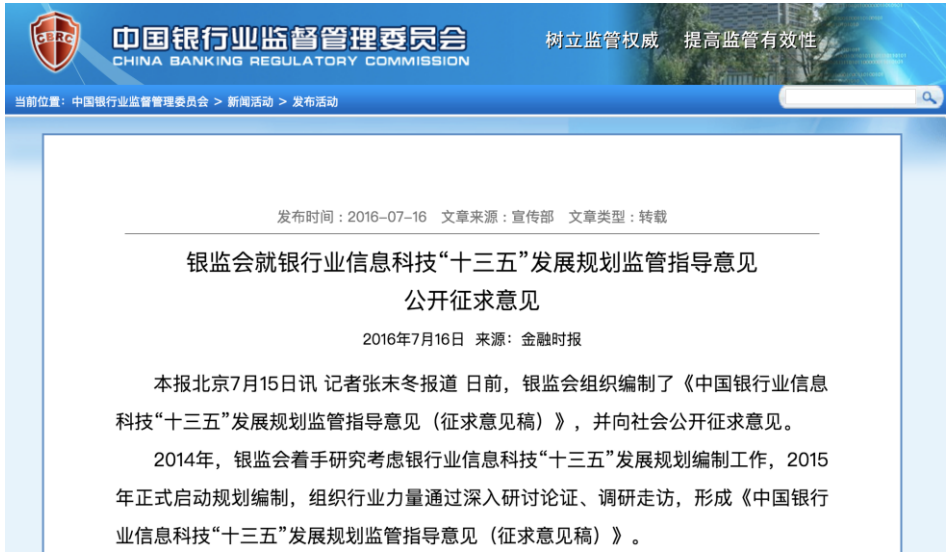
金融数据中心云转型过程中的网络挑战与应对

顾晓奕

2018/06/28 @ 上海

金融IT上云，科技引领业务

- 2016年7月15日，银监会发布《中国银行业信息科技“十三五”发展规划监管指导意见》征求稿，要求到“十三五”末期（2020年），银行业面向互联网场景的重要信息系统全部迁移至云计算架构平台，其他系统迁移比例不低于60%。此举意味着银监会明确制定了银行业上云时间表。



中国银行业监督管理委员会
CHINA BANKING REGULATORY COMMISSION
树立监管权威　提高监管有效性

当前位置：中国银行业监督管理委员会 > 新闻活动 > 发布活动

发布时间：2016-07-16　文章来源：宣传部　文章类型：转载

银监会就银行业信息科技“十三五”发展规划监管指导意见公开征求意见

2016年7月16日 来源：金融时报

本报北京7月15日讯 记者张末冬报道 日前，银监会组织编制了《中国银行业信息科技“十三五”发展规划监管指导意见（征求意见稿）》，并向社会公开征求意见。

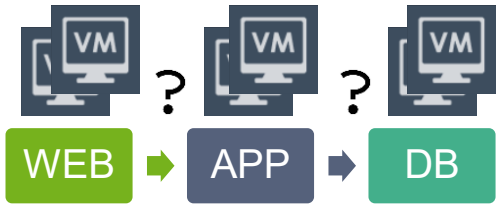
2014年，银监会着手研究考虑银行业信息科技“十三五”发展规划编制工作，2015年正式启动规划编制，组织行业力量通过深入研讨论证、调研走访，形成《中国银行业信息科技“十三五”发展规划监管指导意见（征求意见稿）》。

1. 银行业应稳步实施架构迁移，到“十三五”末期，面向互联网场景的重要信息系统全部迁移至云计算架构平台，其他系统迁移比例不低于60%。
2. 2014年9月，银监会、发改委、科技部、工信部出台《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》，指出从2015年起，各银行业金融机构对安全可控信息技术的应用以不低于15%的比例逐年增加，直至2019年达到不低于75%的总体占比（2014年应用的技术和产品可纳入2015年度计算）。

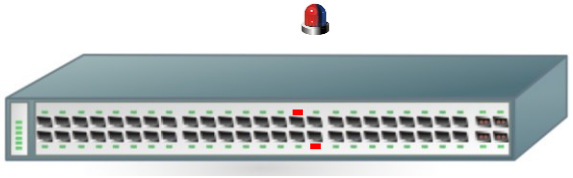
---《中国银行业信息科技“十三五”发展规划监管指导意见（征求意见稿）》

大家遇到的问题

云平台无报警，但用户报障了



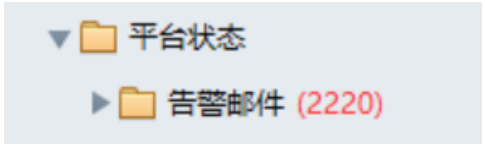
都是虚拟机，是哪一段有问题



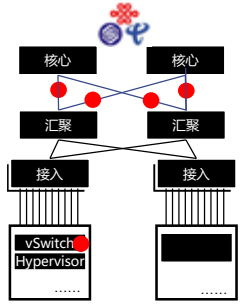
端口告警了，是什么业务突发还是攻击

内网受到攻击了，能否提前发现

业务慢了，是应用问题还是网络问题



告警来了，到底是几个问题

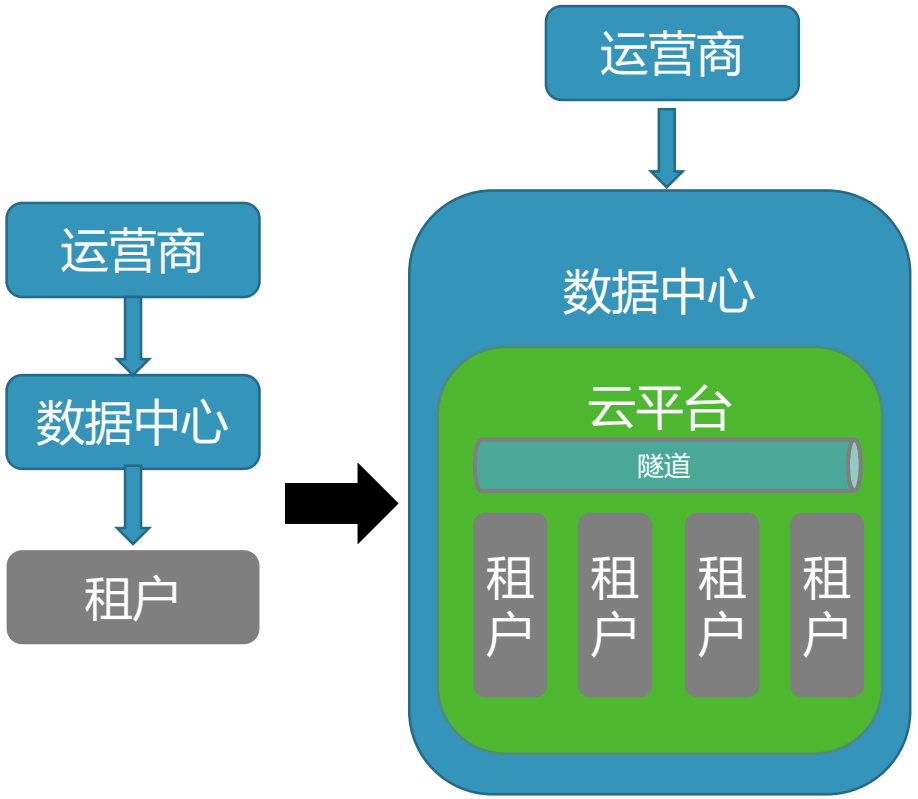


带宽占满了，哪个租户的哪个ISP的流量

云平台资源分配完了，马上扩容还是资源回收

. . . . . .

