金山云混合云网络架构设计与实现

金山云 侯震宇

完备的基础设施和存储资源

19个
大型数据中心

600+个
全球CDN节点数量

500G+
BGP带宽储备

80000+台
服务器总量

20T+
全网CDN带宽总量

100G+
长途骨干网带宽总量

金山云用三年的时间构建出完善的公有云服务基础设施，具备充足的储备资源环境。

5T+
城域骨干网带宽总量

全球网络布局

六大数据中心集群： 北京 上海 杭州 扬州 香港 新加坡

混合云产品矩阵


全局智能流量调度
多云管理解决方案
异地互联解决方案
云主机
云物理机
专属云
公有云
King--stack
BM
云 IDC
金山云
多云互联解决方案
专线/VPN 解决方案
云主机
其他云
King--stack
BM
客户 IDC

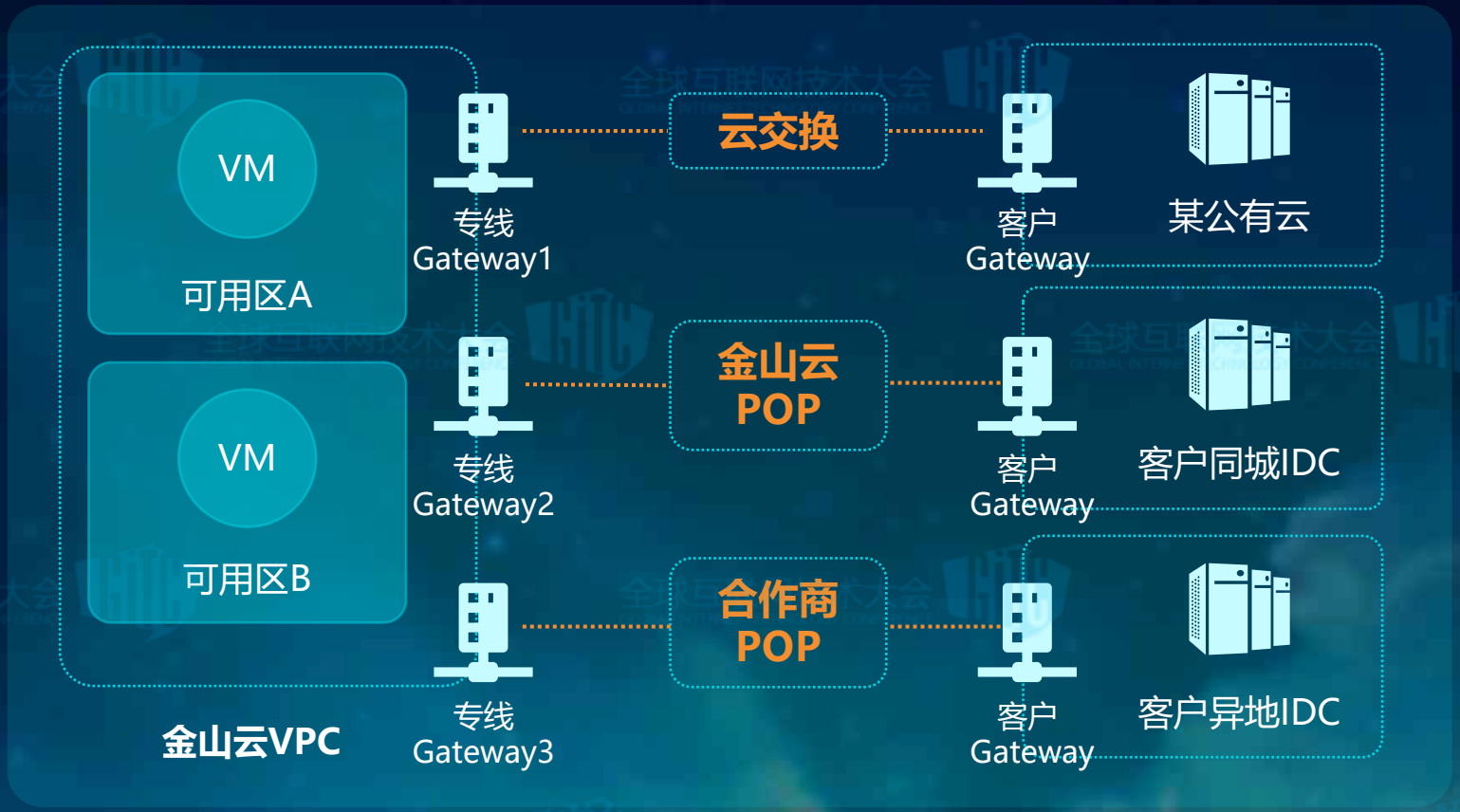
支撑混合云的网络产品

金山云网络产品是以优质的IDC网络，同城，异地骨干网络，自建BGP网络为基础，以自主研发技术为核心，高可用，高性能，软件定义的基础产品。

- 单网关集群可支撑**2万物理机**
- 国内**最早全Region VPC化**提供服务
- 自建北京，上海，广州三地**冗余骨干网络**
- **80线BGP公网**，超**500G公网带宽**
- 提供云物理机（EPC），托管云（KIS）

