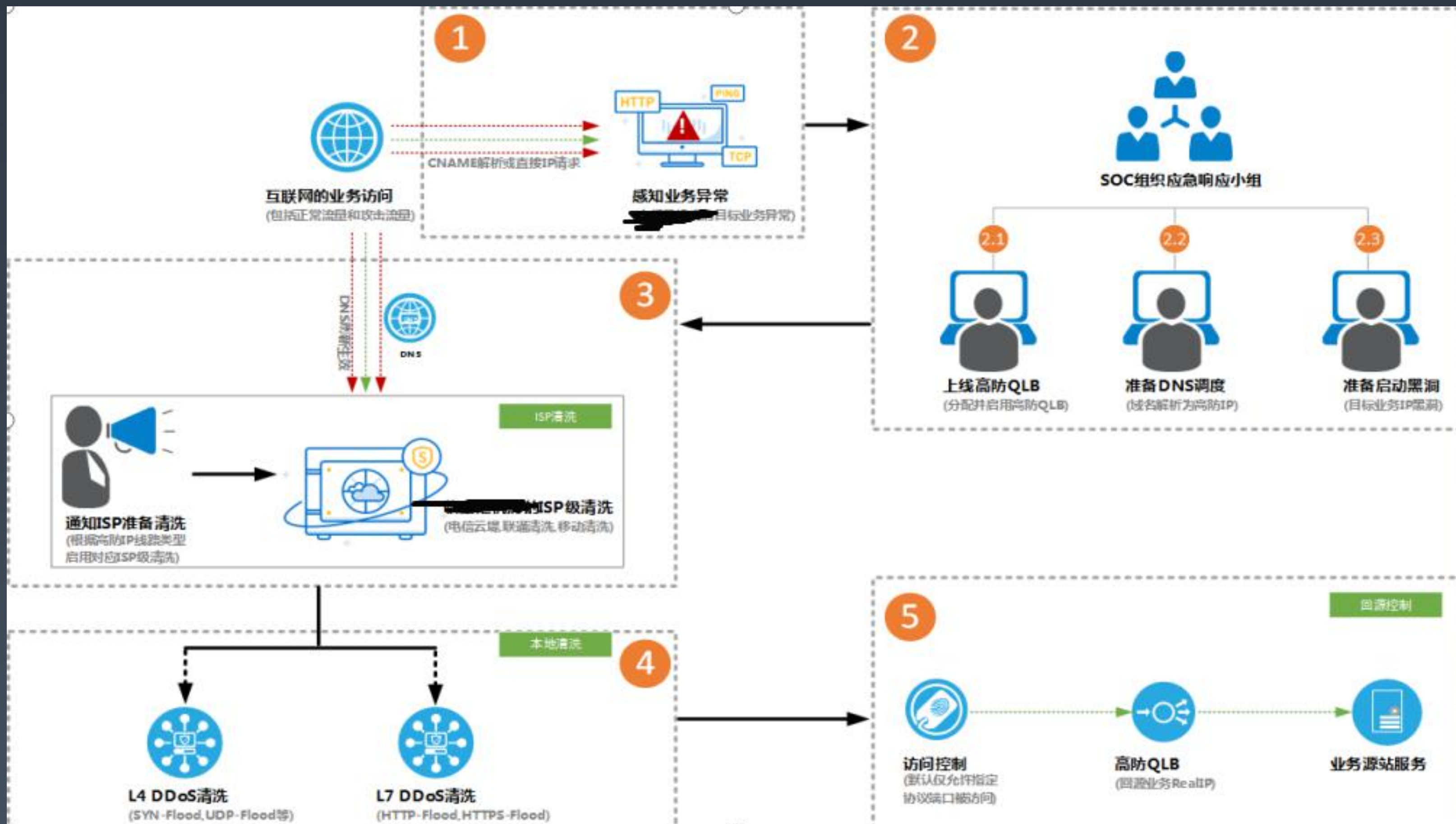
和边控中心、风险应急体系形成协同联动

异地机房只检测，受攻击流量入口切到清洗机房

商用NTA(TSA) v.s. QNSM

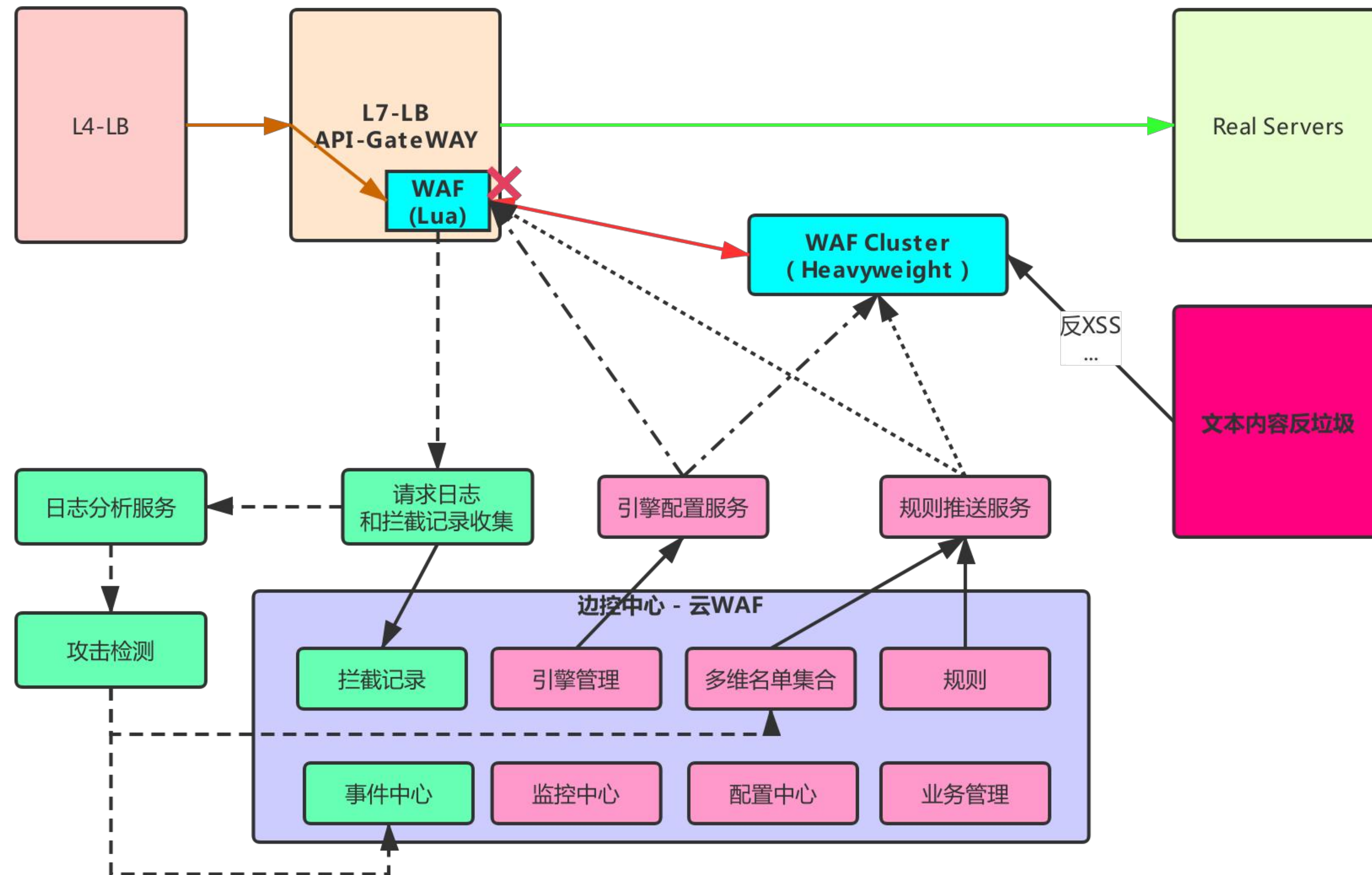