问题产生原因？——架构变了

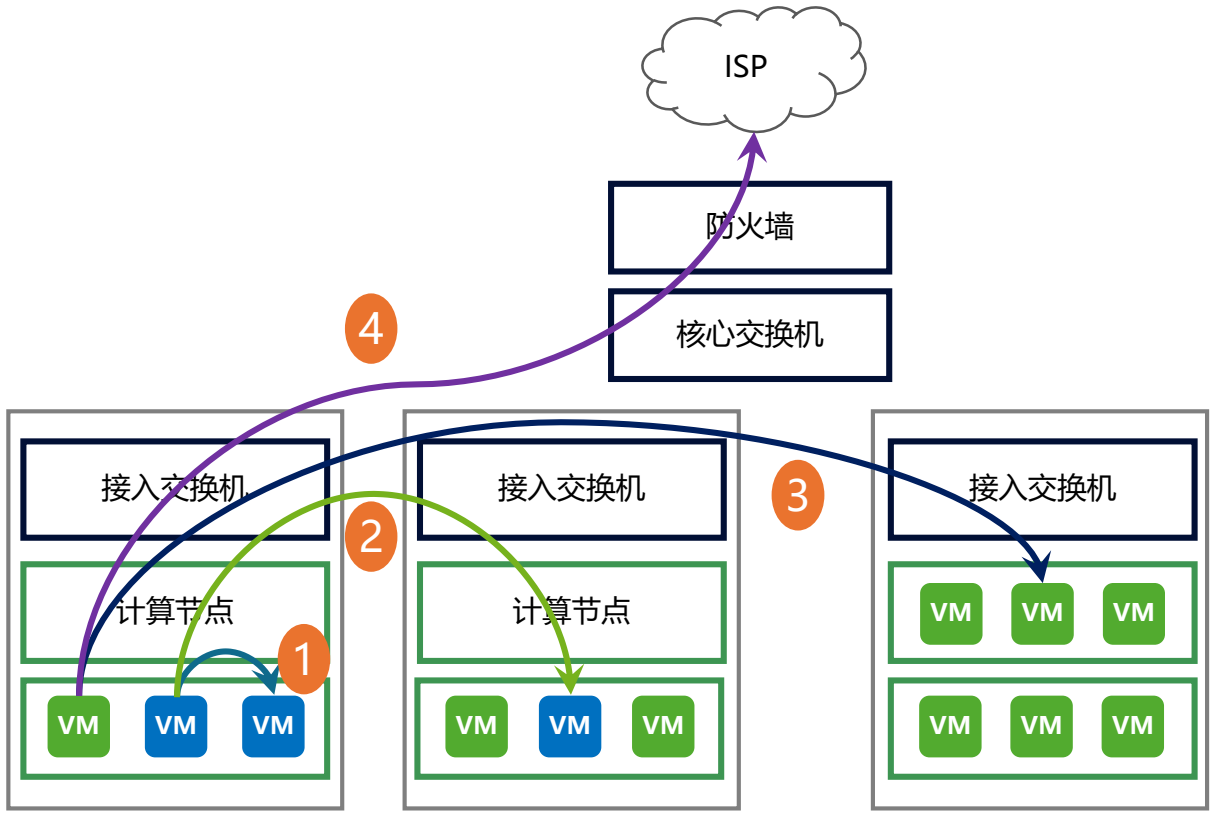


传统IDC　　云数据中心

由实到虚

- 从“烟囱式”到“集中化”：单租户独享物理基础网络转变为多租户共享物理基础网络。
- 从“Underlay”到“Overlay”：在物理网络之上，随业务需求打通“网络隧道”（基于VxLAN/GRE...），为不同业务构建虚拟网络（VPC/VNET/SubNet...）。

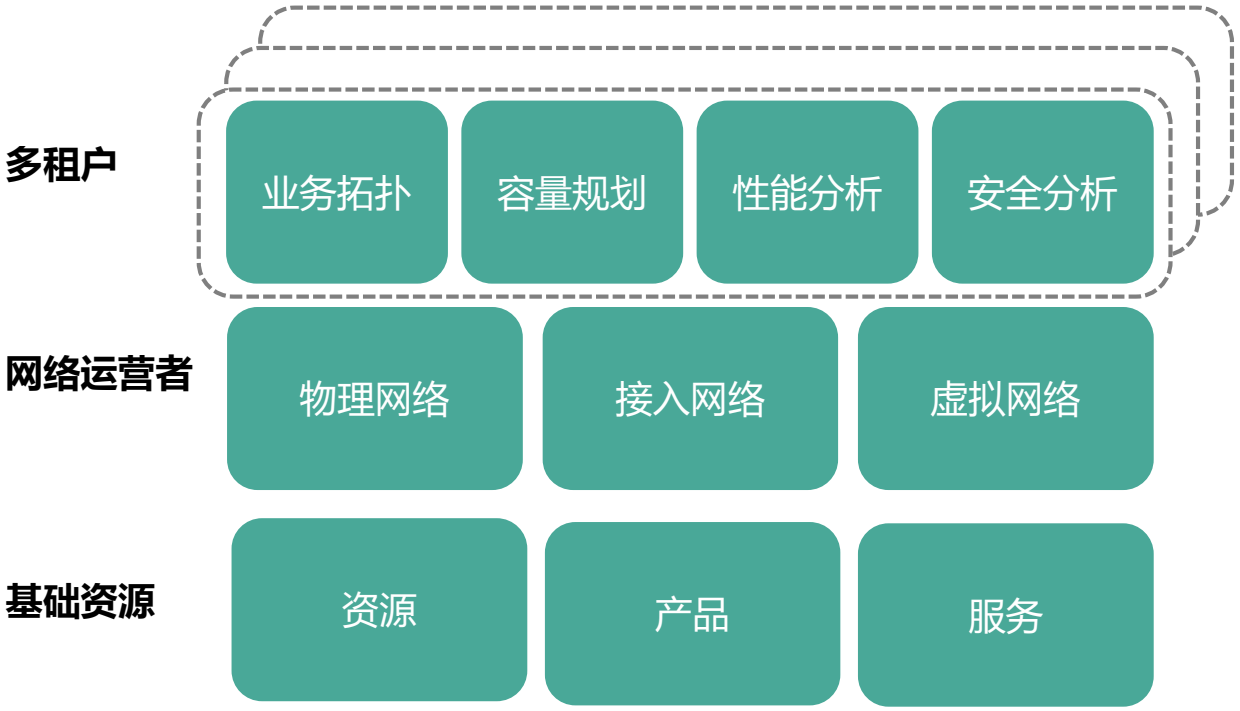
问题产生原因？——网络流量变了



由外到内

- 2020年，云数据中心将处理92%的工作负载。
- 多租户共享资源池、分布式系统、数据备份、开发转生产部署等场景，使得数据中心东西向（内部）流量将占据总流量的77%。
- e.g. 某金融服务企业的数据中心东西向流量占80%，而同宿主机虚拟机间的流量占15%。

问题产生原因？——业务交付变了



由静到动

- 业务增长、节假促销，促使业务负载弹性伸缩，网络随之动态配置。
- 物理网络可以“部署后不管”，但虚拟网络却需要随业务“毫秒级变更”。
- e.g. 某行业云在同一时间上百个租户动态创建VM及访问规则（IP+端口+协议），自定义规则+全局规则，可达每秒上千条规则的增删改查

金融云的要求？

金融BCC
专属物理集群
高级安全服务
高质量IO保障
高品质客户服务
...

