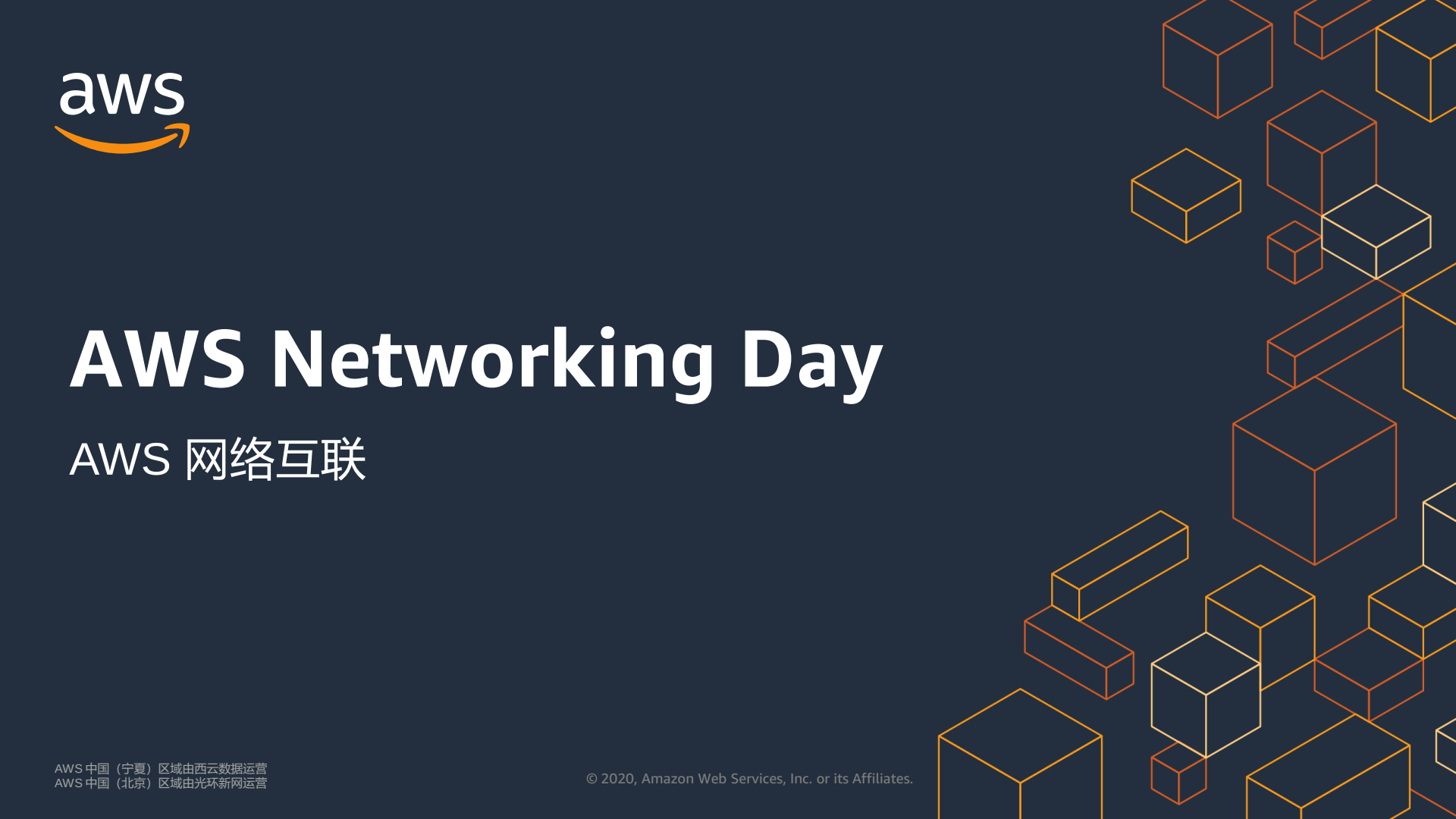


AWS Networking Day

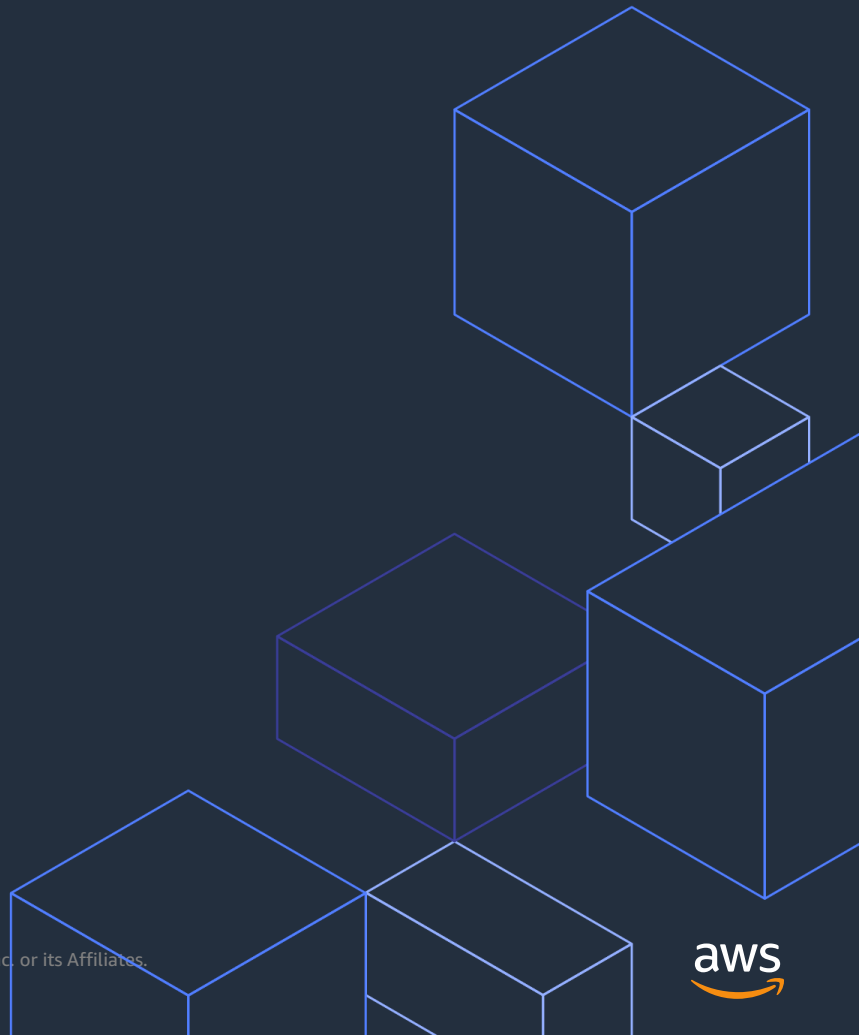
AWS 网络互联

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

内容概要

- 多VPC 网络架构
- VPC Peering(对等体连接)
- AWS Transit Gateway(中转网关)
- TGW 路由表
- Direct Connect 和Site to Site VPN
- 实验环节介绍

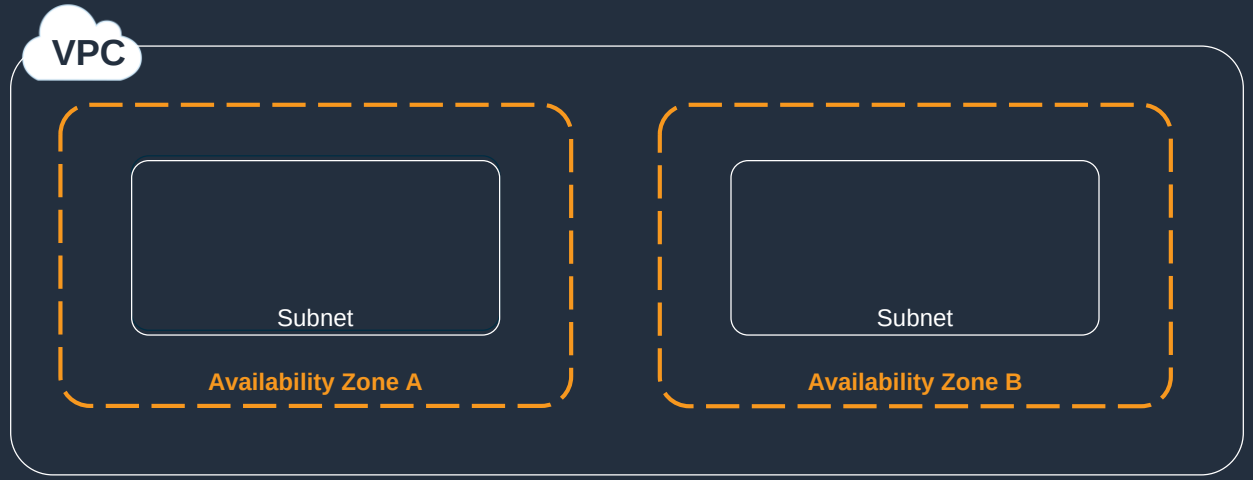
多VPC 网络架构



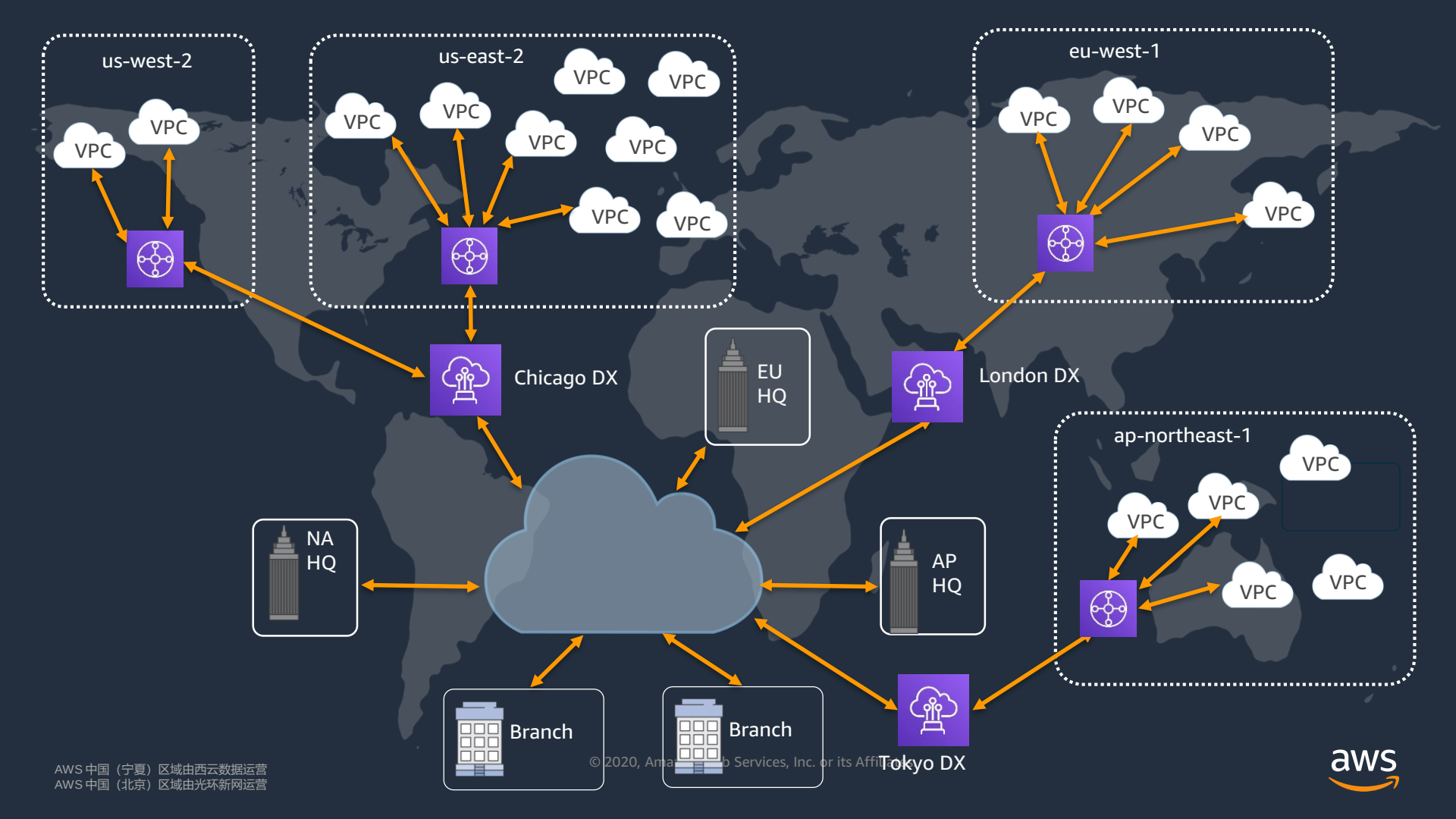
AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

aws

单一VPC



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

选择少账户大规模VPC还是多账户小规模VPC

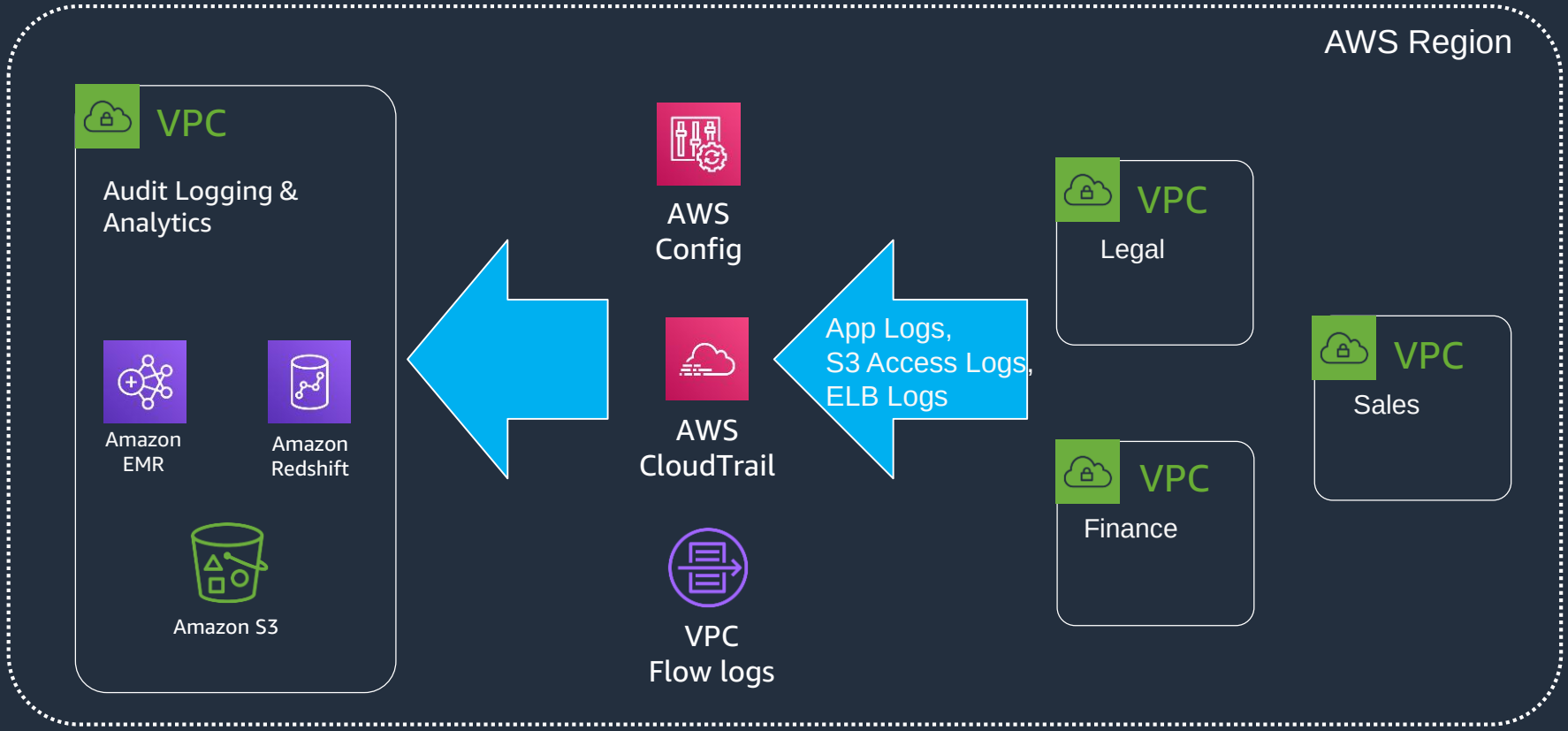
少账户大规模VPC

- 更少的账户和网络创建配制
- 帐户或VPC内的控制更加严格
    - 身份和访问管理（IAM）
    - 严格的安全组和路由配置管理
    - 使用标签识别资源
- 每账户账单的复杂性增加
- 有更大的广播风暴和故障半径
- AWS 配额限制

多账户小规模VPC

- 更多的账户和网络创建配制
- 部署的标准化控制的更加严格
    - 基础设施自动化
    - AWS Direct Connect 和VPN标准化配置
    - 子网和路由标准化规范化
- 每账户账单复杂性低
- 有更小的广播风暴和故障半径