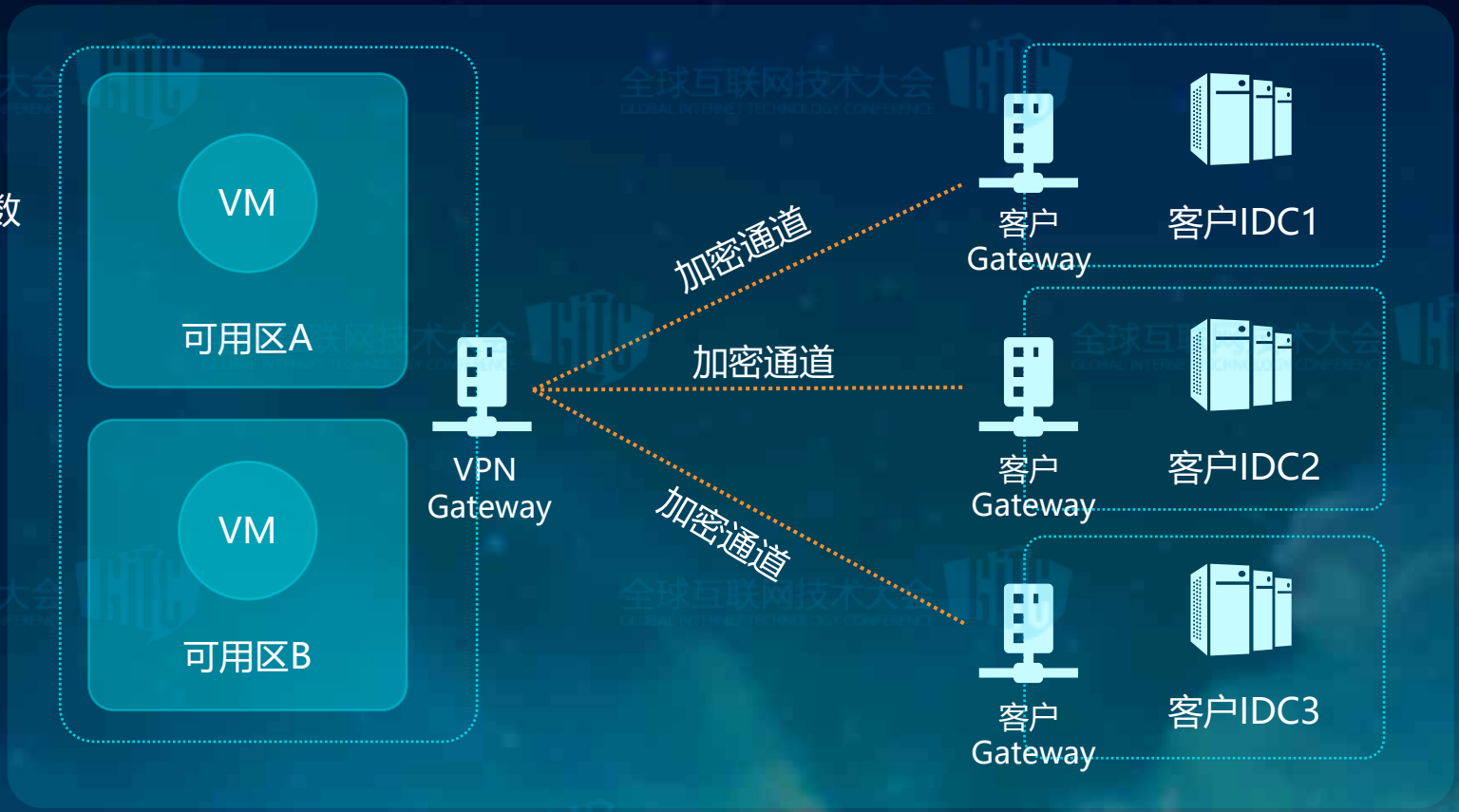
混合云-专线

- **专线特性**
  - 大吞吐，低延时
  - 用户独占，数据传输安全，无泄漏风险
  - 全链路冗余部署，高可用
  - POP点全球覆盖，客户就近接入



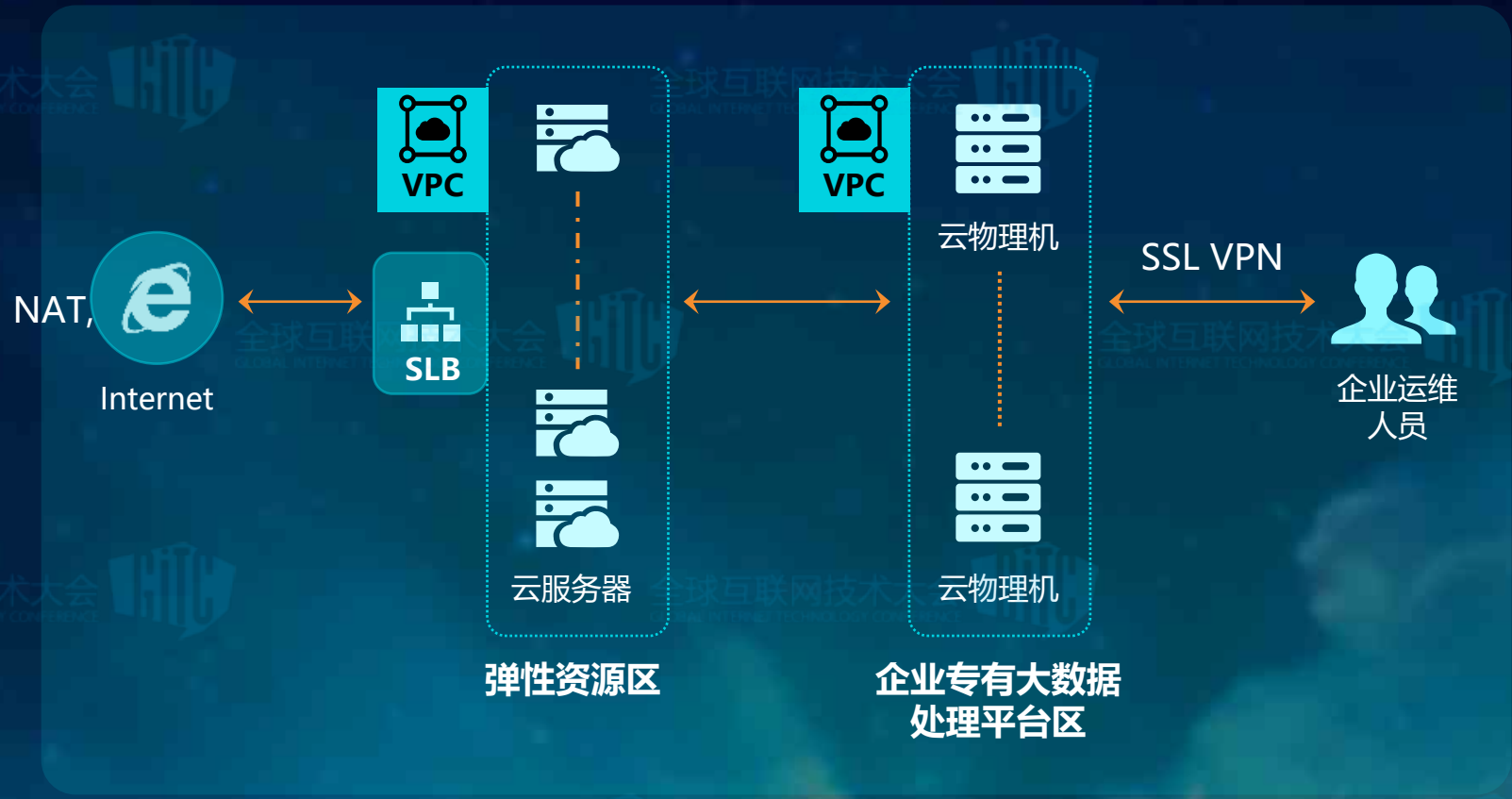
混合云-VPN

- **VPN特性**
  - Site to Site VPN 隧道
  - IPSec ， GRE ， IKEV2 保证数据传输安全可靠
  - 多机部署，自动容灾
  - 监控告警，弹性扩容



混合云-云物理机(EPC)

- **EPC特性**
  - 独享裸金属物理机，按需购买按量付费，稳定可靠
  - 无缝对接公有云VPC，使用高质量的公网 BGP ， SLB等功能。
  - 云监控；自助化带外管理；专业高效7*24小时运维服务
  - 灵活自定义配置，满足多样性计算，存储需求。



