深证云 IPv6 改造网络技术方案分享

（深圳证券交易所供稿）

一、IPv6 改造背景

深圳证券通信有限公司金融云平台平台自 2013 年发布以来，陆续推出行情、灾备、数据存管等多种行业 SaaS 服务以及向行业金融机构提供 IaaS 服务，服务对象包括行业协会、证券交易所、区域股权交易中心等市场核心机构，证券、基金、期货、销售机构、银行、保险等金融机构，以及上市和拟上市企业。为了助力行业机构的技术系统向 IPv6 迁移，近年来，深证通开展了深证云的 IPv6 的改造工作，主要建设云平台以下 IPv6 技术能力：

1、云平台自身支持 IPv6 访问：包括云平台官网、运维界面、租户界面，均应支持 IPv6，以满足租户的双栈访问需求；

2、云上产品支持 IPv6：比如云上虚拟机、云负载均衡、云 NAT 网关等关键网络组件，需要以 IPv4/ IPv6 双栈访问；

3、云上业务场景支持 IPv6：比如云上虚拟机之间互访、云上组网等场景，需要支持 IPv4/ IPv6 双栈，以满足租户业务的 IPv6 合规需求；

4、云上基于 IPv6 的安全防护：引入 IPv6 后，意味着云内将同时存在 IPv4 和 IPv6 两种流量，所以云上的安全产品要求具备对 IPv4 和 IPv6 流量相同的防护能力；

5、运维管理：行业云引入IPv6能力后，必将对运维带来新的挑战,云平台需要提供IPv6/IPv4一致的运维能力。

6、其他考虑：由于IPv6的报文长度比IPv4更长，对行业云上的各类设备的性能也提出了要求，在方案建设时，需要综合考虑性能与容量问题。

二、技术选型与建设目标

目前，业界的IPv6改造方案主要分为三类：

1、NAT64地址转换：利用网关设备（如路由器、负载均衡器或防火墙）进行IPv4到IPv6的地址转换，将网络划分成为两个域：面向公众提供服务的IPv4/IPv6双栈环境，面向内部服务的纯IPv4环境，在网络边界处进行NAT64地址转换。

2、隧道穿越：在访问者的源端和目的端构建“IPv6 in IPv4”隧道,以实现在纯IPv4环境内完成IPv6协议的互访，需要在客户端和服务端配置隧道穿越策略。

3、IPv4/IPv6双栈：该方案旨在利用网络设备、服务器、操作系统、应用软件来构建双栈网络环境,整网支持IPv4和IPv6访问。

三类改造方案各有优缺点：

	NAT64地址转换	隧道穿越	IPv4/IPv6双栈
实现机制	通过前置NAT设备，实现IPv6 to IPv4的协议转换。	通过隧道技术，把IPv6的请求封装在IPv4报文里，外层报文继续使用IPv4协议，和VPC的GRE封装类似。	同一个主机同时运行IPv4和IPv6两套协议栈,称为双栈节点，它们可以使用IPv4与IPv4结点互通,也可以直接使用IPv6与IPv6结点

			互通。
优势	快速达成 IPv6 接入，不需要改造应用，应用无感知，过渡阶段最佳方案。	无信息丢失，易实现，只要在隧道的入口和出口进行修改。应用解开报文后，能获取到 IPv6 的信息。	处理效率高、无信息丢失，充分发挥 IPv6 协议的所有优点，更小的路由表、更高的安全性。
劣势	NAT 转换后，应用完全不感知 IPv6，没法回溯 IPv6 信息。对外网 IPv4 地址没有节省。	隧道需要进行封装解封装，转发效率低，其他 IPv6 的优点没有发挥到。	内部网络和主机改造比较大，改造成本高，改造周期性较长。

改造前，深证云已经储备了一定的 IPv6 服务技术能力改造的工作重点在互联网侧的南北向访问的改造。深证通结合行业云现状与未来规划，制定的改造目标为：

1、基于隧道+双栈技术完成改造，实现对物理网络的改动最小化，同时又可以具备 IPv6/IPv4 的应用服务能力；

2、可提供无需应用改造的 NAT64 服务能力，可以帮助云上租户快速实现外网业务的 IPv6 接入，租户业务仅需改造客户端，无需改造后端服务，便可平滑实现外网接入 IPv6；

3、云内的 VPC、子网、弹性网卡等产品支持在原有 IPv4 基础能力，扩展出 IPv6 双栈能力，可以实现业务无缝升级到 IPv6，确保应用系统在改造过程中连续不中断运行。