CDN的超大空闲上行带宽作为最终托底

定期的应急演练



- 及时修补安全漏洞，降低风险发生可能性
- 两地三中心的业务架构，增加蓄意者的攻击难度，切换的自由度
- 静态网页使用CDN发布，分散攻击面
- 接入高防服务

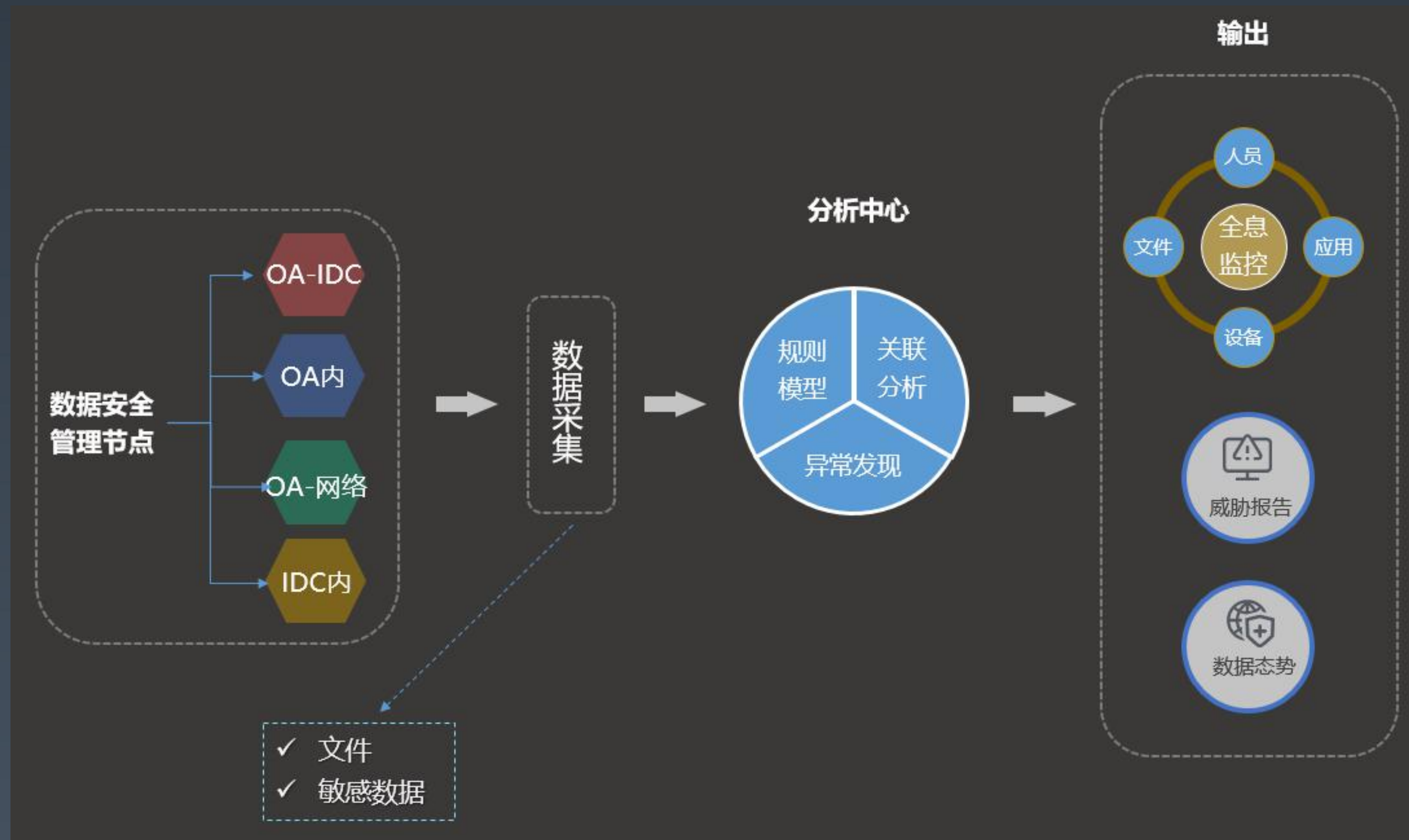
爱奇艺云WAF



- 轻量级和重量级(商用)WAF组合使用
- 轻量级引擎 1ms 注重召回
- 重量级引擎 注重准确
- 集成到7层LB服务或者API网关, 自动扩展, 一键接入
- 威胁情报和攻击检测自产的多维黑名快速转换为规则
- 外网暴露后台和高危接口必备, 执行规则运营
- 案例: 云打印机防护, 文本反垃圾过滤XSS