安全合规的金融机房
金融云的计算、存储资源集群，从物理服务器层面完全独立于公有云，金融机房建设遵从银行级的安全监管与合规要求，符合金融监管一级等保要求

多中心容灾能力
目前提供杭州、深圳、青岛的多个金融专区，您可便捷部署同城双活和异地灾备业务容灾架构，默认具备同城灾备特性，机房级别的故障自动秒级切换，保障业务连续性。

安全灵活网络接入

VPC虚拟网络

金融客户专属服务

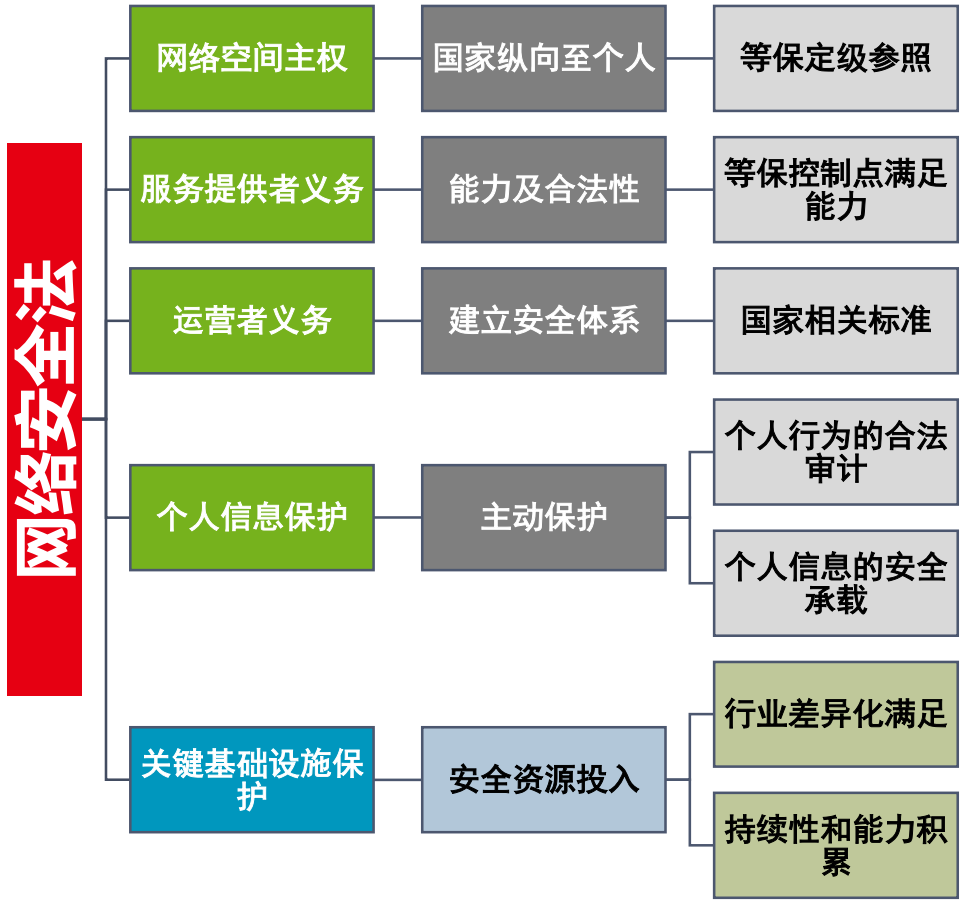
助力金融业务创新

多中心金融合规专区
"两地四中心"合规机房，通过等保四级，可信云等多重认证，协助您顺利通过合规验收，数据异地自动同步，业务无忧

30+安全机制立体防护
多重防护保障数据安全，秒级抵御网络攻击，P级黑产数据，90%恶意用户识别率，降低金融欺诈风险

稳定 安全 合规

政策法规



中央网信办
对外提供服务的专有云平台

- 《关于加强党政部门云计算服务网络安全管理的意见》
- 《信息安全技术云计算服务安全指南》（GB/T 31167-2014）
- 《信息安全技术云计算服务安全能力要求》（GB/T 31168-2014）

公安部
承载等保业务的云平台

- 《网络安全等级保护基本要求 第1部分：安全通用要求》
- 《网络安全等级保护基本要求 第2部分：云计算安全扩展要求
- **《网络安全等级保护条例2.0》2.0把云计算、大数据、物联网等新业态也纳入了监管，监管对象从体制内扩展到全社会**

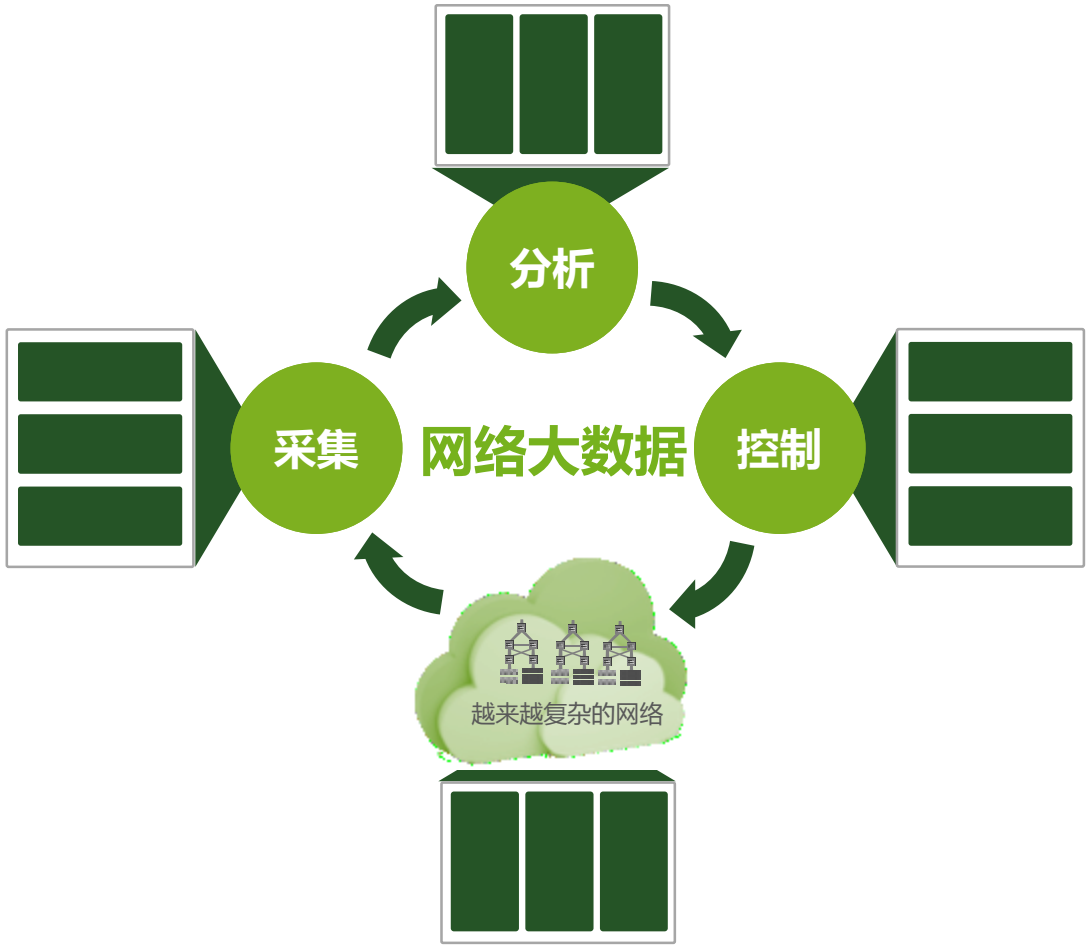
网信办与公安部共同牵头的《关键信息基础设施保护条例》起草完成，目前正在走司法程序。

