AWS Summit

AWS技术峰会2015 · 上海

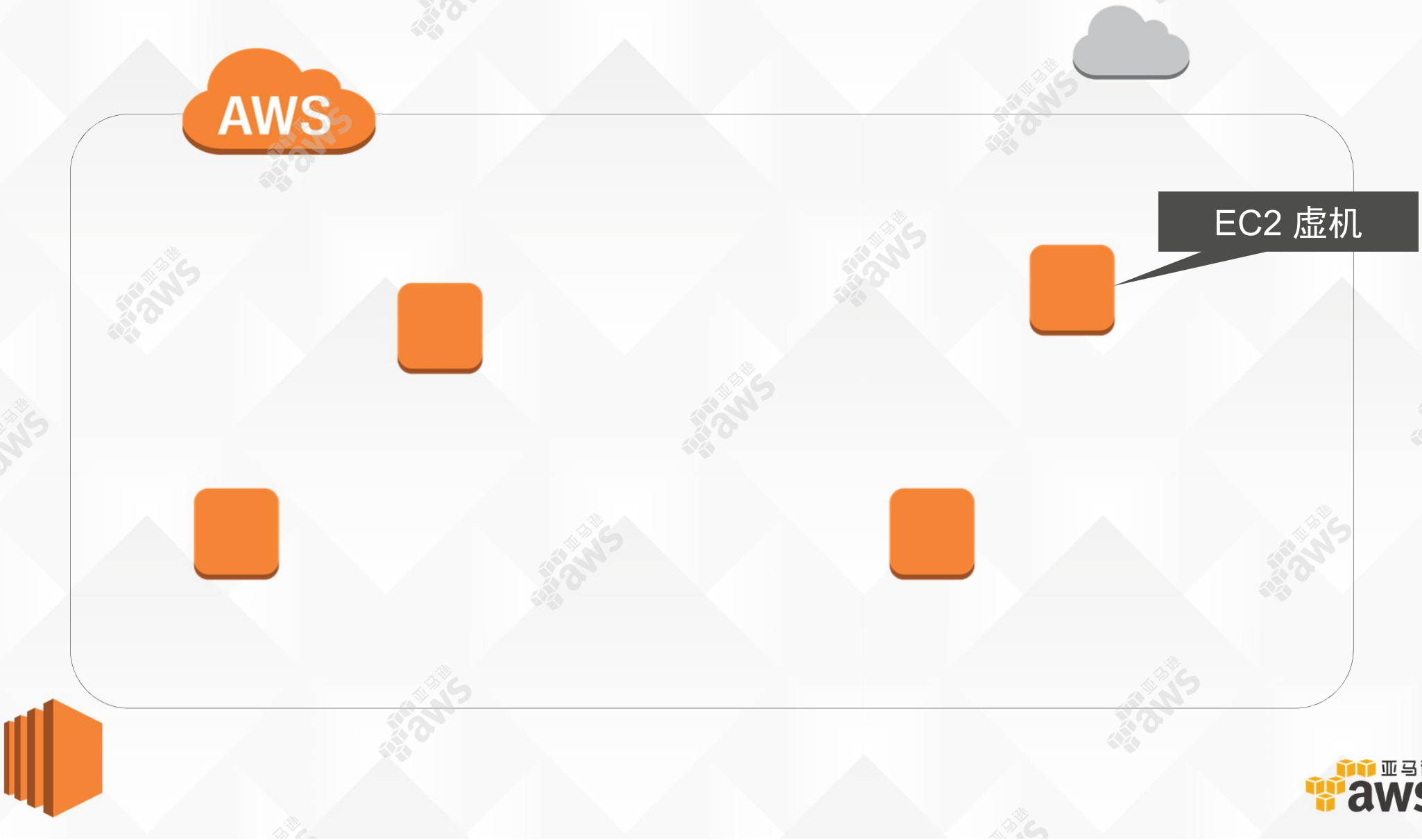
亚马逊 aws

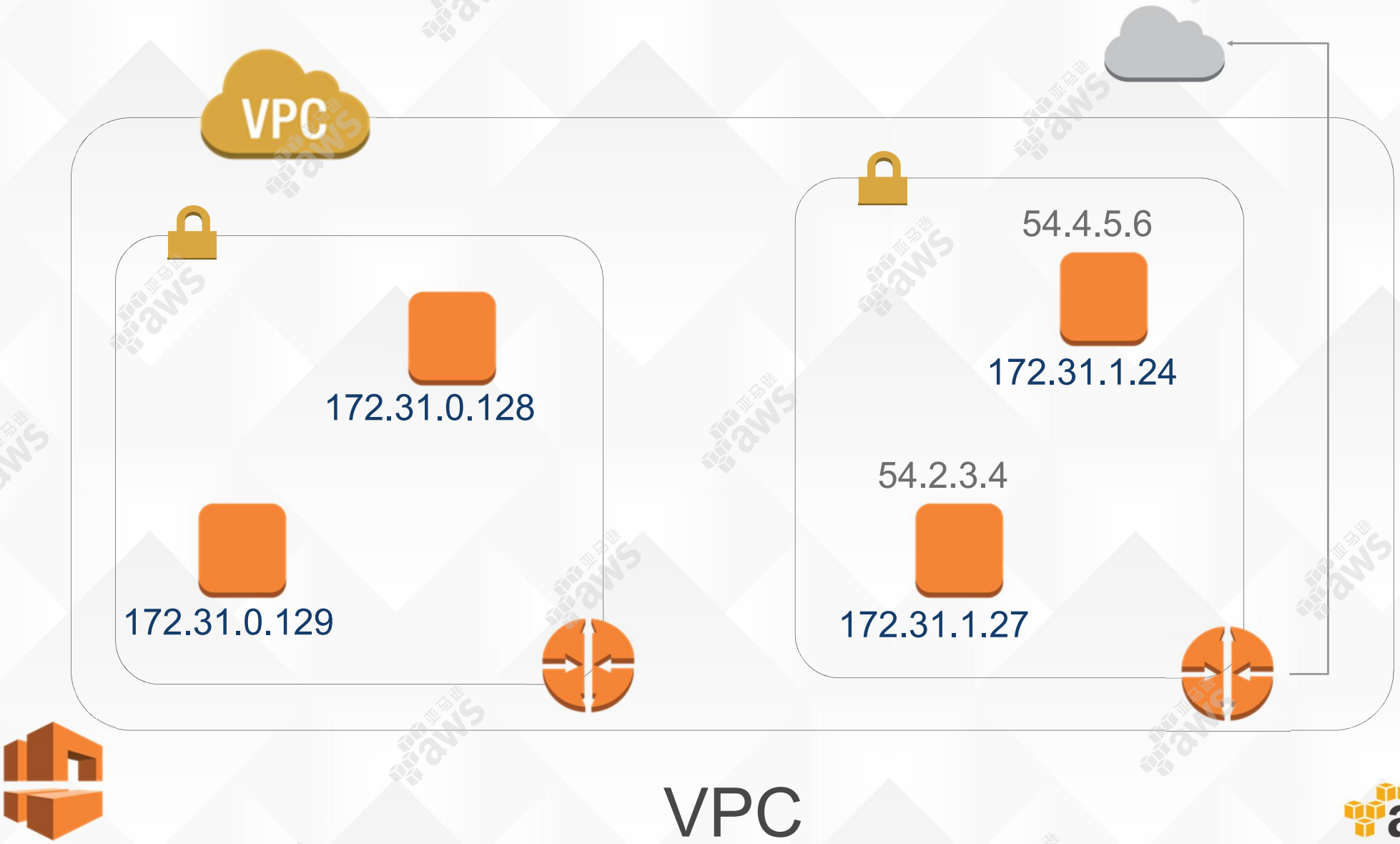
创建你的虚拟数据中心

VPC 基础

AWS 技术销售部 陈耀炜

2015-12-17


AWS
EC2 虚机



VPC

我们会涵盖的内容

- 熟悉VPC的概念
- 建立一个基本VPC的流程

流程:建立一个互联网联通的VPC

建立一个互联网联通的VPC：步骤

选择一个地址段

在一个可用区内建立子网

创建一条指向互联网的路由

对进出VPC的流量进行控制

选择一个地址段

CIDR 命名规则

- CIDR 段举例:
  - 172.31.0.0/16
  - 1010 1100 0001 1111 0000 0000 0000 0000

为你的VPC选择一个IP地址段

请注意一定要避免和你将要联通的网络地址段冲突重复

172.31.0.0/16

建议: RFC1918 range

建议:
/16
(64K addresses)

