环宇数通
sotote.com

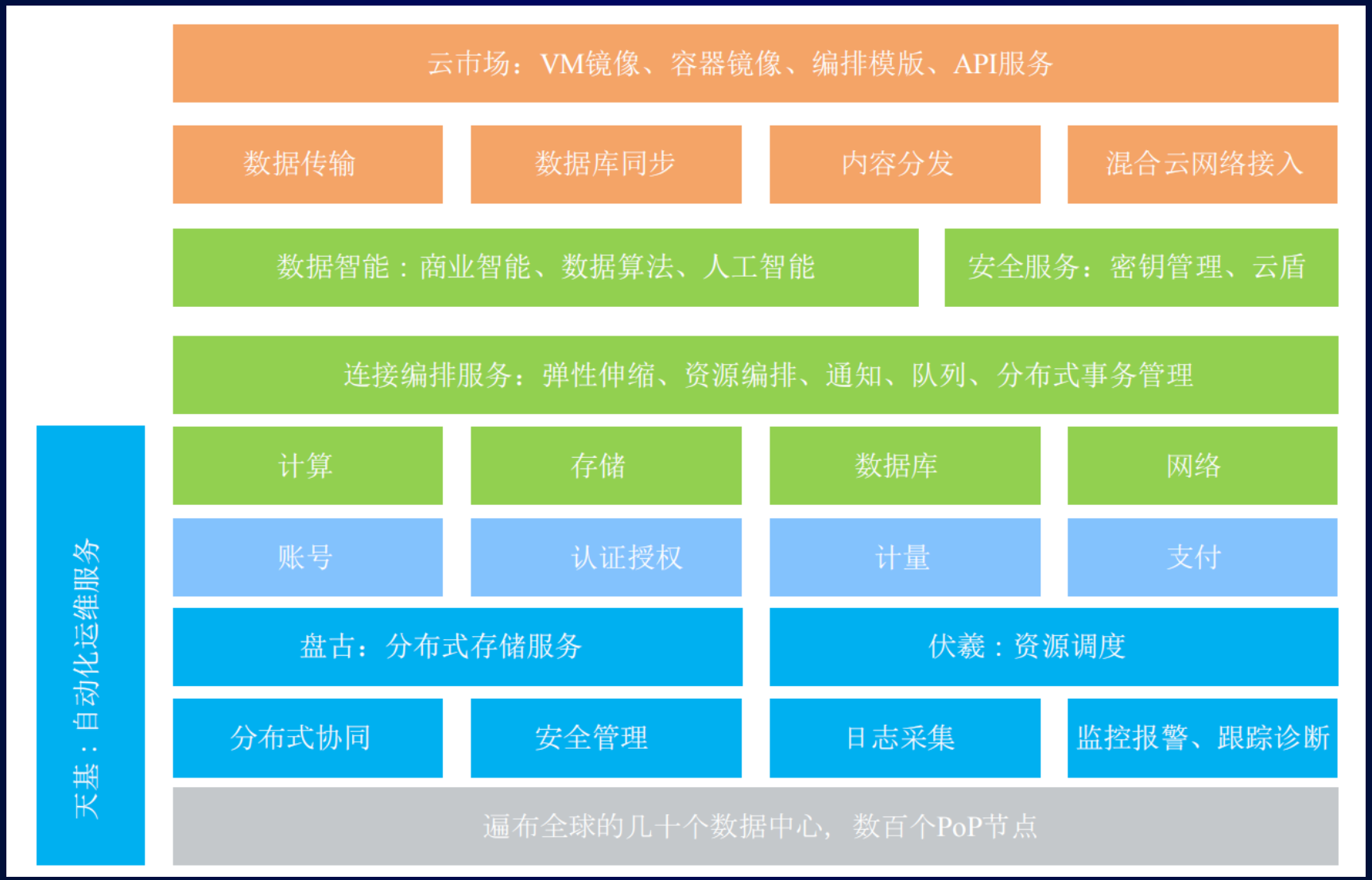
云构架设计

降本增效 云上创新

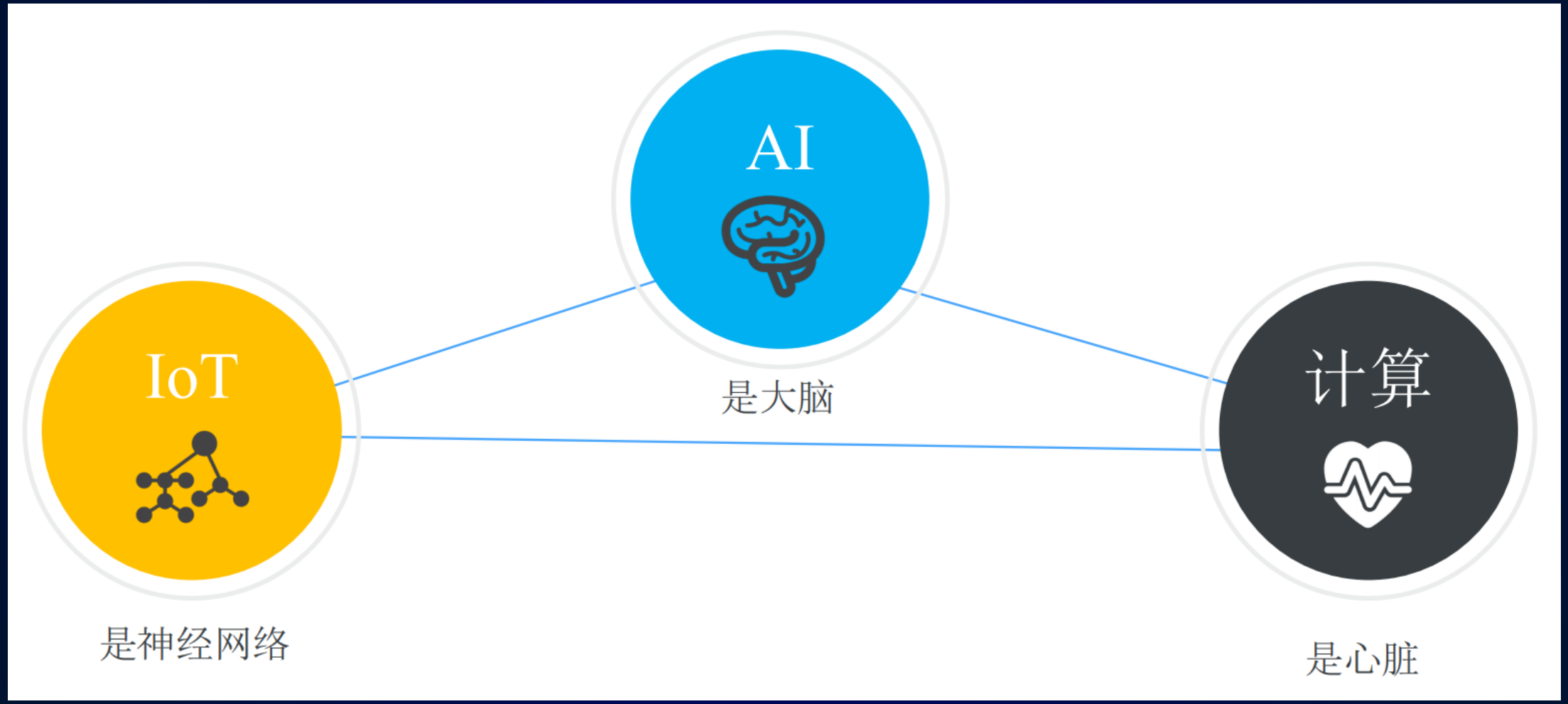
北京环宇数通科技有限公司

中国领先的云安全服务商

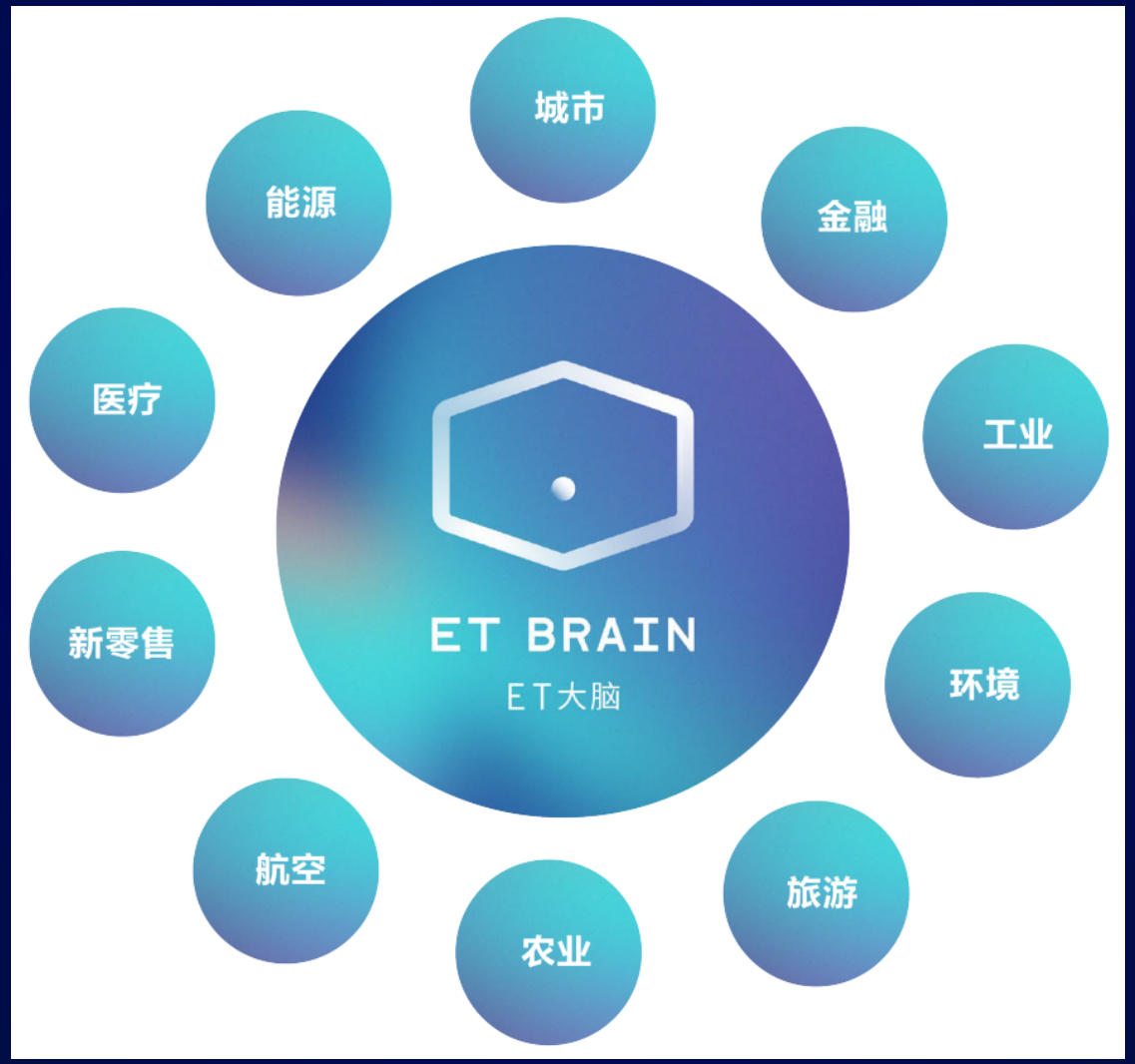
阿里云飞天平台


云市场：VM镜像、容器镜像、编排模版、API服务
数据传输
数据库同步
内容分发
混合云网络接入
数据智能：商业智能、数据算法、人工智能
安全服务：密钥管理、云盾
连接编排服务：弹性伸缩、资源编排、通知、队列、分布式事务管理
计算
存储
数据库
网络
账号
认证授权
计量
支付
盘古：分布式存储服务