现阶段1000台以上的服务器规模的云计算平台也算作关键基础设施

解决之道

Simplify the Growing Complexity of Cloud Networking

数据源->分析引擎->数据洞察->决策控制



网络监控方案演进及云网诉求

YunShan Networks | IT大咖说 知识共享平台

抓包工具

- Wireshark/tcpdump
- 适用物理网络
- 人工分析，依赖经验
- 无法回溯流量
- 缺乏直观信息

NPM

- 交换机端口镜像
- 专用物理探针+分析仪
- 大规模采集部署复杂
- 无法采集虚拟网络流量
- 难以应对云环境大流量

Tap as a Service

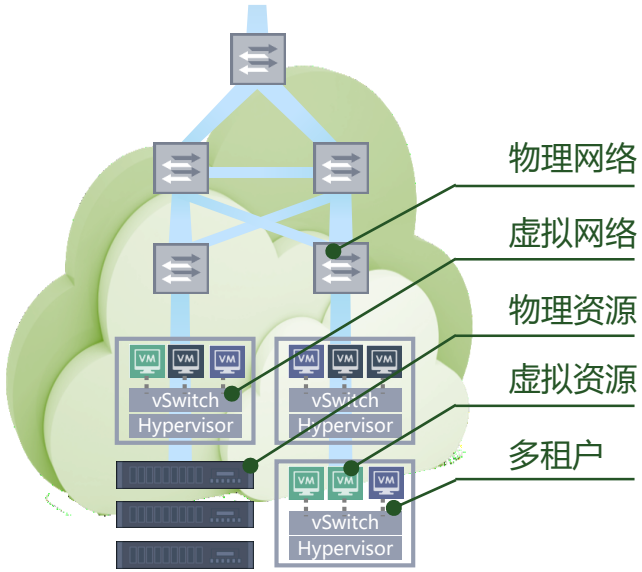
- 通过Neutron端口镜像
- 部署采集虚拟机
- 消耗计算资源
- 占用业务流量带宽
- 无法精细控制镜像策略

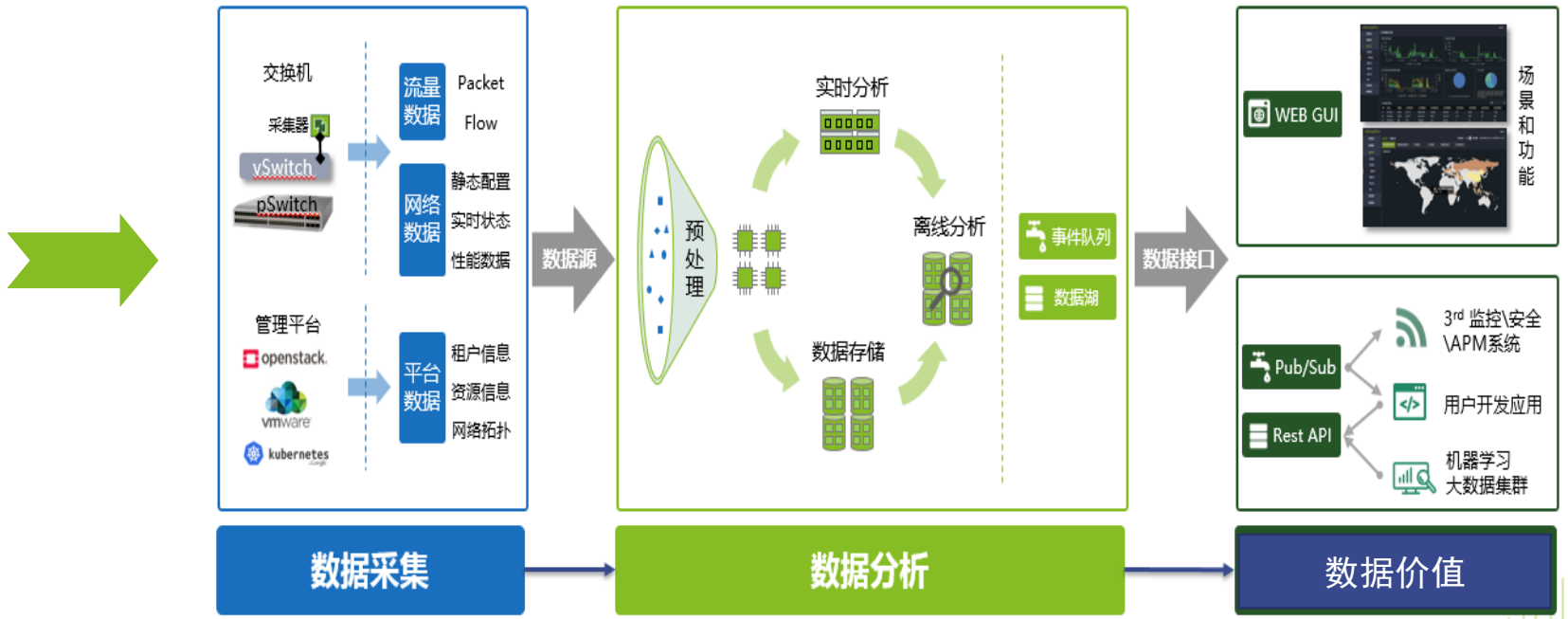
云网分析

- **应对云的大规模东西向流量**
- **对生产网络微/零干扰**
- **采集方式轻量/大规模易管理**
- **符合云的管理运营方式(按需)**

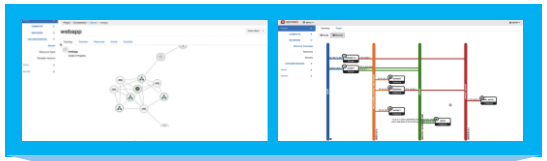
DeepFlow

面向大规模云网的网络数据分析平台





采集——物理网络



资源管理

openstack. vmware

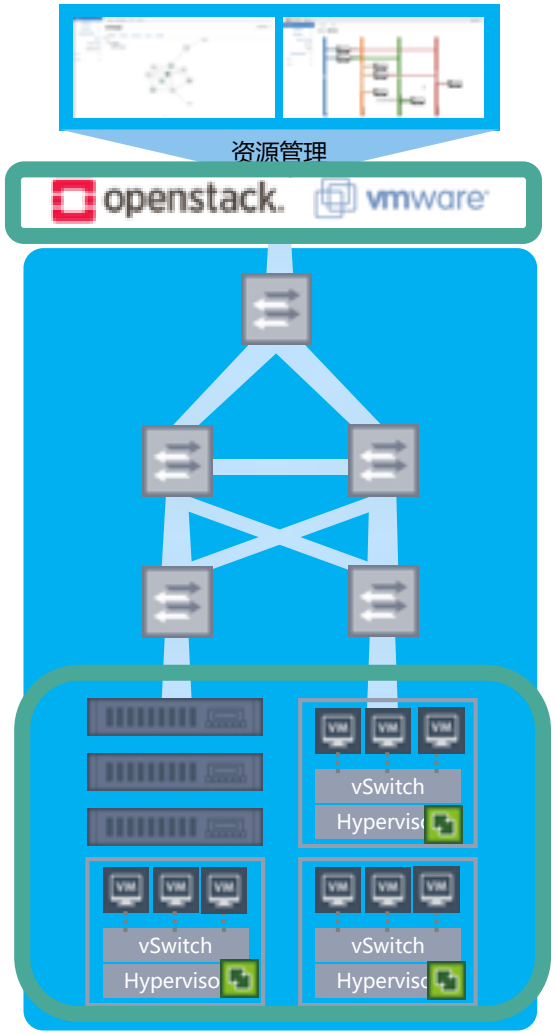
TAP TAP

SPAN SPAN

- TAP/SPAN
  - 硬件（分光器/端口）投入
- sFlow
  - 固定采样比
- NetFlow
  - CPU/TCAM消耗
- Telemetry
  - 设备能力、开放度

综合使用

采集——虚拟网络



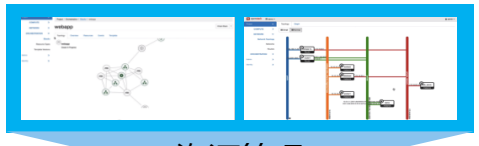
第一代技术：修改vSwitch → 性能要求严苛：OvS-DPDK
新增/修改内核模块，干扰业务策略

