网络环境设计

区域选择

- 是否满足数据主权和合规性要求
- 区域与用户或其数据中心的距离（即反映为服务访问延迟）
- 区域是否能够提供所需要服务，可能有些服务无法提供，用户仍然可以在自己的环境中搭建
- 区域是否是最经济高效的?

可用区选择

- 建议使用两个可用区
- 主要是为了确保可用区故障时应用不受到影响
- 大多数应用都能同时支持两个可用区
- 数据库服务建议在两个可用区开启主从服务以实现高可用
- 通常选择两个以上的可用区经济性较差，除非有大量EC2竞价实例获取更低的价格

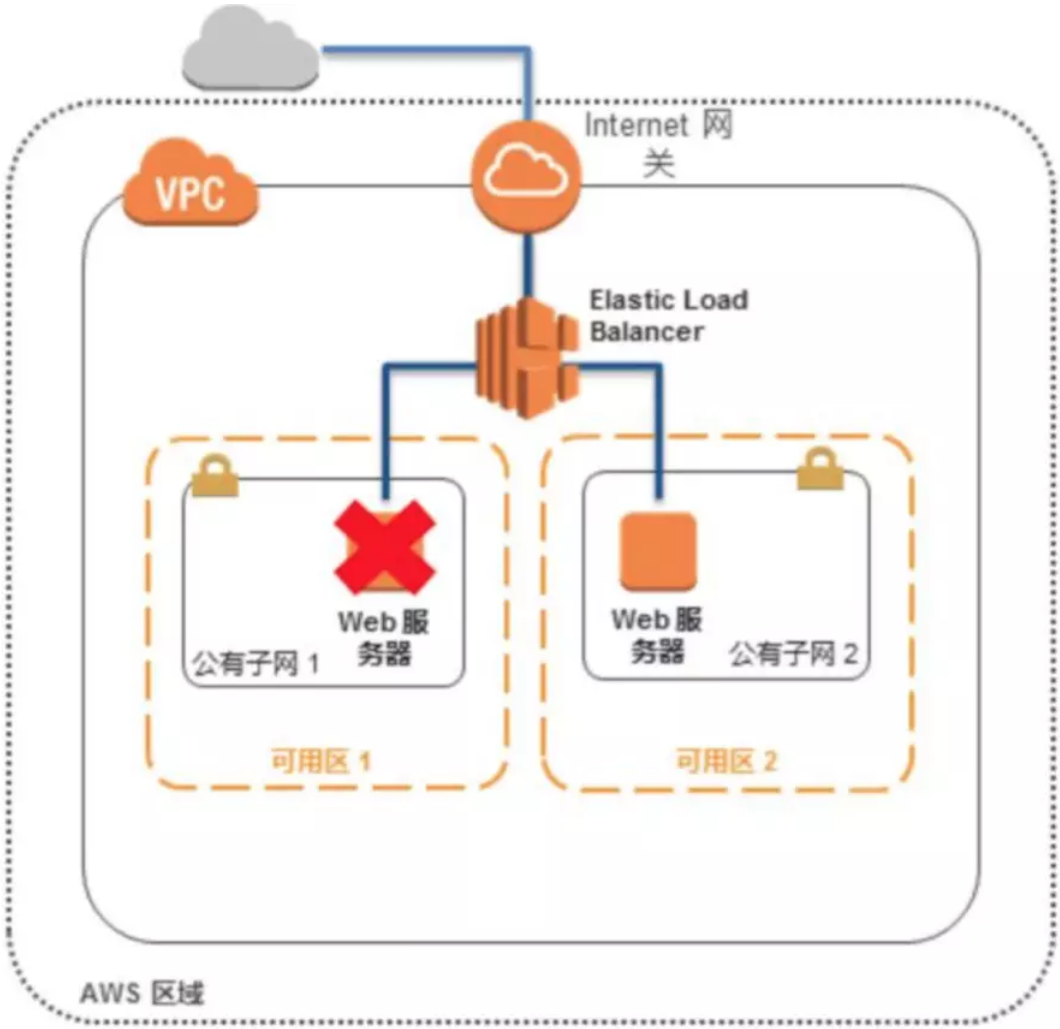

image.png

账户和VPC管理模式

原则和模式

- 主要考虑组织架构的复杂性和工作负载隔离
- 单VPC管理
  - 单一VPC通常适用于以下环境
    - 高性能运算 （VPC内部的延迟极低）
    - 统一的身份管理服务
    - 非常小的团队和单一的应用
- 多VPC管理
  - 适合单一团队的复杂工作
  - 使用一个AWS账户
  - 但使用多个VPC来组织应用程序环境
  - 团队规模有限使得维持标准和管理访问更加容易