混合云-专属云

专属云是金山云提供的用户专属虚拟化资源池，用户可在专属宿主机上创建自定义配置的专属云服务器，应用领先的虚拟化技术满足资源独享、安全等需求。

特点

资源物理隔离　灵活分配资源　安全可靠

异地互联多活/灾备连接解决方案

案例场景1-VPC上部署多层web应用

需求

云上业务快速部署，安全可控，业务分层。

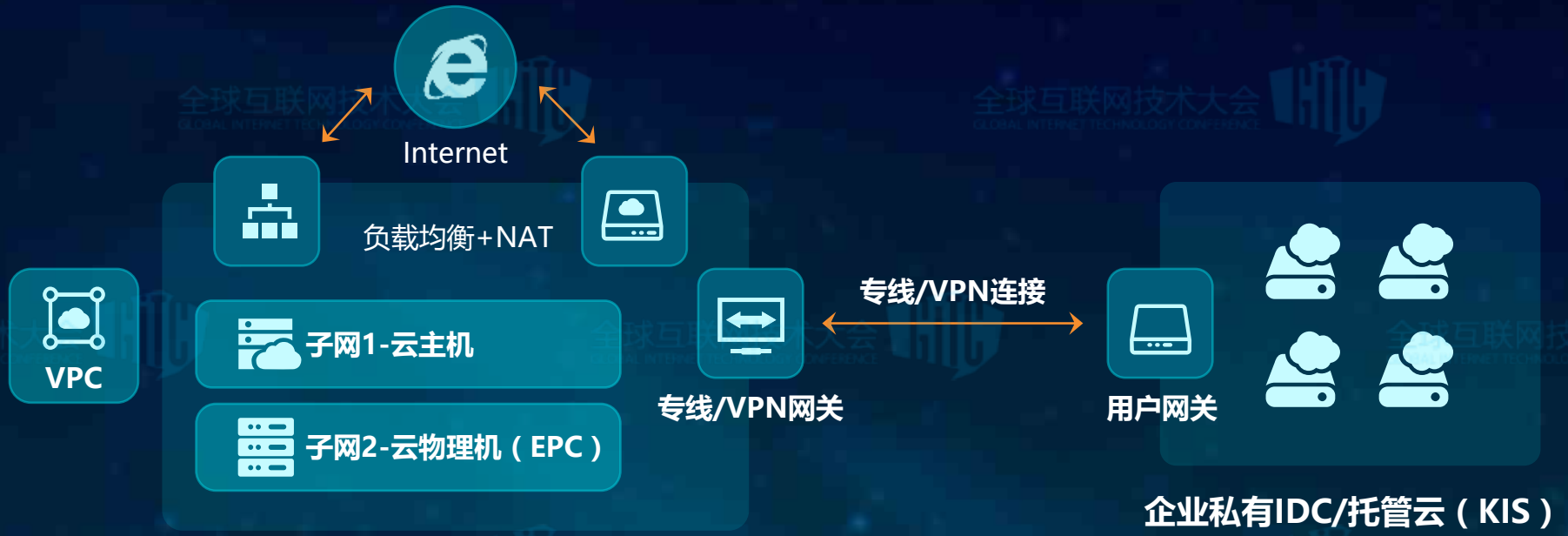
部署方式

网络规划三级，配合安全组，ACL等功能进行访问控制；SLB和NAT，实现统一接入接出，并隐藏内部服务。

受益

网络规划分钟级完成，业务隔离化，服务可扩展。

案例场景2-混合云电商大促



需求

某大型电商业务具有较强的时效性，双11、6.18大促销活动，需应对突增访问量。

部署方式

内部核心系统与核心数据存储在用户自建数据中；
云上部署服务应用服务，应对用户实时业务访问激增。

受益

企业原有核心业务安全，同时给客户每年节省数百万成本。

案例场景3-智能家居生态云

案例场景4-医联体专属云+私有云

混合云网络产品核心优势

软件定义网络

- 100% 自研核心网关；
- 分钟级网络环境自主化部署(OpenAPI，SDK，或者控制台)；
- 混合云，多云互通。

高可用

- 全系产品SLA 99.99%；
- AZ内，跨AZ，跨Region三级高可用部署；
- 80线BGP（三大运营商+数十家中小运营商）覆盖。

高性能

- 负载均衡最大支撑吞吐带宽120Gbps，每秒新建连接数1800w，最大并发连接数8亿；
- 云解析单节点超800wpps，全国数10个节点，最大可防御超过200G攻击。

设计原则


• SLA 99.99%
稳定性
性能
• 自研设备性能
• 用户QOS性能保障
• Scale out
• Scale up
• 十万级VM，EIP管理
• 多AZ扩展
可扩展性
灵活性
• 云产品之间互联
• 用户多样访问场景
• 尽量与传统网络无差异

实现方式

使用技术

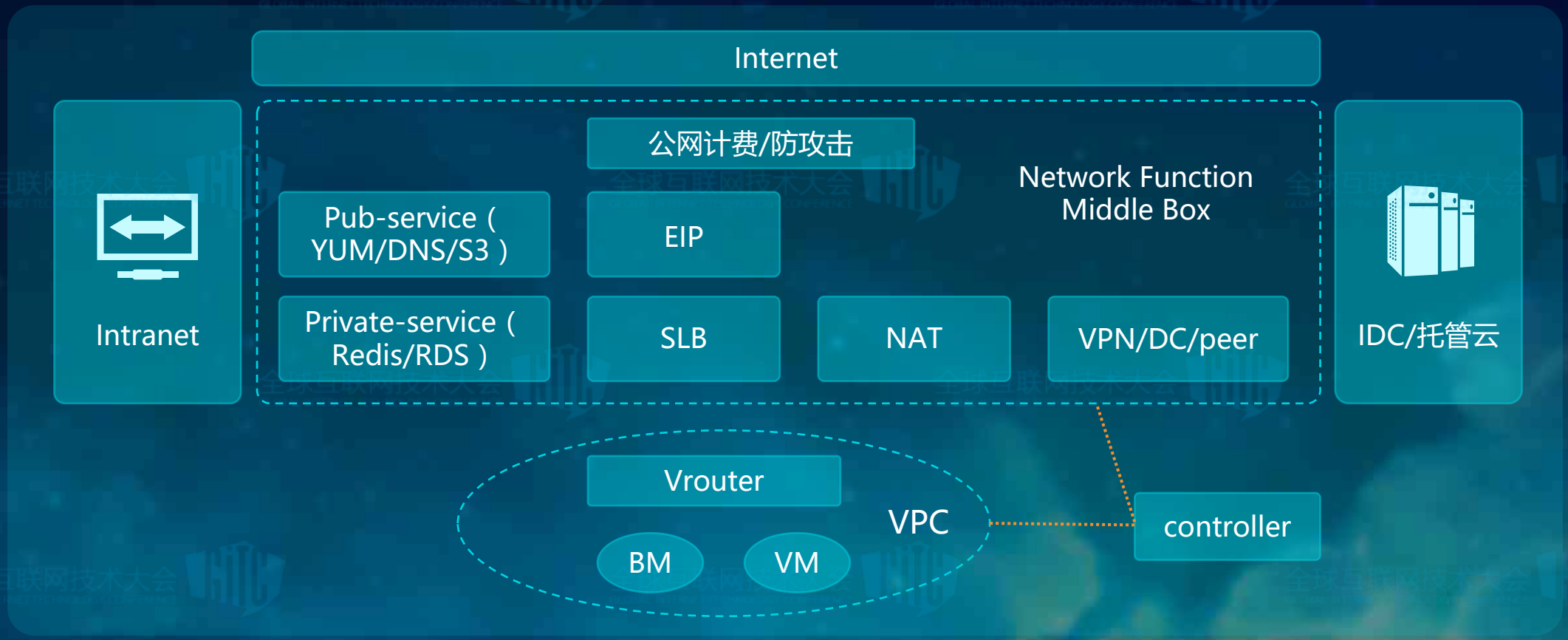
- Vxlan
- DPDK
- Kernel Vrouter
- 10G/25G/40G/100G
- Smart NIC
- EVPN