爱奇艺绿盾

关注敏感数据的流动态势，是DLP架构的重要组成部分，实现数据流动关键节点的可视化和数据异常风险识别和管控



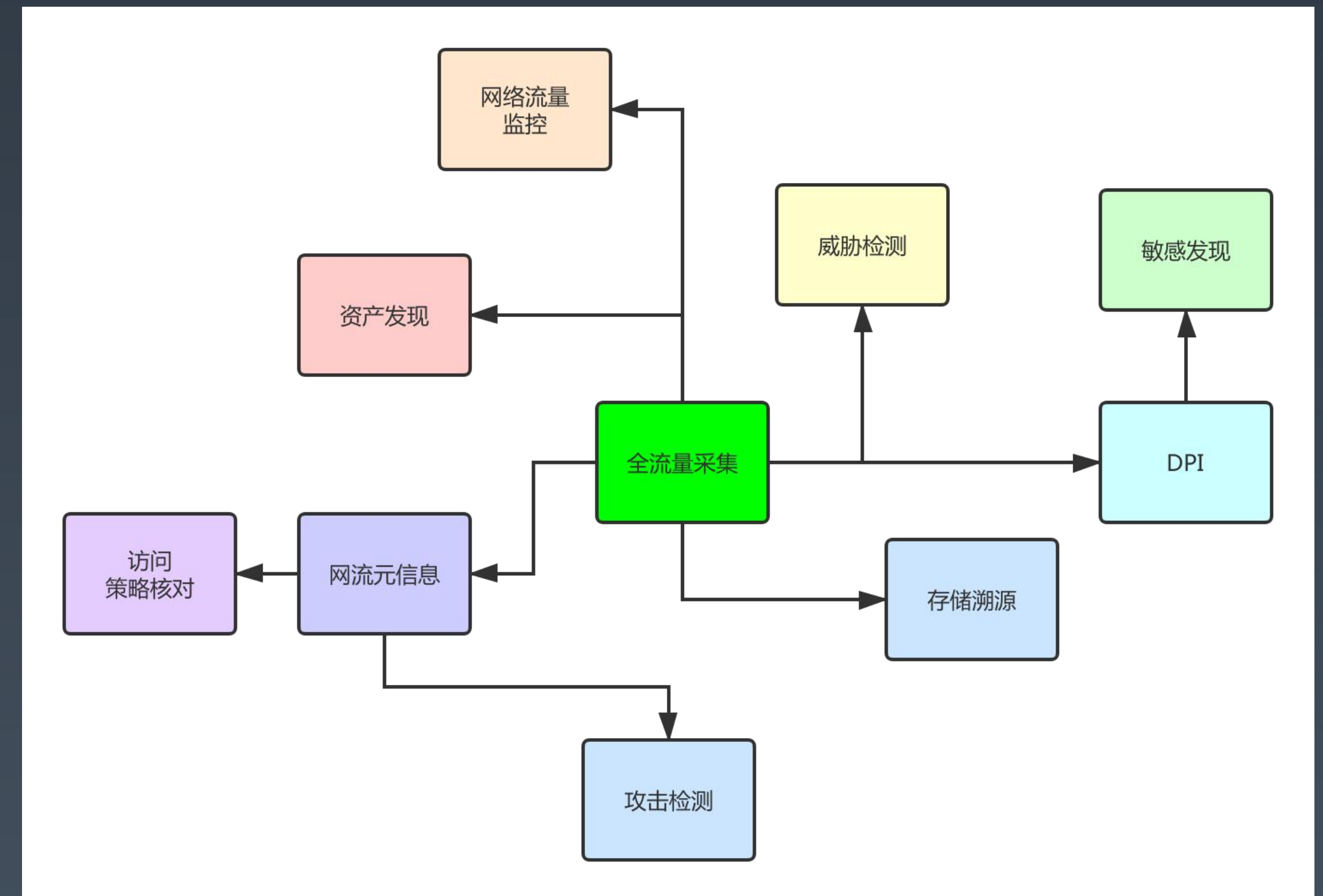
- 基于QNSM
 - 敏感文件和数据识别
 - 敏感数据库异常访问识别
(结合数据库审计日志和敏感库表字段发现)

全流量分析重要性

前面的场景都用到了一个非常重要的组件 **QNSM**

全流量采集对网络运维和安全运维意义重大

- 资产发现
- 网络监控、可视化、AIOPs
- 异常预警、威胁和攻击检测
- 内容提取、敏感发现、泄露检测
- 行为和流量基线建模和ACL策略核对
- 精细分析: 机器学习、专家分析
- 取证溯源、事件回查
- . . .