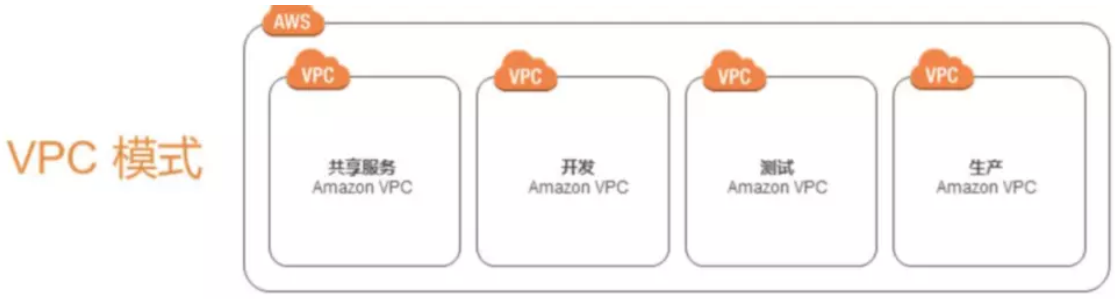

image.png

- 多账户管理
  - 具有很多IT团队的大型组织或期待快速增长的中型组织

- 工作负载隔离要求高
- 使用多个AWS账户，但每个AWS账户只一个VPC
- 在复杂组织中，管理访问和标准更具有挑战性

image.png

其他重要因素

- 很多AWS服务可能实际并不在VPC内
- VPC内外资源通信会经过公共的AWS网络
- S3 可以为VPC提供终端节点服务

VPC IP设计

- VPC 是区域有效的，可以跨过可用区
- 子网在可用区有效，需要指定。
- 每个账户每区域只支持5个VPC
- VPC CIDR 和子网：
  - CIDR - 指定VPC IPv4的范围，大小支持 /16 ~ /28
    - 每个VPC最多有1个主CIDR+4个辅助CIDR块
    - 默认VPC 172.31.0.0/16
  - VPC - 可以包含多个子网，但是子网不能跨可用区
    - 子网地址段必须在CIDR内
    - 默认VPC会在每个可用区包含一个/20的公有子网
- 子网分类

- 公有子网：包含指向Internet网关的路由条目，可以支持对公共Internet出入站访问
- 私有子网：没有指向Internet网关的路由条目，通常使用NAT/代理/堡垒主机(Bastion Host)来支持受限的仅供出站的公共Internet 访问
- 仅限VPN子网：关联路由表将流量引导到VPC的VPG，但没有到IGW的路由

- VPC 类型
  - 仅带有一个公有子网的 Amazon VPC
  - 带有公有和私有子网的 Amazon VPC
  - 带有公有和私有子网以及提供 AWS 站点到站点 VPN 访问的 Amazon VPC
  - 仅带有一个私有子网以及提供 AWS 站点到站点 VPN 访问的 Amazon VPC

- 子网
  - 每个VPC默认最多200个子网，需要申请提交扩展
  - 所有未指定VPC的实例等都会放入默认VPC
  - 通常一个VPC建议有一个公有子网，和多个私有子网
  - 通过公有子网来控制私有子网与Internet之间的访问
  - 建议使用更大的子网，因为子网IP耗尽将无法添加
  - 规划子网时不需要考虑广播域问题，VPC已经解决了这个问题
  - 建议将更多的实例放入私有子网，而仅仅暴露ELB或少量Web服务器在公有子网
  - EC2的公有IP是随机分配，关机即释放。 私有IP可以指定并且可以始终绑定，需要关机才能解除绑定，辅助地址可以随时绑定和解绑。
  - EC2的公有地址并不能被EC2本身管理，他是绑定到EC2的私有IP上进行转译的。
  - 规则属性
    - AWS默认每个子网需要自动预留5个IP，即前4个和最后一个IP
      - .0 网络地址
      - .1 VPC 网关路由器
      - .2 预留，用于VPC内部DNS
      - .3 预留
      - . 255 广播地址，但VPC内只支持单播
    - 从经验来讲，私有子网应是公有子网IP地址数的一倍

VPC最佳实践

- 每个账户都有一个默认VPC，在默认VPC中 ， EC2默认会被自动分配私有和公有地址
- 尽量使用大子网而避免多个小子网
- 使用合适大小的CIDR块
- 保持子网的简单性并按公有\私有进行划分
- VPC部署在多个可用区实现高可用
- 利用安全组来控制资源之间的流量
- 使用VPC流日志进行监控和追踪
- 通过API调用或者AWS管理控制台来检查VPN链路运行情况