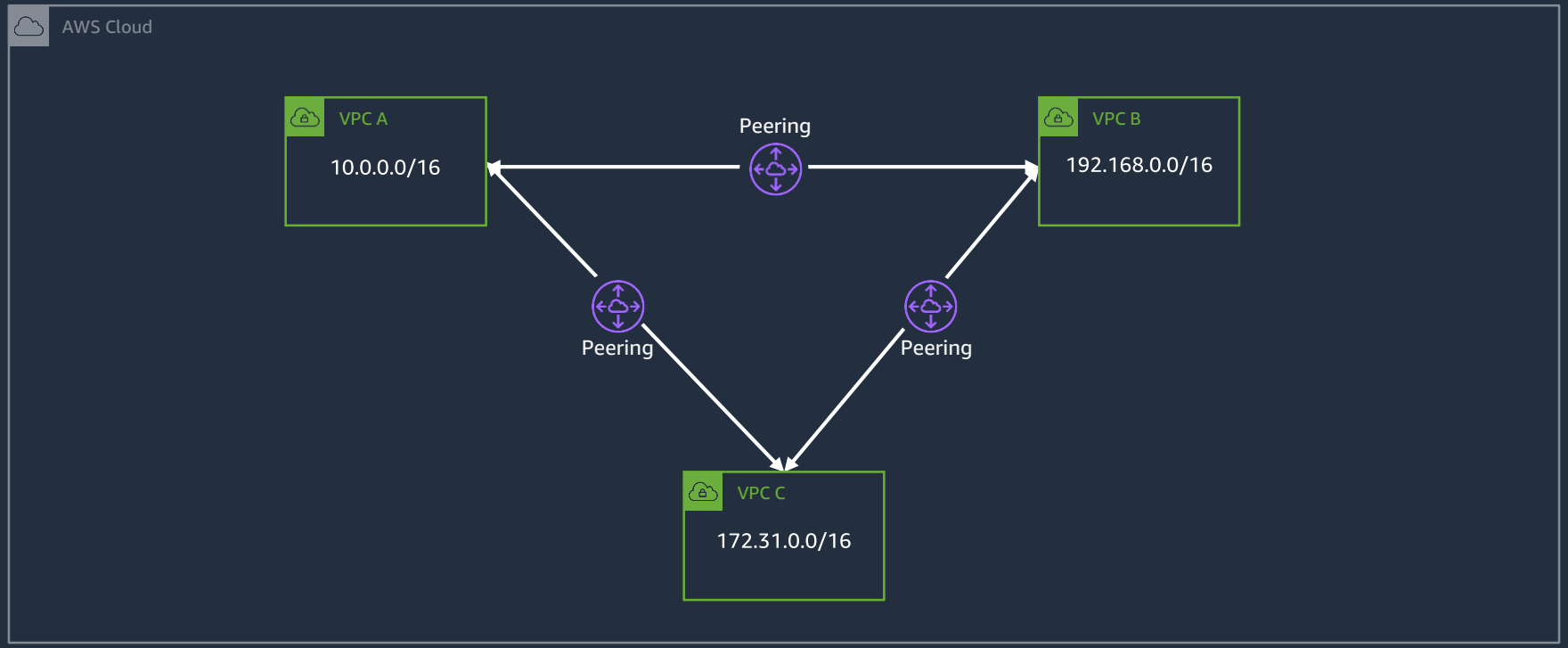
多VPC的部署架构



VPC peering(对等连接)

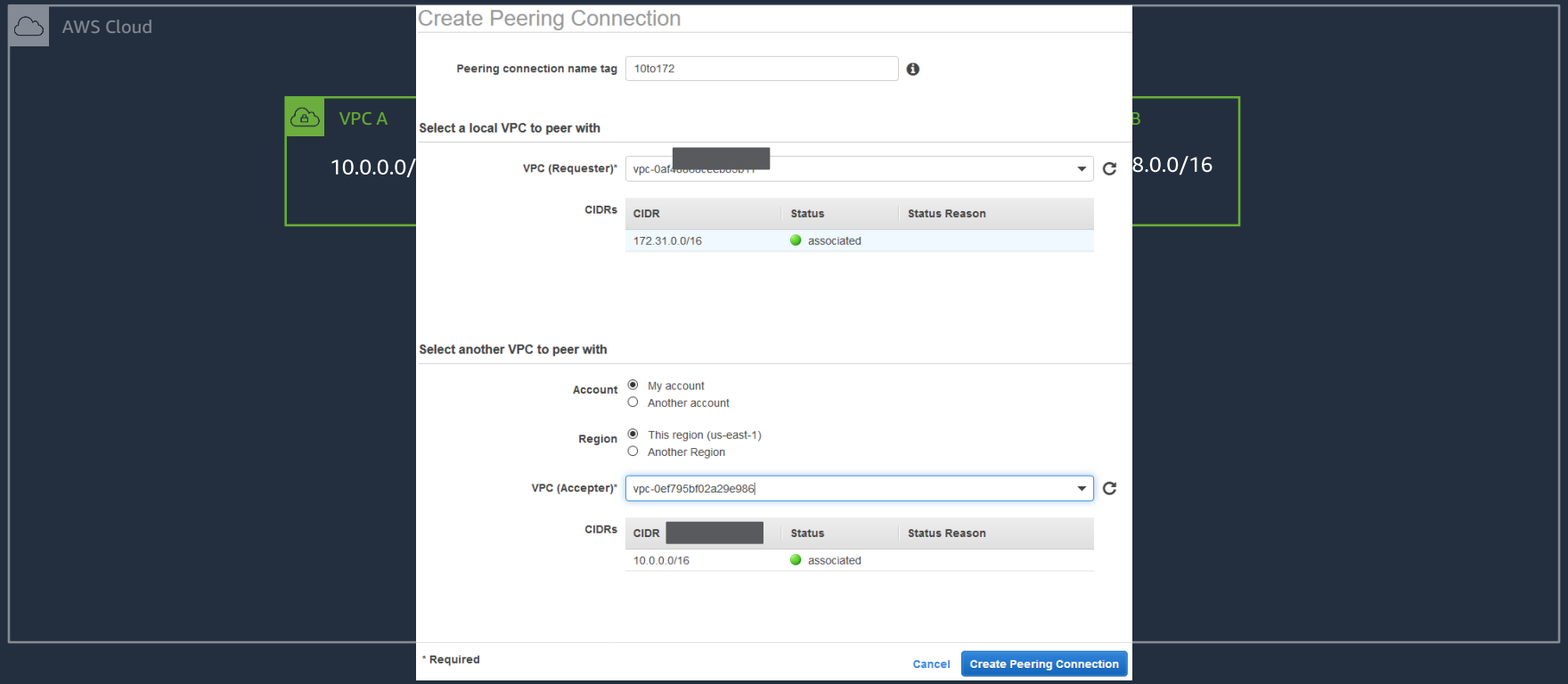
VPC间互联

区域内，区域间，帐户间均可

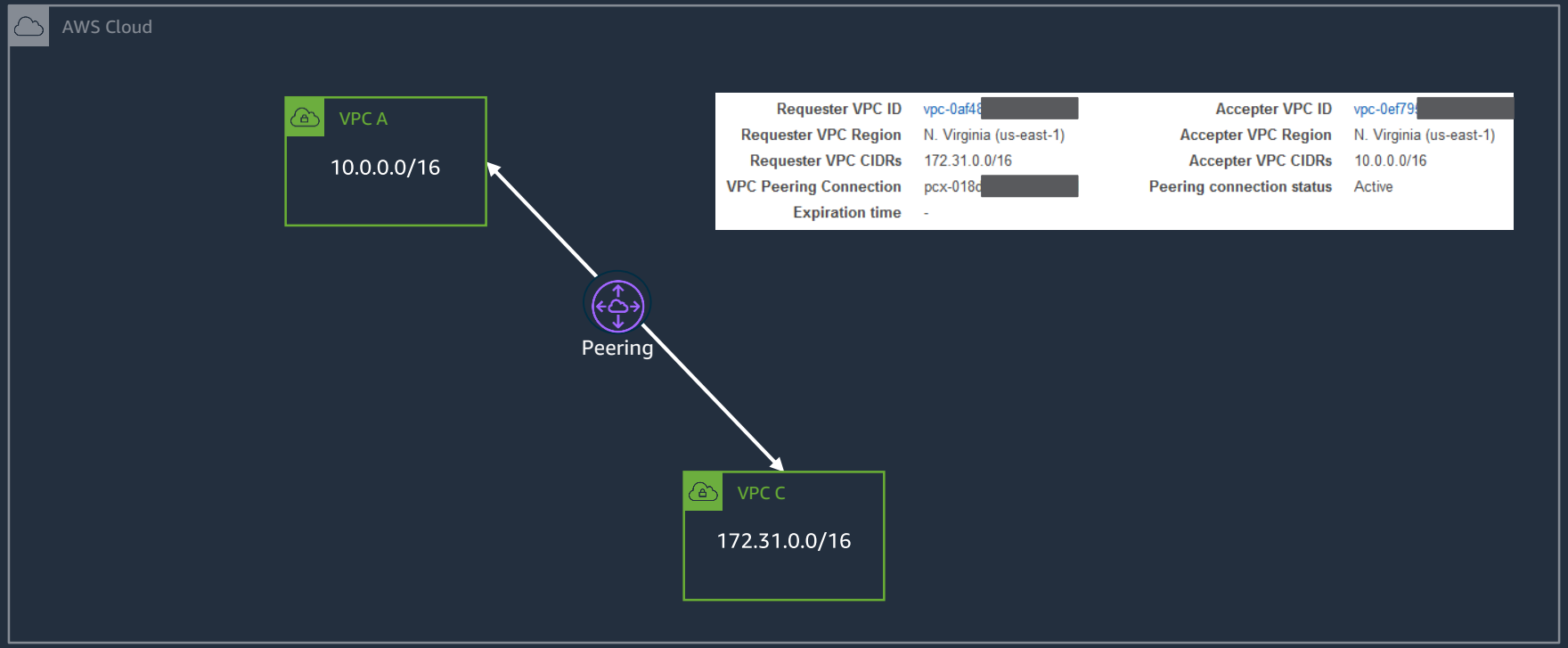


AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

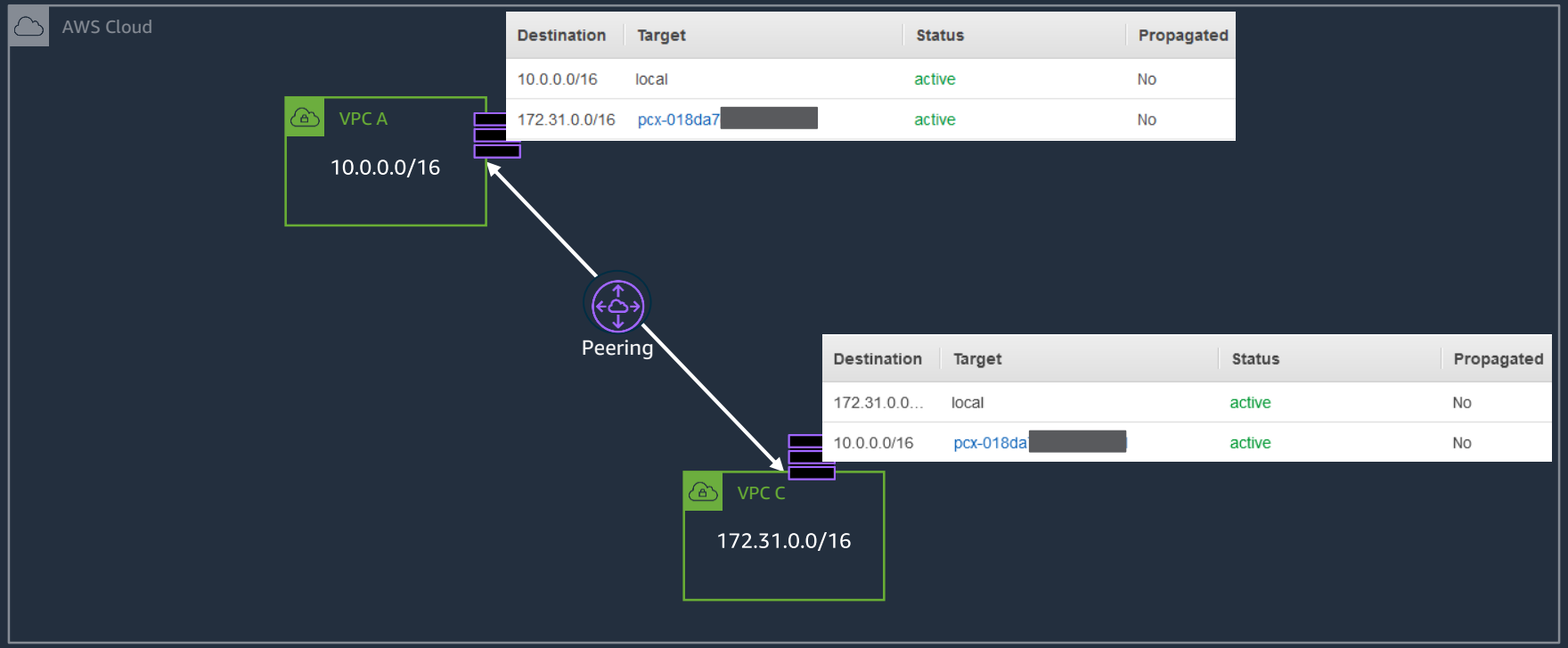
创建VPC peering



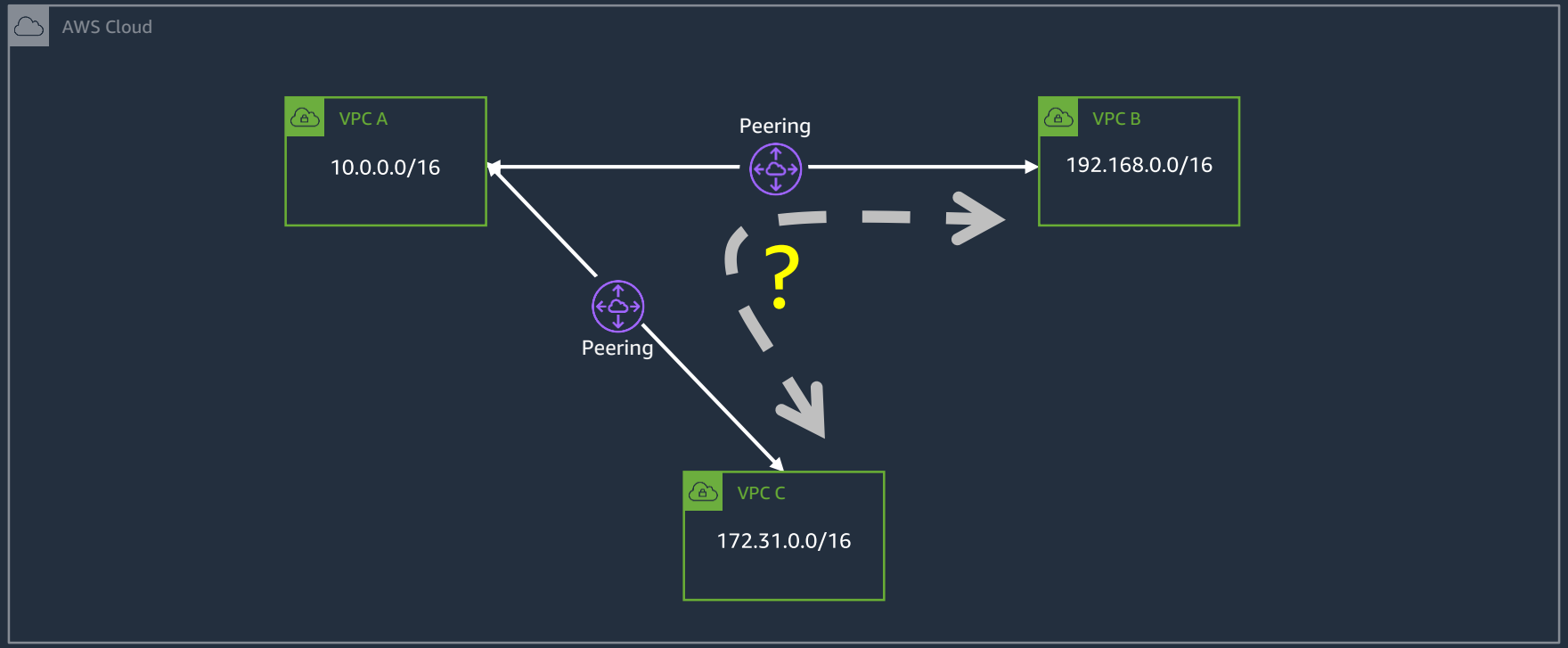
VPC peering 对等体连接信息



VPC peering 路由表信息

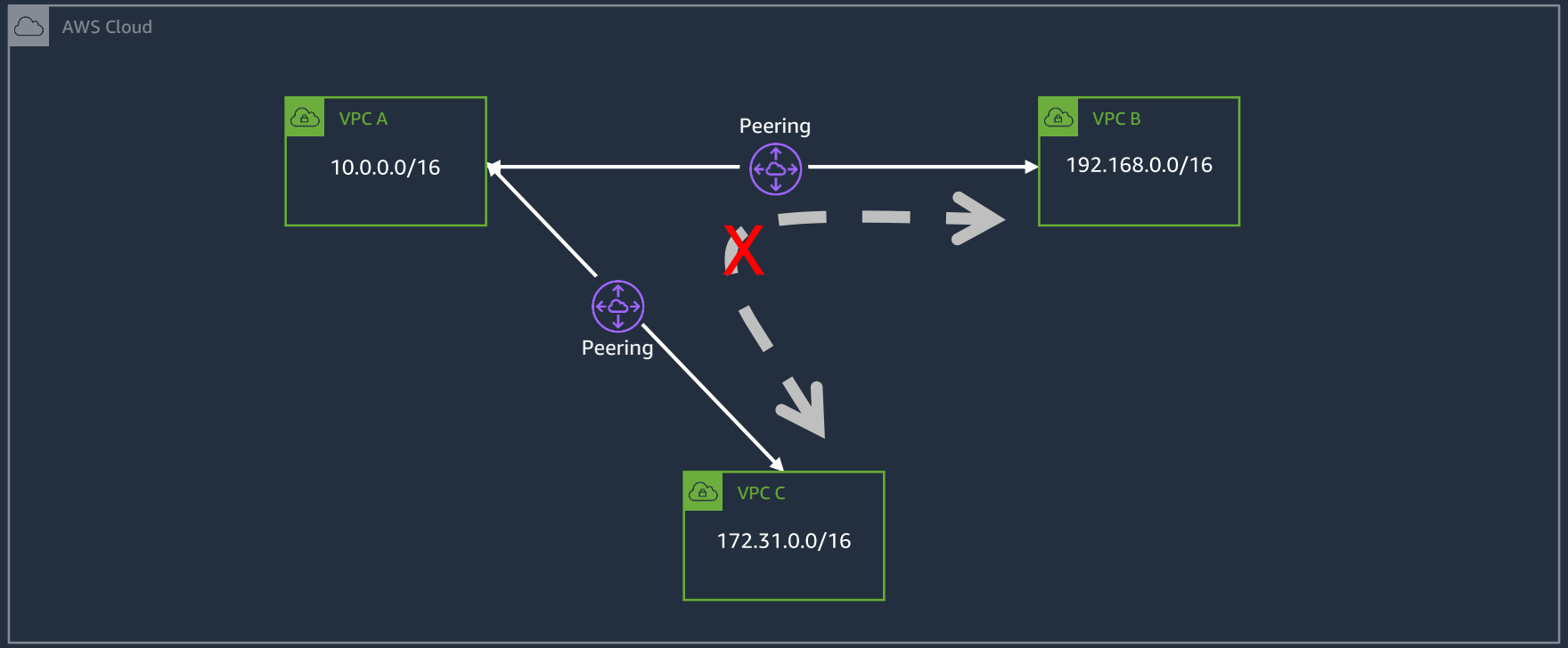


VPC peering 是否支持传递对等关系?