伏羲：资源调度
分布式协同
安全管理
日志采集
监控报警、跟踪诊断
遍布全球的几十个数据中心，数百个PoP节点
天基：自动化运维服务

基于云计算的三驾马车



AI大脑：将AI技术与垂直行业结合的超级智能体



云架构设计原则

安全性

网络安全
主机安全
服务安全
数据安全
账号体系安全
……

可扩展性

网络规划
负载均衡
弹性伸缩
手动升降配
……

服务可用性

服务可用性
服务器可用性
网络可用性
RTO
……

数据可靠性

快照备份策略
数据备份策略
RPO
……

成本优化

产品性能选择
产品数量选择
计费方式选择
……

云架构设计-设计流程

项目启动

- 确定启动会议的甲方、乙方以及第三方干系人
- 准备项目启动会议报告并招开启动会
- 确定项目目标及验收标准
- 准备项目计划并达成一致

评估系统现状

- 采用调查表、访谈、工具等方式获取现有业务系统的平台、配置、架构及关联等信息
- 评估获取业务系统的现状
- 确定服务部署方式

设计云上架构

- 结合最佳实践设计云上架构
- 选择合适的云产品组合
- 设计系统的云上及迁移方案

实施及验收

- 创建账号
- 根据网络规划创建网络环境
- 云产品开通及配置
- 应用迁移/数据库迁移/非结构化数据迁移
- 功能与性能测试
- 业务上线或割接

云架构设计-网络规划

VPC规划

- VPC是专有的云上私有网络，用户可以完全掌控自己的专有网络，例如选择IP地址范围、配置路由表和网关等。
- 用户可以在自己定义的专有网络中使用云资源，如云服务器、云数据库和负载均衡等。