三、方案介绍

（一）网络访问场景梳理

深证云提供的服务主要包括 IaaS 服务、PaaS 服务以及相应的安全管理和运营运维保障。在此基础之上，可提供面向行业的特色应用。目前行业云建设了深圳、北京两个站点，组成南方-北方双 Region 结构，云网络架构如下：

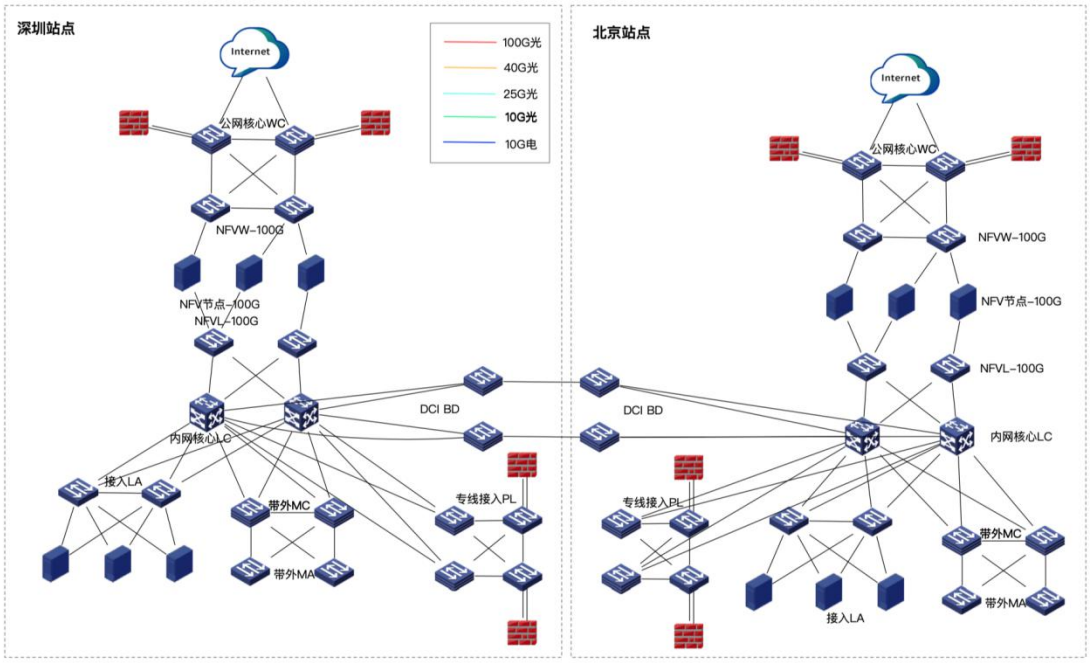

图 2 深证云多 Region 结构示意图

结合网络架构图，可以分析得出行业云上的流量主要分成两类：

东西向流量：云内资源之间互访，通过服务器-接入交换机 LA-核心交换机 LC 的路径即可实现互访；

南北向流量：云内资源与互联网之间互访，通过服务器-接入交换机 LA-核心交换机 LC-NFV 节点-NFV 交换机-互联网核心的路径实现互访。

经过详细梳理得出各个子产品之间的互访关系与业务场景之间的对应关系如下：

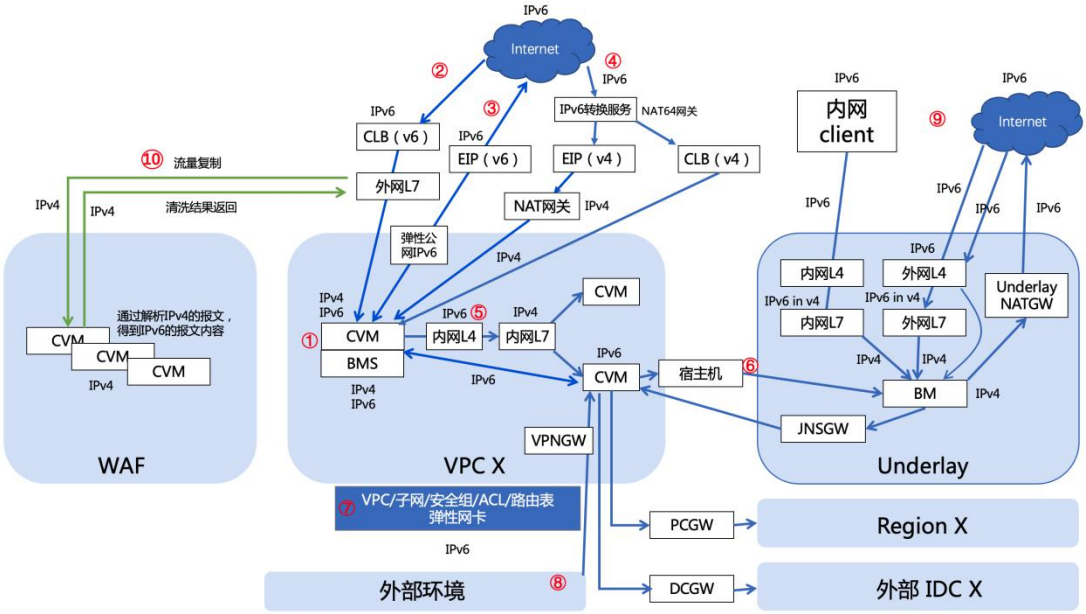

图 2 业务场景流量示意图

访问关系描述与现状分析如下表：

序号	场景描述	现状
场景①	云主机 CVM 之间通过 IPv6 地址互访。	已支持
场景②	子场景 1：外网客户端通过 IPv6 地址以 L4 负载的方式访问 CLB，CLB 将流量转发至云主机； 子场景 2：外网客户端通过 IPv6 地址以 L7 负载的方式访问 CLB，CLB 将流量转发至云主机。	不支持，需要改造 L4/L7CLB
场景③	云主机绑定 IPv6 公网 IP 后，直接与互联网进行互访。	不支持，需要改造 EIP
场景④	在云上提供 NAT64 服务，供租户进行 IPv4-IPv6 之间的地址转换，以适应租户业务的平	不支持，需要建设 NAT64 网关

	滑过渡。	