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

VPC peering 不支持传递对等关系



VPC peering – 注意事项

Region内可以引用对等 VPC 安全组的安全组规则

VPC 对等连接，DNS 可解析私有 IP 地址

对等连接支持 IPv4 & IPv6 地址

对等连接的 VPC 必须拥有互不重叠的 IP 范围

不能在相同两个 VPC 之间同时建立多个 VPC 对等连接

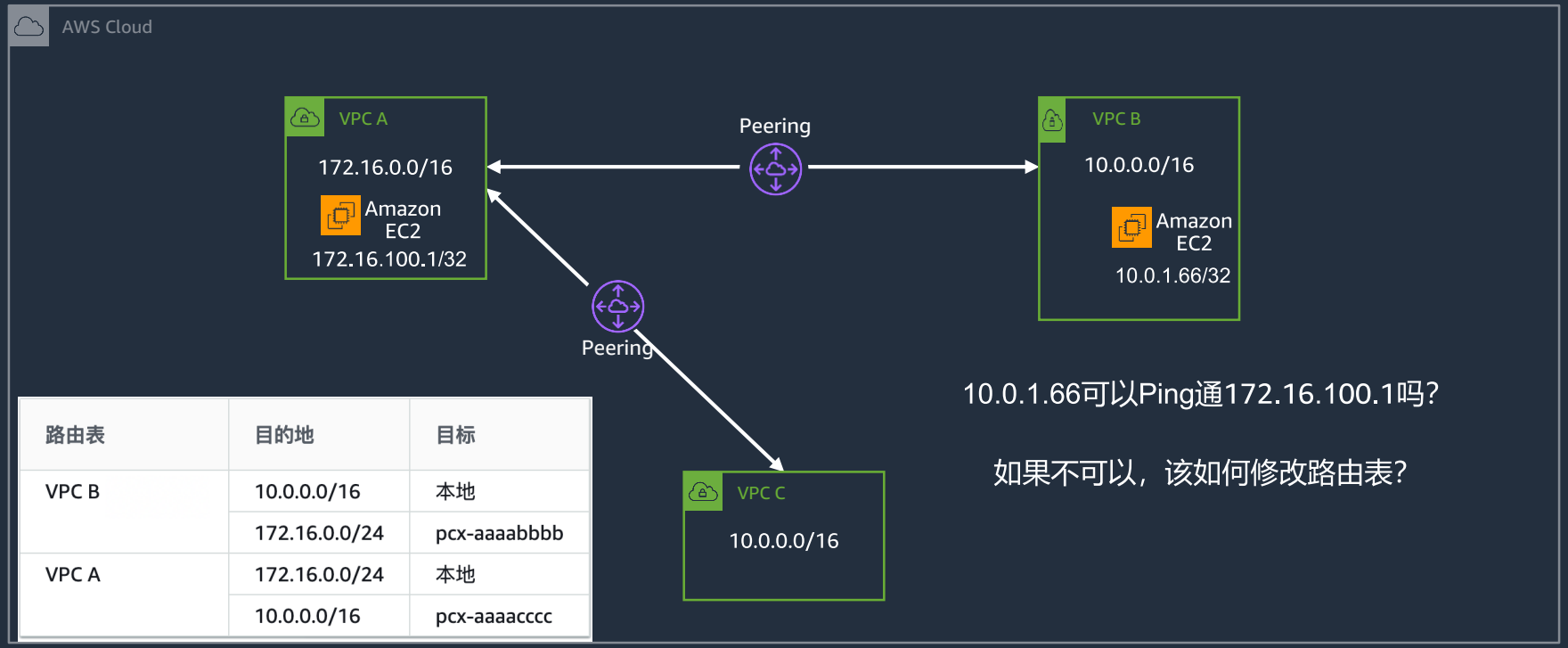
跨区域(Region)不允许传超大包jumbo frames

VPC peering 配额

资源	默认值	Comments
每个 VPC 的活动 VPC 对等连接	50	每个 VPC 的最大配额为 125 个对等连接
未完成的 VPC 对等连接请求	25	每账户
未接受的 VPC 对等连接请求的过期时间	1 周 (168 小时)	无法提高此配额

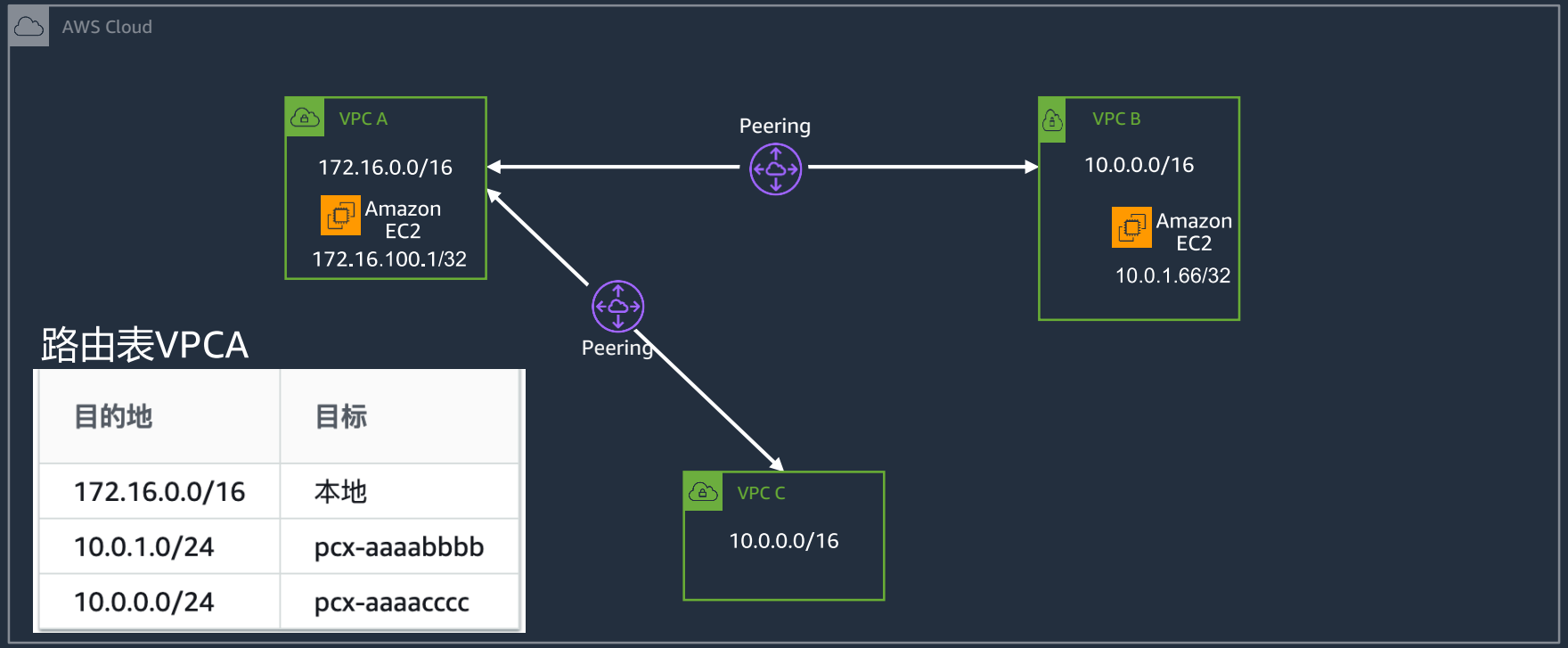
https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html

思考题



路由表	目的地	目标
VPC B	10.0.0.0/16	本地
	172.16.0.0/24	pcx-aaaabbbb
VPC A	172.16.0.0/24	本地
	10.0.0.0/16	pcx-aaaacccc

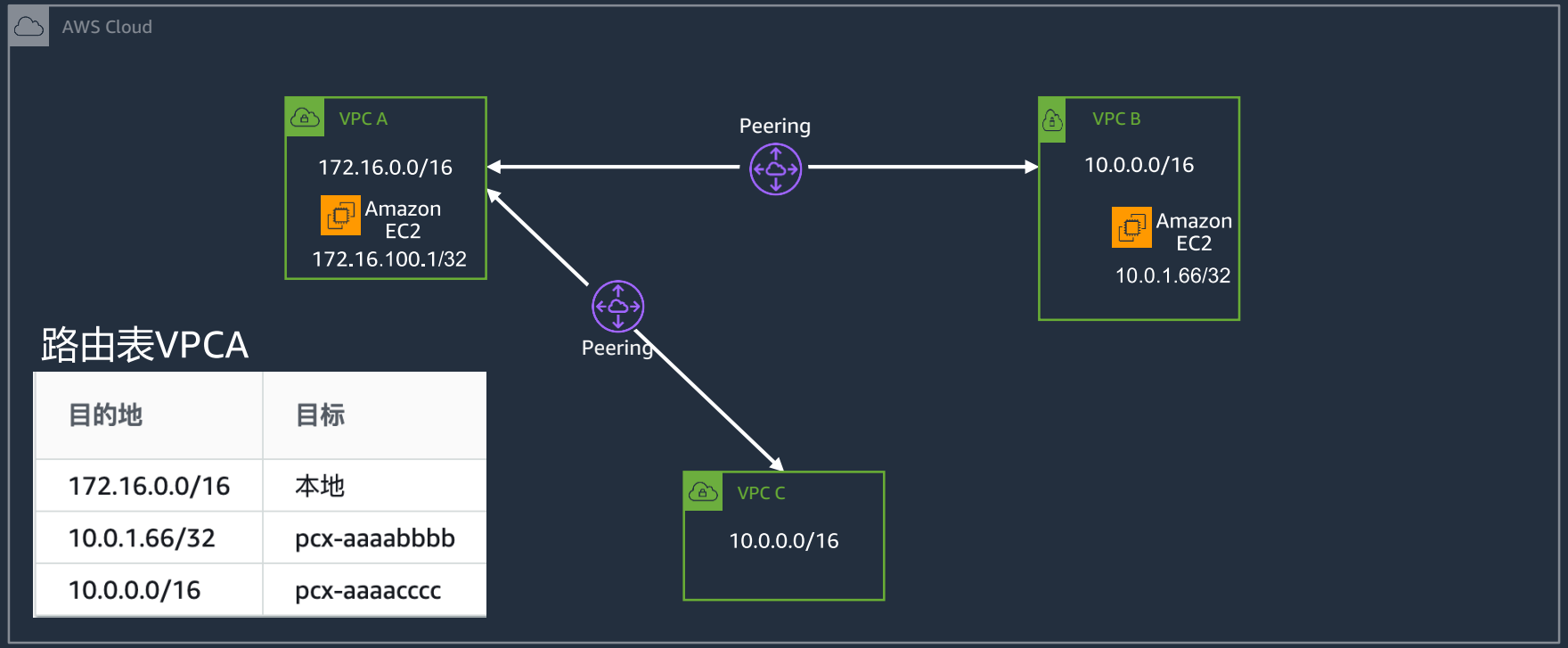
思考题



路由表VPCA

目的地	目标
172.16.0.0/16	本地
10.0.1.0/24	pcx-aaaabbbb
10.0.0.0/24	pcx-aaaacccc

思考题



路由表VPCA

目的地	目标
172.16.0.0/16	本地
10.0.1.66/32	pcx-aaaabbbb
10.0.0.0/16	pcx-aaaacccc

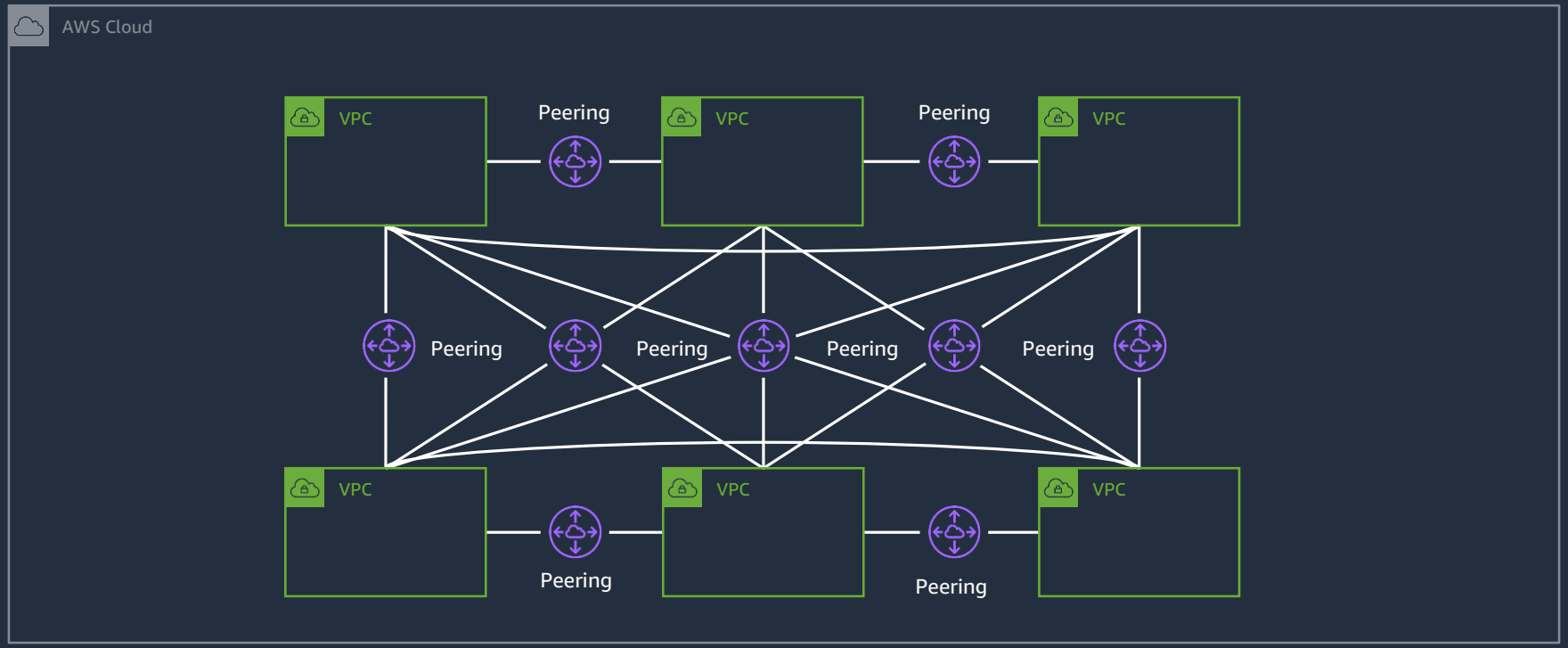
AWS Transit Gateway(中转网关)

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

AWS Transit Gateway

- AWS Transit Gateway (TGW)充当区域虚拟路由器，用于附件(attachments)之间的流量流动
- TGW可根据网络流量灵活地进行扩展
- TGW 可以简化连接
    - Amazon VPCs
    - 本地数据中心
    - 分支机构和办公室

多VPC互联peering遇到的困境



如果有10个VPC全互联，需要多少个Peering?

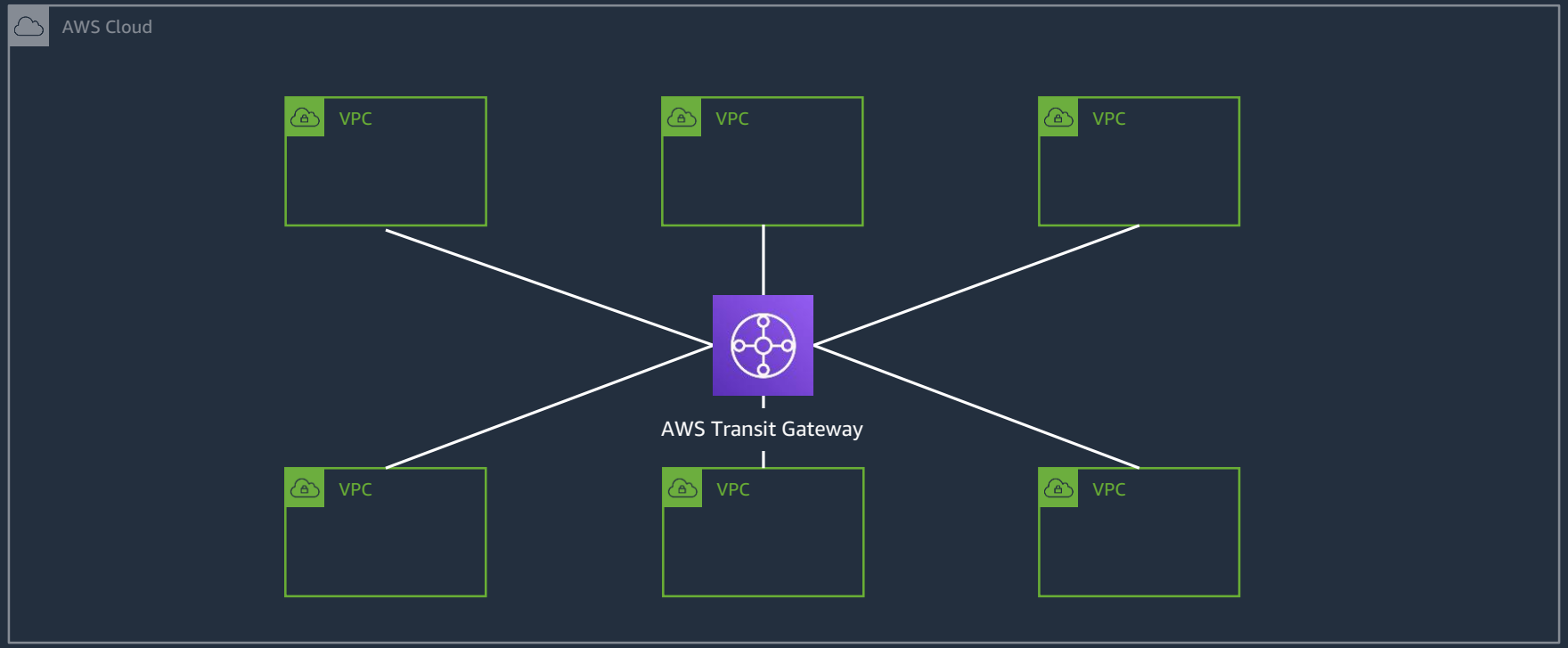
Full mesh: 需要多少个VPC Peering?