具体实现

- 以VPC为核心
- Network Function Middle Box 实现Service Chain
- Controller实现配置管理，流量路径控制
- SDN + NF

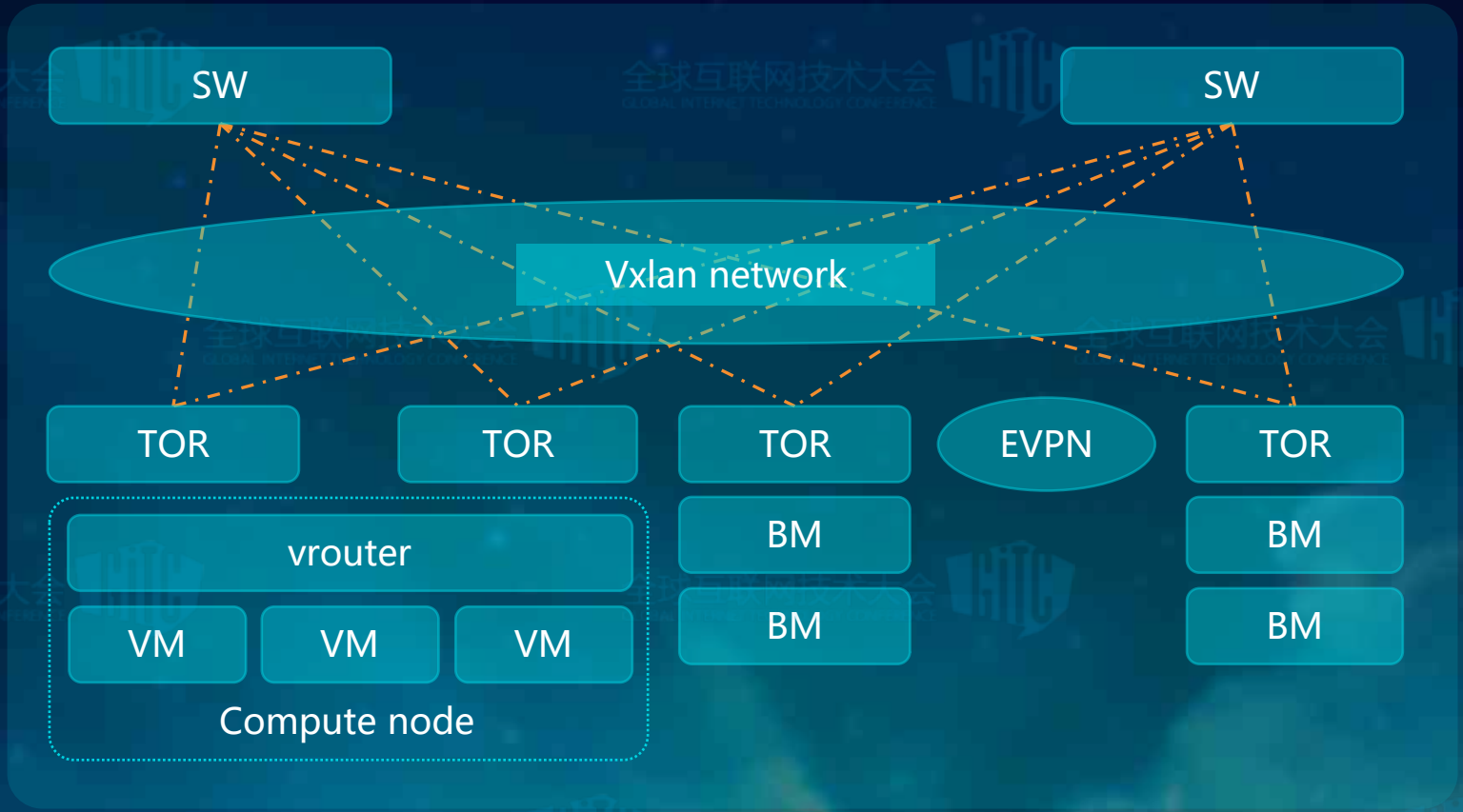
实现方式

- **Vrouter+NFMB+Controller**



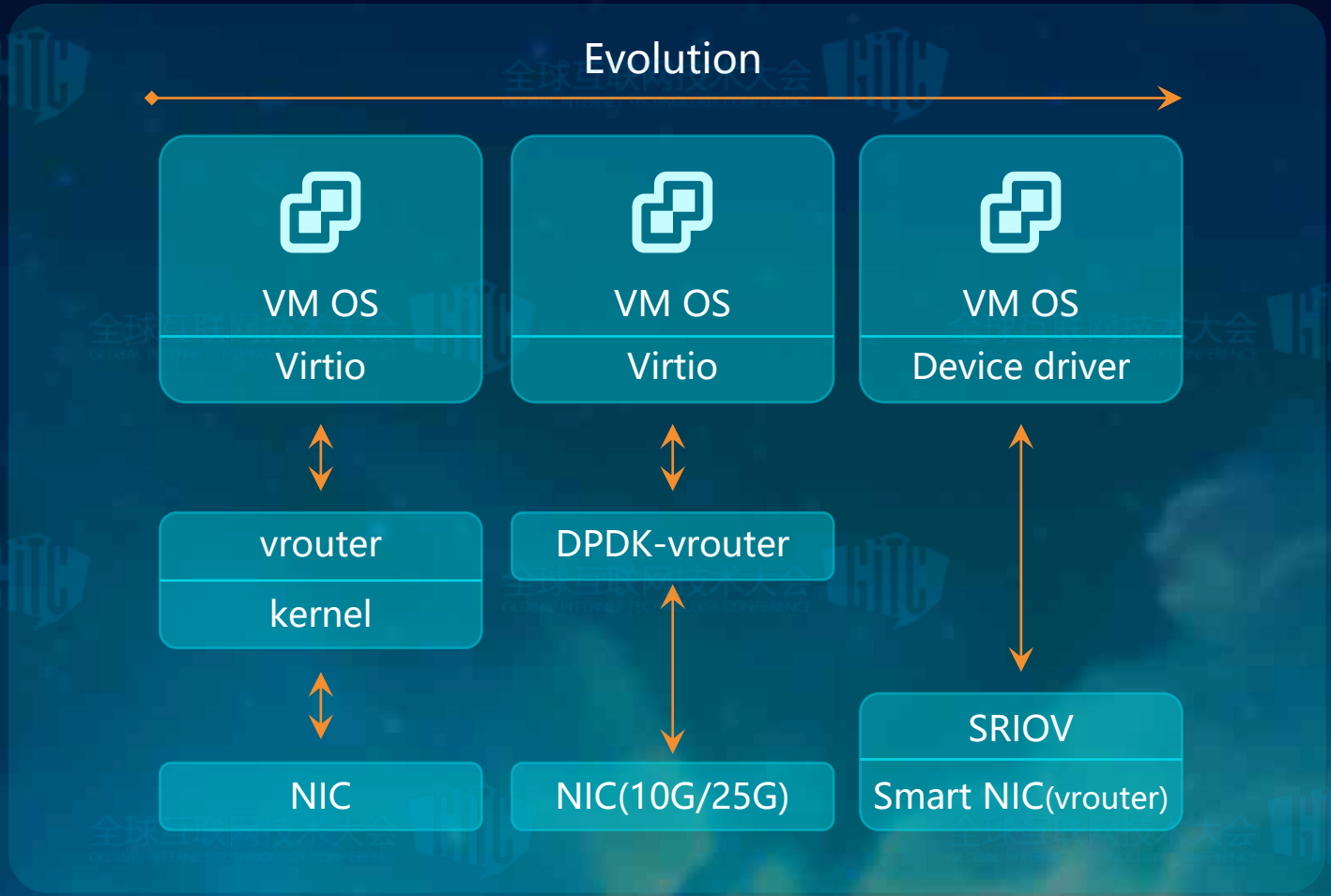
Vrouter