场景⑤	子场景 1：源云主机通过 IPv6 地址以 L4 负载的方式访问 CLB，CLB 将流量转发至目的云主机； 子场景 2：源云主机通过 IPv6 地址以 L7 负载的方式访问 CLB，CLB 将流量转发至目的云主机	不支持，需要改 L4/L7CLB
场景⑥	云主机可通过 IPv6 地址访问 Underlay 网络平台的服务（比如访问 yum）	不支持，需要改造 VPCGW
场景⑦	云内的网络功能支持 IPv6：比如 VPC、子网、安全组、ACL、路由表、弹性网卡	大部分支持，其中路由表和 ACL 需要改造。
场景⑧	专线接入支持 IPv6，举例外部环境（如云下 IDC 环境）通过 IPv6 地址与云上 VPC 互联	不支持，需要改造 DCGW
场景⑨	云下 Underlay 网络支持以 IPv6 地址访问	不支持，需要改造 Underlay CLB
场景(10)	云上 WAF 支持 IPv6 流量检测	不支持，需要改造 WAF

（二）IPv6 改造方案

根据网络访问场景梳理，深证通需要对场景 2-场景 10 进行改造以支持 IPv6。改造的产品/组件涉及：L4/L7 负载均衡、EIP、NAT64 网关、VPC 网关（路由表、ACL）Underlay 改造、WAF 改造等。

1、L4/L7 CLB 改造方案

利用 IPv6 双栈网关提供 IPv6 的四层负载均衡能力。

四层负载均衡的流量路径如下图所示，CLB 和云主机 CVM 之间为 IPv4/IPv6 双栈访问。

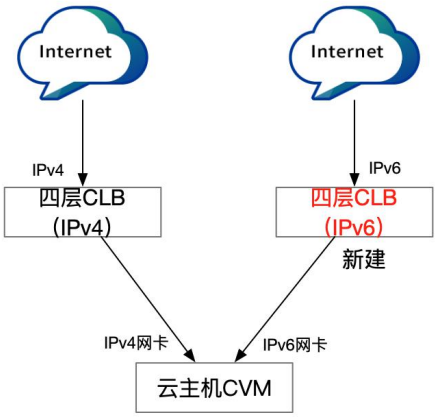

图 3 L4 CLB 改造示意图

七层负载均衡的流量路径如下图所示，四层 CLB 和七层 CLB 之间、七层 CLB 和云主机 CVM 之间，利用 IPv6 in IPv4 技术构建隧道，实现网络互通。