用户、设备、应用、数据、流量

QNSM - 全流量，实时，高性能网络安全监控引擎

高性能

Kernel Bypass: **DPDK** 用户态实现
单x86服务器(24核)最高可处理10Gpbs
Master-Worker + Pipeline**流水线**
网卡队列/CPU **绑定**
关键数据**无锁化**、跨CPU无锁通信

实时性

IDPS引擎实时检测
DDOS检测以10s周期输出聚合数据
支持**Kafka**输出，方便安全分析系统对接

可扩展

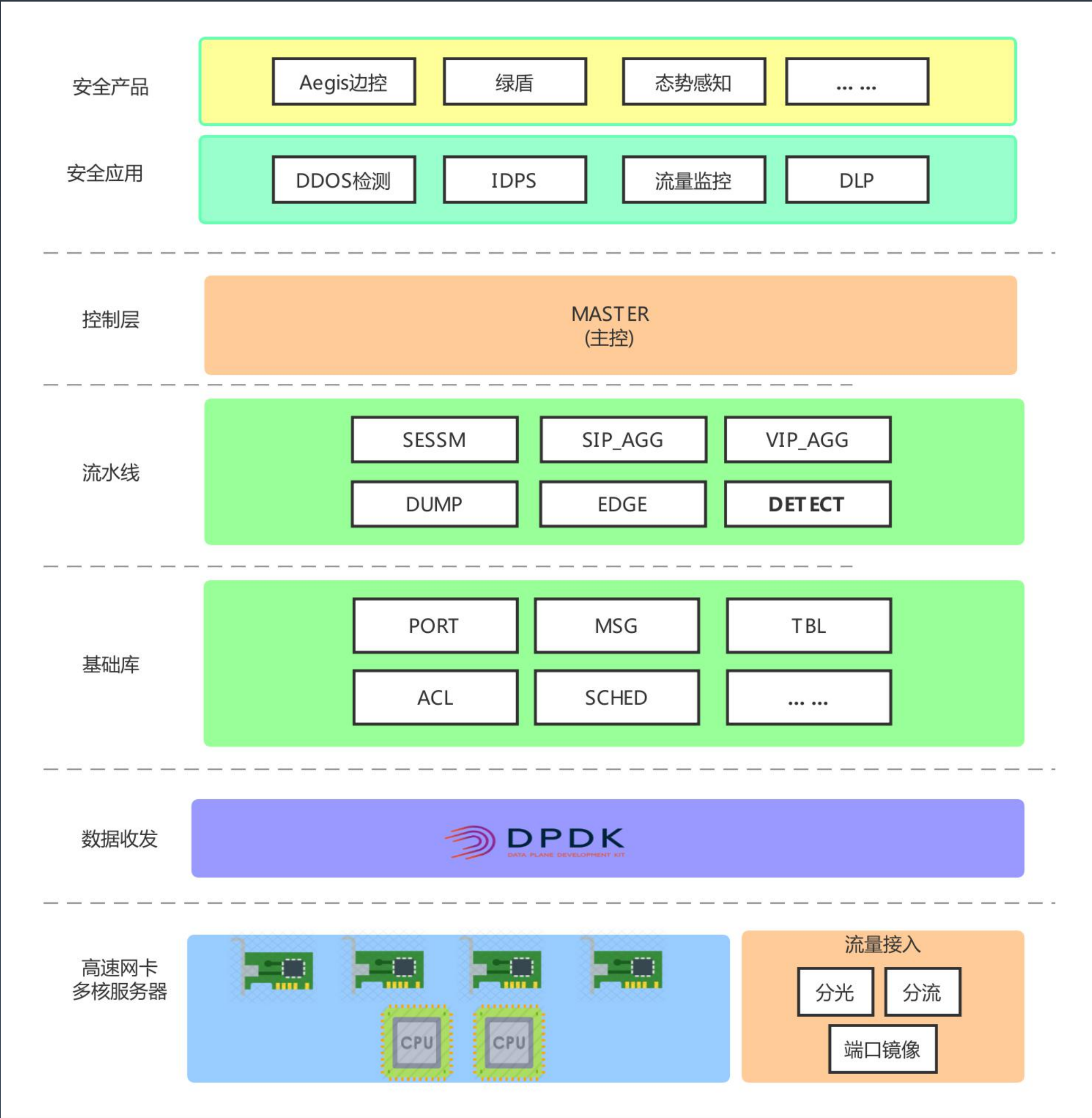
旁路部署, 结合分流可横向扩展
流水线灵活的**组件式**实现和插入
支持IPv4&IPv6**双协议**



多元特征

支持DDoS**攻击特征**计算
支持基本的**DFI/DPI**
静态库方式集成Suricata 的IDPS检测

QNSM – 架构



基础库

- PORT: 网卡队列、核心之间的rte_ring等逻辑封装
- MSG: 支持回调的CPU核心之间传递的通信消息（策略消息、数据集合、）
- ACL: 支持回调的基于五元组的策略描述
- TBL: 基于mempool的表项存储
- SCHED: 工作线程封装，支持自定义逻辑和包处理、策略执行、消息分发和定时回调等