控制VPC 流量

路由表

- 每个VPC有一个主路由表，并默认路由到本地网络实现VPC之间的通信
    - 每个子网必须与一个子路由表与之相关联，
    - 每个路由表都默认有一条到本地网络的路由，
    - 如果不设置子路由表，其路由条目将继承主路由表
- 建议将主路由表设置为默认状态，显式的关联和配置所有子网的子路由表
- 默认避免了MAC欺骗和ARP欺骗等传统二层网络攻击

防火墙安全组

- 虚拟防火墙，用于控制EC2实例的出站和入站流量
- 安全组是作用于一个EC2的，而不是传统意义上的边界防火墙
- EC2安全组 和 VPC安全组 都可以作用于EC2，每个EC2至少需要与一个安全组绑定，若不指定则关联到默认安全组
- 安全组是默认拒绝所有入站流量的，所有允许必须显式声明
- 多个安全组共同作用时，所有规则允许规则将被组合生效
- 安全组的属性包括，端口、协议、源目标IP地址段，但不能指定特定IP地址
- 安全组是有状态防火墙，记录外出消息允许响应，而不需要明确的入站规则
    - 会对连接进行跟踪
    - 对全允许 如0.0.0.0 和 0-65535的条目，则不会跟踪
    - 删除安全组规则后通常跟踪连接不会删除，需要等几分钟甚至最多5天
    - 除TCP/UDP/ICMP之外的协议，仅跟踪IP地址和协议编号

- 任何主机安全组对VPC内部通信都无效
- 任何虚拟主机都不能直接修改VPC防火墙安全组，若要操作只能通过API调用
- 只在区域内有效
- 规则
    - 默认拒绝所有传入流量，需要手工显式允许，而且只能允许规则不能拒绝规则
    - 安全组执行规则是首先整体评估所有规则后再做操作
    - 任何一条允许配置则该流量被放行
    - 安全组是有状态允许，即允许入站流量则自动允许相应的出站流量
    - 默认情况下，安全组是允许所有出站流量的
    - 安全组策略修改后即时生效
- 属性
    - 每个VPC最多支持500个安全组
    - 每个EC最多支持5个安全组，即最多将5个安全组与每个实例的每个网络端口关联
    - 每个安全组支持50条入站规则和50条出站规则
    - 可以使用标准协议号支持任何协议
- 实践
    - 可以将源和目标定义为另一个安全组或者CIDR块以便处理自动扩展情况
    - 可以将不同的实例划入一个安全组中实现统一的流入流出和资源间的流量控制管理
    - 建议安全组的入站规则是针对应用程序的某一个功能层的

image.png

网络ACL

- 可选的虚拟网络防火墙，可以控制传入传出子网的流量
- 默认情况下允许所有传入传出流量，且是无状态的
- ACL执行规则是按条目顺序逐句匹配执行操作
- 建议主要使用安全组，配合使用NACL
- NACL通常需要允许出站的随机端口（1024-65535）

image.png

Internet网关 IGW

- 允许VPC实例与Internet通信
- 托管服务默认支持在区域内横向扩展和冗余高可用
- VPC路由表中为Internet 可路由流量提供目标
- 1个VPC只能关联一个IGW，一个IGW也只能挂载到1个VPC
- 默认VPC默认标配
- 操作：
    - 将Internet 网关连接到VPC

