

银行云平台 异构SDN网络管理实现

SDN对于金融云计算平台的意义

网络架构是机构开展金融云基础平台建设最为核心关键的因素，其主要体现如下方面;

- 双模IT中网络是唯一必须兼容两种IT模式的平滑互通的基础资源
 - ✓ 为兼顾新技术、新架构、新模式于既有的传统信息技术体系结合，双模IT将是金融机构IT发展的主要形态
 - ✓ 处于两种IT模式下的金融应用无必须共享服务器和存储的要求，但必须在网络层面实现互联互通。
- 金融合规性与安全性在IT基础设施中主要体现在数据中心网络
 - ✓ 多区域隔离
 - ✓ 应用间的强访问控制
 - ✓ 外部防护攻击均
- 以软件定义网络为代表的新技术应用是云平台发展的必然趋势
 - ✓ 基于云计算、大数据与区块链等新技术的金融创新应用产生了新的数据网络交换模型
 - ✓ 软件定义网络技术效果与之契合金融数据中心网络的强自动化与合规性的行业要求尤为契合

SDN在金融云计算平台上的挑战

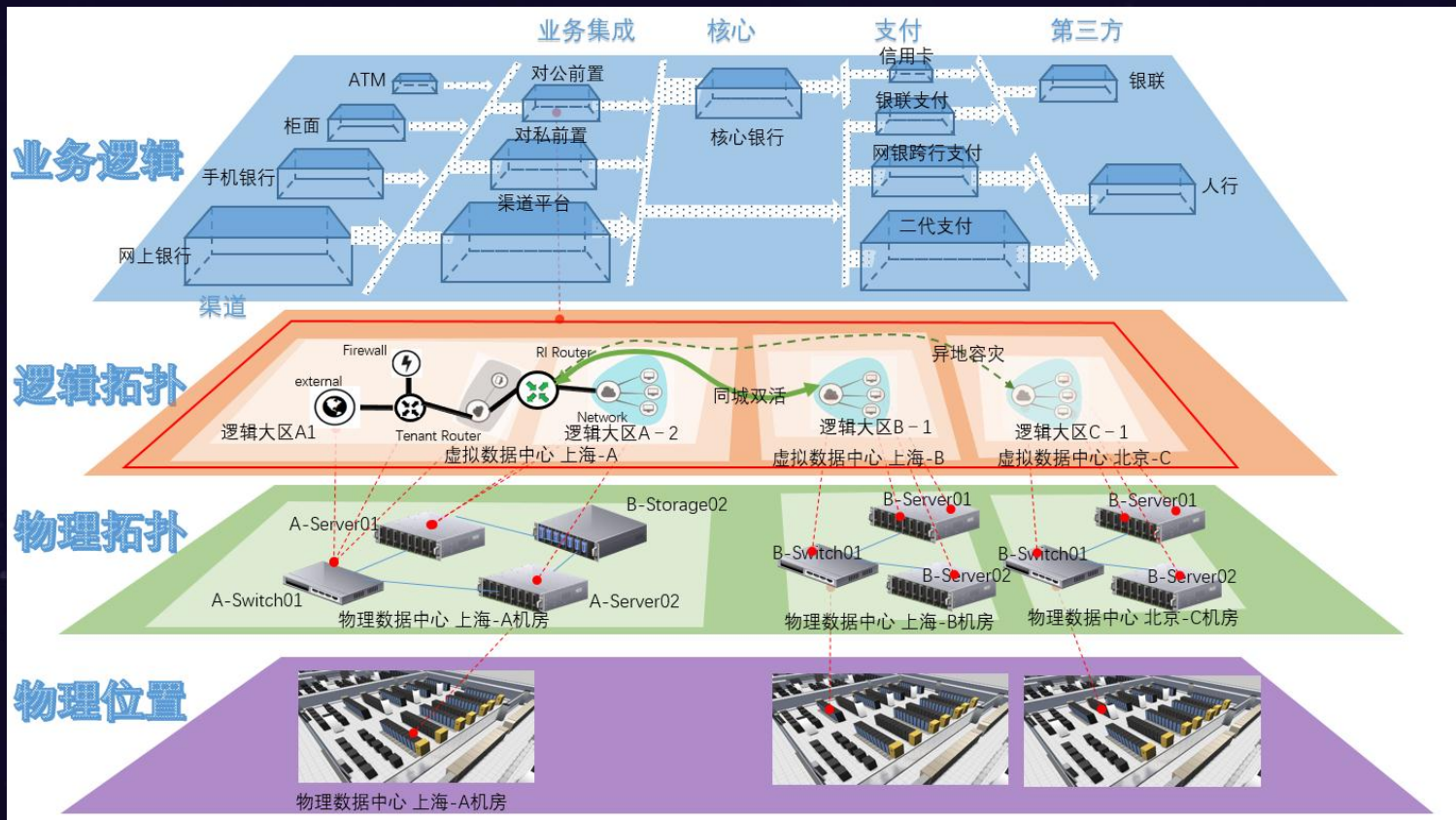
- 业务应用变革式创新发展的业务挑战
 - ✓ 面向互联网方式的金融创新应用
 - ✓ 网络资源的开通从周为单位提升到分钟级别，支撑应用快速投产。
- 以云计算为代表的新技术应用的技术挑战
 - ✓ 资源的漂移迁移能力
 - ✓ 云的多租户特性要求在共享的物理网络设备下提供可独立解耦的网络地址路由空间
 - ✓ 云弹性伸缩则要求网络有更高地弹性扩展能力
 - ✓ 巨大的云平台规模，也要求云网络服务也必须具备足够的网络容量与健壮性。
- 金融IT成本与效率优化新要求的成本挑战
 - ✓ 新常态下金融机构的运营压力要求IT架构可实现更高效与低成本
 - ✓ 从纯商业“产品”解决方案向“自主”网络方案演进
 - ✓ 金融数据中心网络技术应用更趋于开放
 - ✓ 要求网络运维人员从单纯的人工维护解放出来，进入高效的自动化方式。

SDN在金融云计算平台上的设计目标

未来金融数据中心网络应用的“五高”要求：

- ✓ 高敏捷：实现业务快速上线，面对应用的变化达到资源的按需变更，通过新技术应用打破因重安全而舍效率的困局，在云计算新环境下安全与高效并重；
- ✓ 高弹性：一是内部弹性强化，打破竖井式架构中网络区域成为限制资源共享的壁垒，实现网络资源池整合与灵活共享与隔离，二是外部弹性兼容，支持新老架构并存，从而使原有网络可以平滑过渡到新架构；
- ✓ 高可管理：一是实现管理的体系的简化，支持多品牌的融合管理，二是实现管理自动化与智能化，使日常运维从大量人工维护的高工作量解放出来；
- ✓ 高可用：网络架构持续稳定影响金融数据中心全局服务能力，网络架构需要基于稳定可靠的技术构建，使网络服务具备7*24小时业务连续性服务的能力；
- ✓ 高性能：面对秒杀等新业务场景等的极限服务能力，实现时延和带宽等关键指标的跨越式提升，同时注重资源的高效利用，用尽可能少的资源实现最大的性能服务。