$$\frac{n(n-1)}{2}$$

n=10，peer总数45

n=100，peer总数4950

AWS Transit Gateway



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

Transit Gateway

Region级别路由器

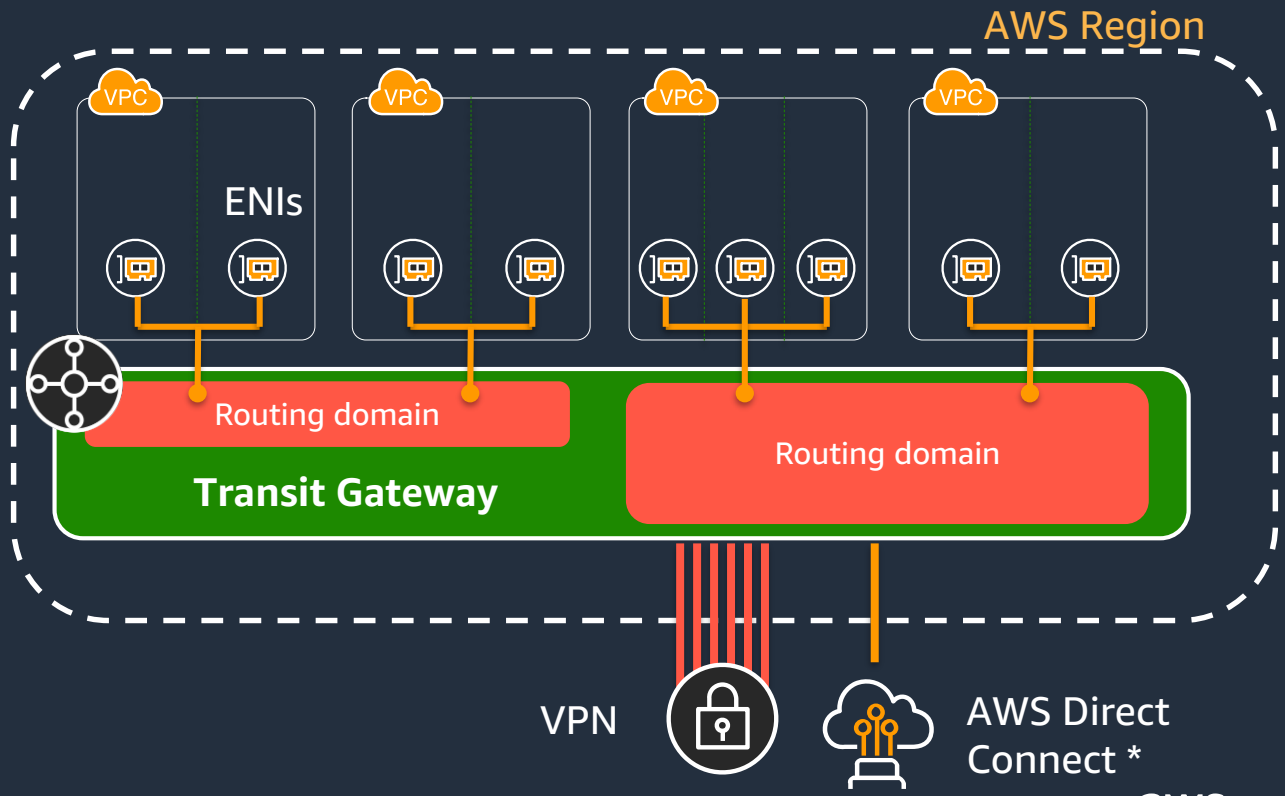
- 集中调度VPN、DXGW、VPC间流量

可扩展性强

- 支持上千 VPC
- 支持跨账户互联
- 支持多个 VPN连接

灵活的路由调度

- 通过配置路由表调度流量
- 多个路由表进行业务隔离



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

TGW 基本概念理解

TGW = Region级别设备

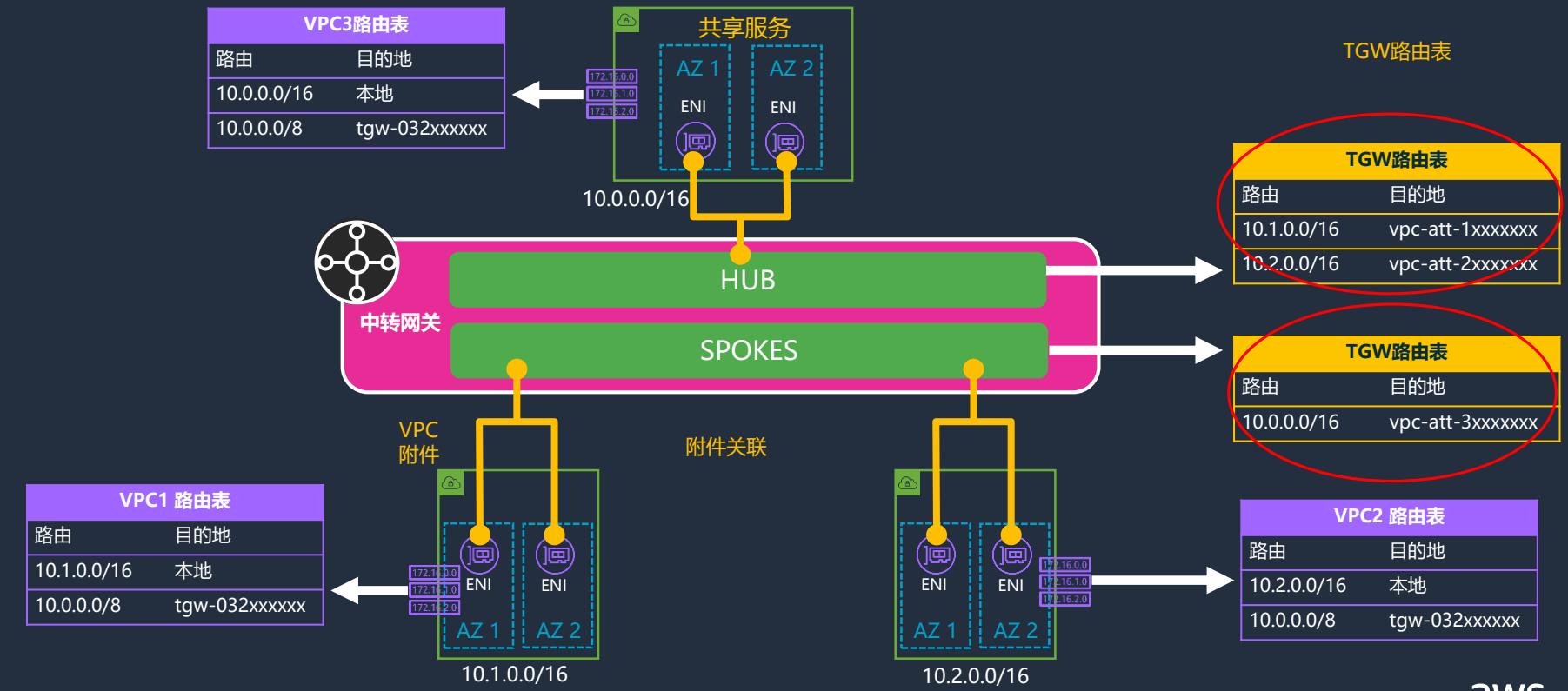
Attachment(附件)= VPN, VPC, DX Gateway and TGW