第二代技术：采集器虚拟机 → 封闭vSwitch：vSphere ESXi
管理大量采集器虚拟机
vSwitch报文复制开销
干扰业务策略

第三代技术：影子交换机 → **绝大多数场景**

	修改vSwitch	采集器虚拟机	影子交换机
部署零依赖	✘	✔	✔，对部署系统没有任何第三方库或组件依赖
业务策略零干扰	✘	✘	✔，无需对vSwitch等虚拟网元配置任何策略
资源低消耗	✔	✘	✔，资源消耗可控，0.4CPU/100kpps，内存平均消耗<400M，带宽平均消耗<5%
运维简单	✘	✘	✔，二进制文件14M，秒级启停，上千台计算节点部署易于管理

采集——云平台租户信息



资源管理

openstack. vmware

Cloud MGMT

10.16.1.0

10.68.1.0

10.18.1.0

FW LB VM VM

租户VPC

租户VPC

租户VPC

可视化——业务流量

YunShan Networks | IT大咖说 知识共享平台

erlay网络和Underlay网络关联映射

业务流量分析 | 虚拟网络性能量化 | 接入网络性能量化

对于有流量关系的资源组间，以分段的形式，追踪网络性能出现瓶颈的点， 排序检测资源组间间/内延迟RTT及对应流量之间的关系；同时可
接时的成功率、与RTT延迟，重传次数/重传率，TCP ZERO WINDOW/TCP PSH URG，并发数量等指标。

RTT延迟详情

RTT延迟

最大延迟：10.100.107.6 -> 10.100.

平均延迟：2.14毫秒

最大延迟端口：42508

流速峰值：10.100.107.5 -> 10.100.

平均流速：261.92Mbps

最大流量端口：80

总重传：237113

总重传率：0.02%

业务

admin

选择开始时间 | 选择结束时间

流量分析 | 项目流量分析 | 回溯分析

超过80% | 超过50% | 正常

内网流量分析 / IP流量分析

时间间隔： 1天

时间范围： 2017-09-04 14:53:49 - 2017-09-11 14:53:49

IP流量分析 | 项目流量分析 | 回溯分析 | 特征分析

监控点拓扑

从探针点所采集IP流量信息，映射层次为：探针点->子网->IP

wExporter-vm15

vlan-2593 | vlan-2509 | vlan-2528 | vlan-1026

192.168.0.14 | 192.168.0.2 | 192.168.0.3 | 192.168.0.15 | 10.1.1.30 | 192.168.0.4 | 192.168.11.27 | 192.168.0.12 | 192.168.0.13 | 192.168.0.16 | 10.1.102.171