VSwitch规划

- 交换机（vSwitch）是组成专有网络的基础网络设备，用来连接不同的云资源。
- 确保地址空间不重叠。
- 交换机的网段不应涵盖专有网络的整个地址。
- 至少创建两个交换机，并部署在不同可用区内，以确保高可用。

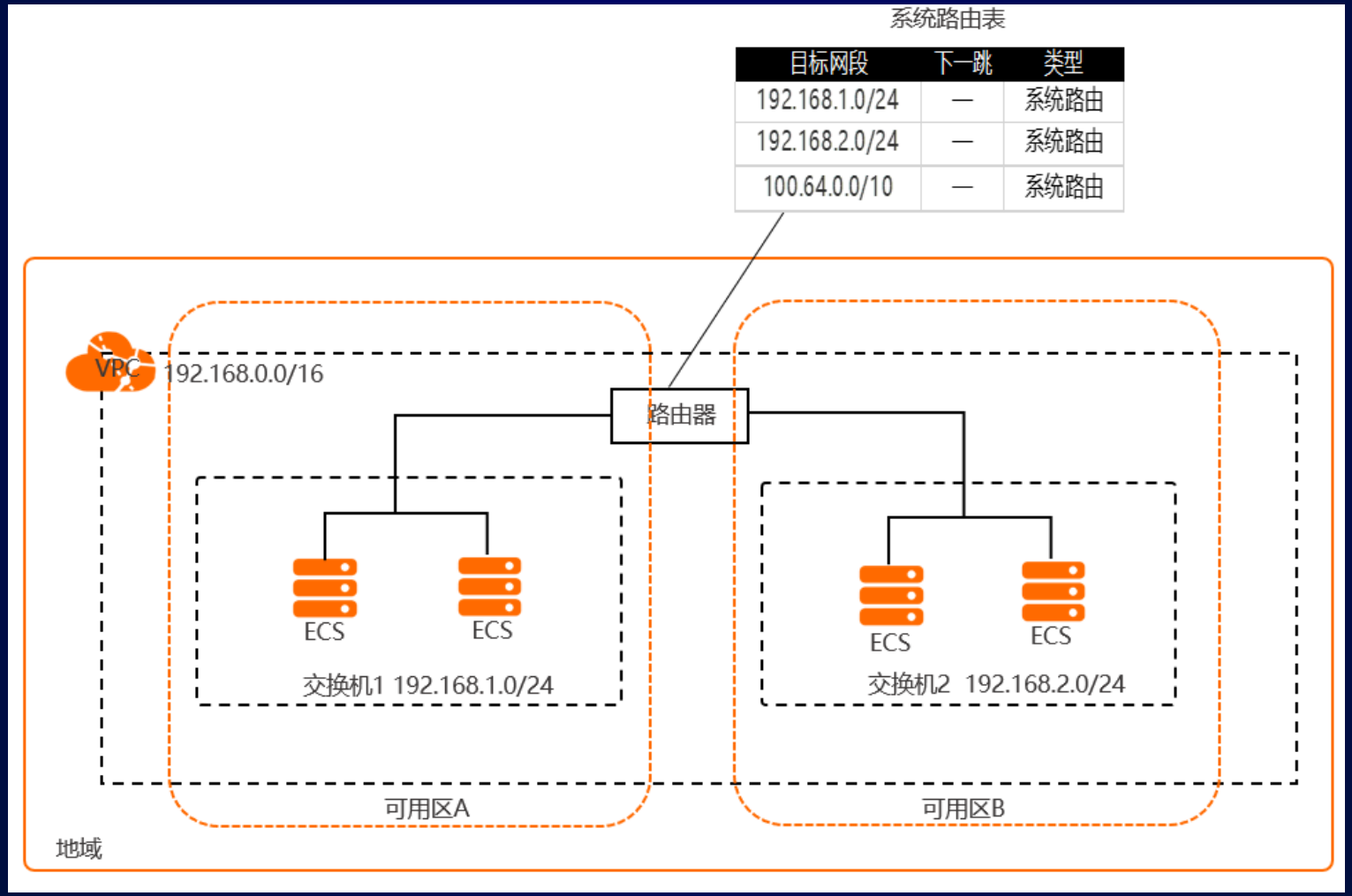
IP段规划

- 基于业务部署的网络架构，进行私网IP段的规划
- 使用192.168.0.0/16、172.16.0.0/12、10.0.0.0/8这三个私网网段及其子网作为专有网络的网络地址。
- 尽可能做到不同专有网络的网段不同，不同专有网络可以使用标准网段的子网来增加可用的网段数。