TGW association(关联) =每个附件与一个TGW路由表关联, 每个路由表可以与零到多个附件关联

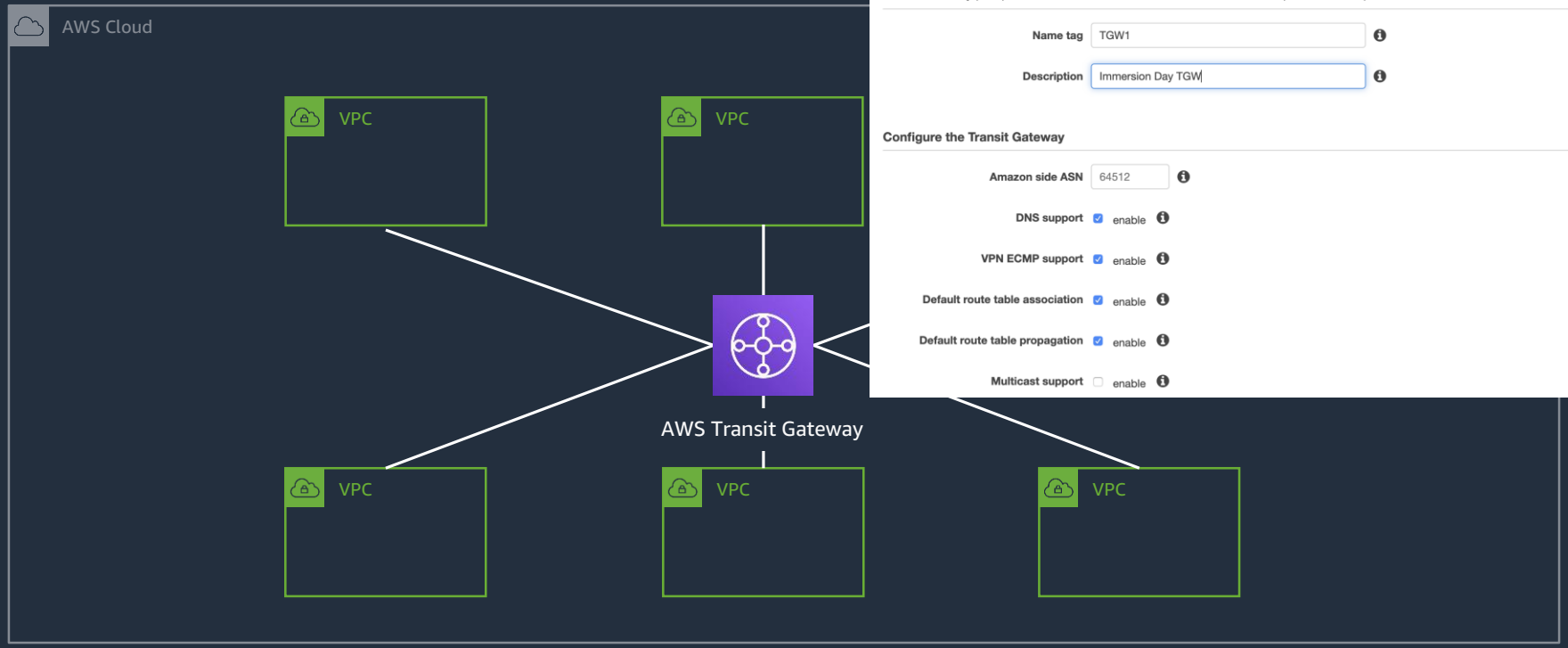
TGW路由表 = 定义数据包如何转发,可以是静态路由也可以是动态路由

TGW propagation = 把附件的子网传播到TGW路由表

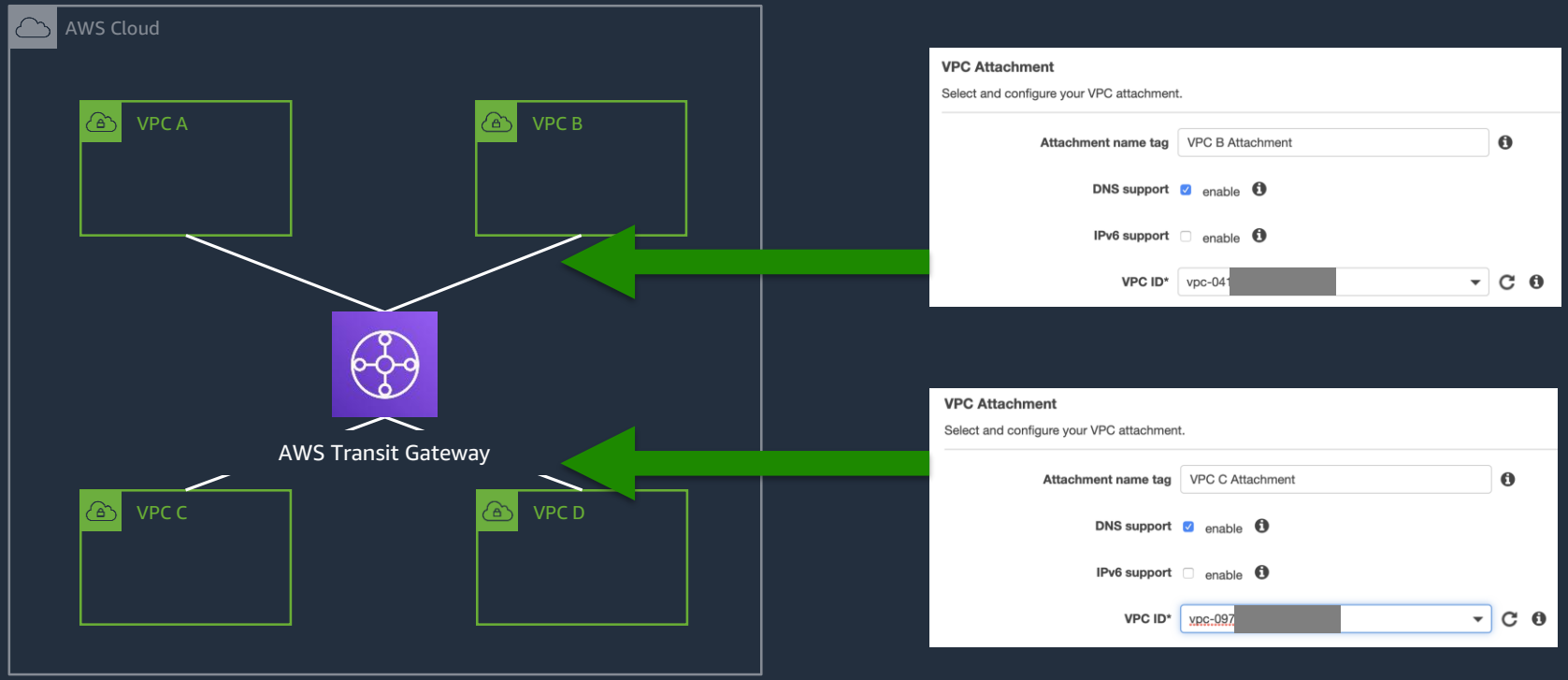
TGW 基本概念理解



创建AWS Transit Gateway

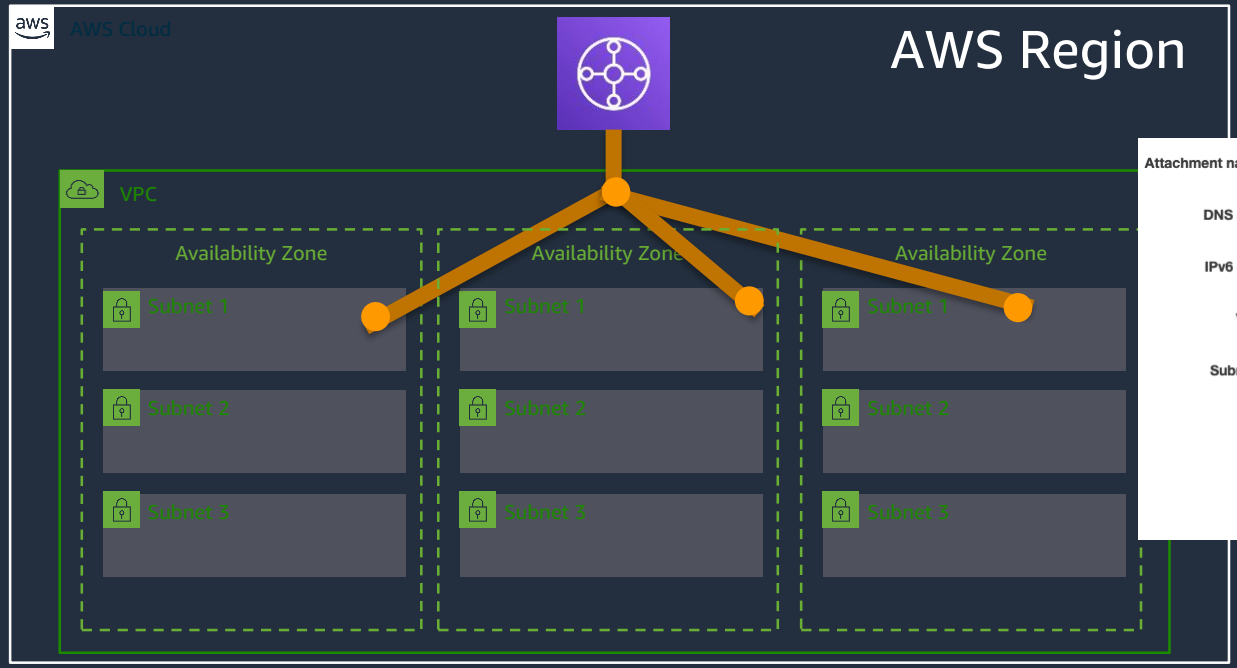


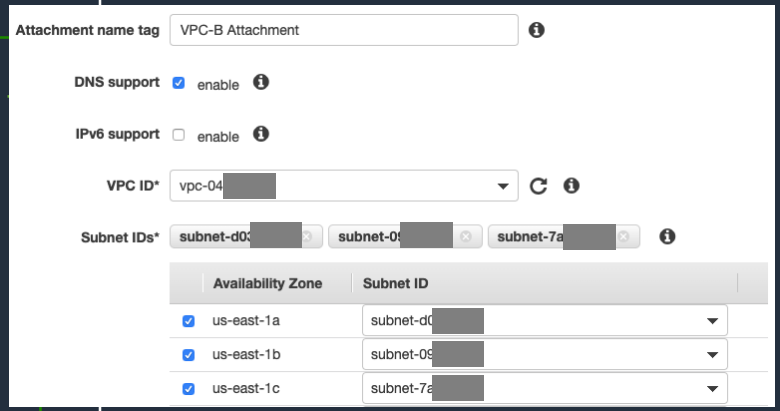
配置AWS Transit Gateway附件



TGW attachment

一个VPC附件可以扩展到多个AZ





最佳实践是VPC附件启用所有AZ

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

AWS Transit Gateway 附件

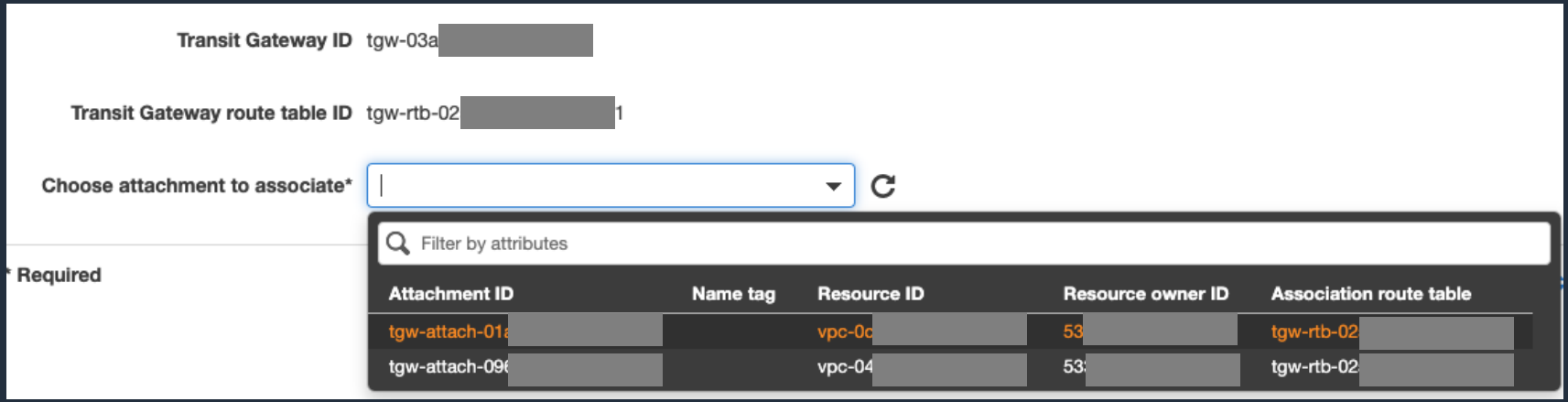
将以下资源附加到transit gateway：

- 一个或多个 VPC
- 一个或多个 VPN 连接
- 一个或多个 AWS Direct Connect 网关
- 一个或多个TGW Peering连接

*Note: 如果附加了*TGW Peering*连接，则 transit gateway 必须位于其他区域中。*

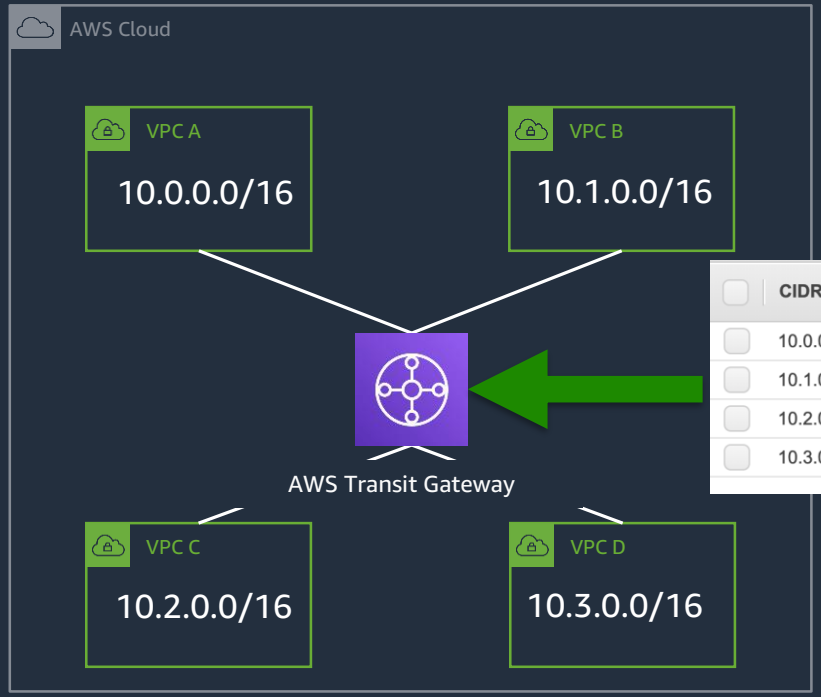
AWS Transit Gateway 关联

- 将transit gateway附件与单个路由表关联
- 允许流量从所在附件发到关联的路由表
- 一个附件只能关联到一个TGW路由表



AWS Transit Gateway 路由表

为每个已关联的附件配置路由表
入向流量根据匹配目标IP地址进行路由



CIDR	Attachment	Resource type	Route type	Route state
10.0.0.0/16	tgw-attach-05b7[redacted] | vpc-07566[redacted]	VPC	propagated	active
10.1.0.0/16	tgw-attach-0d48[redacted] | vpc-04144[redacted]	VPC	propagated	active
10.2.0.0/16	tgw-attach-0f26f[redacted] | vpc-09719[redacted]	VPC	propagated	active
10.3.0.0/16	tgw-attach-00f05[redacted] | vpc-0f3f10[redacted]	VPC	propagated	active

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

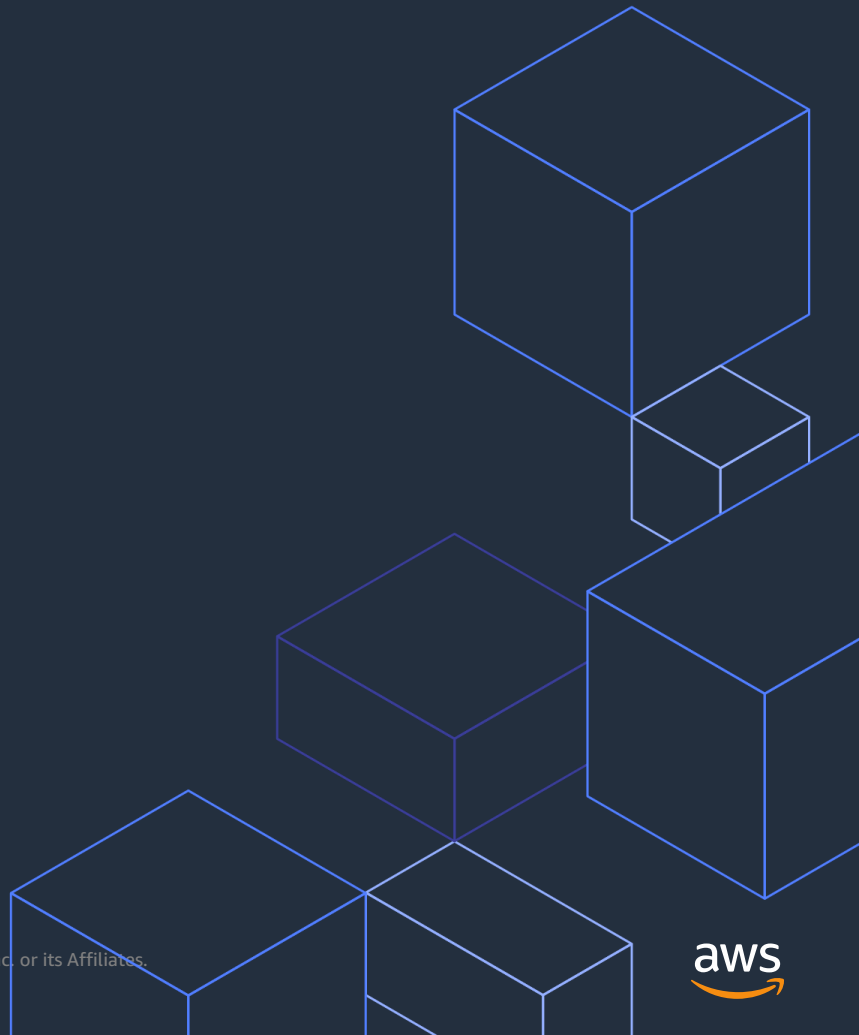
aws

AWS Transit Gateway - Performance and limits

Limit	Default
每个中转网关的Transit Gateway 挂载总数	5,000
每个 VPN 隧道的最大带宽	1.25 Gbps
每个 VPC、Direct Connect 网关或TGW对等连接的最大带宽	50 Gbps
每个账户在每个区域可创建的 AWS Transit Gateway 数量	5
每个VPC绑定的TGW数量	5
TGW的路由数量	10,000
每个 AWS Transit Gateway 的 Direct Connect 网关数量	20

Additional Information: https://aws.amazon.com/transit-gateway/faqs/

TGW 路由表



TGW Route Tables

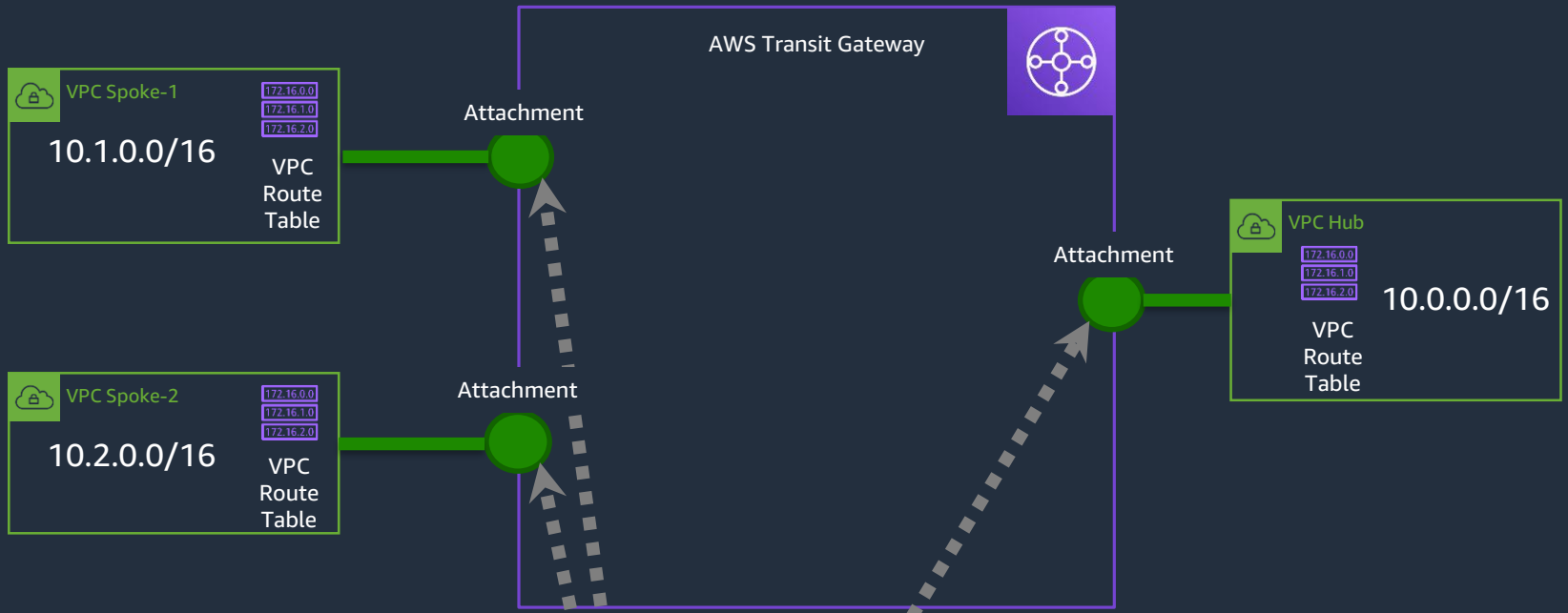
- TGW可以有多张路由表
- 概念类似于路由器和交换机的VRF/VPN instance
- 可以构建复杂拓扑，比如Hub & Spoke
- 可以通过路由传播(propagation)学习路由
- 可以自行配置静态路由和黑洞路由

TGW路由表

搭建Hub and Spoke解决方案

TGW路由表

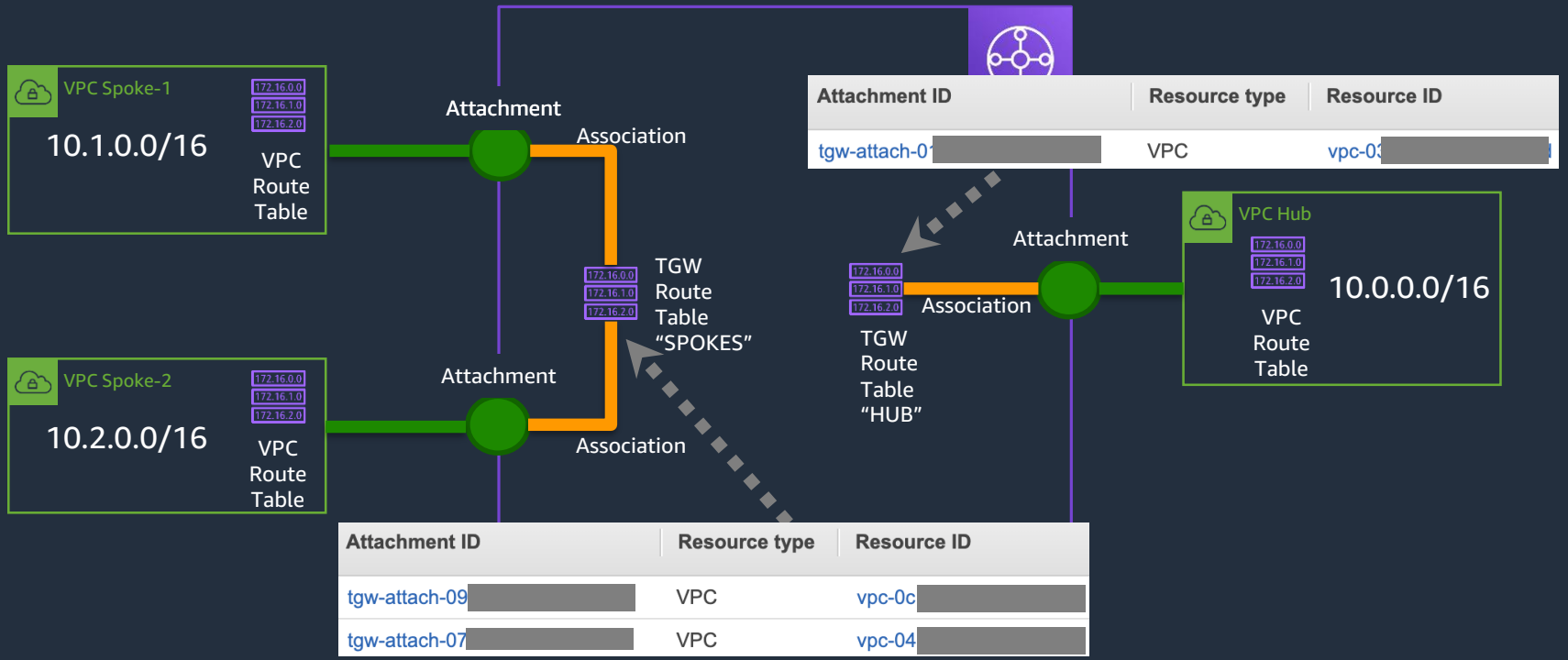
创建VPC附件



Name	Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID
Hub	tgw-attach-011[redacted]	tgw-032[redacted]	VPC	vpc-036[redacted]
Spoke-1	tgw-attach-09b[redacted]	tgw-032[redacted]	VPC	vpc-0c1[redacted]
Spoke-2	tgw-attach-072[redacted]	tgw-032[redacted]	VPC	vpc-043[redacted]