金融机构从业务到基础架构透视图



SDN在金融云计算平台设计模型

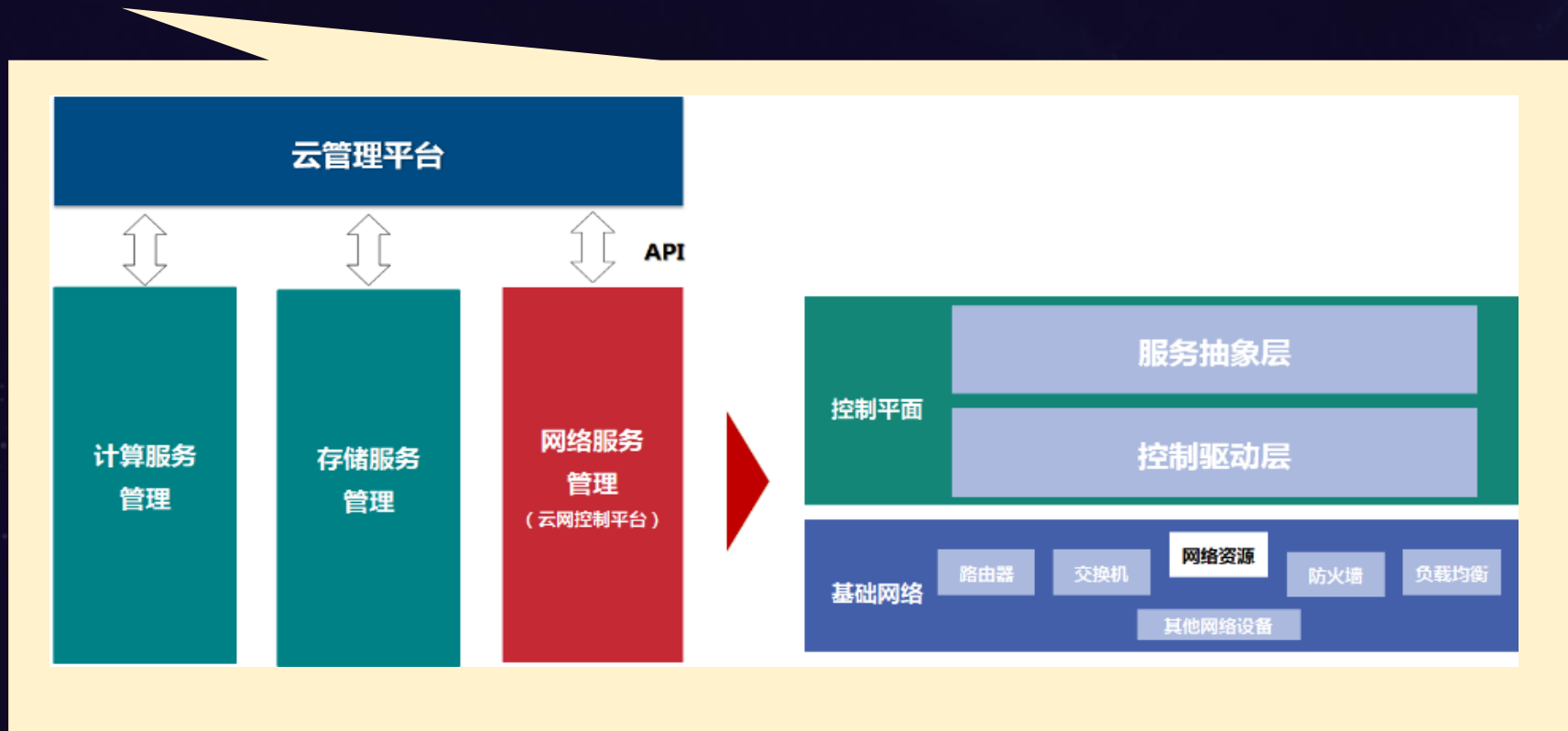
管理控制模型

网络分区模型

分区互联模型

防火墙和负载均衡模型

两地三中心模型



SDN在金融云计算平台设计模型

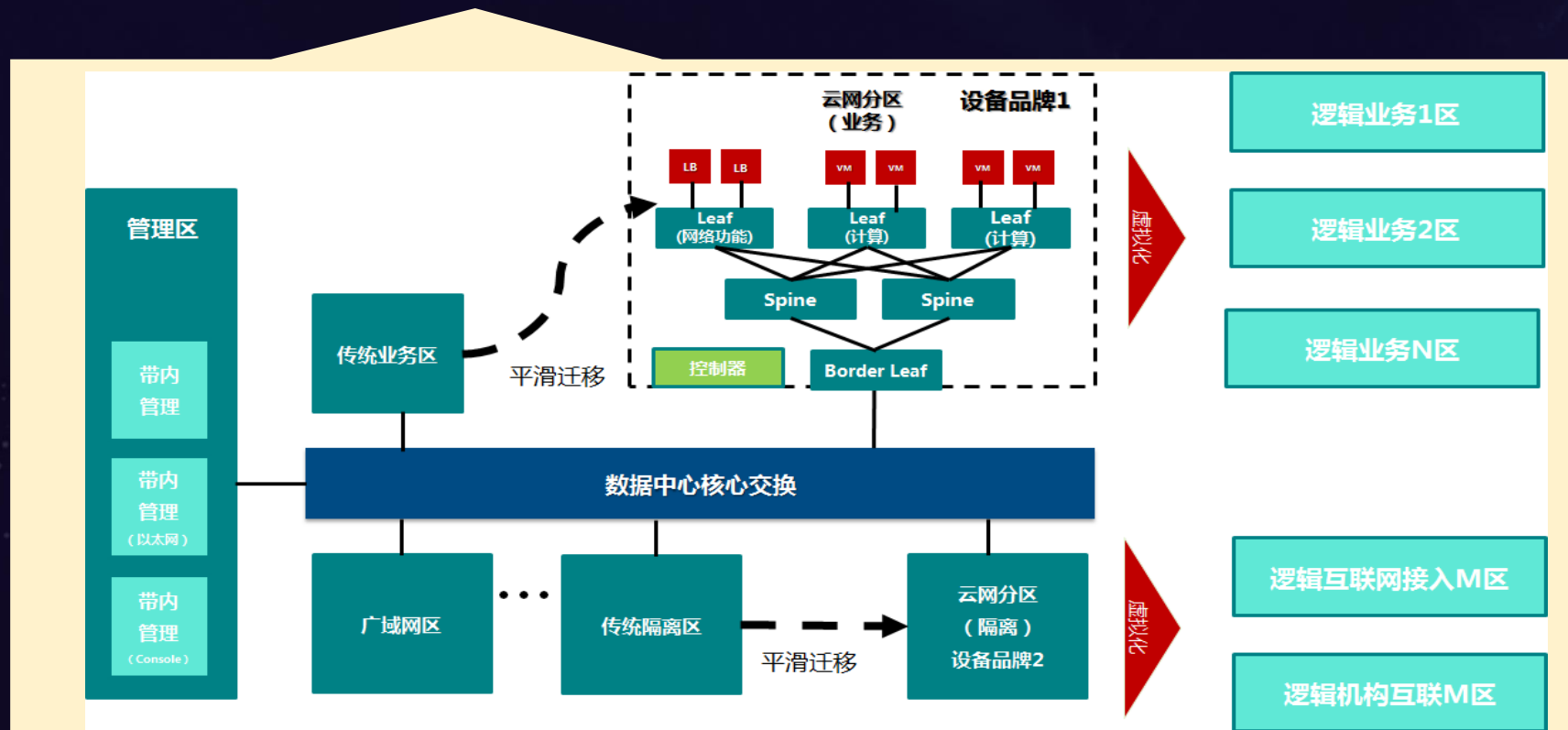
管理控制模型

网络分区模型

分区互联模型

防火墙和负载均衡模型

两地三中心模型



SDN在金融云计算平台设计模型

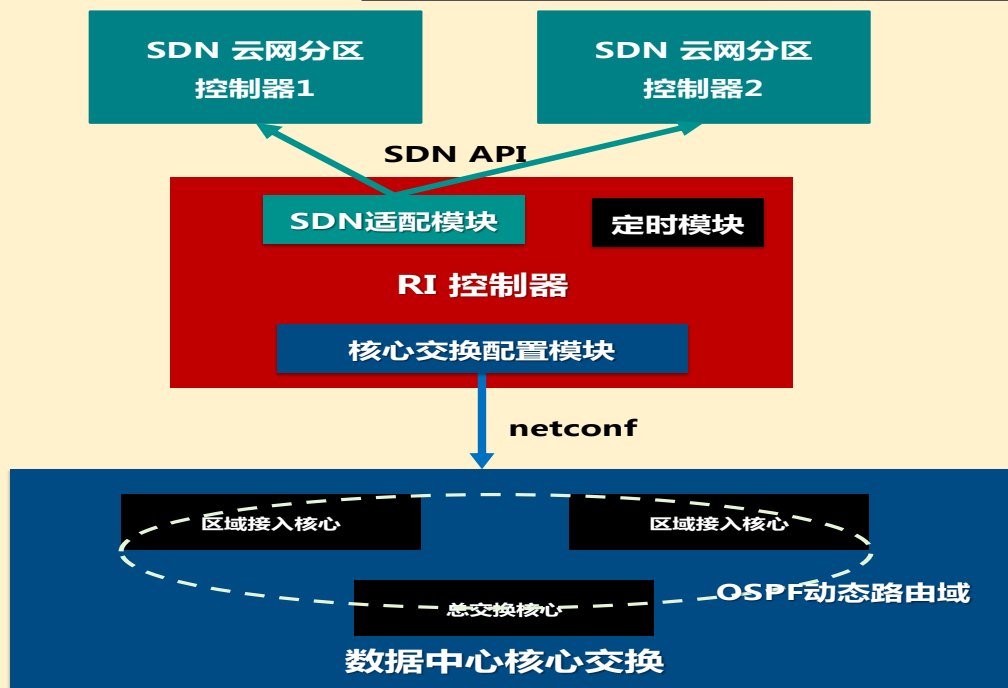
管理控制模型