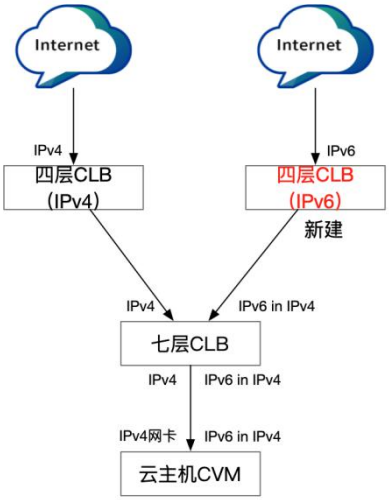

图 4 L4/L7 CLB 改造示意图

改造后的 CLB 功能清单如下表：

功能清单	功能项	功能描述
CLB 集群 IPv6 地址管理	CLB 集群 IPv6 地址管理运营端理支持 IPv6 协议	CLB-IPv6 地址资源录入、删除、查询、资源列表展示；CLB-IPv6 VIP 组创建、删除、查询、列表展示
CLB 集群管	CLB 集群管理运营端支持	CLB-IPv6 集群创建、删除、查询

理	IPv6 协议	
CLB 集群节点管理	CLB 集群节点管理运营端支持 IPv6 协议	CLB-IPv6 节点创建、删除、查询、列表展示
CLB 集群专区管理	CLB 集群专区管理运营端支持 IPv6 协议	CLB-IPv6 专区创建、删除、查询
4 层 CLB 管理	4 层 CLB 负载均衡器租户端支持 IPv6 协议	IPv6 tcp/udp 负载均衡器创建、修改、删除、修改带宽、监控
	4 层 CLB 规则管理运营端支持 IPv6 协议	4 层 CLB IPv6 tcp/udp 规则绑定、解绑列表展示、权重修改真实服务器
	4 层 CLB 规则管理租户端支持 IPv6 协议	4 层 CLB IPv6 tcp/udp 规则绑定、解绑列表展示、权重修改真实服务器，IPv6 tcp/udp 规则真实服务器健康检查配置、健康状态拉取。
	4 层 CLB 监听器运营端支持 IPv6 协议	4 层 CLB IPv6 tcp、udp 监听器创建、修改、查询、删除、列表展示
	4 层 CLB 监听器租户端支持 IPv6 协议	4 层 CLB IPv6 tcp、udp 监听器创建、修改、查询、删除、列表展示
	4 层 CLB 健康检查运营端支持 IPv6 协议	4 层 CLB IPv6 tcp/udp 规则真实服务器健康检查配置、健康状态拉取
7 层 CLB 管理	7 层 CLB 负载均衡器租户端支持 IPv6 协议	IPv6 http/https 负载均衡器创建、修改、删除、修改带宽、监控
	7 层 CLB 规则管理运营端支持 IPv6 协议	7 层 CLB IPv6-http/https 规则绑定、解绑、列表展示、权重修改真实服务器
	7 层 CLB 规则管理租户端支持 IPv6 协议	IPv6 http/https 监听器列表展示，IPv6 http/https 规则绑定真实服务器,IPv6 http/https 规则真实服务器列表展示和权重修改,IPv6 http/https 规则真实服务器健康检查配置和健康状态拉取。
	7 层 CLB 监听器运营端支持 IPv6 协议	7 层 CLB IPv6 http/https 监听器创建、修改、查询、删除、列表展示
	7 层 CLB 监听器租户端支持 IPv6 协议	7 层 CLB IPv6 http/https 监听器创建、修改、查询、删除、列表展示
	7 层 CLB 健康检查运营端支持 IPv6 协议	7 层 CLB IPv6 http/https 规则真实服务器健康检查配置、健康状态拉取