IP关联图

云外IP地址 | 广播IP地址

IP流量关联信息图，为在固定时间段内采集到的所有相关联IP的会话关系

OVS - 5

vm-1 | vm-2 | vm-3 | vm-4 | vm-5 | vm-6 | vm-7 | vm-8 | vm-9 | vm-10

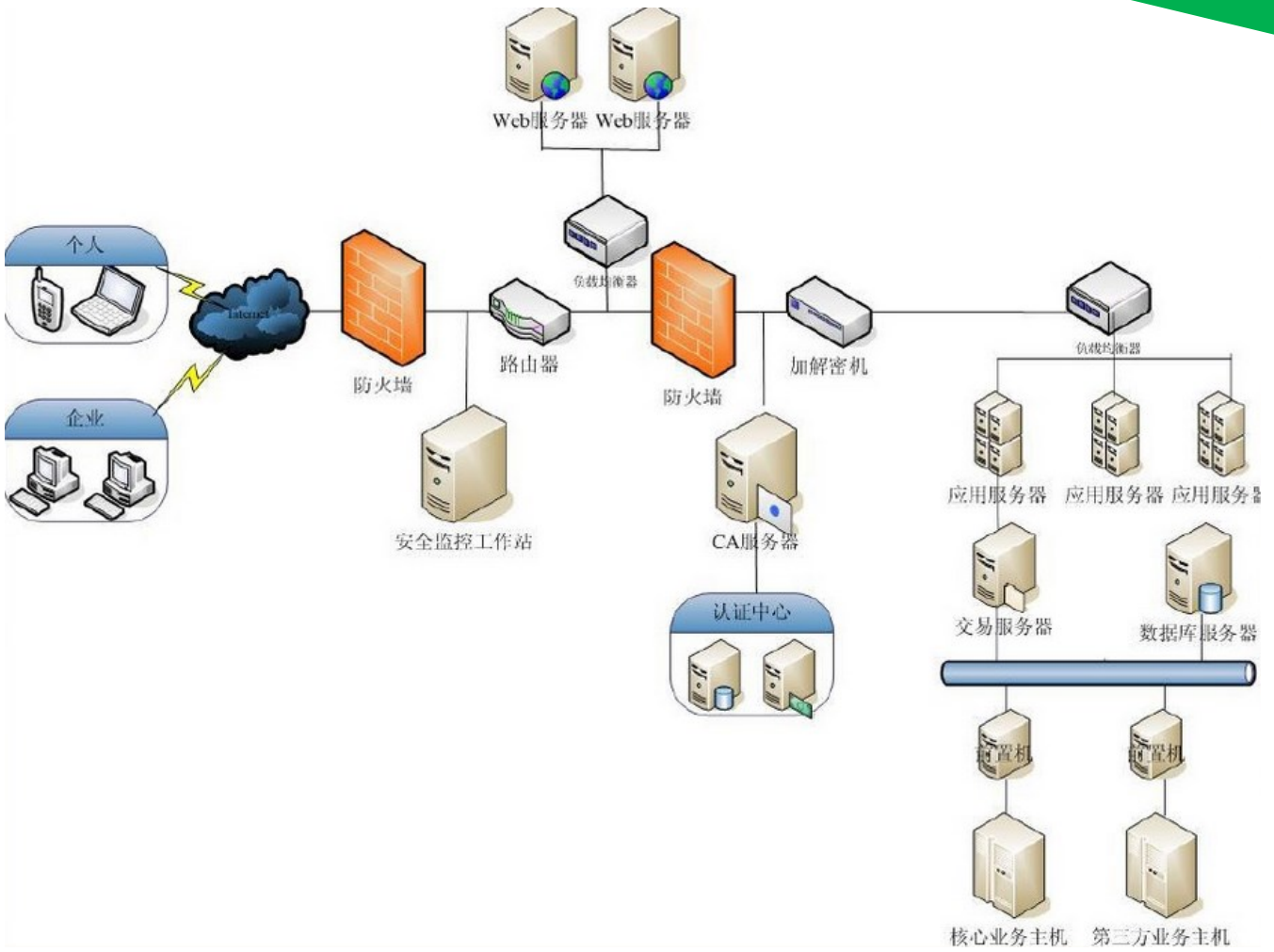
更多

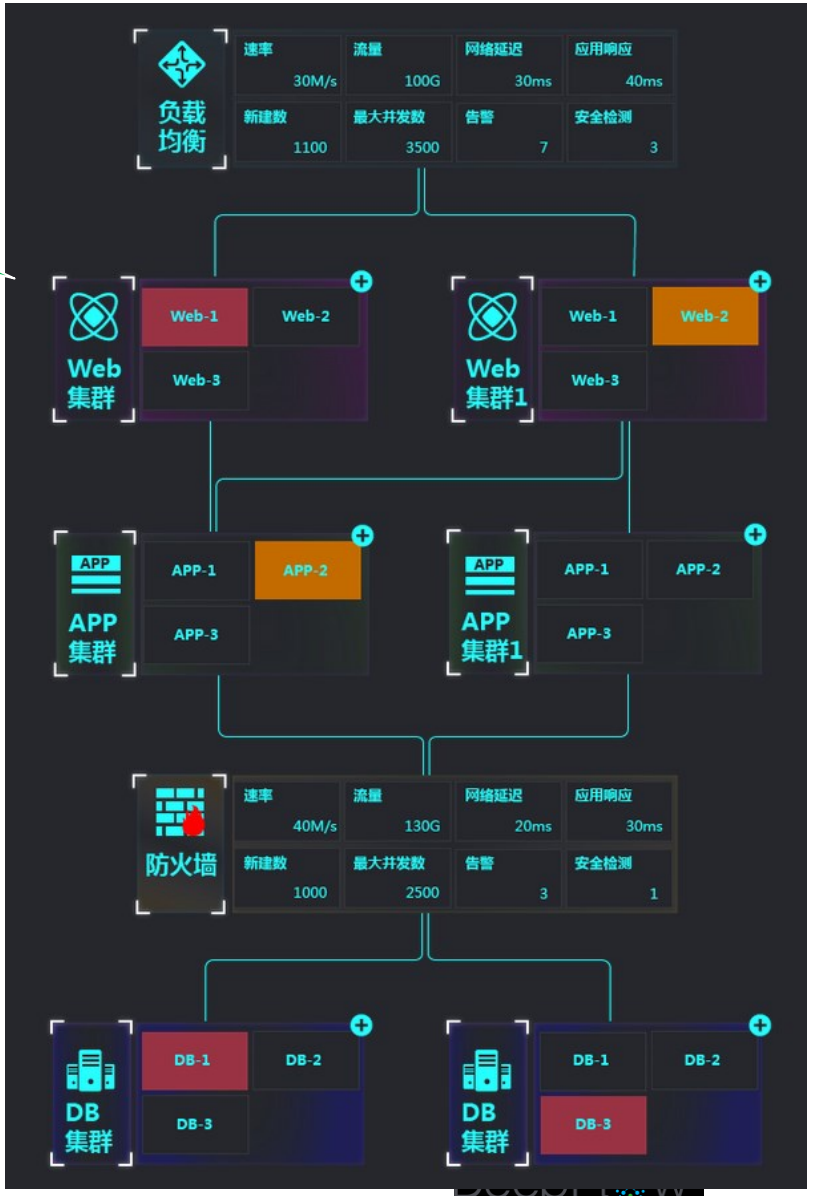
实时业务流量拓扑

DeepFlow

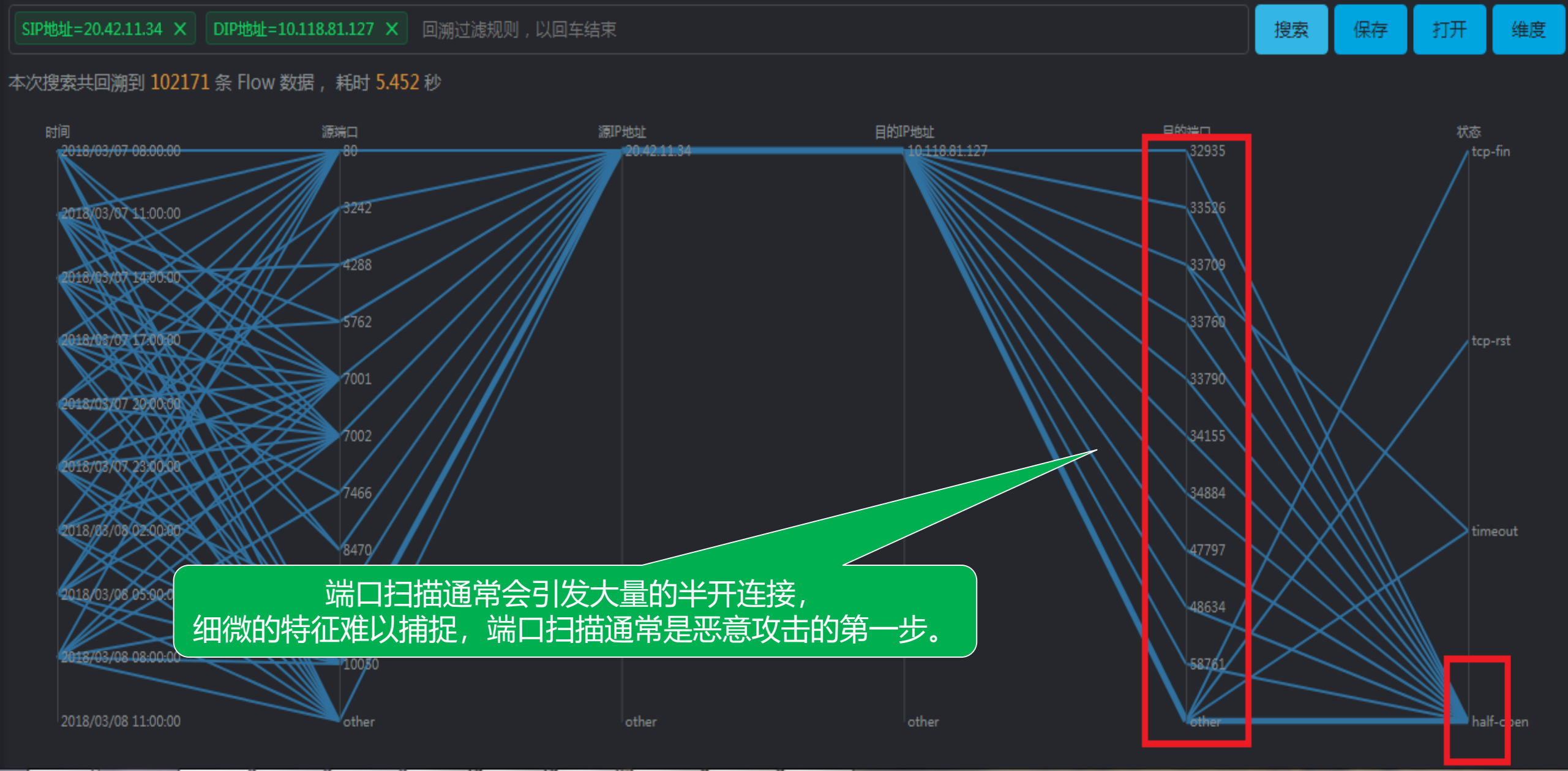
分析——业务画像

针对业务网络中每个分段的网络用量及性能统计分析，并周期性输出报表



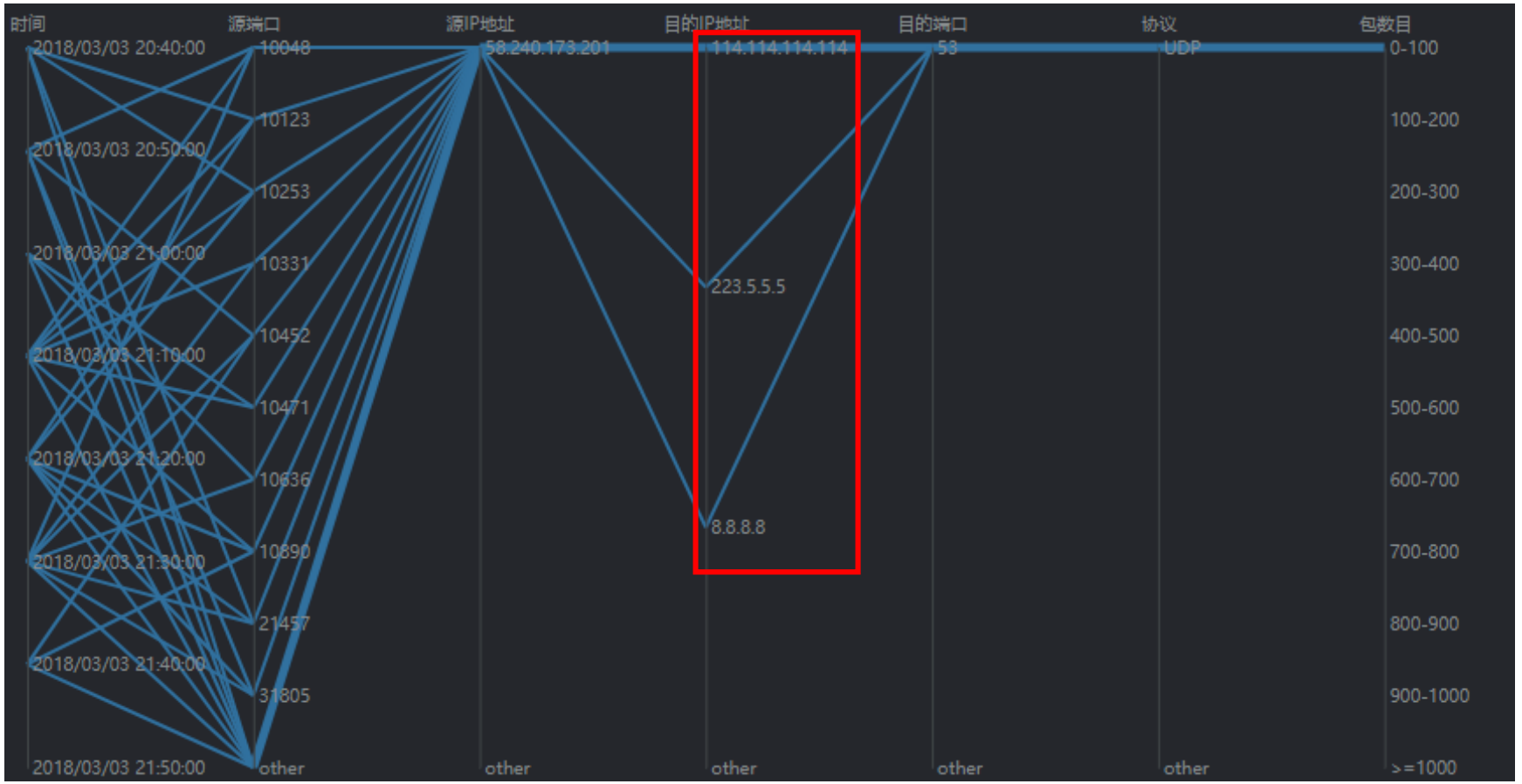


分析—安全诊断


SIP地址=20.42.11.34
DIP地址=10.118.81.127
回溯过滤规则，以回车结束
搜索
保存
打开
维度
本次搜索共回溯到 102171 条 Flow 数据， 耗时 5.452 秒
时间
源端口
源IP地址
目的IP地址
目的端口
状态
2018/03/07 08:00:00
2018/03/07 11:00:00
2018/03/07 14:00:00
2018/03/07 17:00:00
2018/03/07 20:00:00
2018/03/07 23:00:00