网络分区模型

分区互联模型

防火墙和负载均衡模型

两地三中心模型



SDN在金融云计算平台设计模型

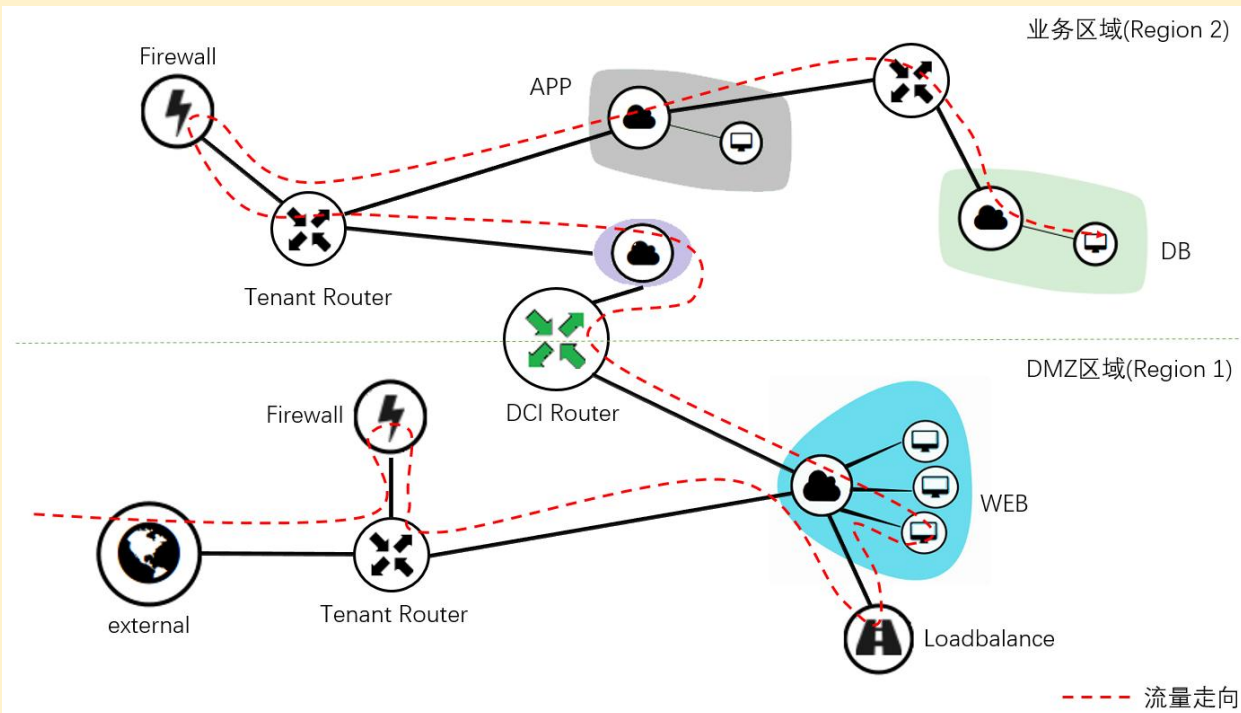
管理控制模型

网络分区模型

分区互联模型

防火墙和负载均衡模型

两地三中心模型



SDN在金融云计算平台设计模型

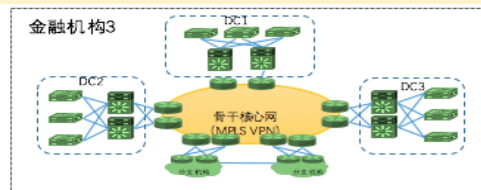
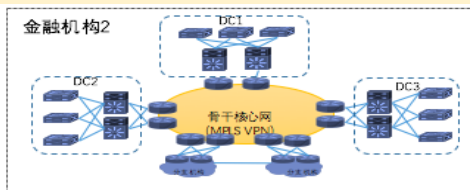
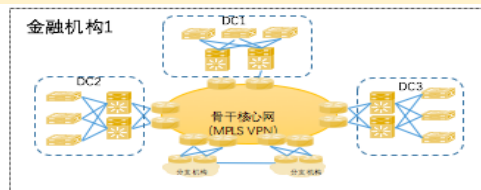
管理控制模型