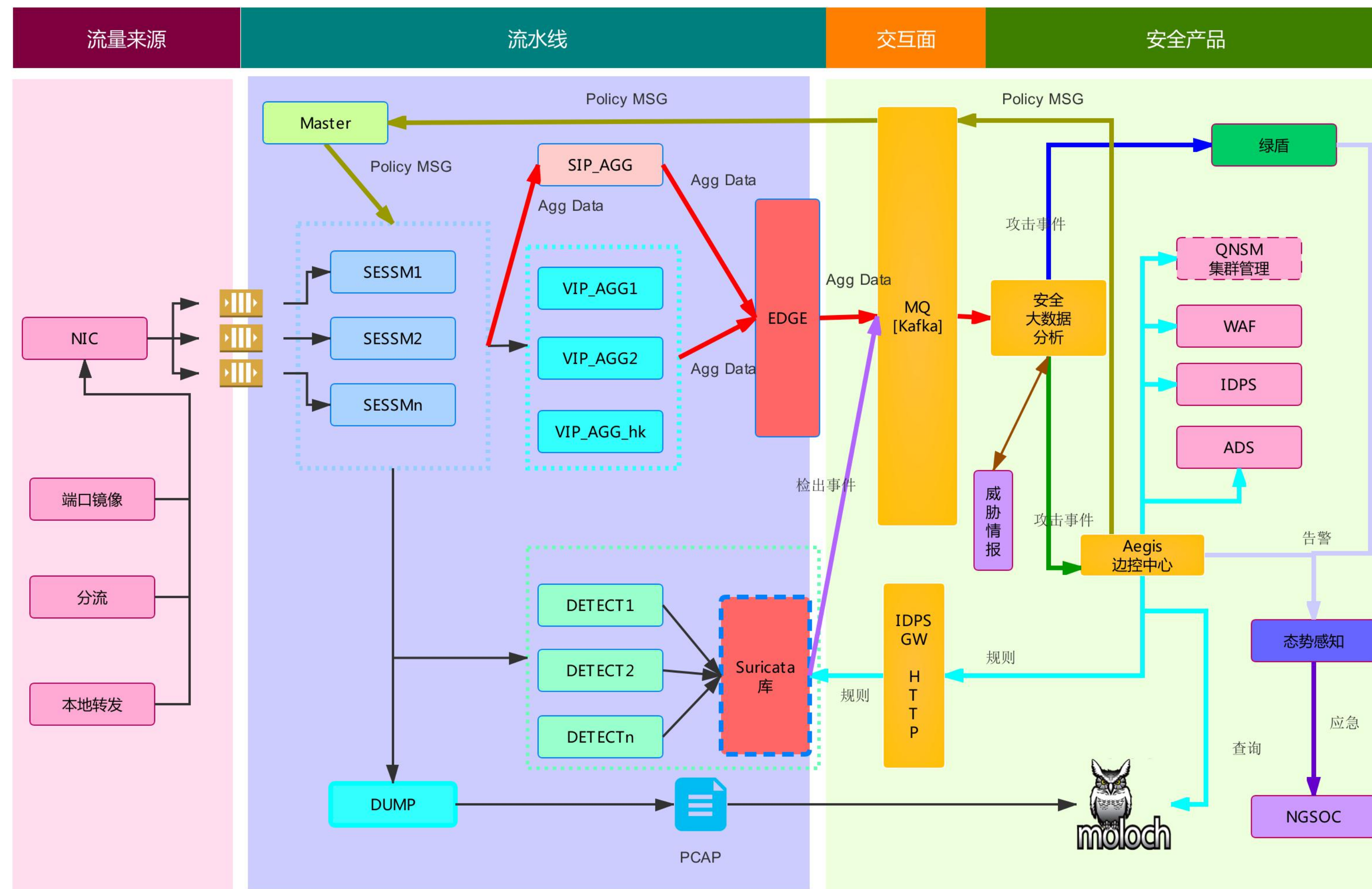
流水线模块

- SESSM：负责IPv4和IPv6数据包解析，采样FLOW数据聚合，ACL模式策略消息下发
- SIP_AGG：基于攻击源IP特征聚合和输出到EDGE
- VIP_AGG：目标VIP自学习，基于目标VIP特征聚合和输出到EDGE
- DUMP：保存为pcap文件供事件回溯和专家分析
- EDGE：输出多维数据至Kafka
- DETECT：基于Suricata 支持 IDPS检测（支持TCP RST&UDP ICMP错误包）