    - 子网路由表指向Internet网关
    - 子网中实例有公网IP或弹性IP
    - NACL和安全组允许了流入流出流量

- Egress-only IGW
    - 用于VPC和Internet之间的IPv6通信

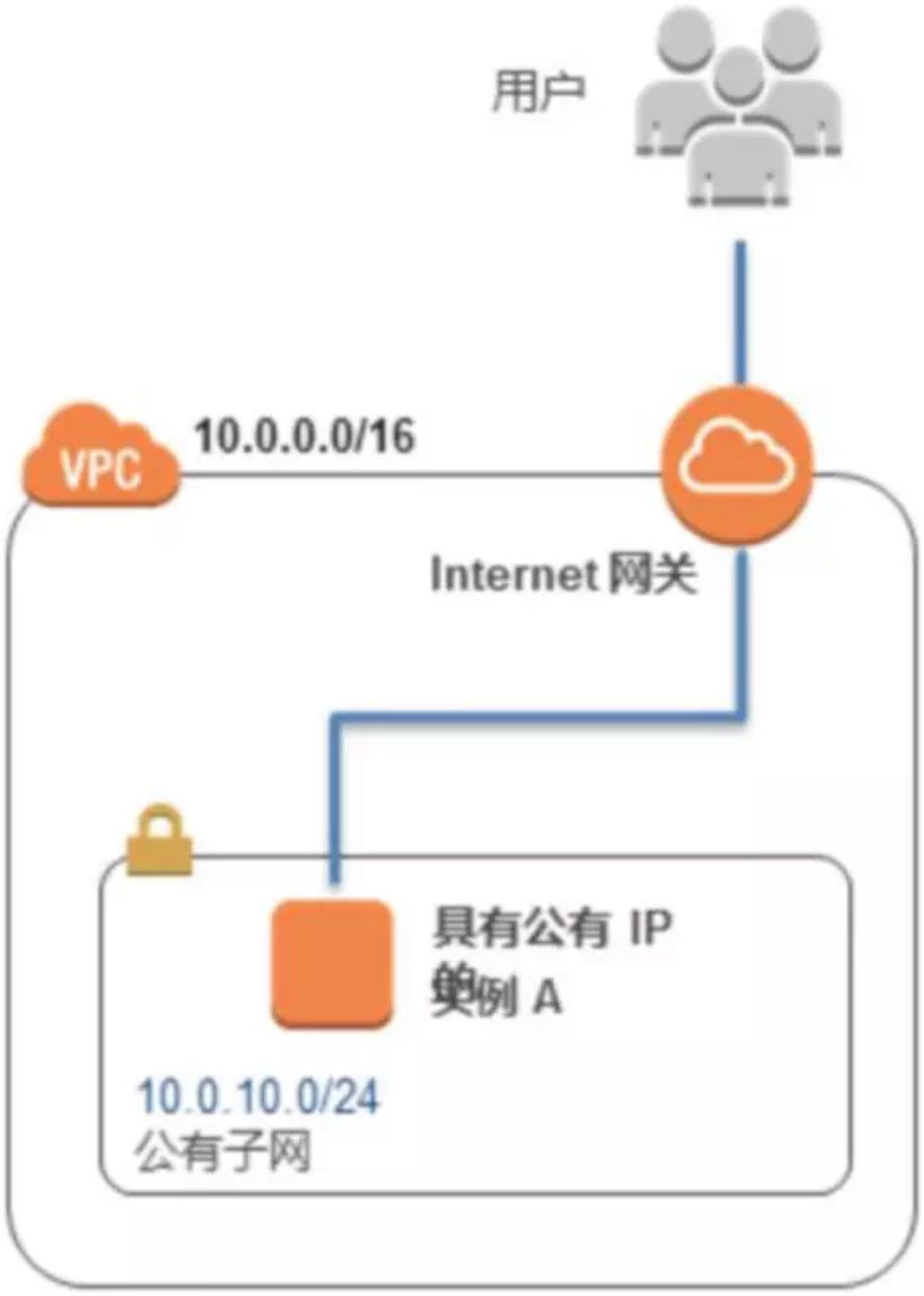

image.png

其他服务

VPC的EC2通信

- VPC内部EC2通信流量在AWS内
- 对等VPC之间的EC2通信流量在AWS内
- 非对等VPC之间的EC2通信流量可能经过IGW

DHCP服务

- DHCP是VPC默认开启的选项，且只能有一个DHCP与之关联
    - 域名服务器 - 默认是AmazonProvidedDNS， 可手工设置最多4个DNS
    - 域名 - 默认是所在区域域名，但可手工指定
    - NTP Server - 最多4个NTP服务器地址
    - Netbios Server - 最多4个Netbios 服务器地址
    - Netbios Node Type - 设置为2

Elastic IP

- EIP允许用户维护一组固定的公网IP地址
- 需要先将EIP关联到某个VPC内部，然后再分配给一个实例
- EIP是和区域关联的，不能跨区域使用
- EIP的最佳实践不是绑定到EC2的ENI，而是关联到EC2的私有IP
- EIP可以自由的在VPC的实例中移动
- 每个用户每个区域默认最多5个EIP，需要申请扩展
- EIP需要与EC2的一个私有IP关联才能使用，且不能用于NAT网关或NAT实例以及用于私有子网EC2
- EIP一旦申请不论是否使用都需要收费
- 支持方向DNS记录
- VPC支持BYOIP