网络分区模型

分区互联模型

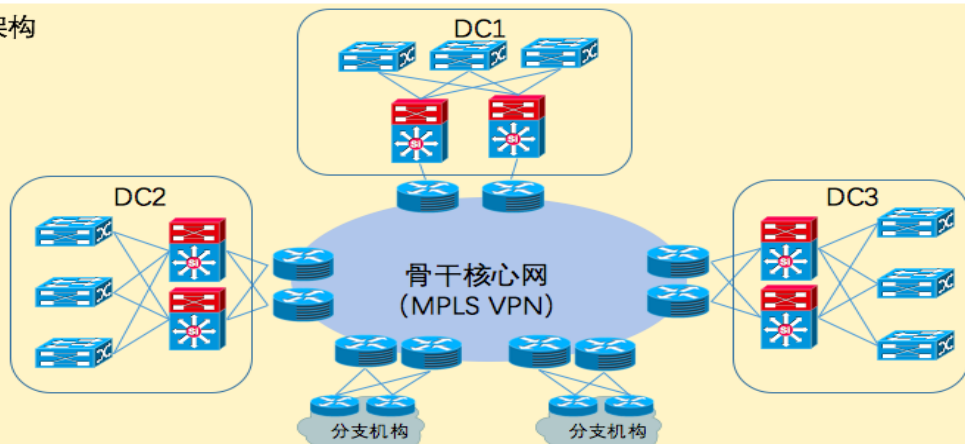
防火墙和负载均衡模型

两地三中心模型

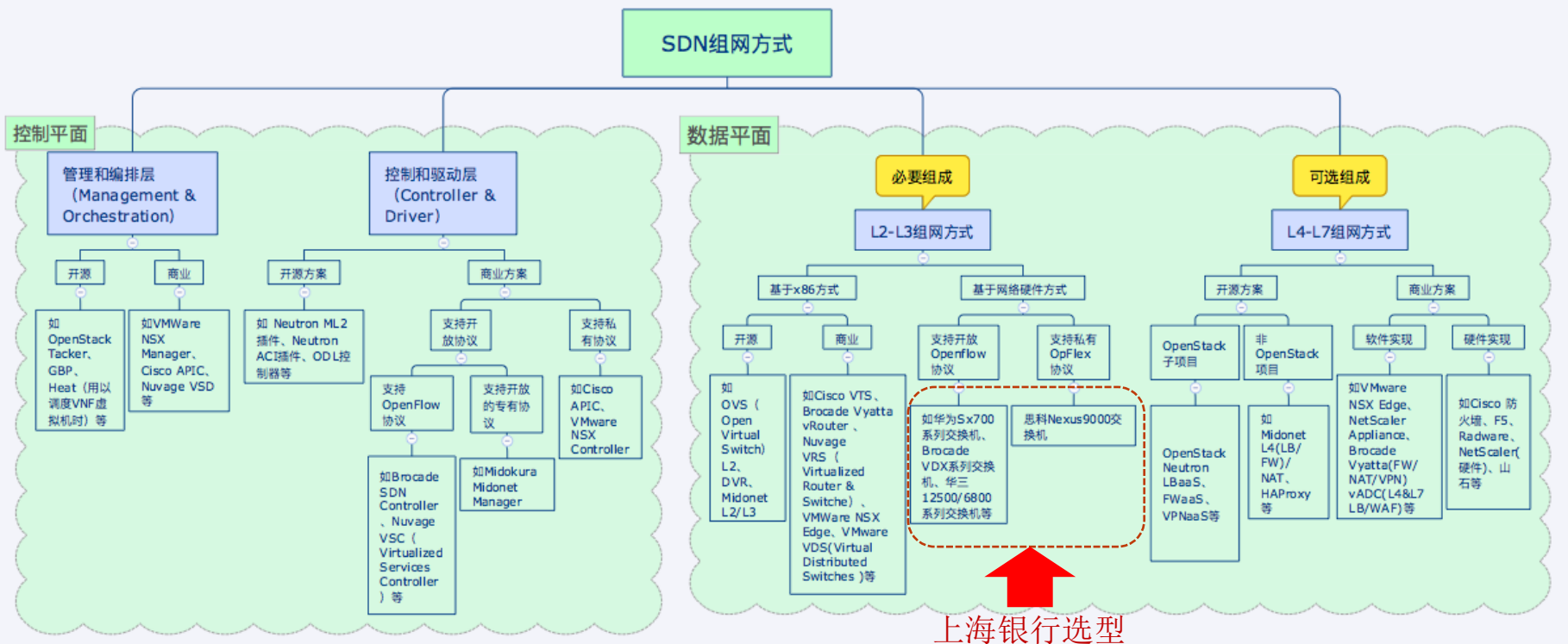


虚拟化

物理架构

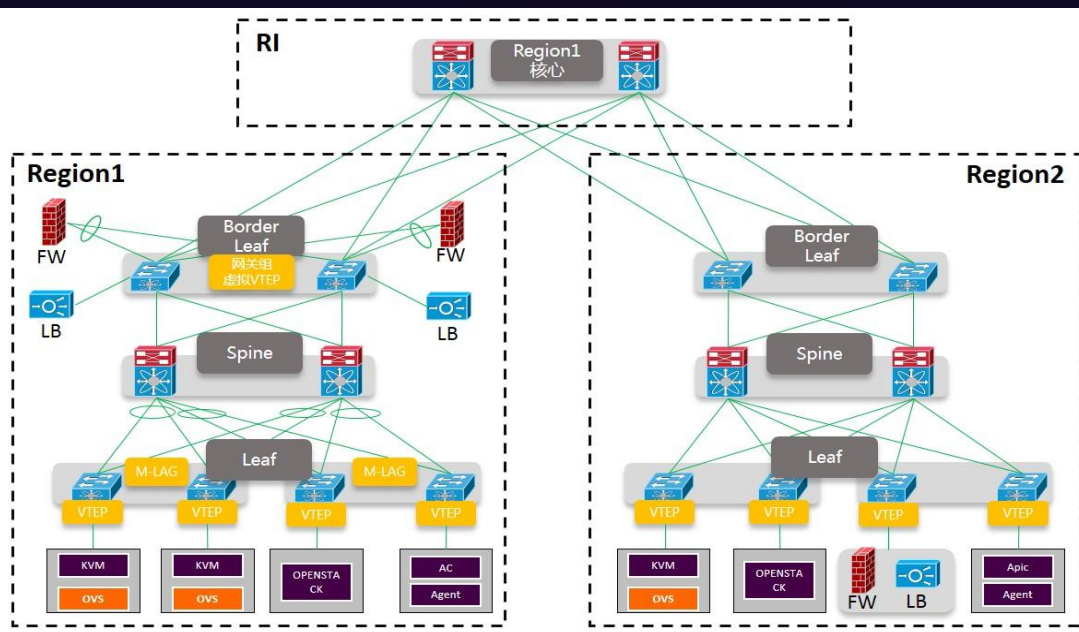


SDN的选型



上海银行面临的问题

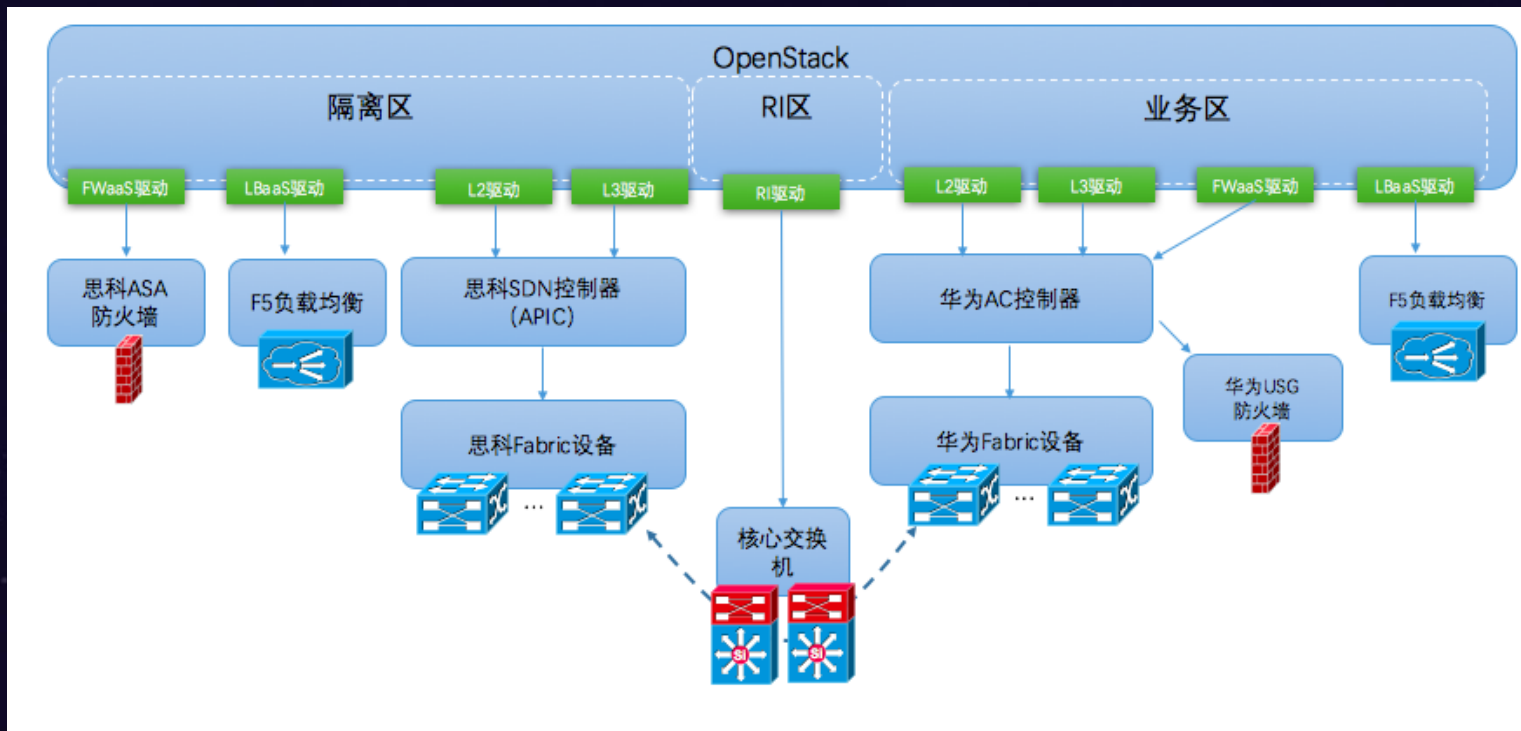
- 如何通过统一控制器实现异构SDN 控制器（华为&思科）的统一管理，消除差异实现高效运维
- 如何管理被SDN控制器排斥在外的其他设备（F5）
- 如何实现隔离分区的逻辑统一
- 如何实现一网多租户能力



分类	厂商	设备类型	设备型号及版本
SDN云网分区	思科ACI	控制器	APIC 2.1.3
		Spine	N9K-C9396PX
		Leaf	N9K-C9336PQ
	华为AC	AC	AC 2.0
		Spine	CE6851-48F6Q
		Leaf	CE6850-48P4Q
核心路由设备	华为	三层交换机	CE6850-48P4Q
防火墙	思科	ASA	ASA 5512
	华为	USG	USG6650
负载均衡	F5	BIG IP	BIG-LTM-1600