- **VM**
  - Vrouter on CN
- **BM**
  - Vrouter on TOR
  - EVPN



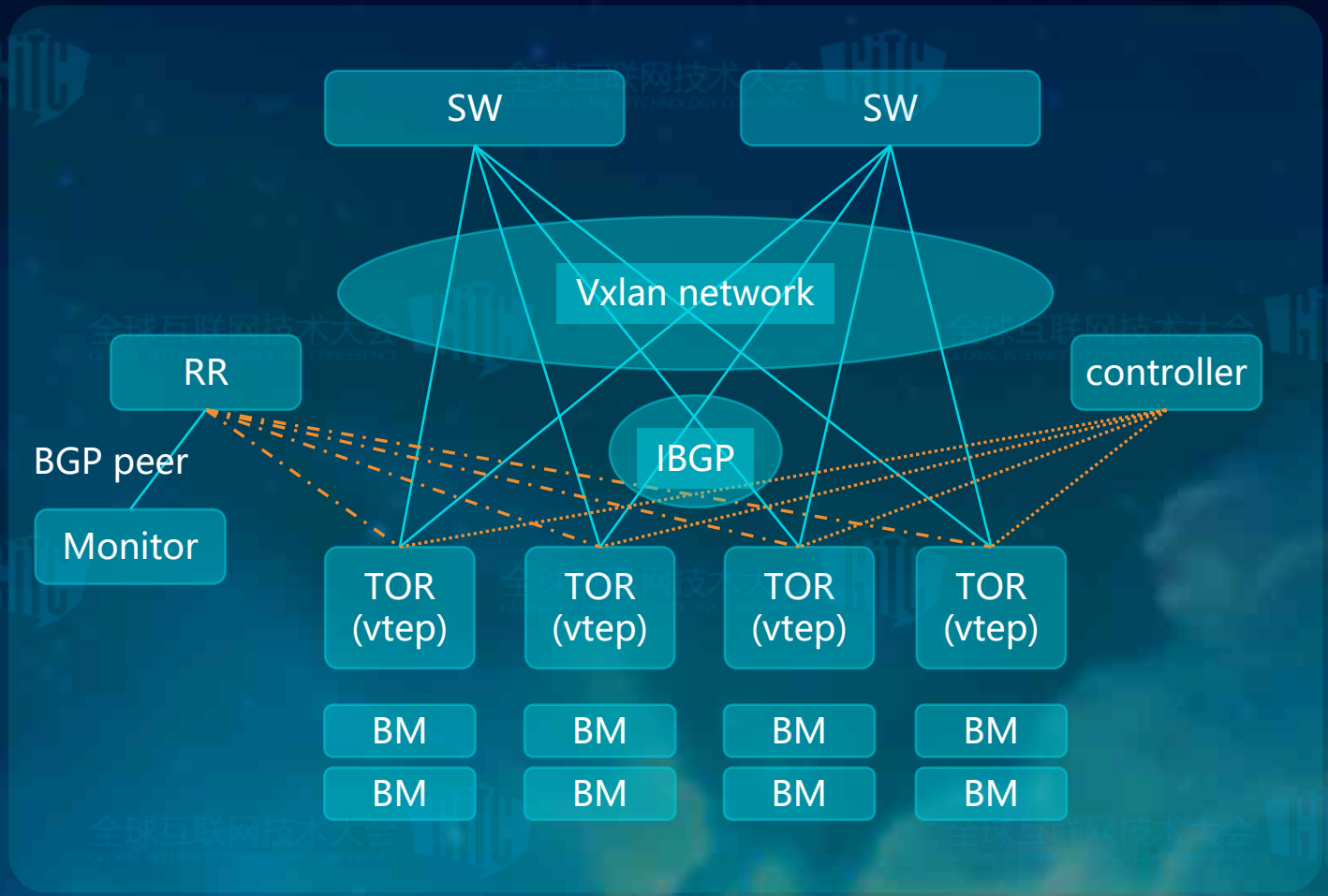
Vrouter

- **VM**
  - Distributed Vrouter
  - Vxlan Stateless Offload
  - Kernel + DPDK version
  - 10G->25G
  - NIC->Smart NIC