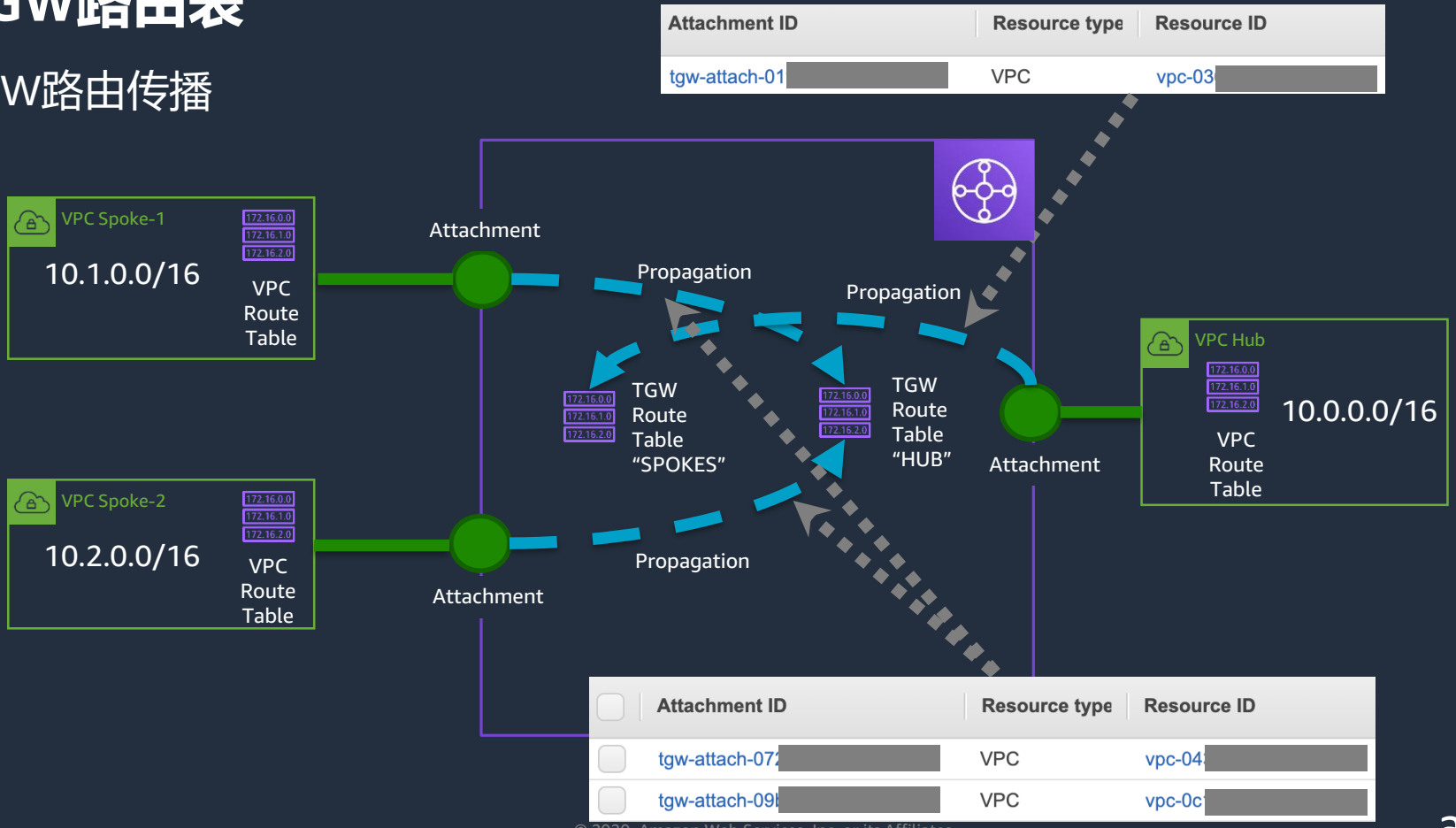
TGW路由表

将VPC附件关联到TGW路由表



TGW路由表

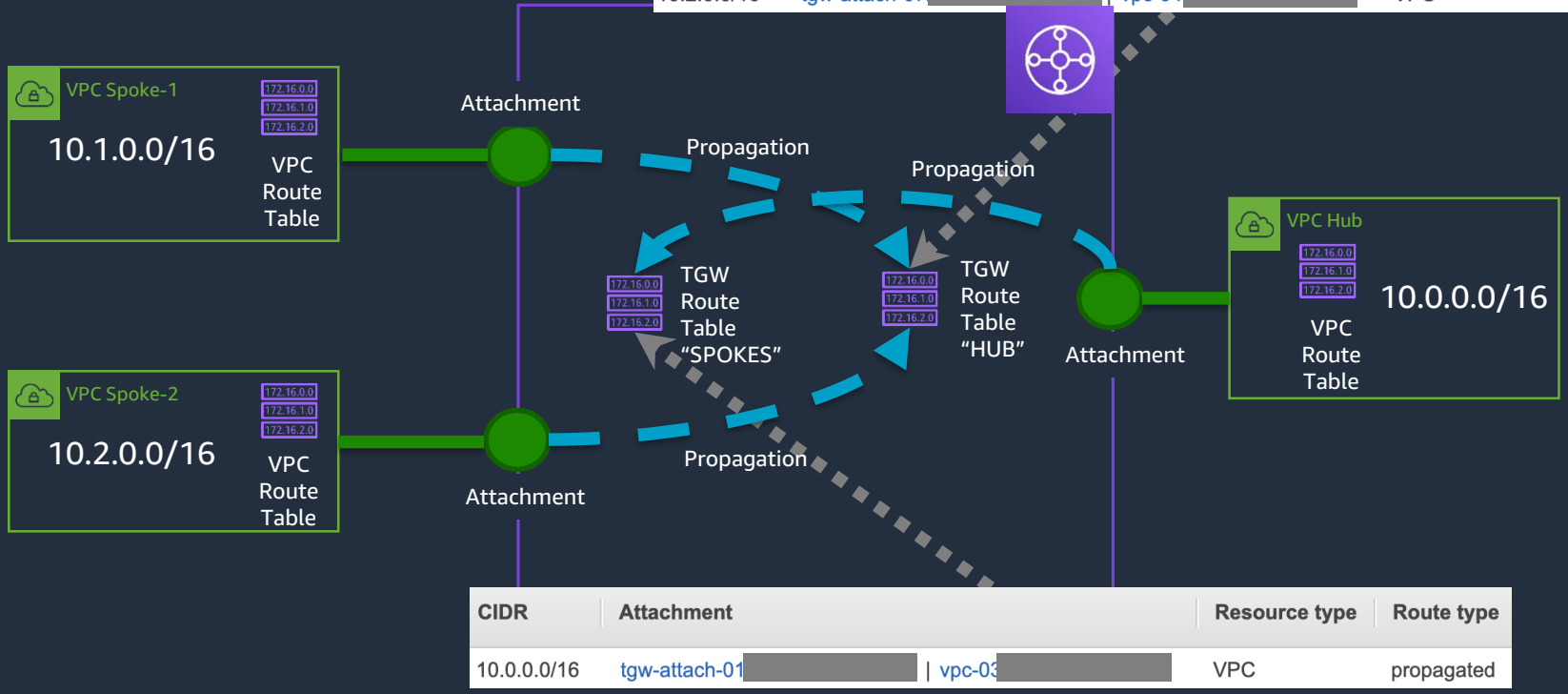
TGW路由传播



TGW路由表

TGW路由表生成

CIDR	Attachment	Resource type	Route type
10.1.0.0/16	tgw-attach-09[redacted] | vpc-0c[redacted]	VPC	propagated
10.2.0.0/16	tgw-attach-07[redacted] | vpc-04[redacted]	VPC	propagated

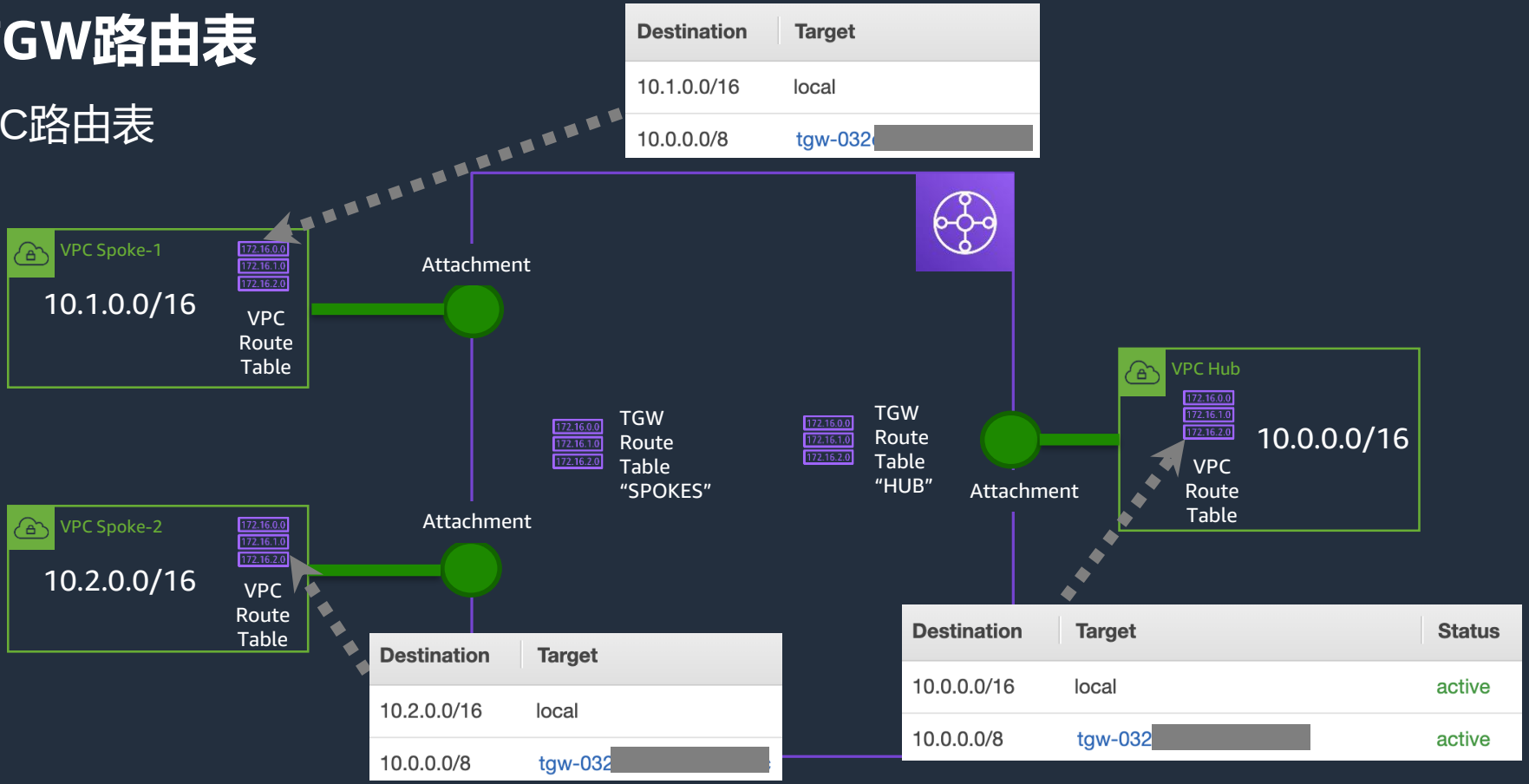


CIDR	Attachment	Resource type	Route type
10.0.0.0/16	tgw-attach-01[redacted] | vpc-03[redacted]	VPC	propagated

aws

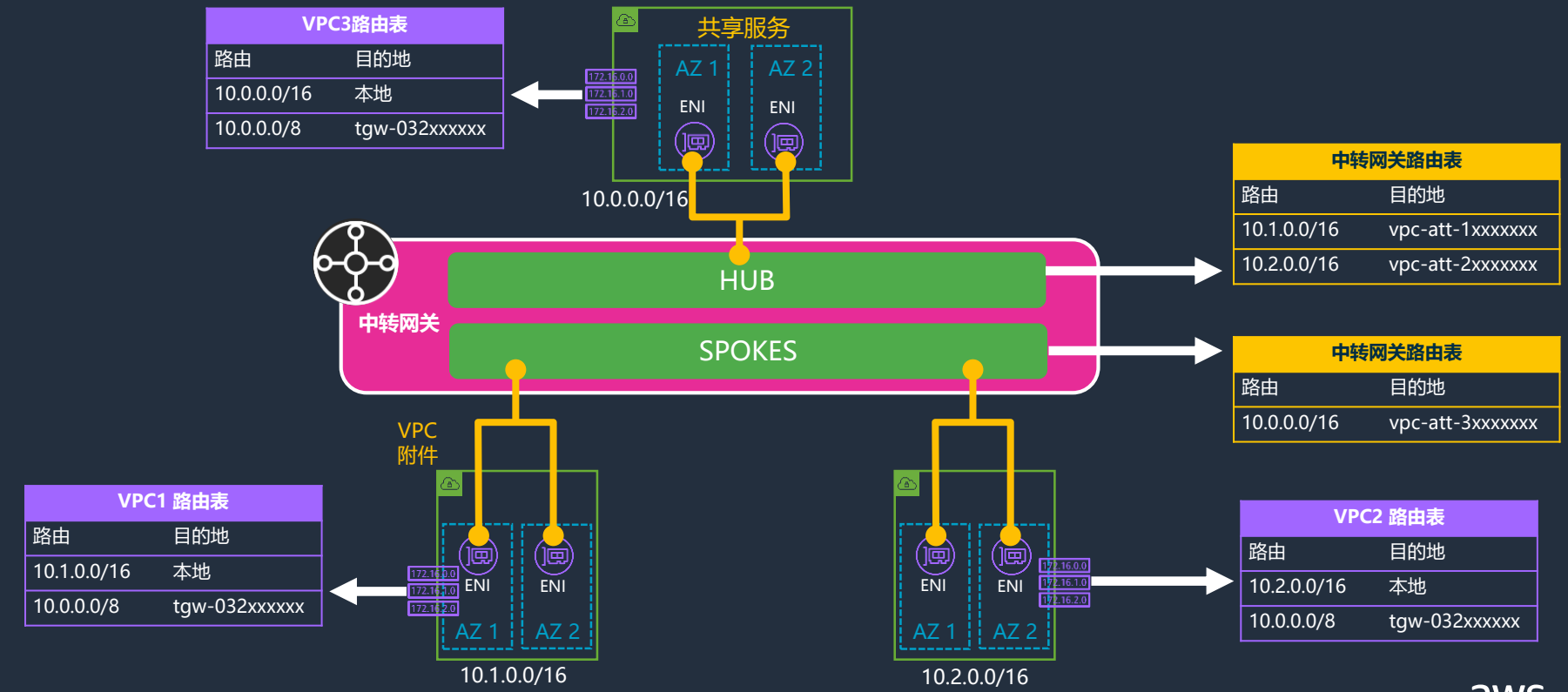
TGW路由表

VPC路由表



aws

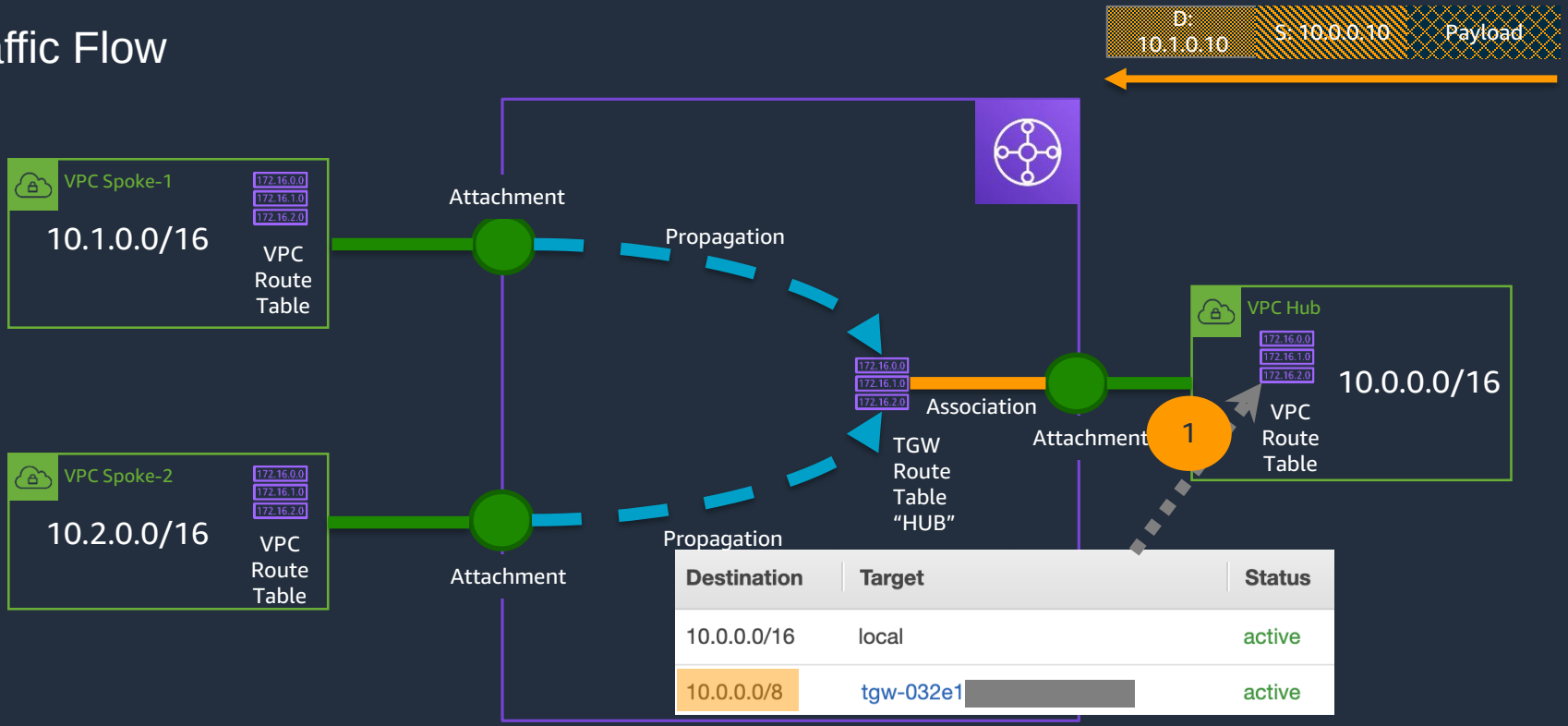
Hub & Spoke方案



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

TGW路由表

Traffic Flow

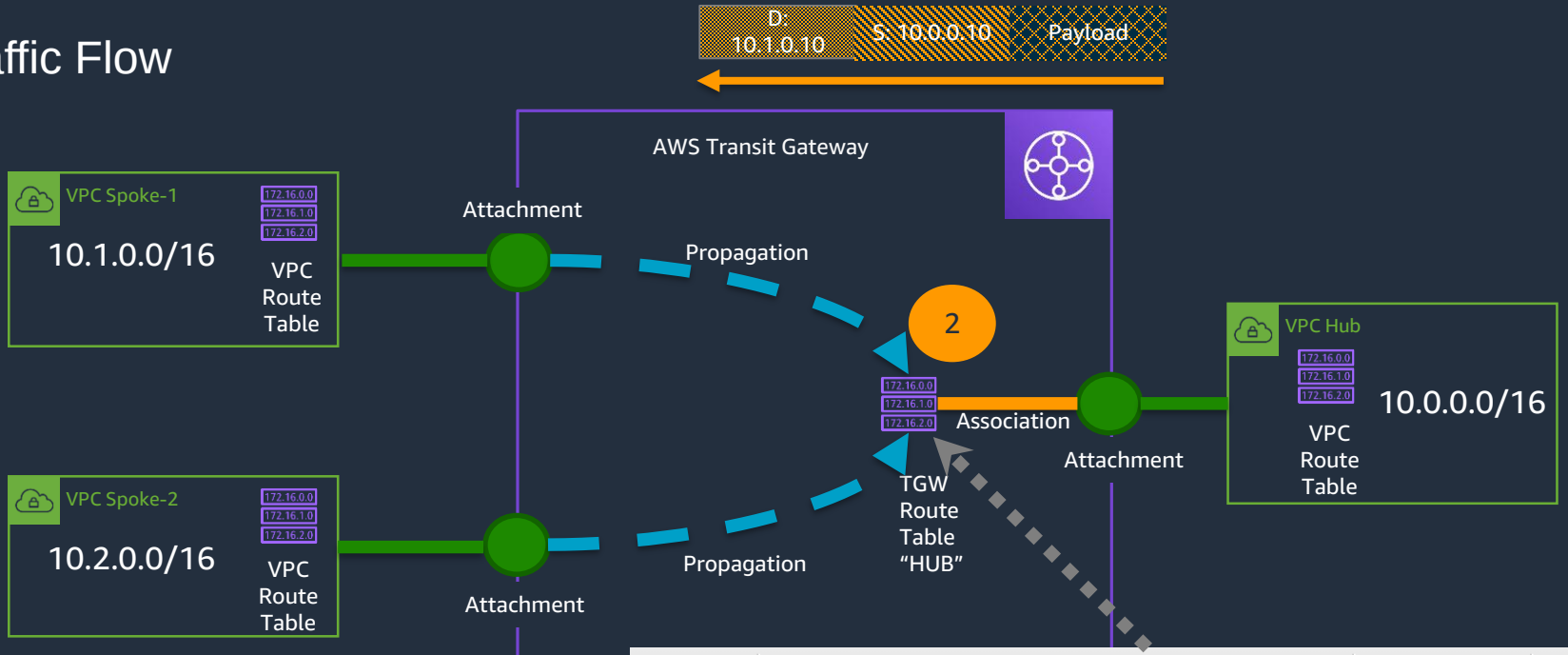


Destination	Target	Status
10.0.0.0/16	local	active
10.0.0.0/8	tgw-032e1[redacted]	active