Elastic Network Interface ENI

- ENI是一个关联到VPC的EC2虚拟网络接口
- 每个ENI支持一个公网IP和多个私有IP，其中一个私有IP需要被设置为主用
- 利用ENI可以实现VPC内的实例具有多个子网连接
- 最常见的场景就是将实例加入到管理网络中

VPC端点 Endpoint

- 实现VPC与其他AWS服务（如S3）的虚拟连接，而不用通过实际的网络进行访问
- 每个服务可以关联多个Endpoint，并且将多个路由表与他们关联
- Endpoint 如果是Interface类型为非高可用，Gateway为高可用（S3和DynamoDB）
- 利用PrivateLink提供链接
- 配置Endpoint操作
    - 指定适用VPC
    - 指定目标服务，前缀格式为com.amazonaws.<region>.<service>
    - 配置Endpoint访问策略
    - 配置路由表指向

NAT

- 私有实例是无法与IGW通信的，NAT用于处理私有实例出站流量
- NAT实例
    - 公有子网中启用NAT的EC2实例，AWS提供专用分NAT AMI
    - 一定要关闭源目标检查
    - 所有后端实例需要一条0.0.0.0/0的路由到NAT实例
- NAT 网关
    - NAT网关支持可用区内的高可用部署
    - NAT网关可以跨可用区共享，但是仍然建议跨可用区实现高可用
    - NAT Gateway也是放在公有子网里的
    - 无需关闭源目标检查
    - 自动分配公网IP
    - NAT网关无法对URL进行过滤，只能使用Proxy

	VPC NAT 网关	NAT 实例
可用性	默认具有高可用性	使用脚本管理故障转移
带宽	可突增至 10Gbps	由实例类型的带宽决定
维护	由 AWS 管理	由您管理
安全性	NACL	安全组和 NACL
端口转发	不支持	支持

image.png

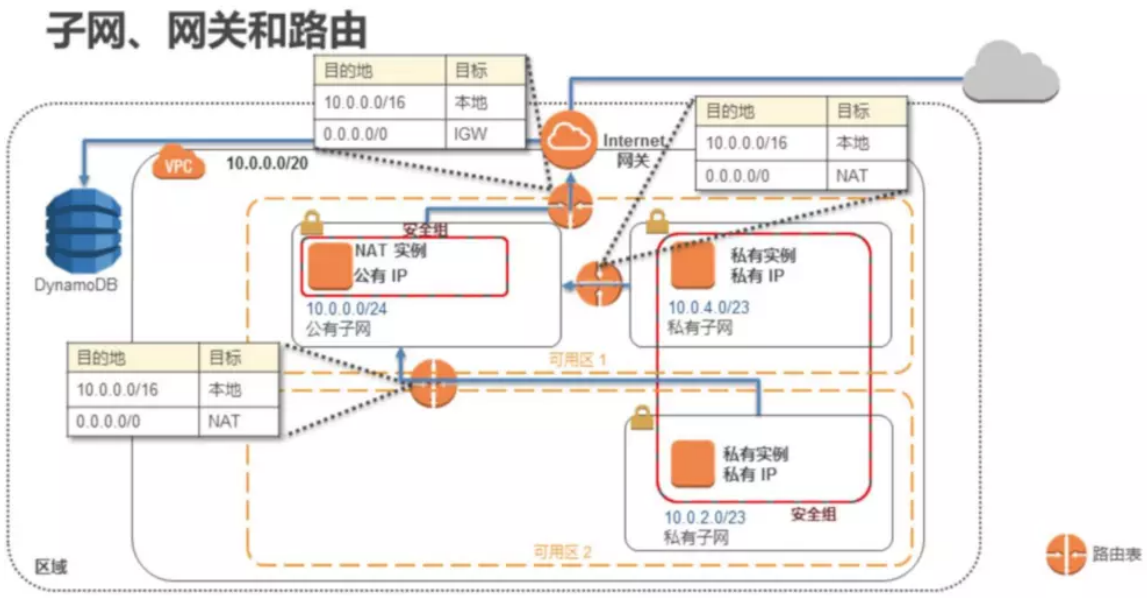

image.png

堡垒主机

- 创建在公有子网中，用于使用SSH/RDP访问私有子网中的EC2

API 访问

- VPC支持通过API调用对VPC进行操作和管理
- API调用必须使用AWS账户安全密钥
- 建议所有API端点的调用操作都使用SSL加密
- IAM还可以对API调用操作进行授权