建立子网

为你的子网选择IP地址段

自动分配公网地址:
所有的实例都会自动获得一个公网地址

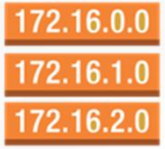
关于子网更多的建议

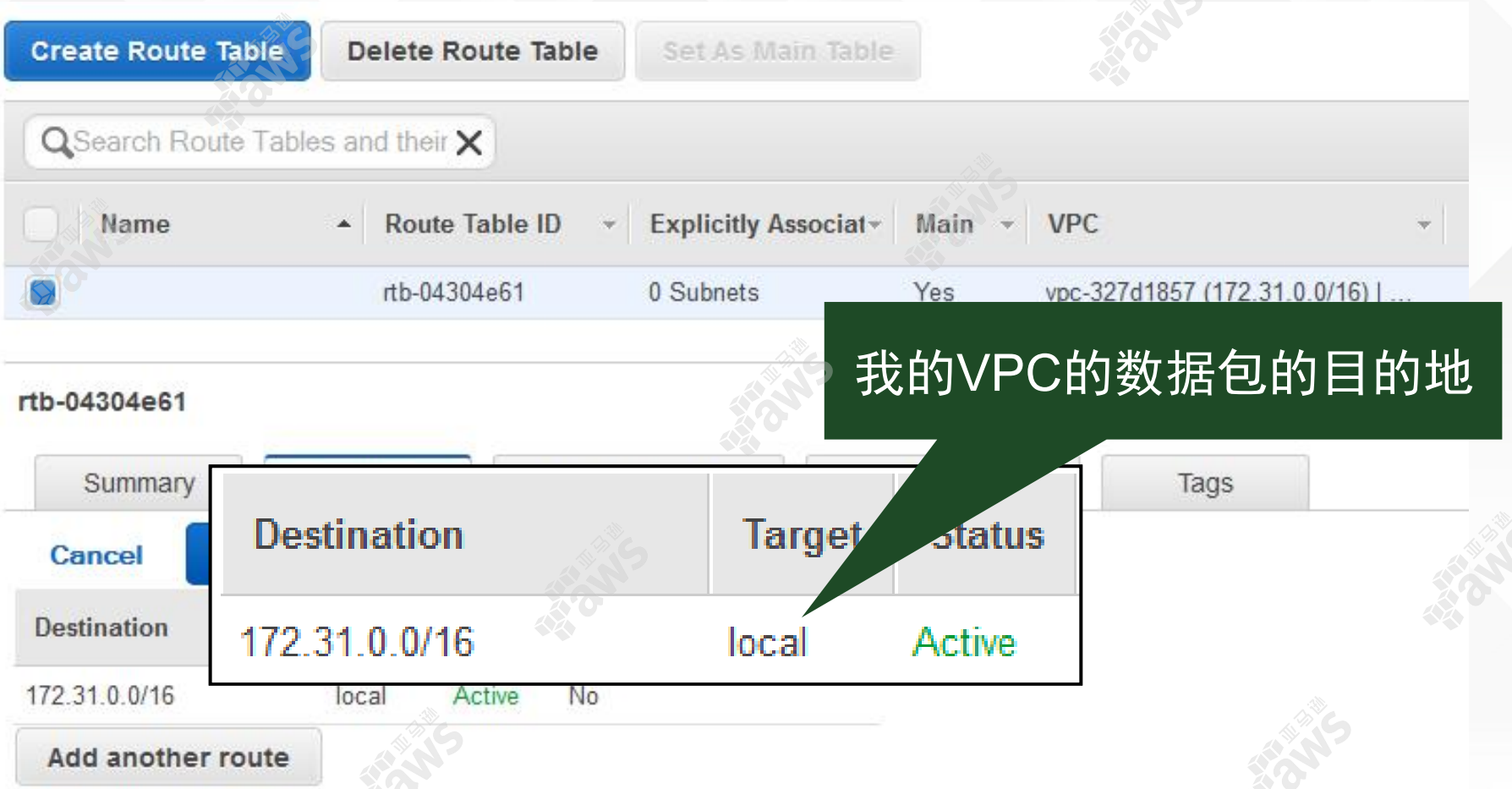
- 适合于大多数客户的建议:
  - /16 VPC (64K addresses)
  - /24 subnets (251 addresses)
  - 每个可用区一个子网
- 这是还有什么需要做的呢