解决方案

- 如何通过统一控制器实现异构SDN 控制器（华为&思科）的统一管理，消除差异实现高效运维

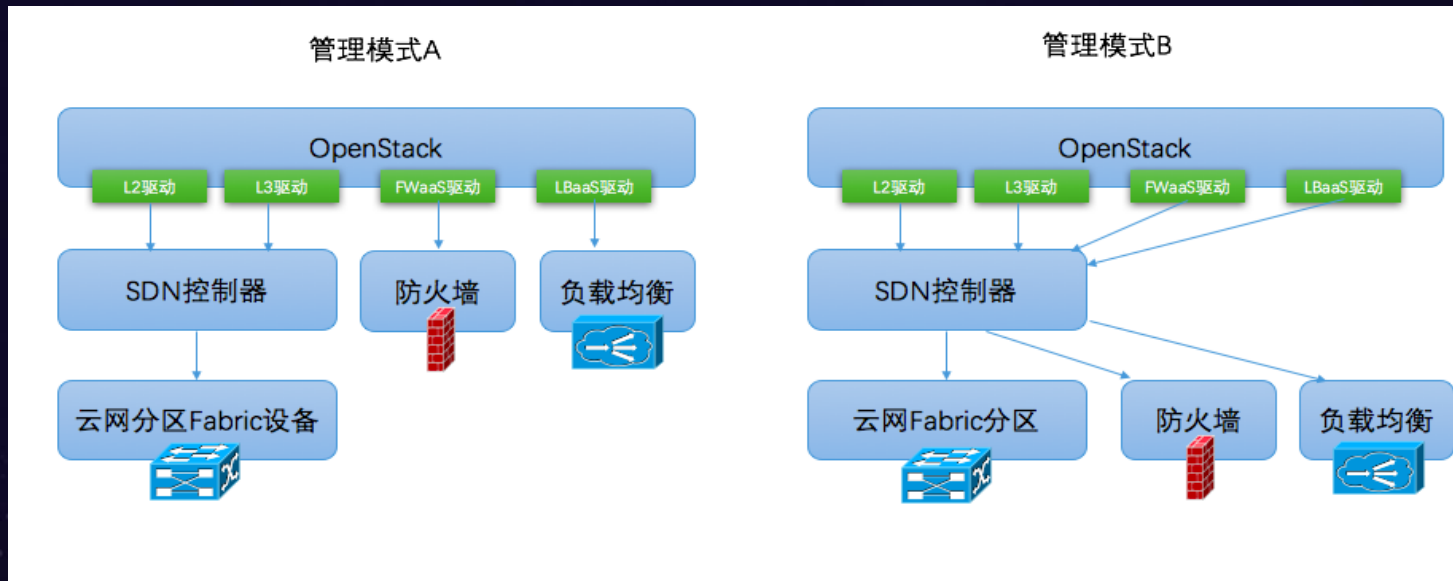


- 如何通过统一控制器实现异构SDN 控制器（华为&思科）的统一管理，消除差异实现高效运维

	思科ACI	华为AC
OpenStack版本		Liberty
SDN控制器版本	APIC2.0	AC2.0
暴露给OpenStack的网络模式	只有一种选项：OpFlex模式	有三种选项：VLAN、VXLAN和GRE
底层网络模式	VLAN、VXLAN和GRE	VLAN、VXLAN和GRE
VLAN/VNI/Tunnel ID 分配方式	通过SDN控制器分配	通过OpenStack分配
控制节点配置	—安装厂商APIC API并激活 —替换原生二层ML2驱动为厂商ML2驱动 —添加厂商L3驱动	—安装厂商AC API并激活 —替换原生二层ML2驱动为厂商ML2驱动 —添加厂商L3驱动
网络节点配置	—安装原生DHCP服务，但DHCP驱动替换成厂商的 —停止原生OVS代理，替换成厂商提供的OVS代理 —安装厂商提供Neutron OpFlex代理 —停止原生L3代理 —停止原生metadata代理	—安装原生DHCP服务，不停止 —安装原生OVS代理，不停止 —无其他厂商定制代理需要安装 —停止原生L3代理 —原生metadata代理不停止
计算节点配置	—安装厂商提供的OVS代理，停止原生OVS代理 —安装厂商提供Neutron OpFlex代理	—安装原生OVS代理 —无其他厂商定制代理需要安装
DHCP驱动	厂商提供	OpenStack原生驱动
DHCP本地代理	实现	未实现
Metadata本地代理	实现	未实现
分布式SNAT	实现	未实现
分布式网关	实现	未实现
策略下发逻辑	计算节点和网络节点上的Neutron OpFlex代理会同步Neutron中的虚拟网络资源，生成Endpoint文件，通知agent-ovs读取，agent-ovs通过OpFlex协议到leaf节点上查询对应EPG的信息，然后通过OPENFLOW协议对OVS完成流表的下发。	复用OpenStack策略下发逻辑

解决方案

- 如何管理被SDN控制器排斥在外的其他设备



	A模式	B模式	
	OpenStack直接驱动	通过思科SDN控制器（APIC）进行管理	通过华为SDN控制器（AC）进行管理
思科ASA防火墙	×	×	×
华为USG防火墙	×	×	√
F5负载均衡	√	×	×

- 如何管理被SDN控制器排斥在外的其他设备

#	OpenStack 抽象资源	F5对应资源	备注
1	Loadbalancer	Partition Router domain Vlan Snat pool Selfip	Partition和router domain用来进行资源的隔离
2	Listener	Virtual server Profile	
3	Pool	Pool	F5 创建Pool时会更新virtual server的session-persistence, 将pool挂载到virtual server上
4	Member	Node	F5生成node时会更新pool中的member
5	Health monitor	Health monitor	F5中对应生成health monitor时会更新pool中的health monitor