2、EIP 改造方案

利用 IPv6 双栈网关提供 IPv6 的 EIP 能力。

EIP 的流量路径如下图所示，EIP 和云主机 CVM 之间为 IPv4/ IPv6 双栈访问。

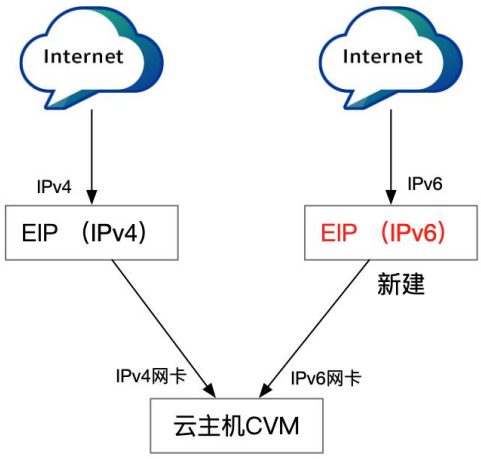

图 5 EIP 改造示意图

改造后的 EIP 功能清单如下表：

功能清单	功能项	功能描述
弹性 IP EIP 支持 IPv6 改造	EIP 地址管理运营端支持 IPv6 协议	EIP-IPv6 资源录入、删除、查询、列表展示
	EIP 地址管理租户端支持 IPv6 协议	EIP-IPv6 多维度监控展示，产品定义接入配置，计量接口对接、数据采集、数据上报、数据校验、数据查询
	EIP 租户端支持 IPv6 协议	IPv6 弹性 IP 地址创建、修改、查询、删除、地址列表展示、地址修改带宽、绑定和解绑资源

3、NAT64 网关新建方案

新建 2 台 NAT 64 网关，服务于租户的业务，为租户 VPC 内的业务提供 IPv6 到 IPv4 地址转换。

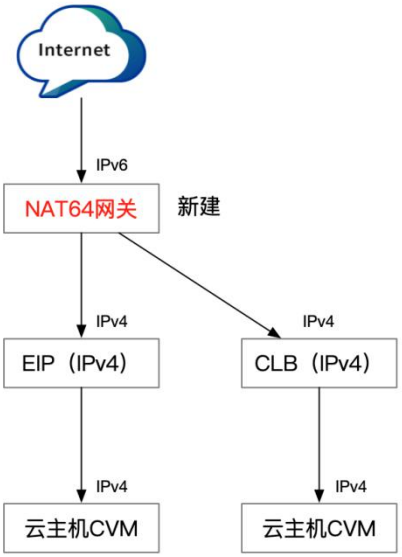

图 6 NAT64 改造示意图

4、VPCGW 改造方案

对 VPCGW 进行软件版本升级与配置，以实现 IPv6 功能：

功能清单	功能项	功能描述
IPv6 地址管理	VPC IPv6 地址管理支持 IPv6 协议	IPv6 地址池的管理、投放、回收、查询，IPv6 已分配和未分配地址的查询
IPv6 路由管理	VPC IPv6 路由管理支持 IPv6 协议	增加 IPv6 rtable、subnet、 subnet route、global route 配置表
IPv6 安全组管理	VPC 入站安全组租户端支持 IPv6 协议	安全组入站添加、编辑、删除、一键放通 IPv6 规则，支持安全组入方向 IPv6 规则查询，
	VPC 出站安全组租户端支持 IPv6 协议	安全组出站添加、编辑、删除、一键放通 IPv6 规则，支持安全组出方向 IPv6 规则查询
IPv6 弹性网卡管理	VPC 弹性网卡运营端支持 IPv6 协议	IPv6 弹性网卡查询（根据租户 id 和地址段查询），IPv6 子机查询（根据租户 id 和地址段查询），IPv6 子机限速、弹性网卡限速，IPv6 子机监控和计量
	VPC 弹性网卡租户端支持 IPv6 协议	弹性网卡 IPv6 申请、释放、列表页和详情页查询
IPv6 VPC 管理	VPC 私有网络运营端支持 IPv6 协议	IPv6 私有网络 VPC 地址段列表查询（根据租户 id 和地址段查询）
	VPC 私有网络租户端支持 IPv6 协议	私有网络 VPC IPv6 地址段申请、地址段信息表处理、地址段查询和释放、VPC 列表页和详情页查询，dhcp 和 dns 支持 IPv6
IPv6 子网管理	VPC 子网运营端支持 IPv6 协议	IPv6 子网列表查询（根据租户 id 和地址段查询）