Vrouter

- **BM**
  - EVPN
  - MPBGP monitor
  - 支持LB/EIP/NAT等网络产品
  - 由controller配置管理

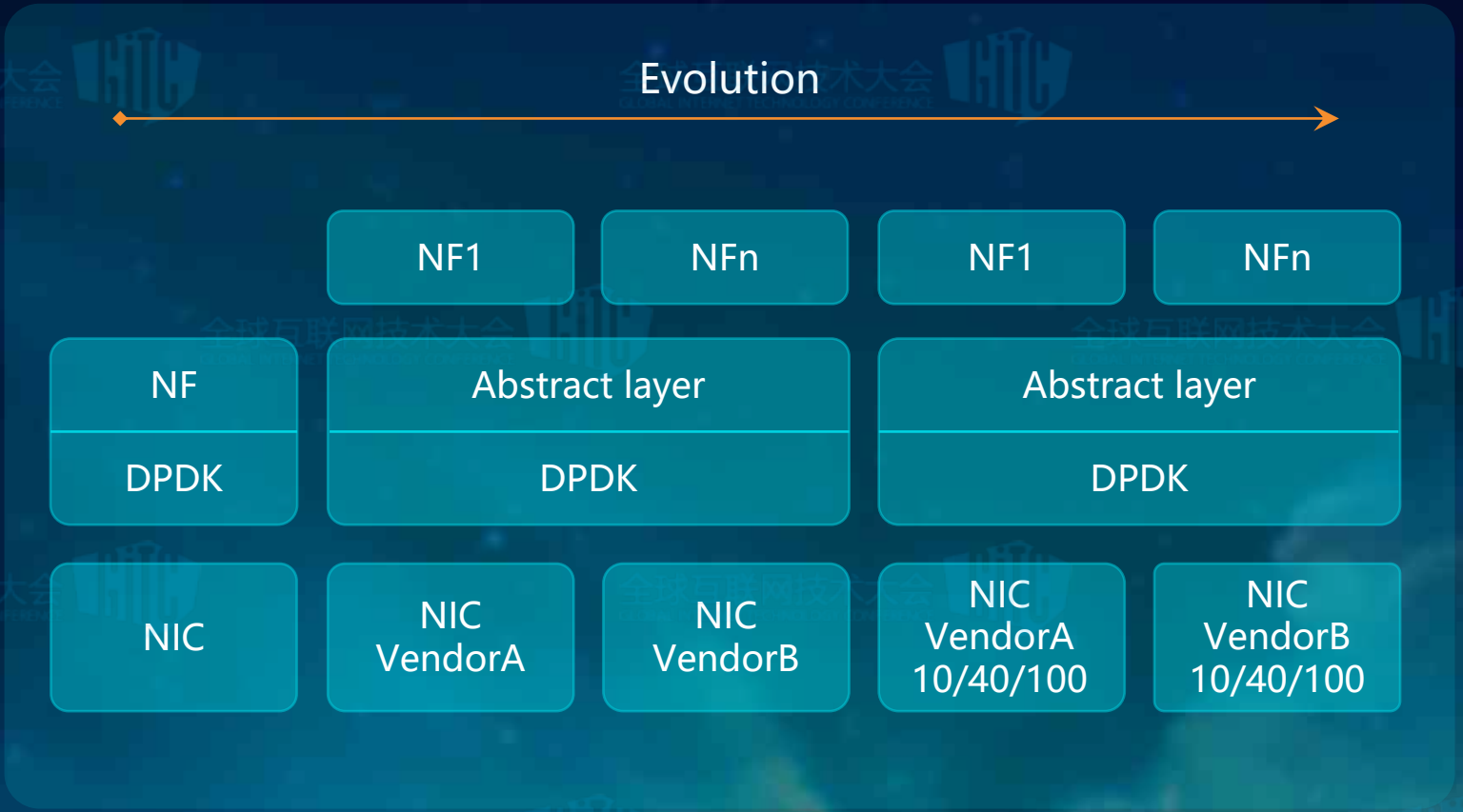


mpbgp

netconf

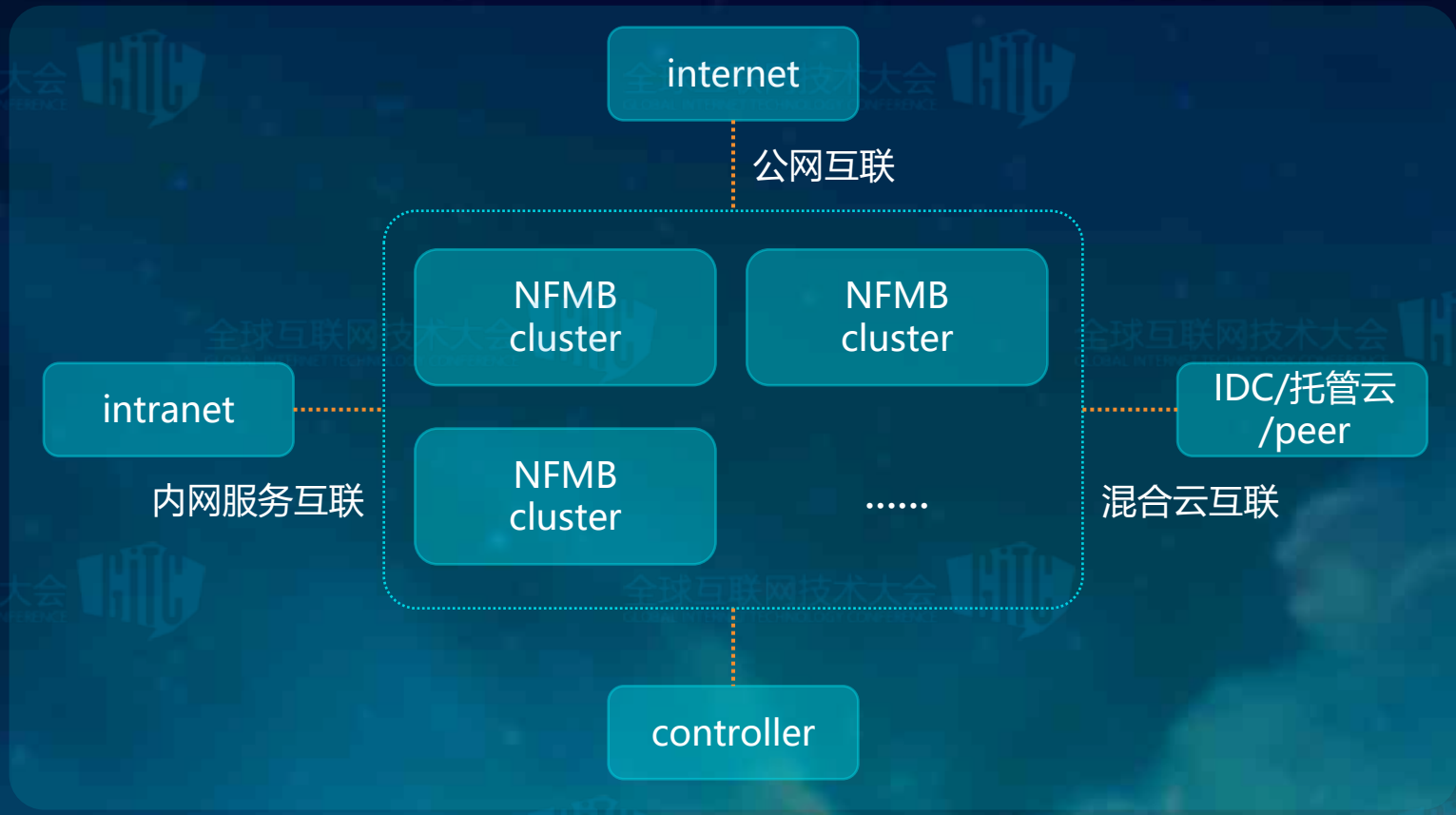
NFMB

- **NFMB**
  - X86 platform
  - Base on DPDK
  - 故障隔离
  - Service chain
  - 10G/40G/100G
  - 集群部署，水平扩展（受限ECMP）