IDC到云上网络连通规划

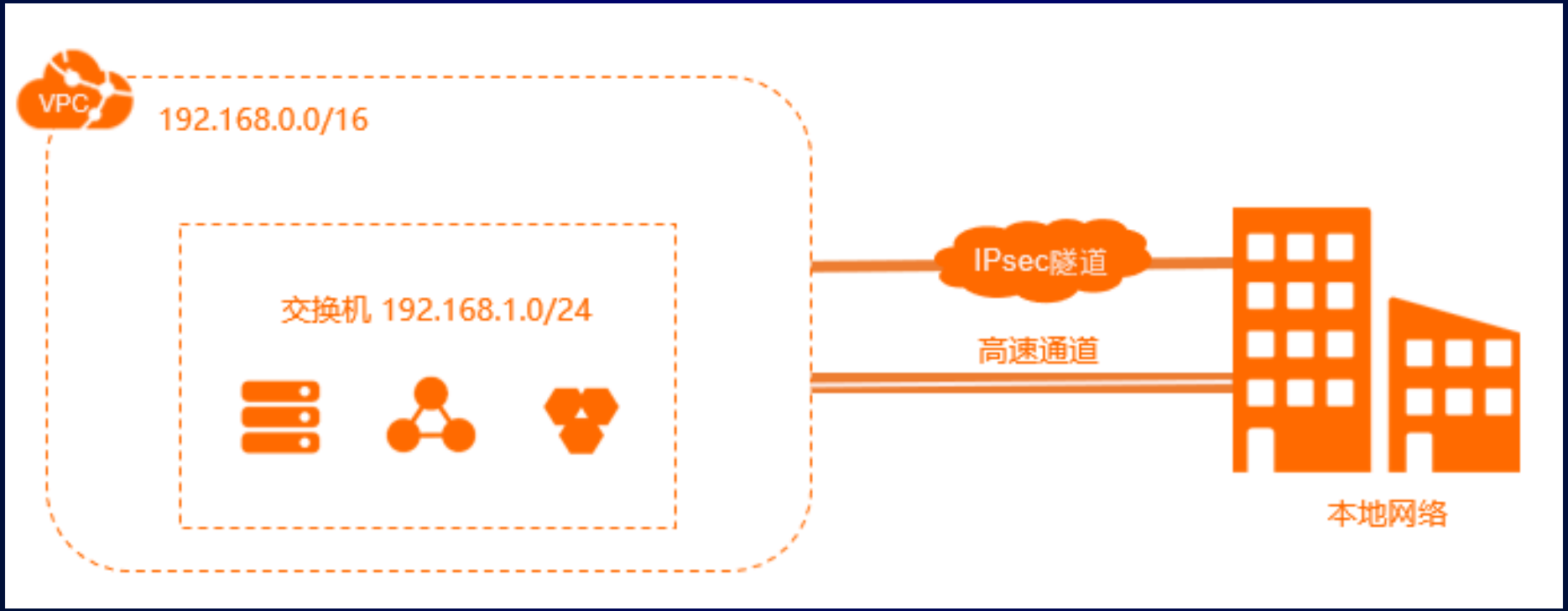
- 如果有专有网络和本地数据中心构建混合云的需求，推荐使用IPsec隧道或高速通道将本地数据中心和VPC连接起来，扩展本地网络架构。

云架构设计-网络构架图


系统路由表
目标网段 下一跳 类型
192.168.1.0/24 — 系统路由
192.168.2.0/24 — 系统路由
100.64.0.0/10 — 系统路由
VPC
192.168.0.0/16
路由器
ECS
ECS
交换机1 192.168.1.0/24
ECS
ECS
交换机2 192.168.2.0/24
可用区A
可用区B
地域