NTP

- AWS 利用 169.254.169.123 提供NTP服务

VPC对等路由

- 同一区域中的不同账户下的AWS也可以建立对等链接
- 目前已经支持建立跨区域对等连接
- IP地址不能相互重叠的私有地址VPC
- 任意两个VPC之间只能建立一个对等链接
- 通过账户ID和VPC ID进行标记
- 对等关系不可传递，只能显式声明
- 管理和配置
    - 建立对等连接后，还需要在VPC路由表指向对等VPC的路由
    - 还需要配置相应的安全组和NACL规则
    - 无需Internet网关和虚拟网关
- 限制
    - 无单点故障和带宽限制
    - 对等VPC MTU=1500 Byte
    - 对等VPC仅能用子网作为安全组出入规则，而无法使用其它安全组作为出入规则
    - 私有DNS无法在对等VPC之间进行解析
- VPC对等安全性设计
    - 双向握手来建立对等连接
    - 通过路由进行对等VPC之间流量控制
    - 安全组和NACL控制出入流量
    - 没有传递性信任减少无意的意外网络连接
    - 区域内VPC对等传输不加密，但是是私密隔离的，区域间采用AEAD算法加密
- ELB，PrivateLink和EFS无法通过VPC对等连接使用

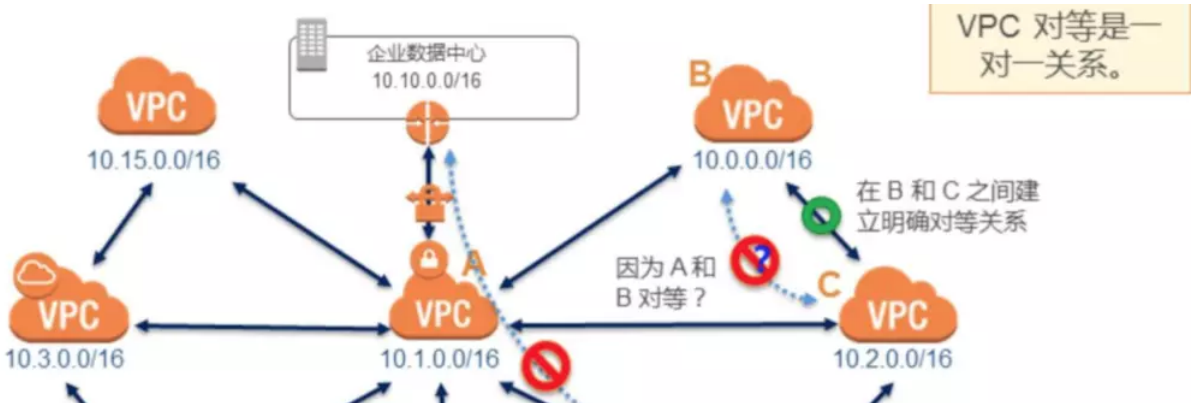

image.png

VPC 流日志 （Flow Log）

- 捕获经过你的VPC的网络流量（入向和出向）
- 日志数据保存在Amazon CloudWatch Logs中
- 在Amazon CloudWatch Logs中查看和检索其数据
- 可以获取接收和拒绝的流量源目的详细信息
- Flow logs可以在以下级别创建：
    - VPC级别
    - 子网级别
    - 网络接口级别
- 还可以在主机级别开启日志监控并转发到S3或者CloudWatch
- 限制
    - 对于Peer VPC不能开启Flow Logs功能，除非这个VPC也在你的账户内
    - 不能给Flow Logs打标签
    - Flow Logs创建后不能更改其配置
    - VPC Flow Logs并不捕获所有经过VPC的流量，
- 以下流量将不会被捕获：
    - 实例访问Amazon DNS服务器（即.2地址）的流量
    - Windows进行Windows许可证激活的流量
    - 访问实例Metadata的流量（即去往169.254.169.254的流量）
    - DHCP流量
    - 访问VPC路由器的流量（即.1地址）

将本地环境连接到AWS

IPSec VPN解决方案

- 可以使用AWS VPC的硬件VPN网关实现
- 可以利用VPC中的EC2实例作为VPN网关实现
- AWS侧网关叫VPG，客户侧网关叫CGW
- VPN的必要组件
    - An on-premise Customer Gateway
    - A Virtual Private Gateway
    - A VPC with Hardware VPN Access
    - A private subnet in your VPC
- VPN多站点连接
    - 提供星型网络拓扑结构构建多条VPN连接不同站点
    - 利用静态或者动态（BGP)路由协议进行通信
    - 在使用BGP时，BGP与IPSec必须终结于同一个网关