创建一条通向互联网的路由

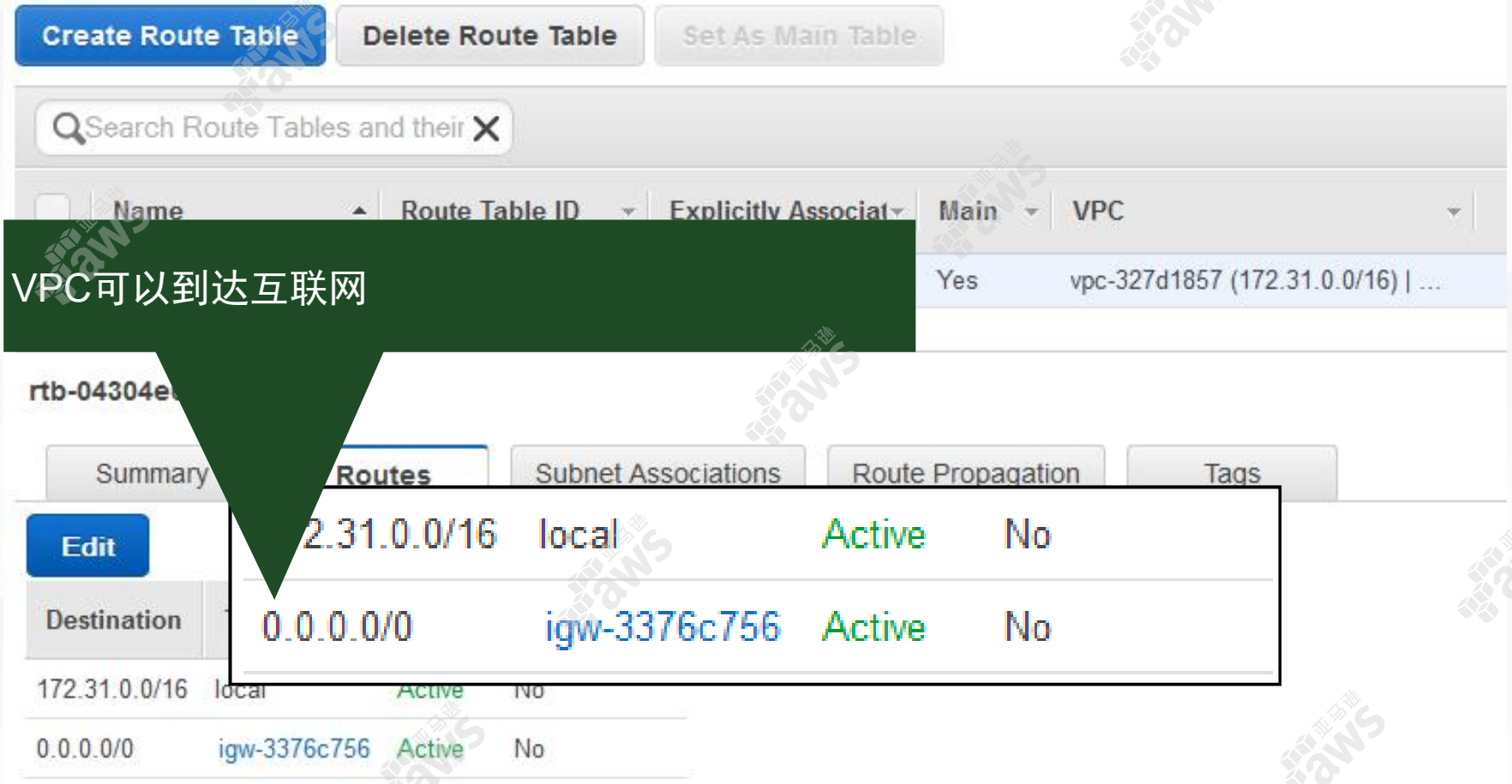
你的VPC的路由

- 路由表保存了你的数据包会去哪里的规则
- 你的VPC有一个默认的路由表
- … 但是你可以分配不同的路由表到不同的子网




Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and their
Name
Route Table ID
Explicitly Associat
Main
VPC
rtb-04304e61
0 Subnets
Yes
vpc-327d1857 (172.31.0.0/16) | ...
我的VPC的数据包的目的地
rtb-04304e61
Summary
Tags
Cancel
Destination
Target
Status
172.31.0.0/16
local
Active
Destination
172.31.0.0/16
local
Active
No
Add another route