aws

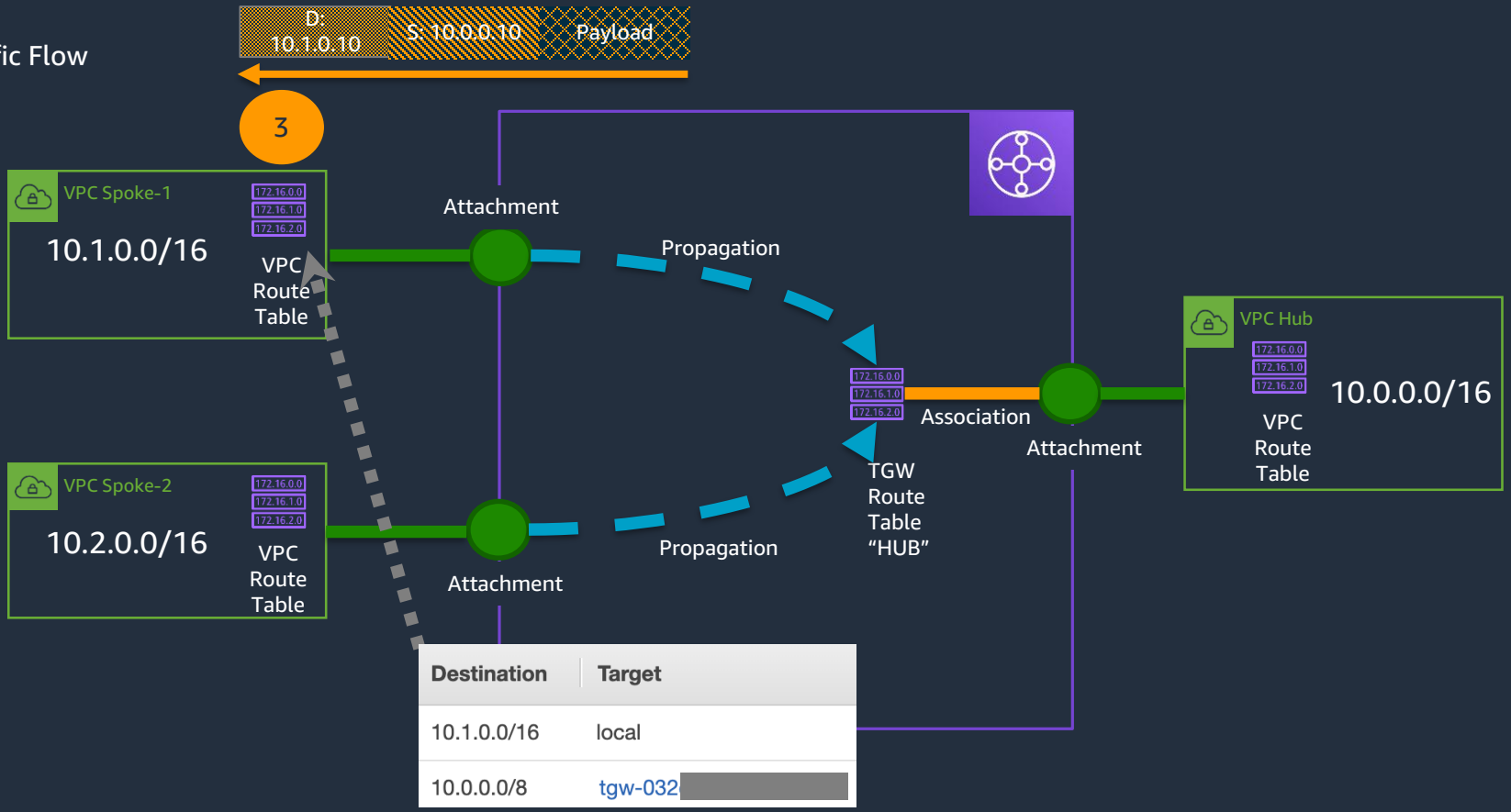
TGW路由表

Traffic Flow

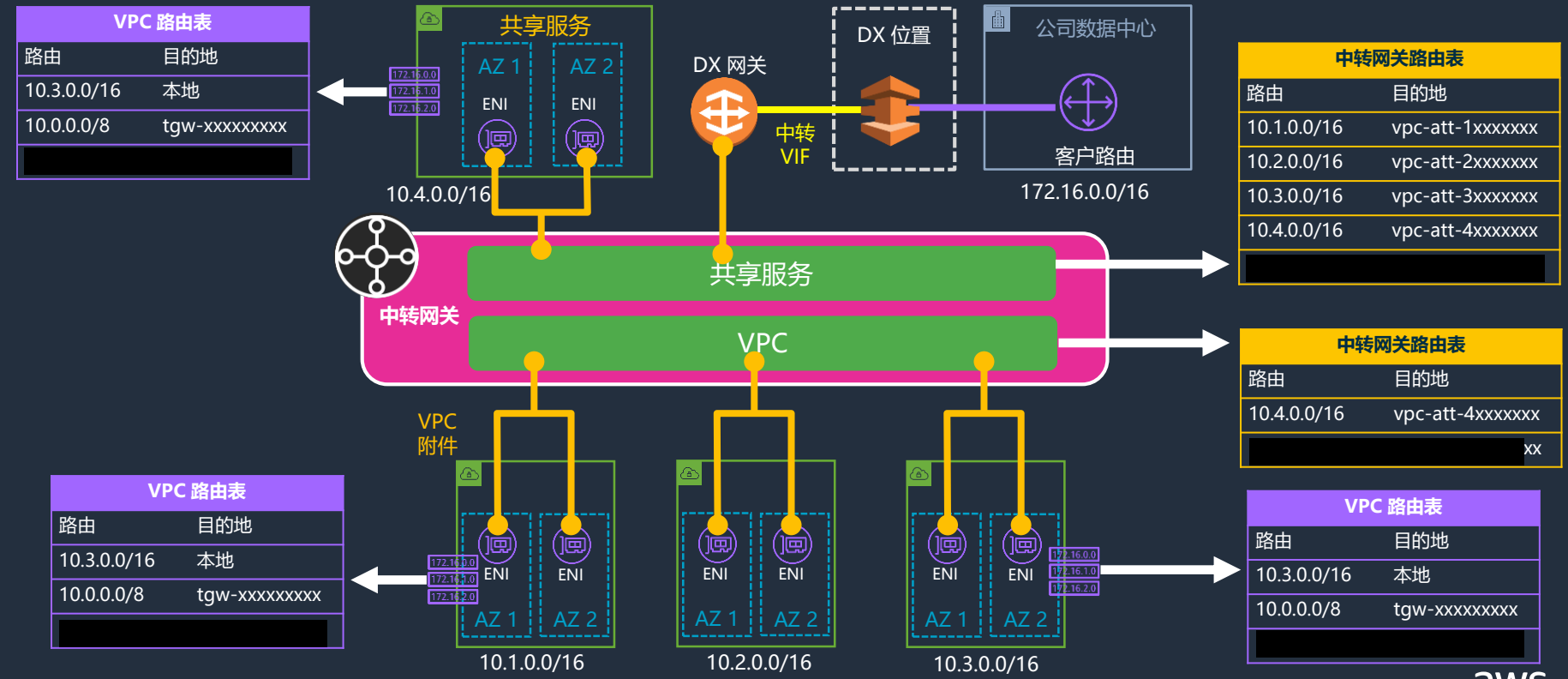


CIDR	Attachment	Resource type	Route type
10.1.0.0/16	tgw-attach-09[redacted] | vpc-0c[redacted]	VPC	propagated
10.2.0.0/16	tgw-attach-07[redacted] | vpc-04[redacted]	VPC	propagated

TGW路由表

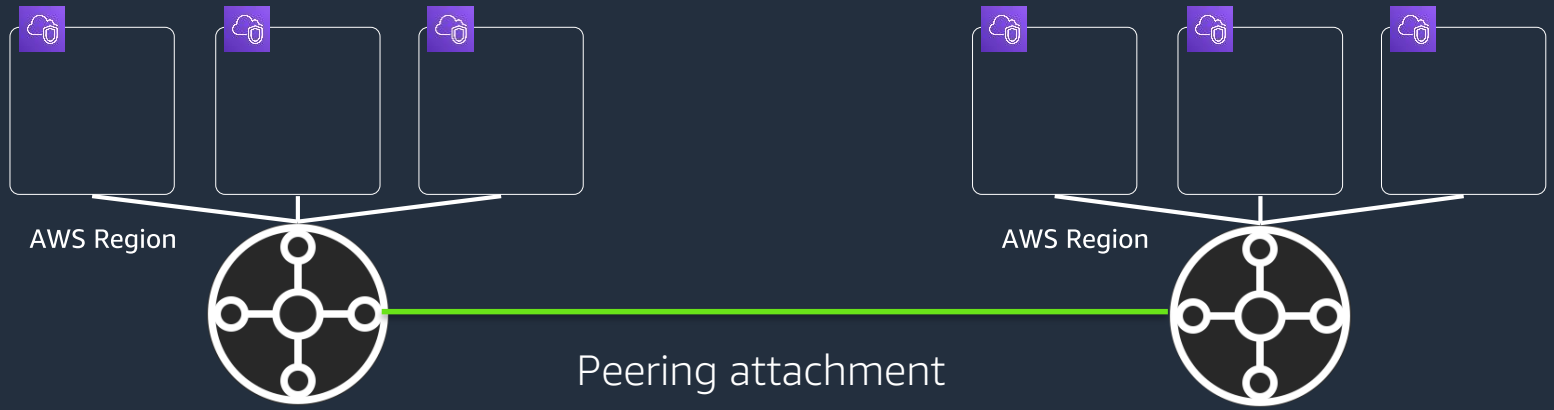


利用 TGW 的 Direct Connect 网关



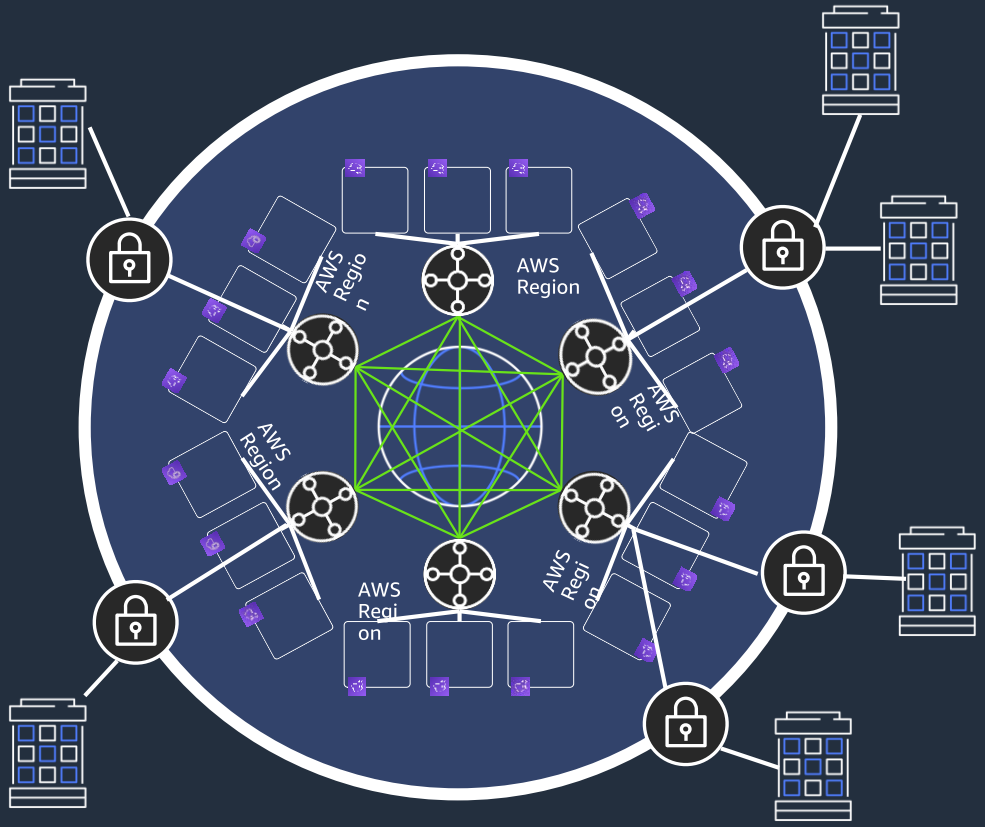
AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

跨区域的Transit Gateway对等连接



- 跨越区域的所有流量加密
- 不允许在相同区域内建立TGW对等连接

使用Transit Gateway部署全球化网络



充分利用AWS全球骨干网

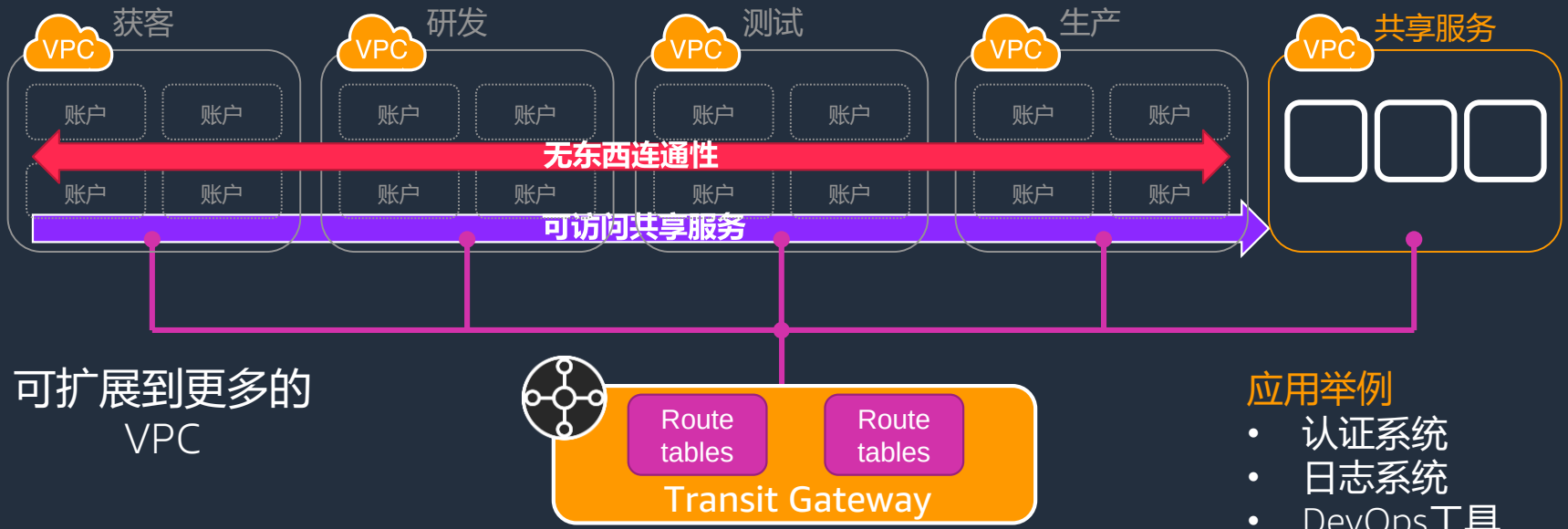
结合AWS VPN和DX产品联合使用

更低的延迟，更少的抖动，一致的连接

分支机构、云上云下的统一架构

aws

使用TGW的共享服务(云内)



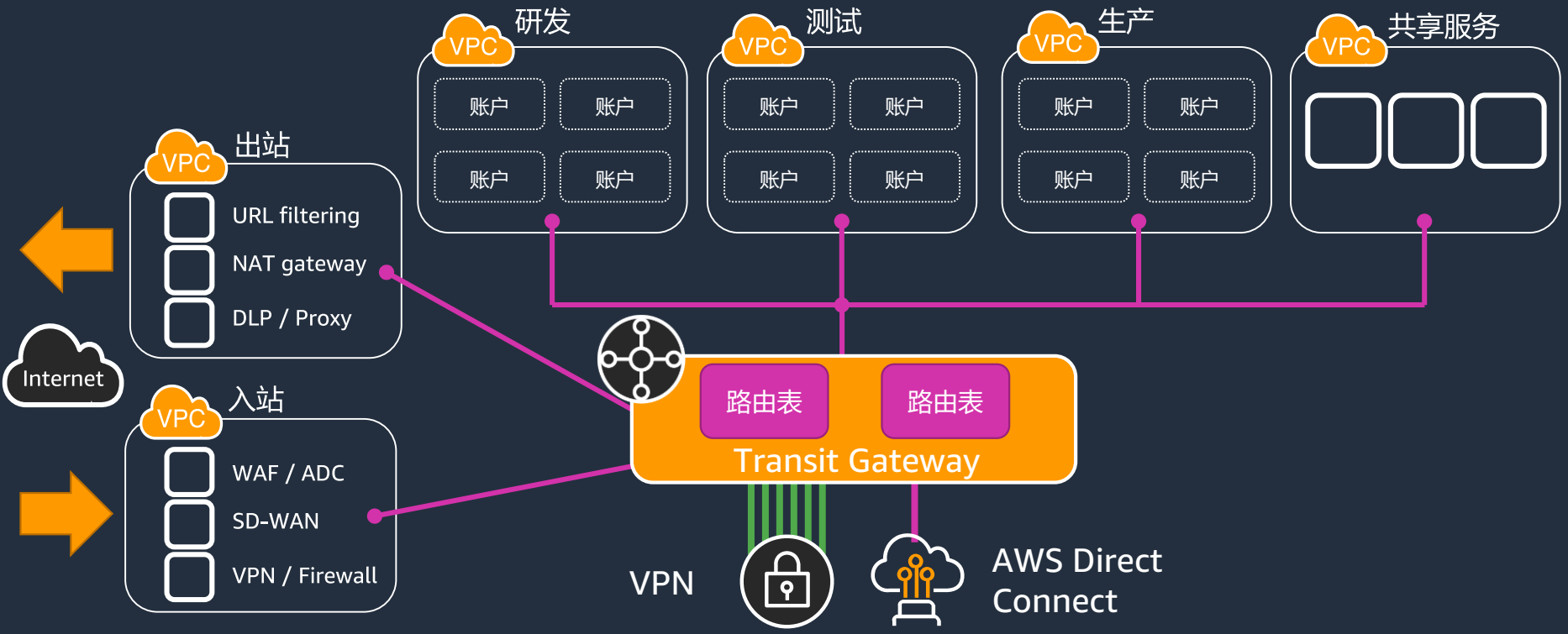
可扩展到更多的
VPC

应用举例

- 认证系统
- 日志系统
- DevOps工具
- 安全性资源

aws

使用TGW的共享服务(出入云)