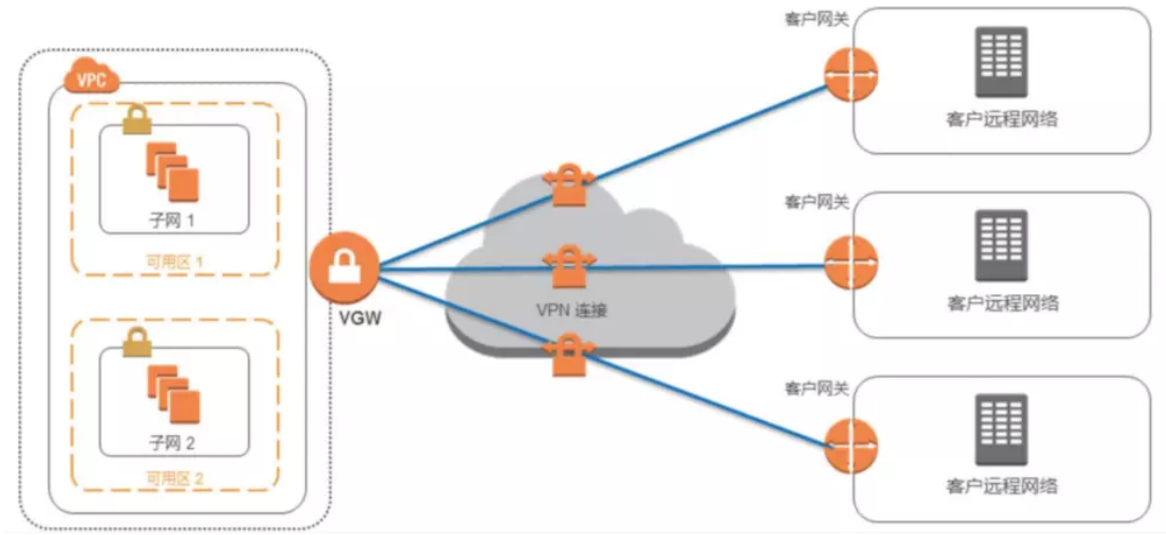

image.png

AWS Direct Connection 解决方案

- 适用于混合云架构和私有数据中心扩展
- 降低网络传输延迟提升网络性能

- 传输大量数据
- 符合安全性和合规性要求
- 1G/10G的预配置连接
- 支持BGP和路由策略
- 需要手工指定去程和回程路由，或者在VPG启用Route Propagation