Internet gateway

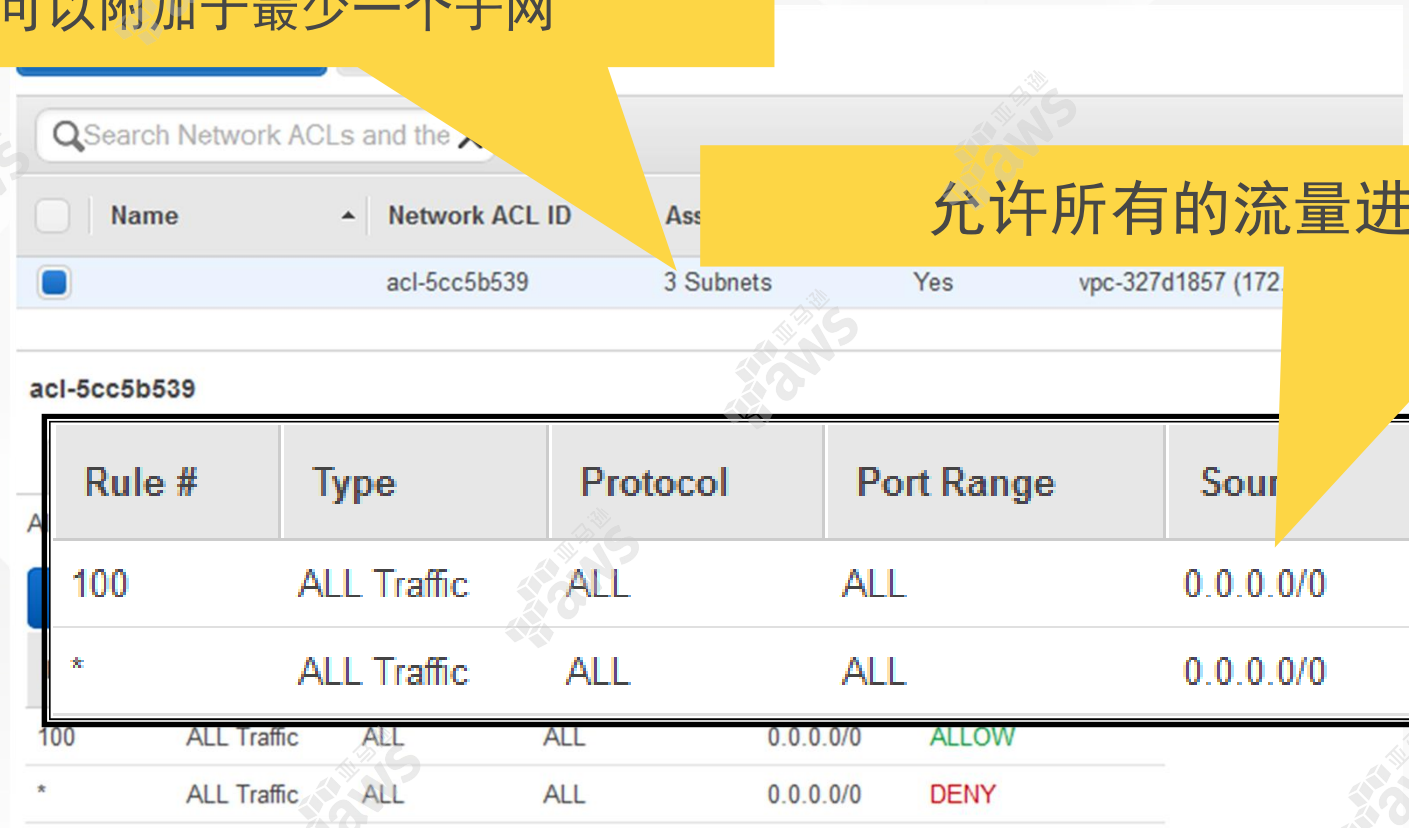

Create Route Table
Delete Route Table
Set As Main Table
Search Route Tables and their
Name
Route Table ID
Explicitly Associat
Main
VPC
Yes
vpc-327d1857 (172.31.0.0/16) | ...
VPC可以到达互联网
rtb-04304e
Summary
Routes
Subnet Associations
Route Propagation
Tags
Edit
Destination
172.31.0.0/16
local
Active
No
0.0.0.0/0
igw-3376c756
Active
No