2018/03/08 02:00:00
2018/03/08 05:00:00
2018/03/08 08:00:00
2018/03/08 11:00:00
80
3242
4288
5762
7001
7002
7466
8470
10080
other
20.42.11.34
other
10.118.81.127
other
32935
33526
33709
33760
33790
34155
34884
47797
48634
58761
other
tcp-fin
tcp-rst
timeout
half-open
端口扫描通常会引发大量的半开连接，
细微的特征难以捕捉，端口扫描通常是恶意攻击的第一步。

分析—业务优化

是否能通过一定的调整，统一服务器虚拟机的配置，不使用8.8.8.8的DNS解析。



分析——安全审计

实时分析　回溯分析　**安全白名单**　会话回溯　服务记录

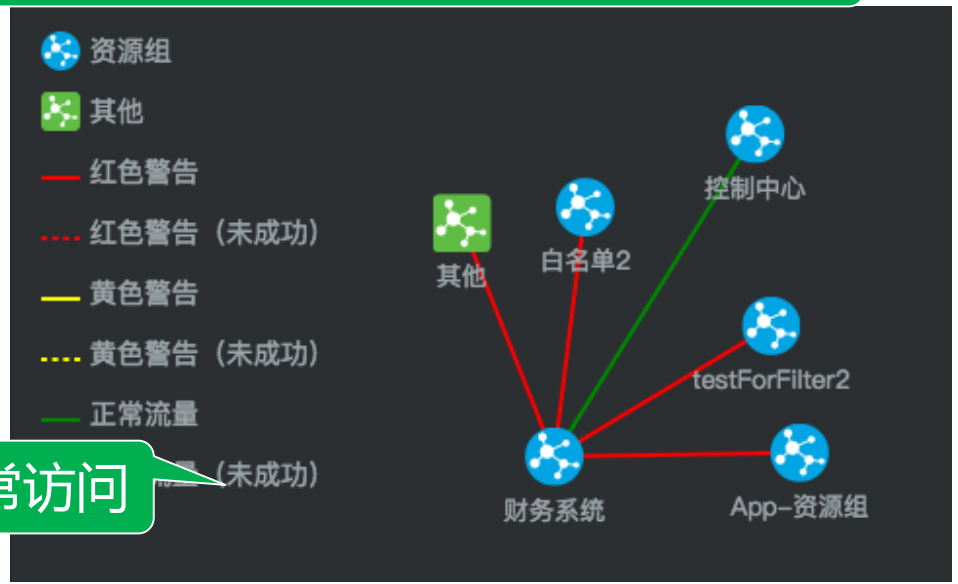
通过对感兴趣的业务设置安全监控规则， 可以分析出实际流量是否符合预期，并以告警方式通知用户

新建

序号	名称	项目	创建时间
1	财务系统访问权限-只有控制中心可访问	admin	2018-03-20 00:52:22

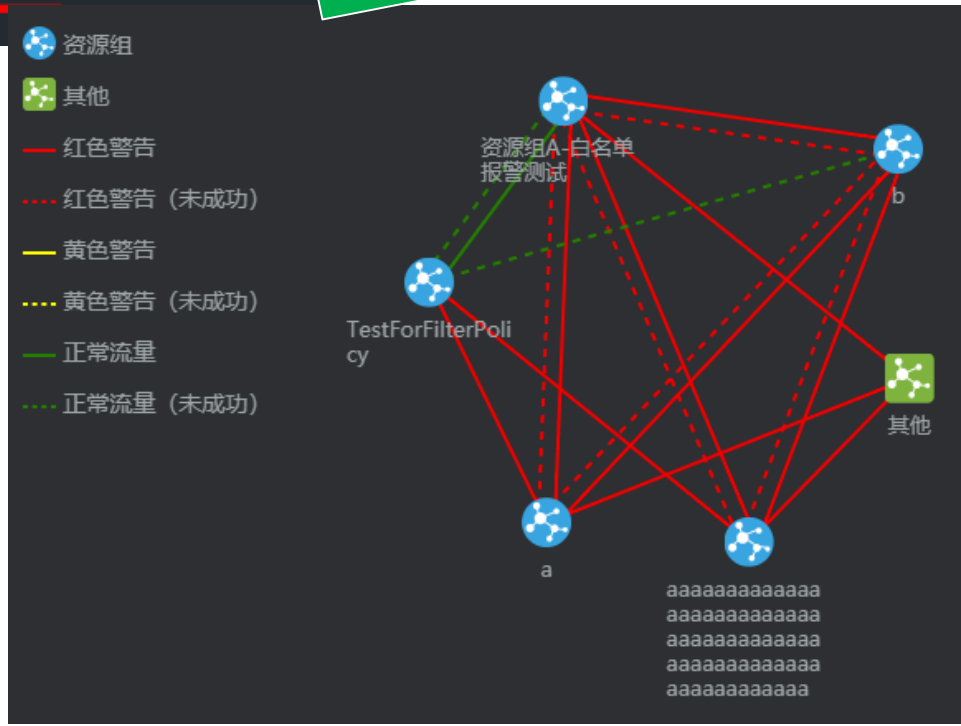
策略名称： 财务系统　可信源： 控制中心　允许访问： 财务系统　协议： TCP　目的端口： 80