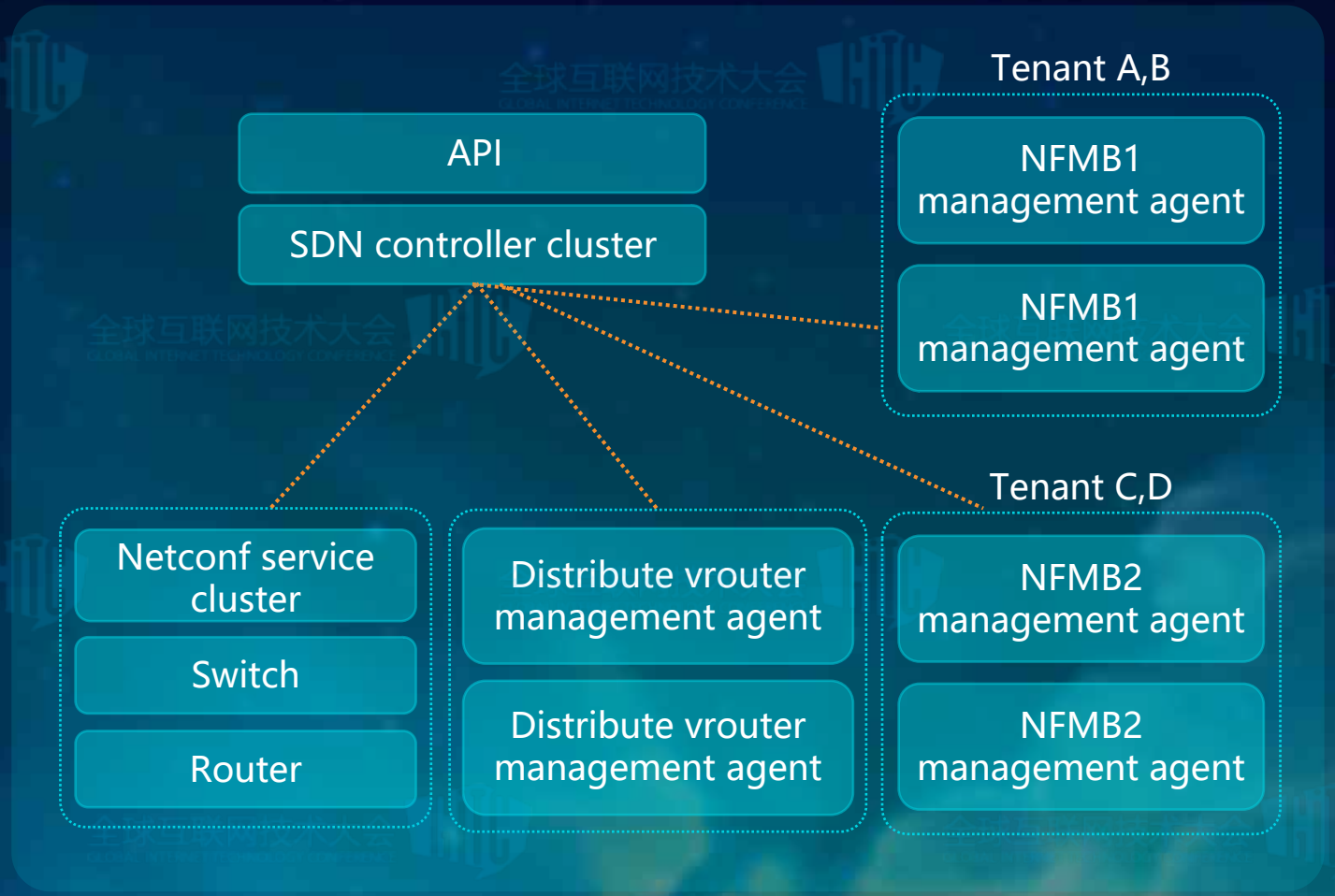
NFMB

- **NFMB**
  - VPC与内网服务（YUM/S3/RDS...）
  - VPC与IDC/其他VPC
  - VPC与Internet



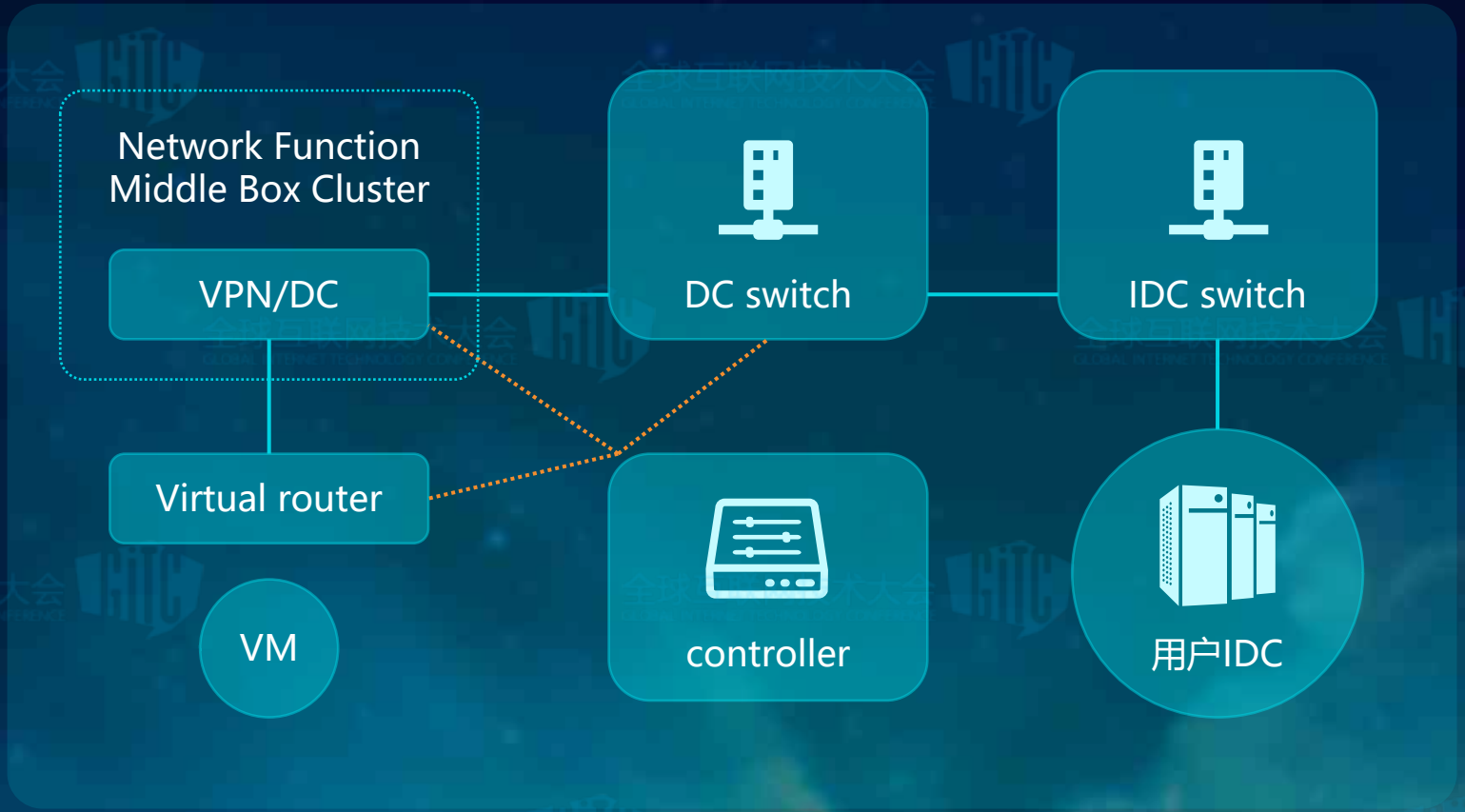
Controller

- **Controller**
  - 管理万级别CN节点，千万级别配置条目