控制面和工具

Master 负责下发策略至相应的转发面组件

QNSM - 流水线



- QNSM自身支持多实例运行
- 流水线内的组件可配置为多个实例同时运行
例如SESSM, VIP_AGG, DETECT等也
- 流复制同时进行多个任务:
例如DUMP, DETECT, VIP_AGG等并行

QNSM - 部署情况

分析集群

22+

分析总带宽

1TBps

分析面

7+

分析节点

130+

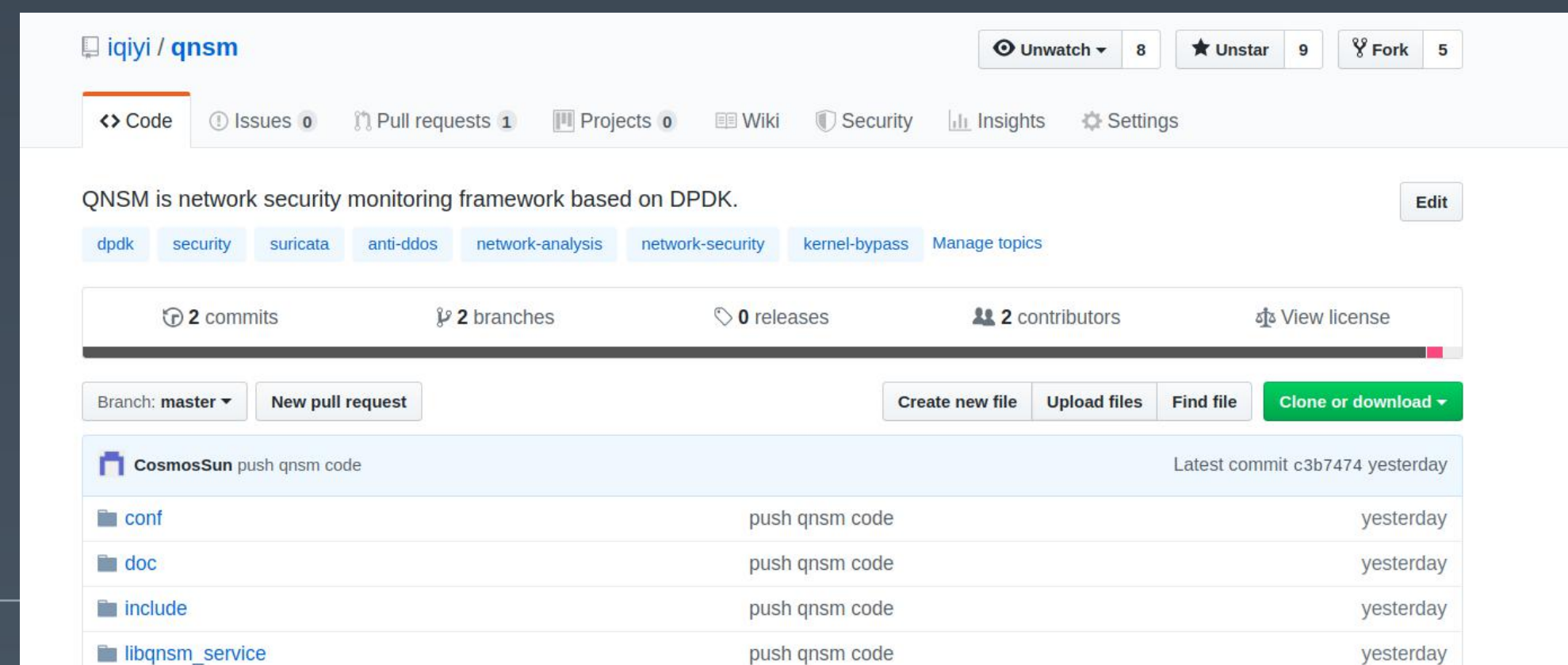
这只是开始，结合产品、服务、体系建设持续深入运营才是关键

QNSM is Open-Sourced!