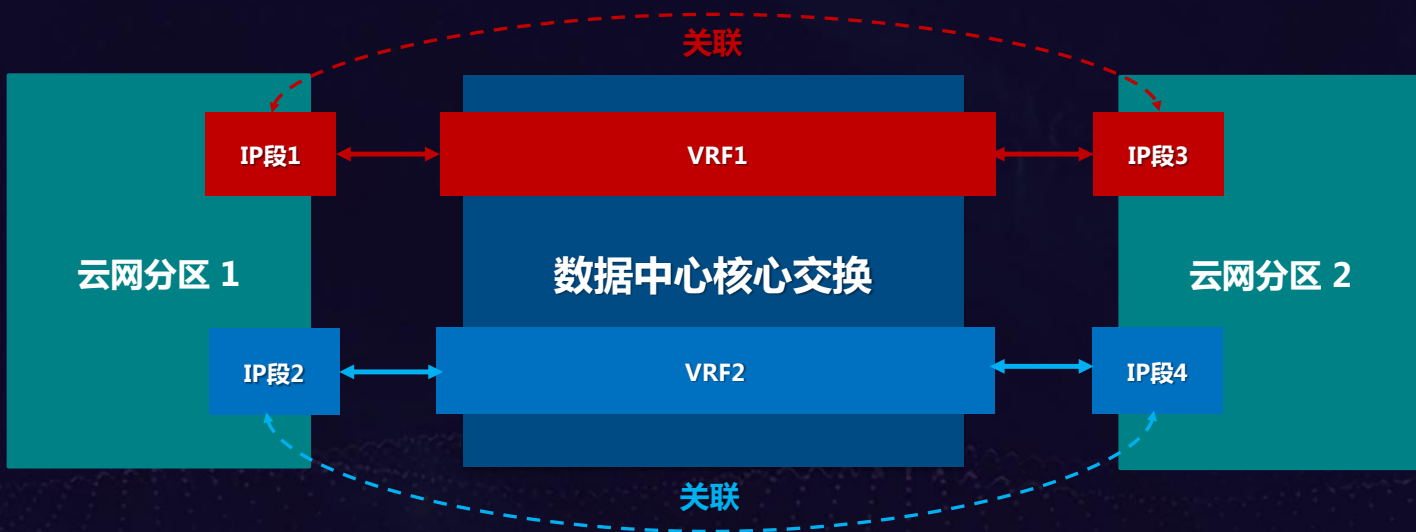
通过OpenStack LBaaS驱动F5

#	OpenStack 抽象资源	思科ASA防火墙对应资源	备注
1	Firewall	Security context	OpenStack中firewall的创建在ASA中对应生成security context, 同时生成internal和external的三层子接口并加入security context来做租户隔离。
2	Policy	Access list	
3	Rule	Access entry	

开发ASA驱动, 通过OpenStack FWaaS驱动思科防火墙

解决方案

- 如何实现隔离分区的逻辑统一和互通

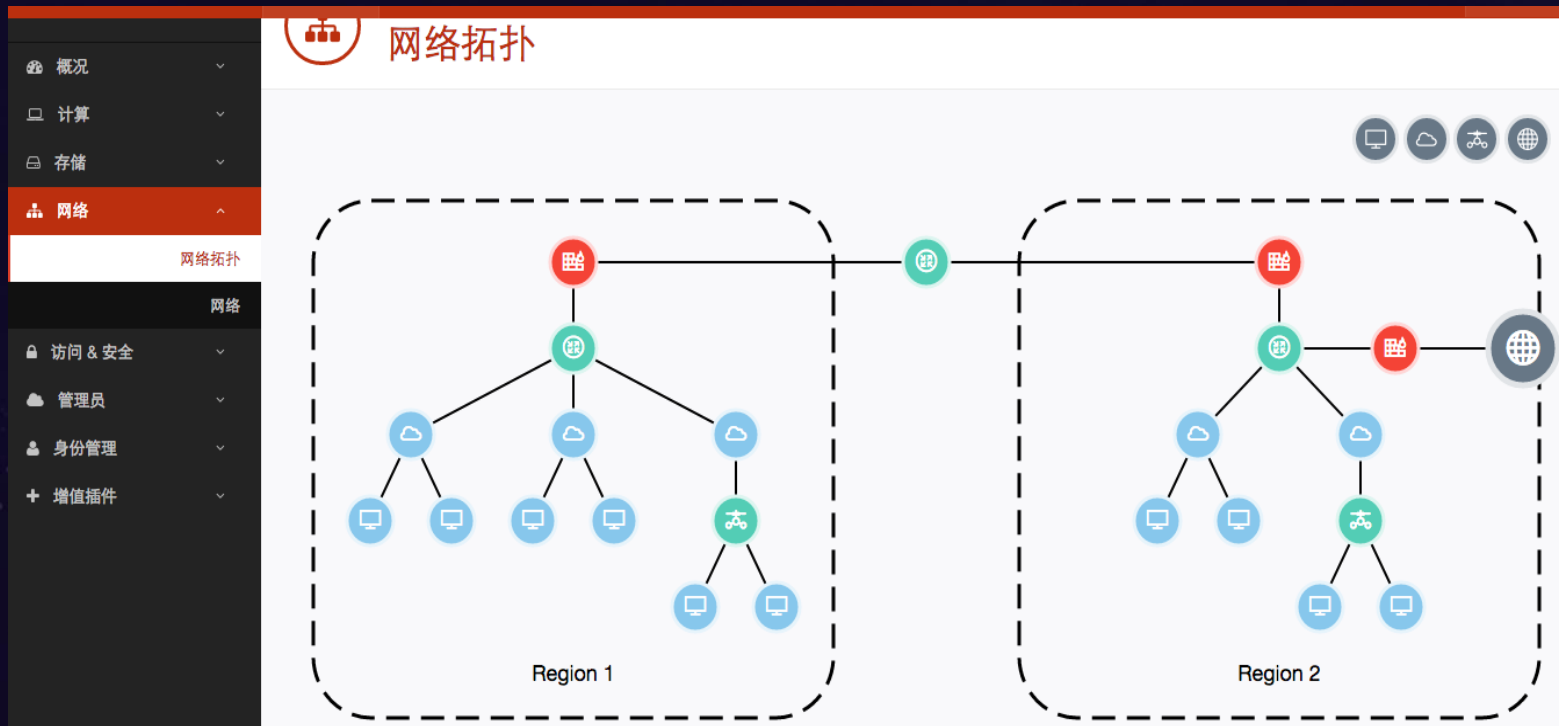


自主研发的区域互联（Region Interconnect）SDN控制器：

- 1) 根据租户变动情况动态创建配置VRF及其相关配置
- 2) 实现在不同SDN 云网分区资源动态变化情况下，路由地址动态发布，以便保持动态变换的网络资源的连通性