	VPC 子网租户端支持 IPv6 协议	IPv6 私有网络 VPC 子网申请、释放，IPv6 子网列表页和详情页查询

5、WAF 改造方案

WAF 依赖于 L4、L7CLB 构建 IPv6 in IPv4 实现，流量路径为：

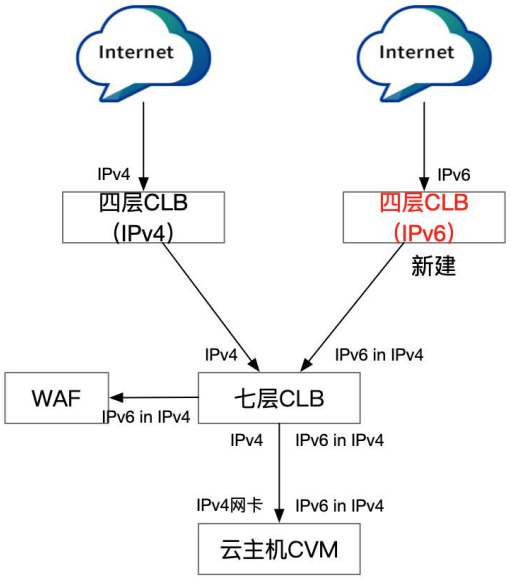

图 7 WAF 改造示意图

6、其他组件改造方案

对云上的其他产品和组件进行软件版本升级与配置，以实现 IPv6 功能：

功能清单	功能项	功能描述
IPv6 裸金属管理	VPC 裸金属运营端支持 IPv6 协议	增加 IPv6 裸金属路由配置表，裸金属间互访逻辑、裸金属和私有网络 VPC 间互访逻辑、裸金属使用 natgw 发访问公网逻辑、裸金属绑定 eip 访问公网逻辑、裸金属内网 lb 访问逻辑、 裸金属外网 lb 访问逻辑、裸金属和 IDC 网络互访逻辑、裸金属和物理网络互访逻辑。裸金属增加录入 IPv6 xgw、sxgw 信息。
	VPC 裸金属租户端支持 IPv6 协议	裸金属增加 IPv6 私有网络 VPC、IPv6 裸金属服务器、IPv6 裸金属子网、IPv6 裸金属子网路由、IPv6 裸金属负载均衡、IPv6 dhcp 获取裸金属子机 ip、IPv6 子机查询。
云服务器云支持 IPv6 改造	云服务器运营端支持 IPv6 协议	运营端实例概览获取云服务器对应私有网络 VPC 所有子网信息，运营端实例概览从子网中获取 IPv6 地址，获取云服务器对应私有网络 VPC 所有子网信息，从子网中获

		取 IPv6 地址，网卡解绑 IPv6 信息，母机投放 IPv6，AS 创建 IPv6 实例获取当前私有网络 VPC 及子网信息，获取当前私有网络 VPC 及子网信息，判断当前 VCP 及子网是否有分配 IPv6。
	云服务器租户端支持 IPv6 协议	云服务器 IPv6 申请、释放、IPv6 列表页和详情页查询，云服务器安全组默认 IPv6 规则页面处理
	云服务器支持 IPv6 协议	操作系统支持 IPv6，母机内核模块支持 IPv6，子机内核模块支持 IPv6，流量转发支持 IPv6

四、经验总结

云平台规模大、业务场景多、产品复杂、安全运营要求高，深证通能平稳顺利、高质量完成深证共建云的 IPv6 改造，主要是得益于以下几方面：

（一）**重视技术方案选择**。由于深证云涉及到数十个子产品，各个子产品所需要实现功能不同，子产品的 IPv6 技术特征不同，所以在设计改造方案时，需结合业务需求、架构现状来选择适合的改造方案,为不同子产品选择了最合适的改造方案，最终选用“IPv4/IPv6 双栈为主+隧道穿越为辅”的 IPv6 改造方案是。

（二）**关注 IPv6 地址规划**。对云的运营者来说，合理的 IP 地址规划可以让云平台架构清晰，租户使用方便。IPv6 地址有 GUA（Global-Unicast） 全局单播地址和 ULA（Unique-Local）局部单播地址等，因深证云互联网出口为 BGP 线路，所获取的 IPv6 地址可在全球互联网使用，深证云建议租户直接选用 GUA 地址，可发挥 BGP 链路的优势且租户使用简便。此外，在子网掩码选择方面，IPv6 地址设计机制使得租户 IPv6 最小子网掩码均为/64，考虑深证云的

用户需求和云平台 IP 地址资源的总体容量，最终确定租户 VPC 内的 IPv6 掩码为/62。

（三）**同步开展网络安全防护工作**。按照通常的云平台的网络安全责任划分，云平台运营方负责平台安全，租户承担租户资源安全，租户使用云平台提供的安全能力并结合自身的安全管理要求实施安全防护。在 IPv6 的场景下，在云平台运营过程中，一方面云的运营者需要持续丰富安全产品，另外一方面需要向租户推荐网络安全方案，协助租户完善安全架构，优化安全策略，例如合理配置 IPv6 安全组以收缩风险暴露面，部署主机安全、WAF 等云安全产品。