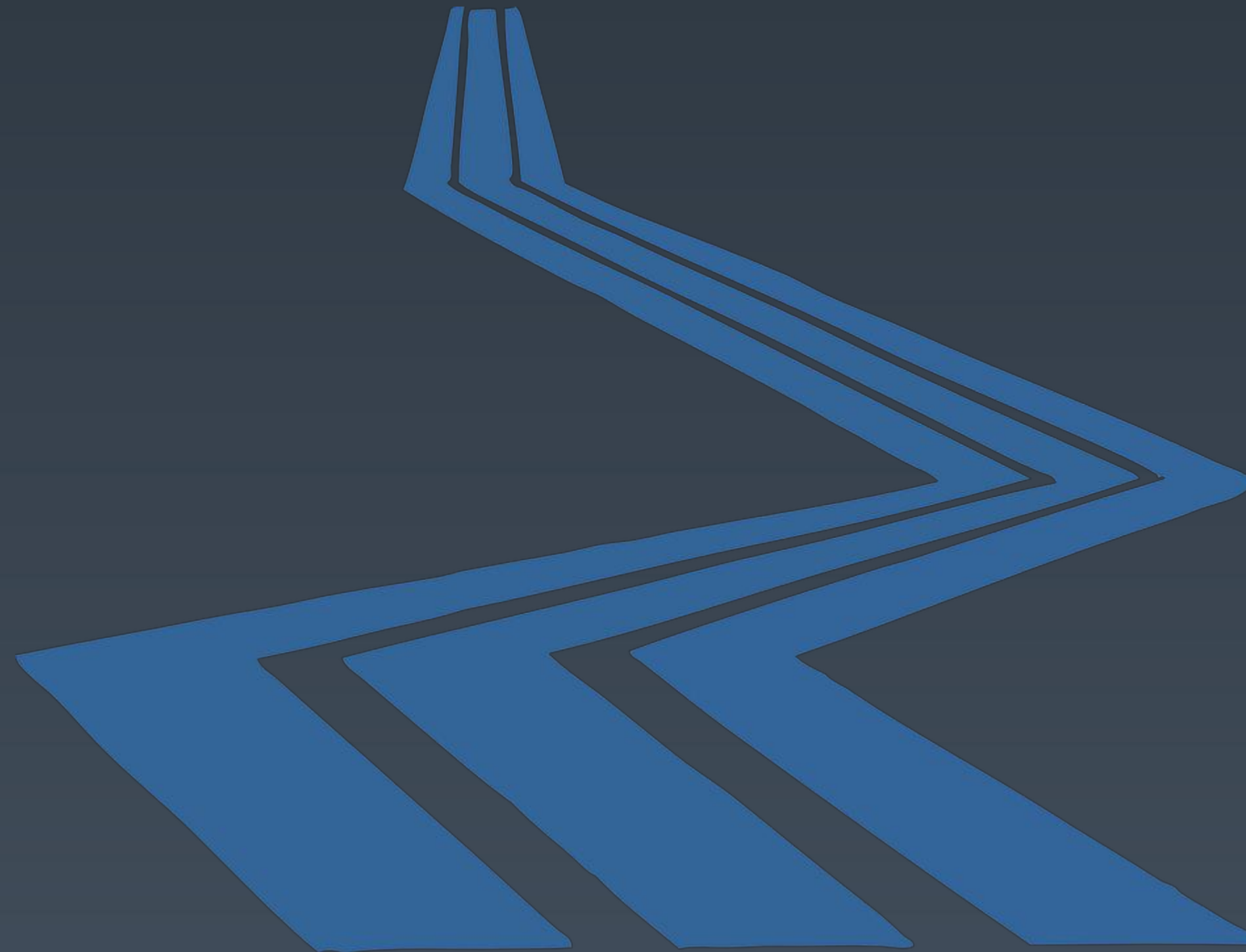
We need you make QNSM better!!!

- ✓ 请访问 <https://www.github.com/iqiyi/qnsn>
- ✓ 欢迎使用，报告Issues 和 提交 Pull-Request



QNSM Next Step

DPDK 中断模式
加密流量特征
高级DPI/DFI
Netflow 标准输出



更多能力集成

Bro/Zeek 集成

沙箱集成

更多工作模式

TAP

Firewall

更多应用场景

AIOPs

旁路设备指纹

TakeAway



- 理解复杂的网络边界和分区
- 理解边界内外的风险
- 构建协同联动的边界防御控制体系
- 灵活可扩展的全流量分析是基础能力
- 和我们一起优化改进QNSM!



关注 QCon 公众号

收获国内外一线大厂实践 与技术大咖同行成长

✓ 演讲视频 ✓ 干货整理 ✓ 大咖采访 ✓ 行业趋势





THANKS!

QCon |  th