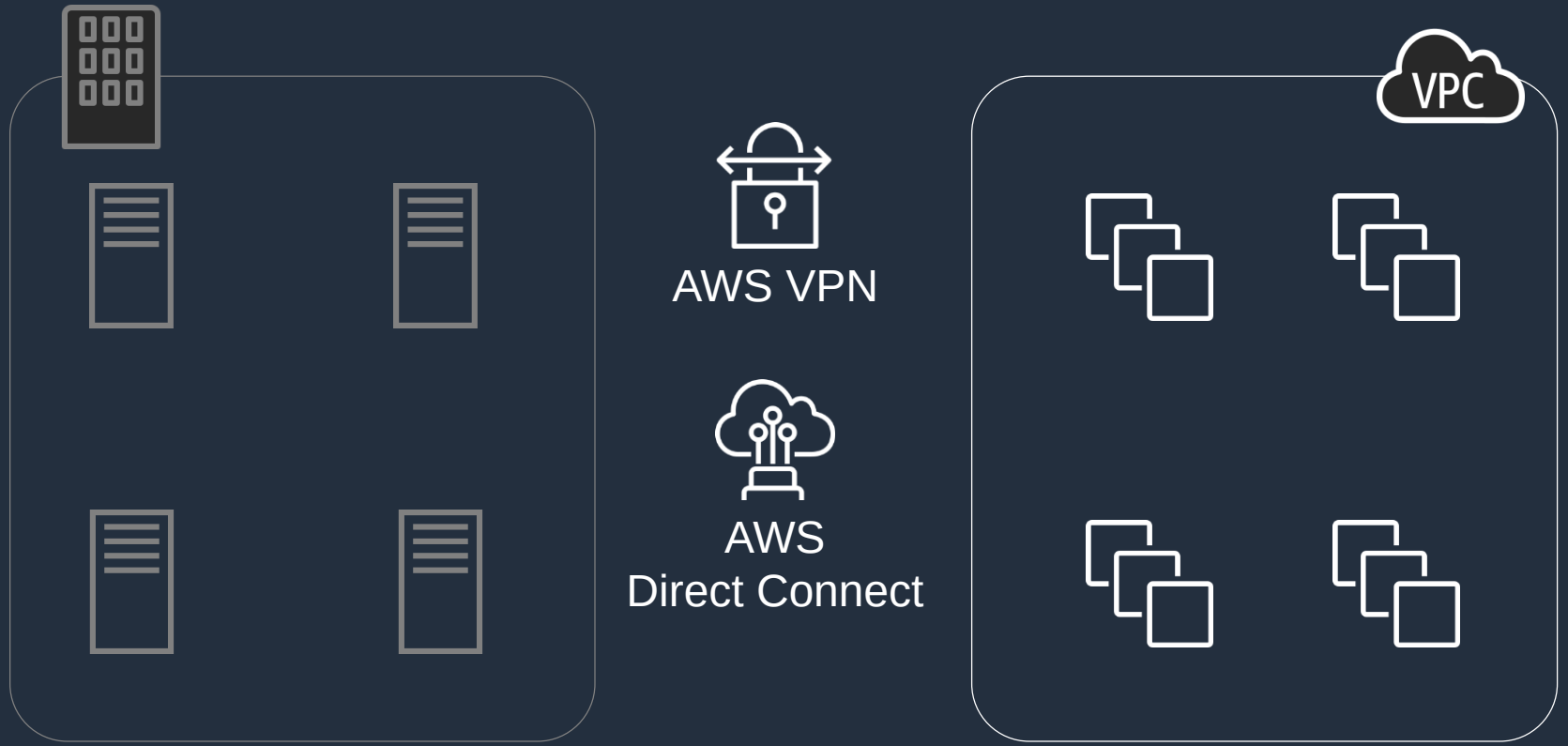


aws

DX和Site to Site VPN

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

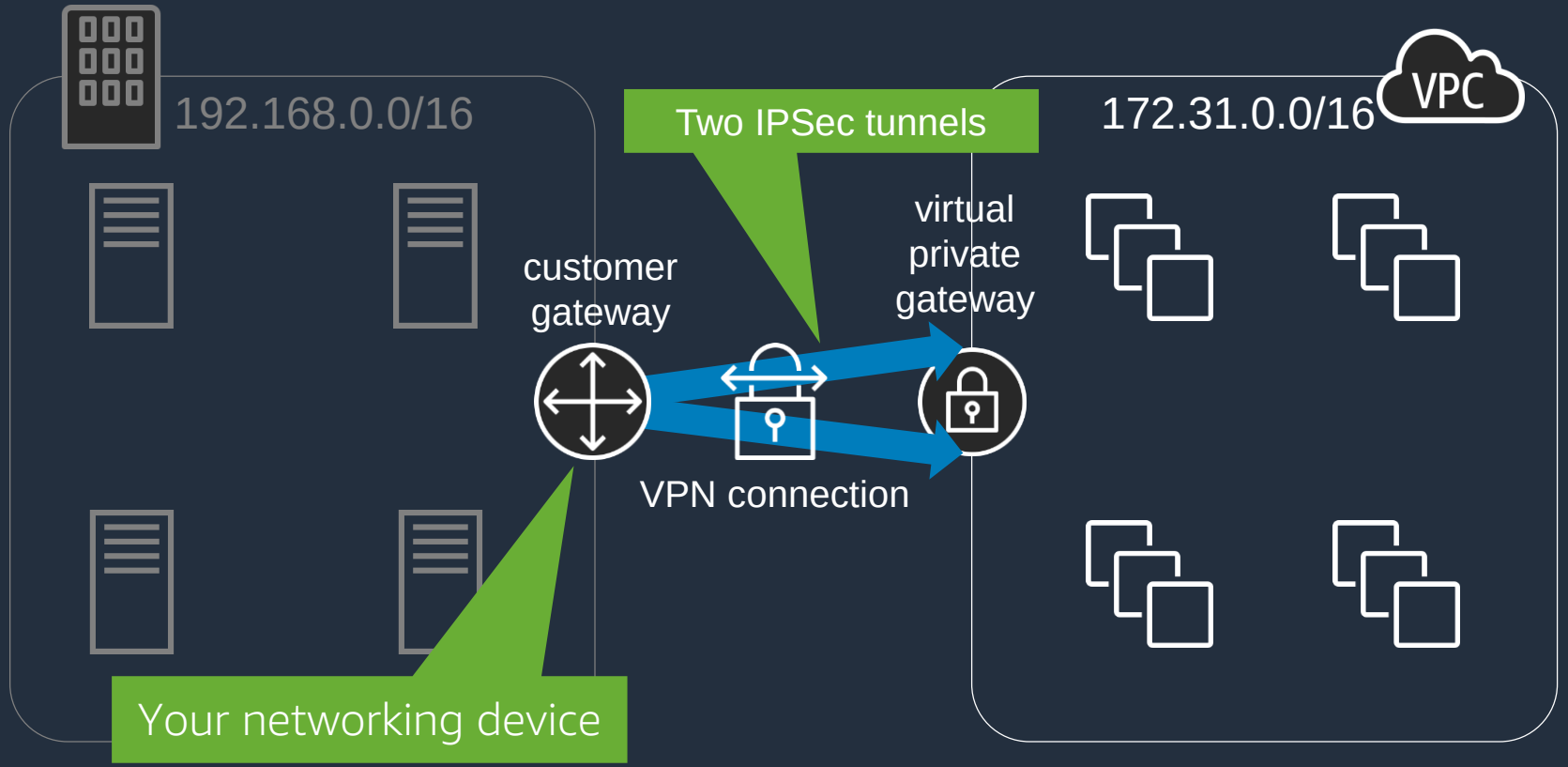
本地网络与 AWS VPC 接入



AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

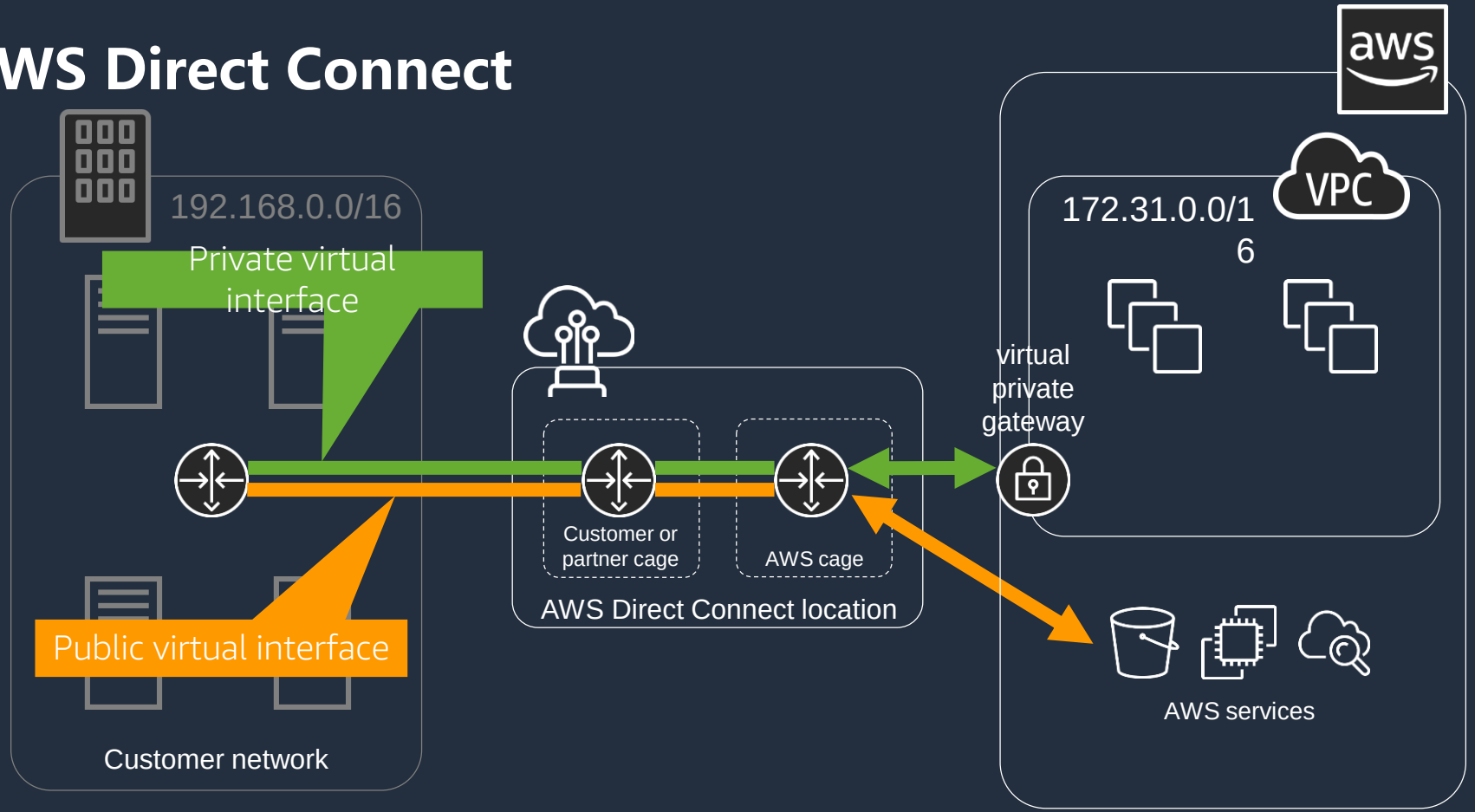
aws

AWS Site-to-Site VPN

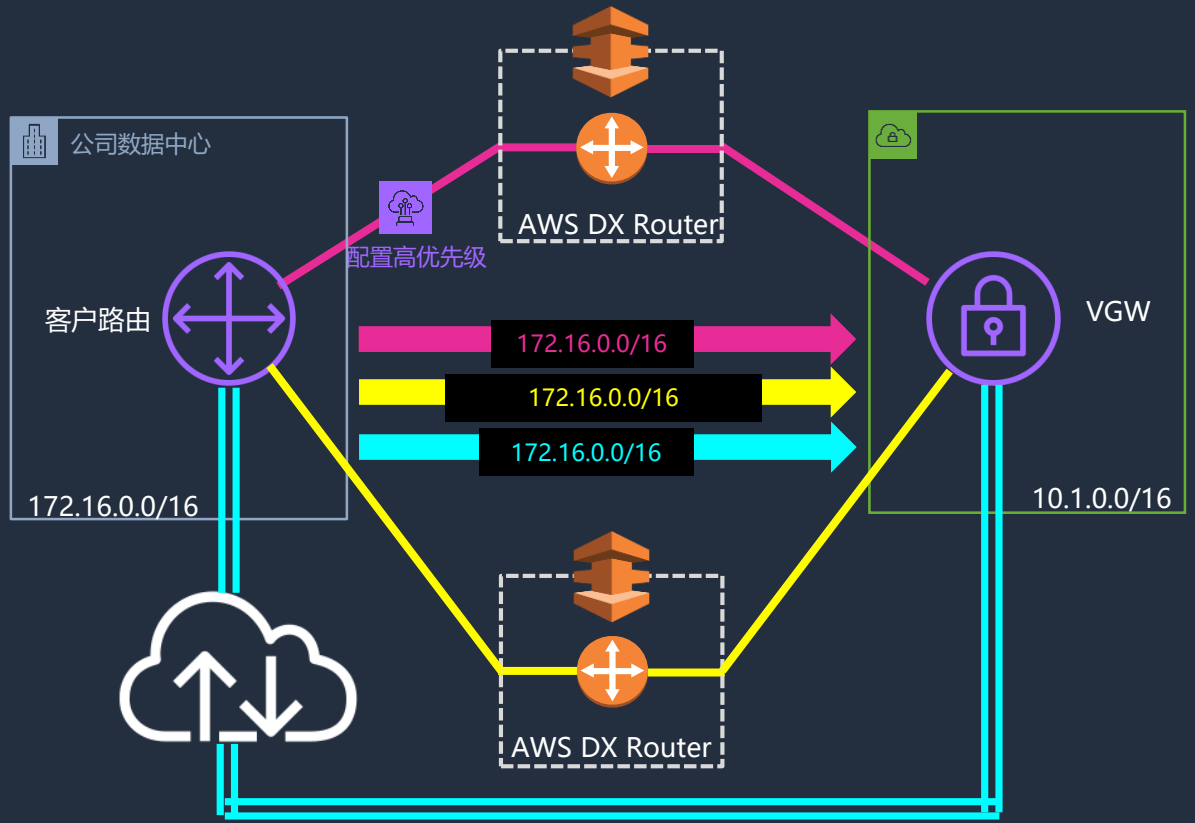


aws

AWS Direct Connect



AWS Direct Connect + VPN 备份



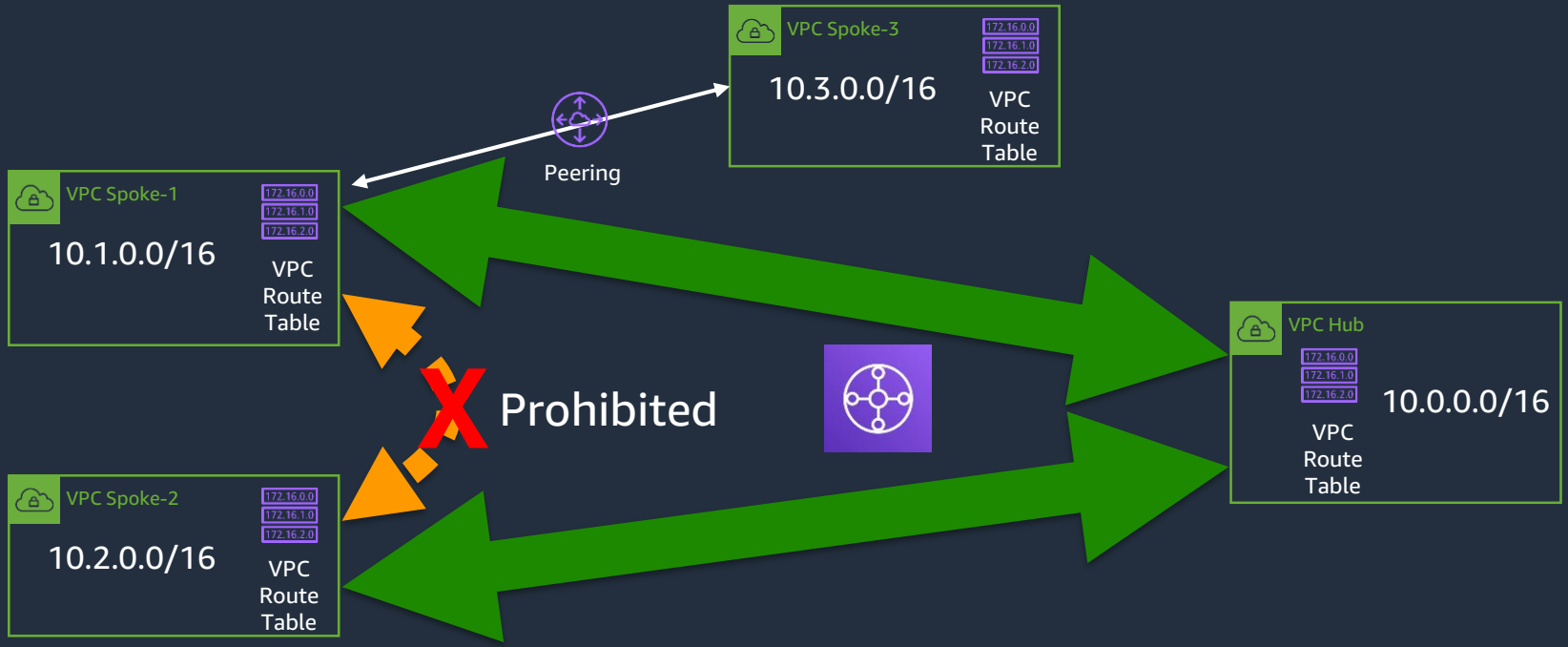
AWS 路由优先选择

- 1st – 本地路由至 VPC
- 2nd – 最长的前缀匹配
- 3rd – 相较于动态路由，优先选择静态路由
- 4th – 动态路由
  - 优先选择 DX BGP 路由
  - VPN 静态路由
  - 来自 VPN 的 BGP 路由

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营

实验环节

搭建Hub and Spoke解决方案



aws

实验任务

1 VPC Spoke-1内的EC2 可以和VPC Spoke-3内的EC2 通信

2 VPC Spoke-1内的EC2 不可以和VPC Spoke-2内的EC2 通信

2 VPC Spoke-1和VPC Spoke-2内的EC2 可以和VPC Hub内的EC2 通信

实验环境

VPC Name	VPC CIDR block	Subnets in Availability Zone	Subnets CIDR block	EC2 Name
VPC Hub	10.0.0.0/16	VPC Hub-sub-1a in AZ1	10.0.0.0/24	hub-sub-1a
		VPC Hub-sub-1b in AZ2	10.0.1.0/24	/
VPC Spoke-1	10.1.0.0/16	VPC Spoke-1-sub-1a in AZ1	10.1.0.0/24	spoke1-sub-1a
		VPC Spoke-1-sub-1b in AZ2	10.1.1.0/24	/
VPC Spoke-2	10.2.0.0/16	VPC Spoke-2-sub-1a in AZ1	10.2.0.0/24	spoke2-sub-1a
		VPC Spoke-2-sub-1b in AZ2	10.2.1.0/24	/
VPC Spoke-3	10.3.0.0/16	VPC Spoke-3-sub-1a in AZ1	10.3.0.0/24	spoke3-sub-1a
		VPC Spoke-3-sub-1b in AZ2	10.3.1.0/24	/

Thank You!

AWS 中国（宁夏）区域由西云数据运营
AWS 中国（北京）区域由光环新网运营