  - 处理10K+cps api请求
  - 网络设备（交换机，路由器）管理
  - 定义用户流量路径
  - NFMB分集群管理，使NFMB具有集群扩展能力



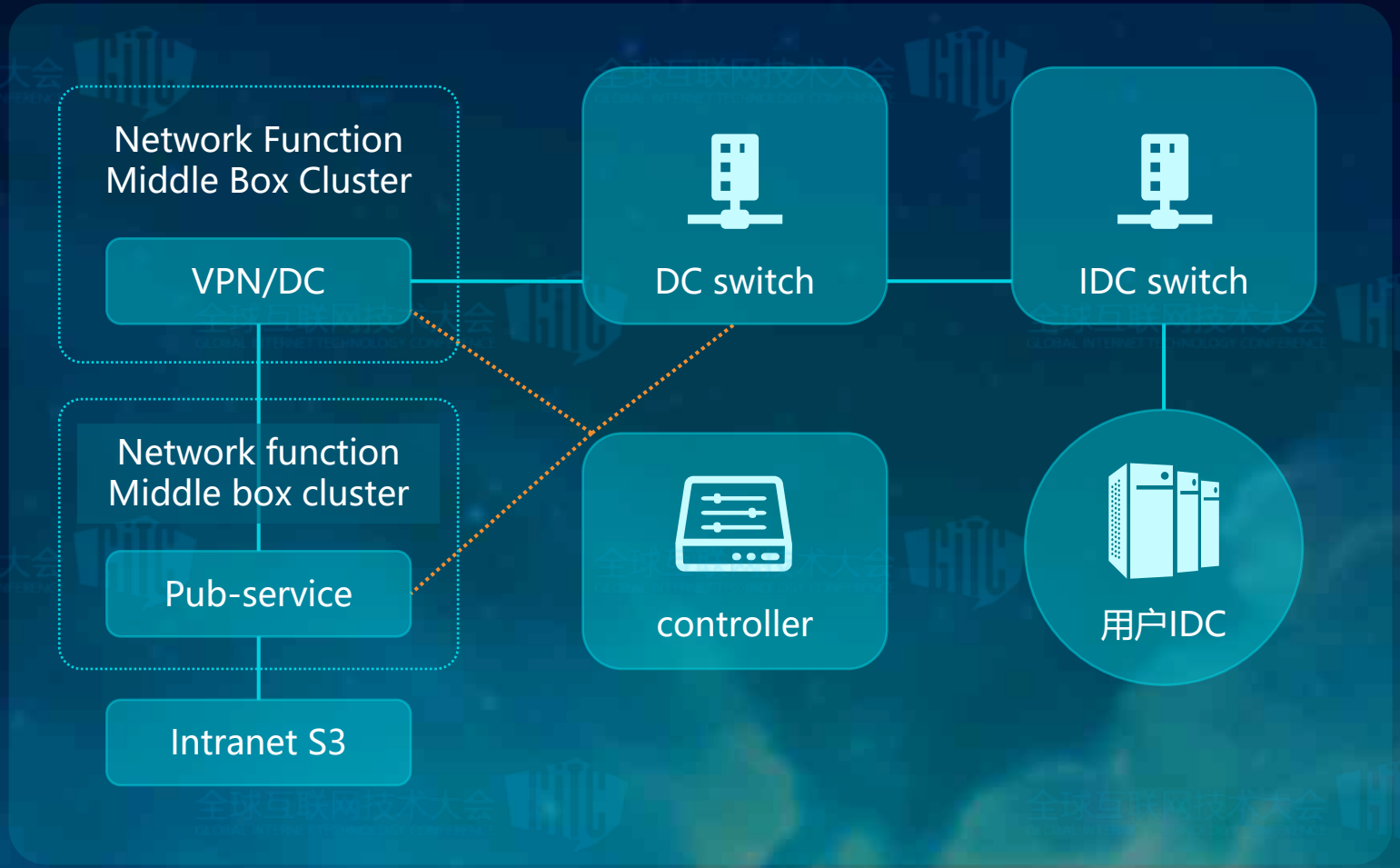
Controller

- **场景1**
  - 用户vpc与自建IDC专线互联



Controller

- **场景2**
  - 用户VPC与自建IDC专线互联，通过专线访问S3



THANKS