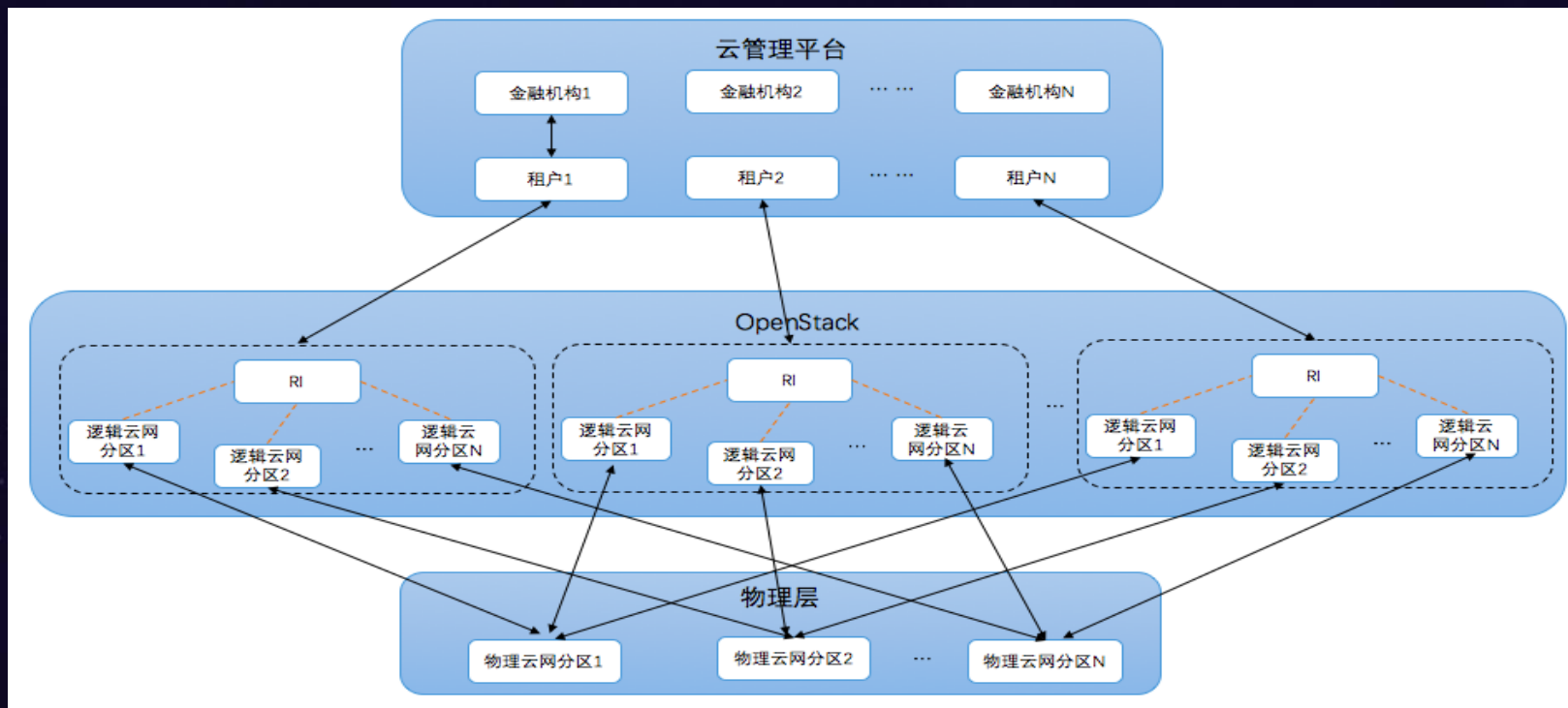
解决方案

- 如何实现隔离分区的逻辑统一和互通



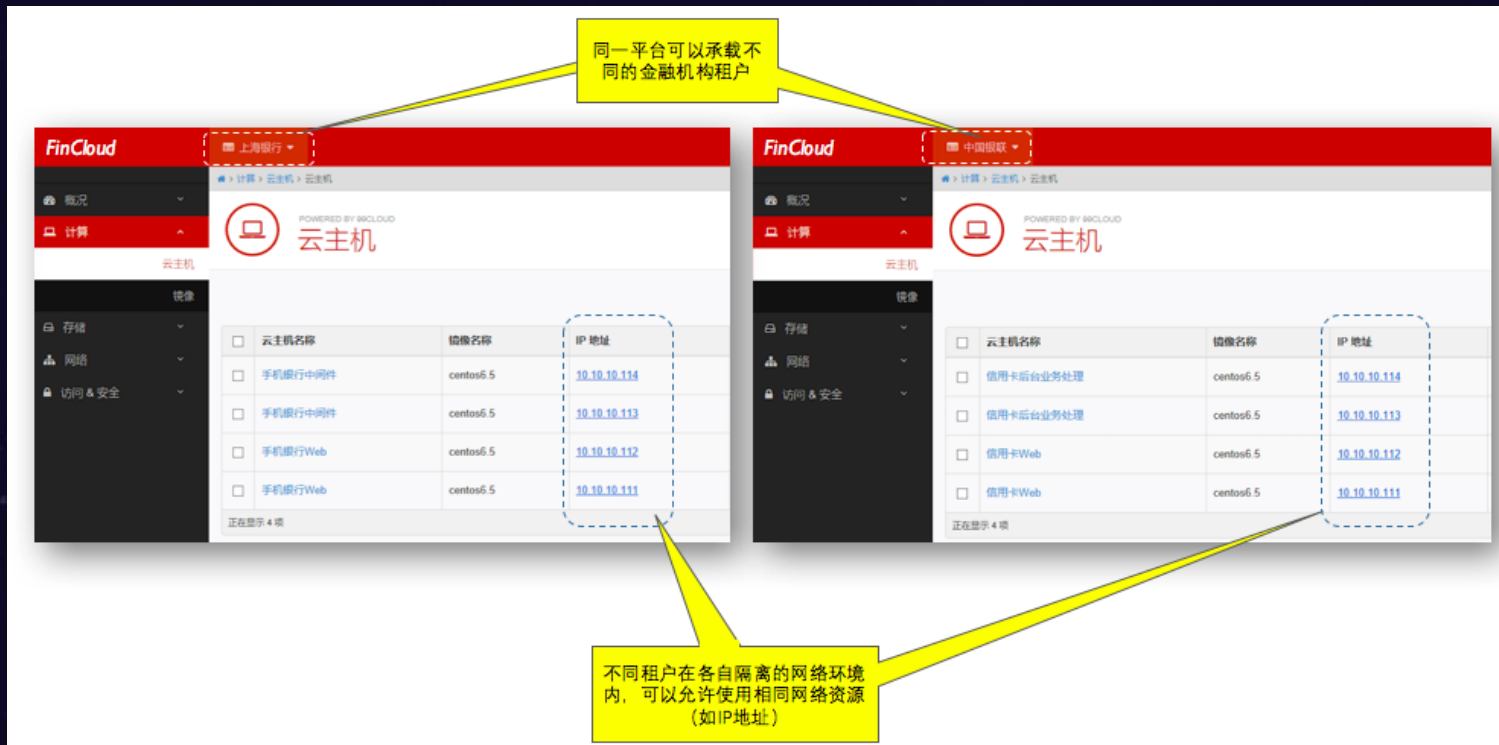
解决方案

- 如何实现一网多租户能力



解决方案

- 如何实现一网多租户能力



待优化问题

- 三层模型双出口
- 暴露更多防火墙能力，如支持IP范围的定义、ALG功能、动态开放端口等
- 负载均衡模型，丰富Listener支持类型、支持会话保持方法较少、支持负载均衡算法较少、支持健康检查方法较少
- 增加对IPS、DDOS网络安全、链路负载均衡等管理

欢迎到九州云索取《金融云技术白皮书》（118页）



源 于 开 源 · 高 于 开 源

北京 | 上海 | 广州 | 重庆 | 福州 | 无锡 | 宁波 | 湖州