根据业务意图，配置白名单验证意图

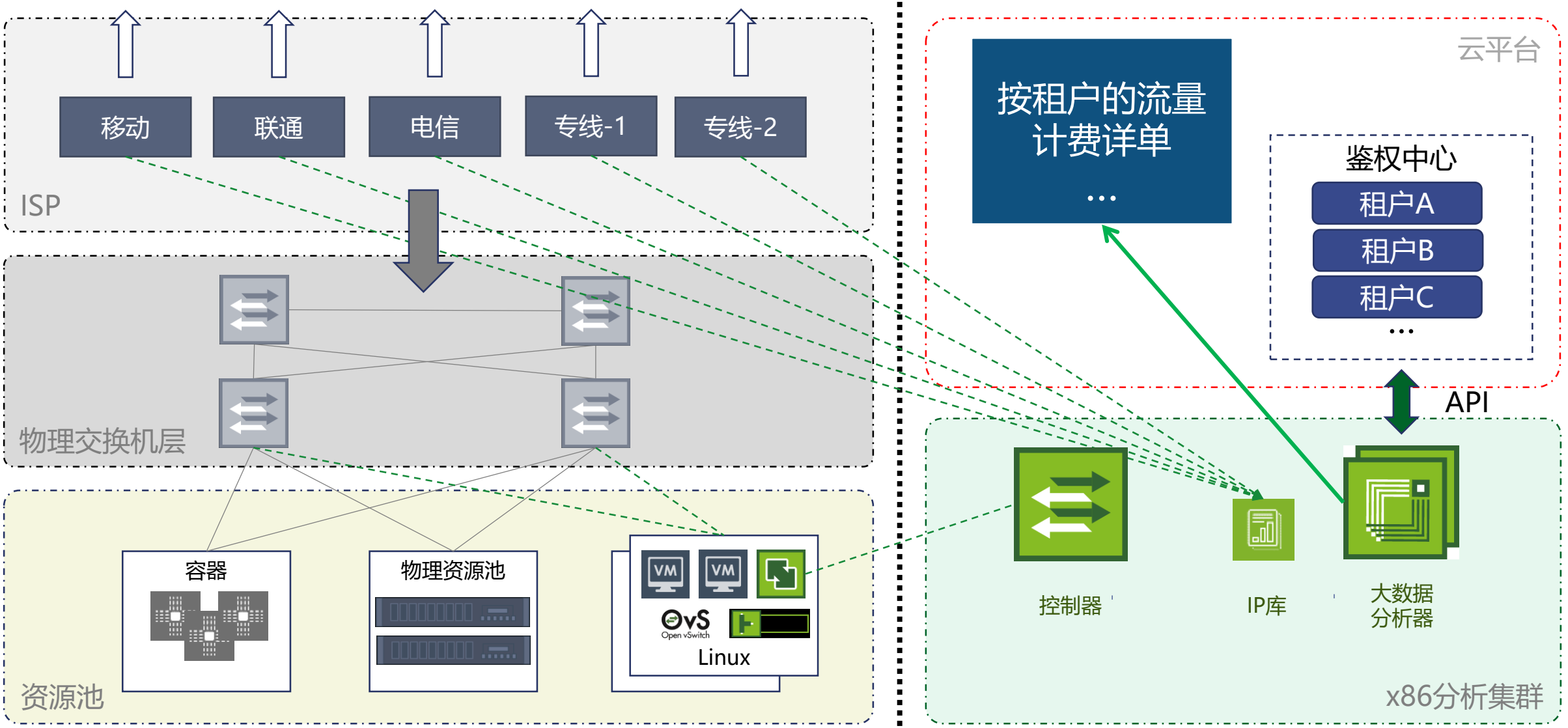


第一时间发现异常访问

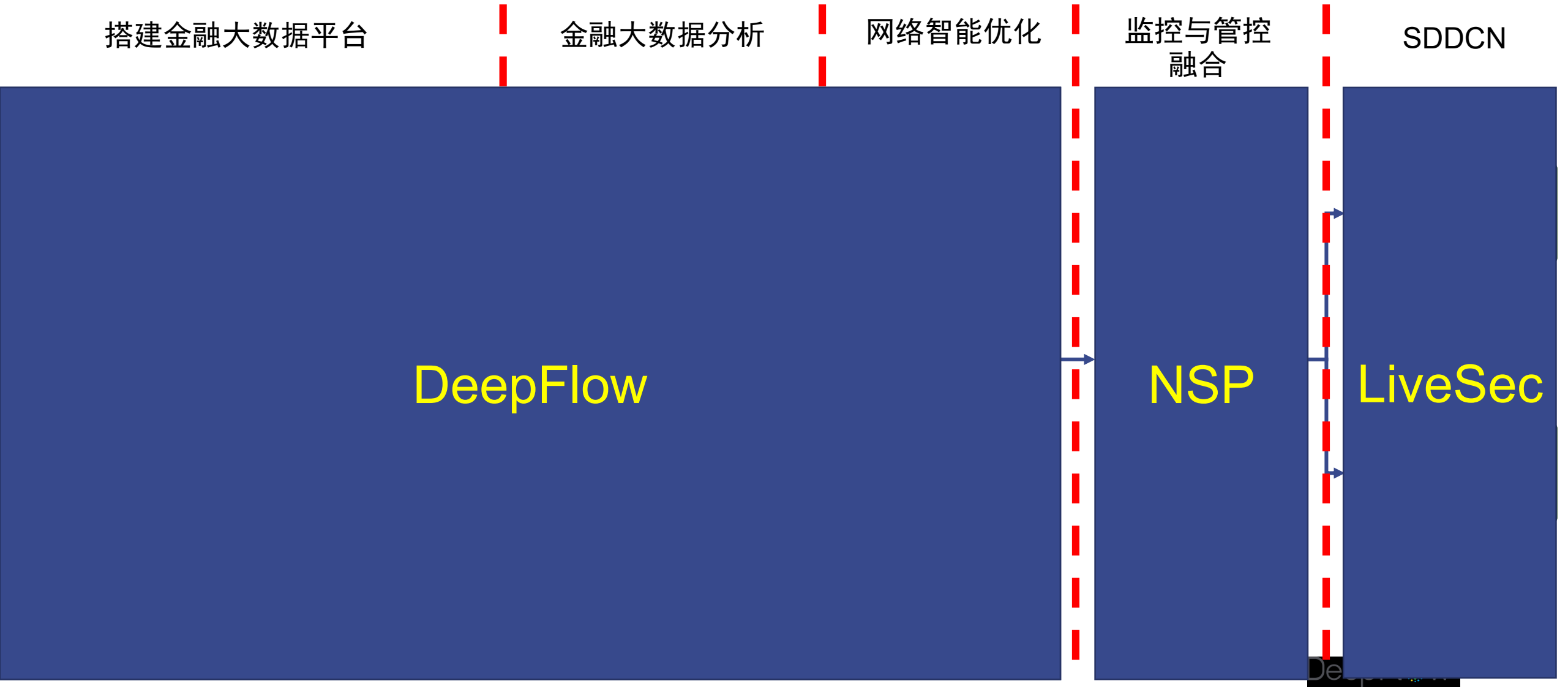
亦可发现未成功的入侵尝试



运营——计量/资源分配


移动
联通
电信
专线-1
专线-2
ISP
物理交换机层
容器
物理资源池
VM
VM
OvS
Open vSwitch
Linux
资源池
云平台
按租户的流量
计费详单
…
鉴权中心
租户A
租户B
租户C
…
API
控制器
IP库
大数据
分析器
x86分析集群

总结—金融云数据中心应对步骤



云杉网络·技术创造价值

www.yunshan.net

Thanks