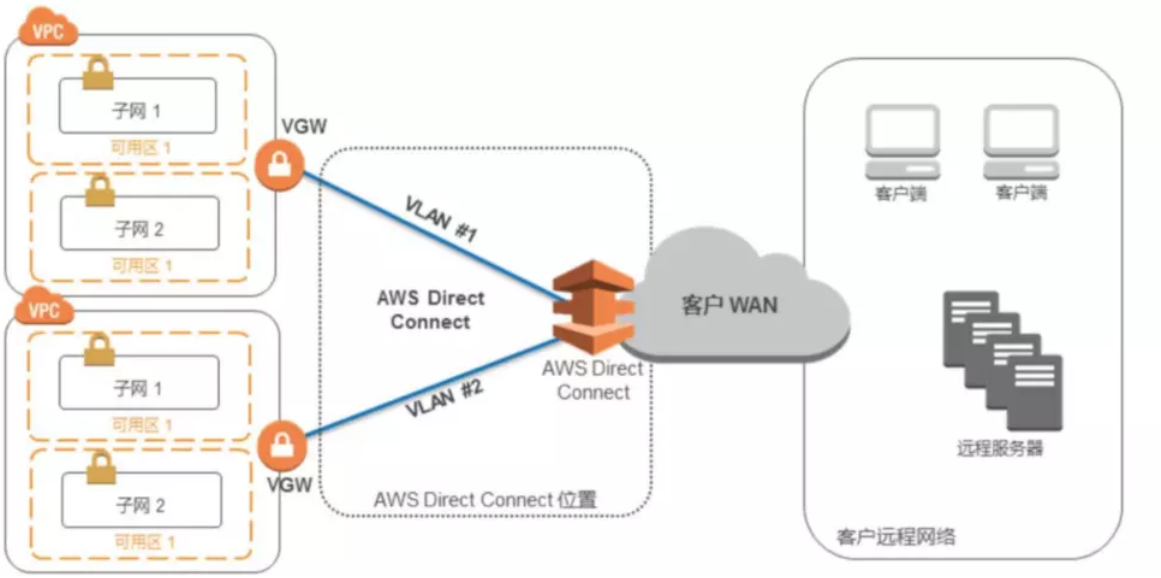

image.png

AWS外部连接的高可用

- 对于VPN连接，利用冗余的客户网管与不同可用区的VPN GW建立连接，通过静态路由或者BGP发现的方式实现路由冗余

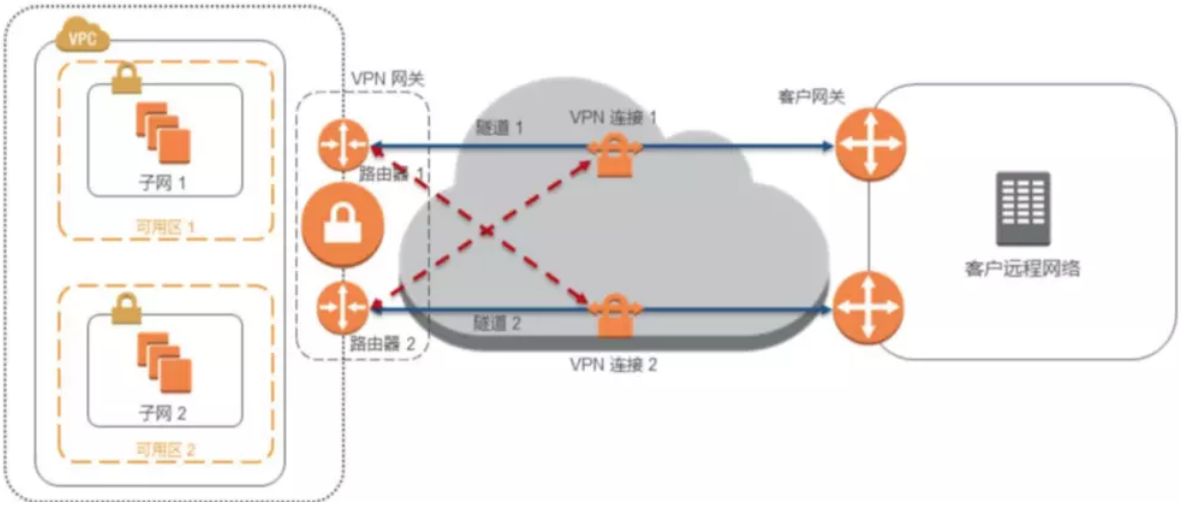

image.png

- 使用Direct Connect服务，部署两条实体链路，依然利用BGP实现冗余，通过BGP策略MED值的设计在平时实现负载均衡。

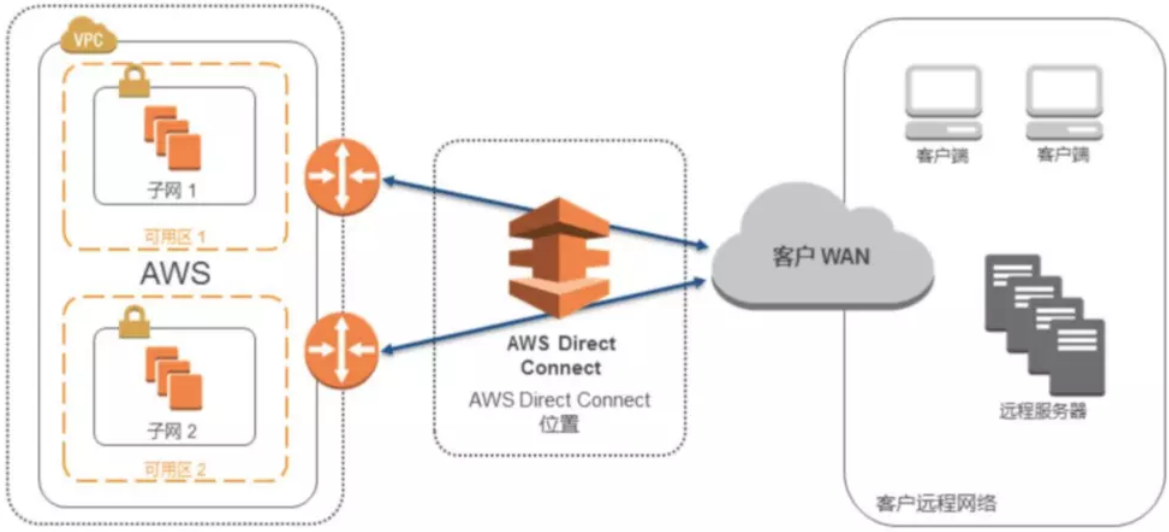

image.png