云架构设计-构建混合云

通过该方式，将本地应用程序与云上进行安全高速互通，并且不必更改应用程序的访问方式。



云架构设计-安全规划

01 安全基础配置

通过平台默认安全能力，减少网络攻击面和权限滥用。

02 基础安全防护

企业安全能力建设的第一道屏障帮助企业抵御攻击和入侵，提高主动安全防御能力。

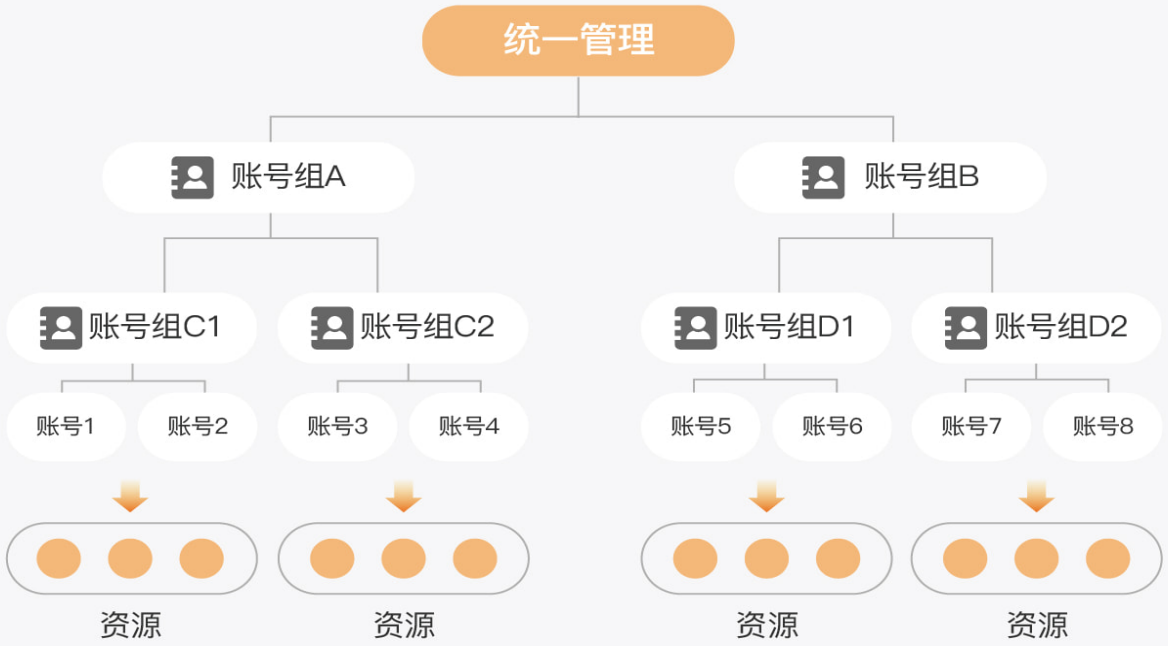
03 增强安全防护

在基础安全防护之上，进一步构建Web应用的安全防护能力并使企业满足等级保护相关合规需求。

云架构设计-安全架构图


用户
运维人员
WAF
SSL证书
防御扫描、WEB攻击、刷接口、刷红包，可按地域封禁请求。
加密HTTP通信，APP强制校验HTTPS证书，提高APP破解难度。
云防火墙
SLB负载均衡
VPC
管理互联网到业务的南北向访问策略和业务与业务之间的东西向微隔离策略，防护恶意入侵行为(IPS)。
业务云服务器
堡垒机
主机安全
OSS
定期对所有域名扫描漏洞并输出扫描报告。
网站漏洞扫描
安全管家服务协助用户对系统进行日常安全监控和应急响应。
安全管家
对开发和运维人员进行合理授权和操作行为审计
数据库
数据库审计
数据库SQL注入、风险操作等数据库风险操作行为进行记录与告警；
定期对服务器和部署应用进行漏洞扫描、配置和弱口令检查，防范入侵。

云架构设计-账户体系设计



当企业拥有多个云账号时，他们希望可以统筹管理这些账号及资源。通过统计资源使用情况将分散的资源账号挂载到企业预设的目录结构下，实现企业对他们的所有资源的集中管理。

云架构设计-云产品选型设计