控制流量:
网络访问控制列表
安全组

网络访问控制列表 = 无状态防火墙规则

可以附加于最少一个子网

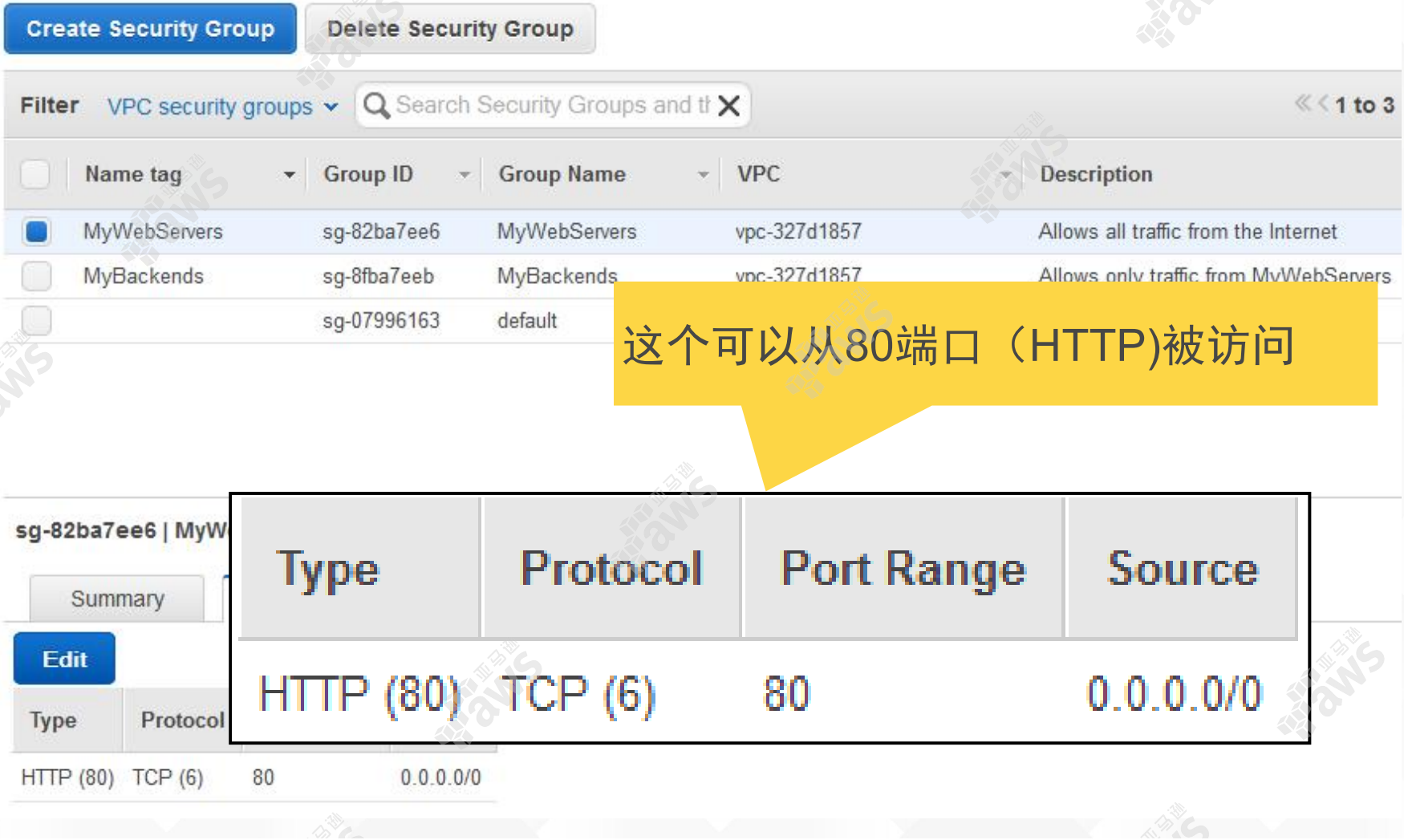
允许所有的流量进入



Rule #	Type	Protocol	Port Range	Sour	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

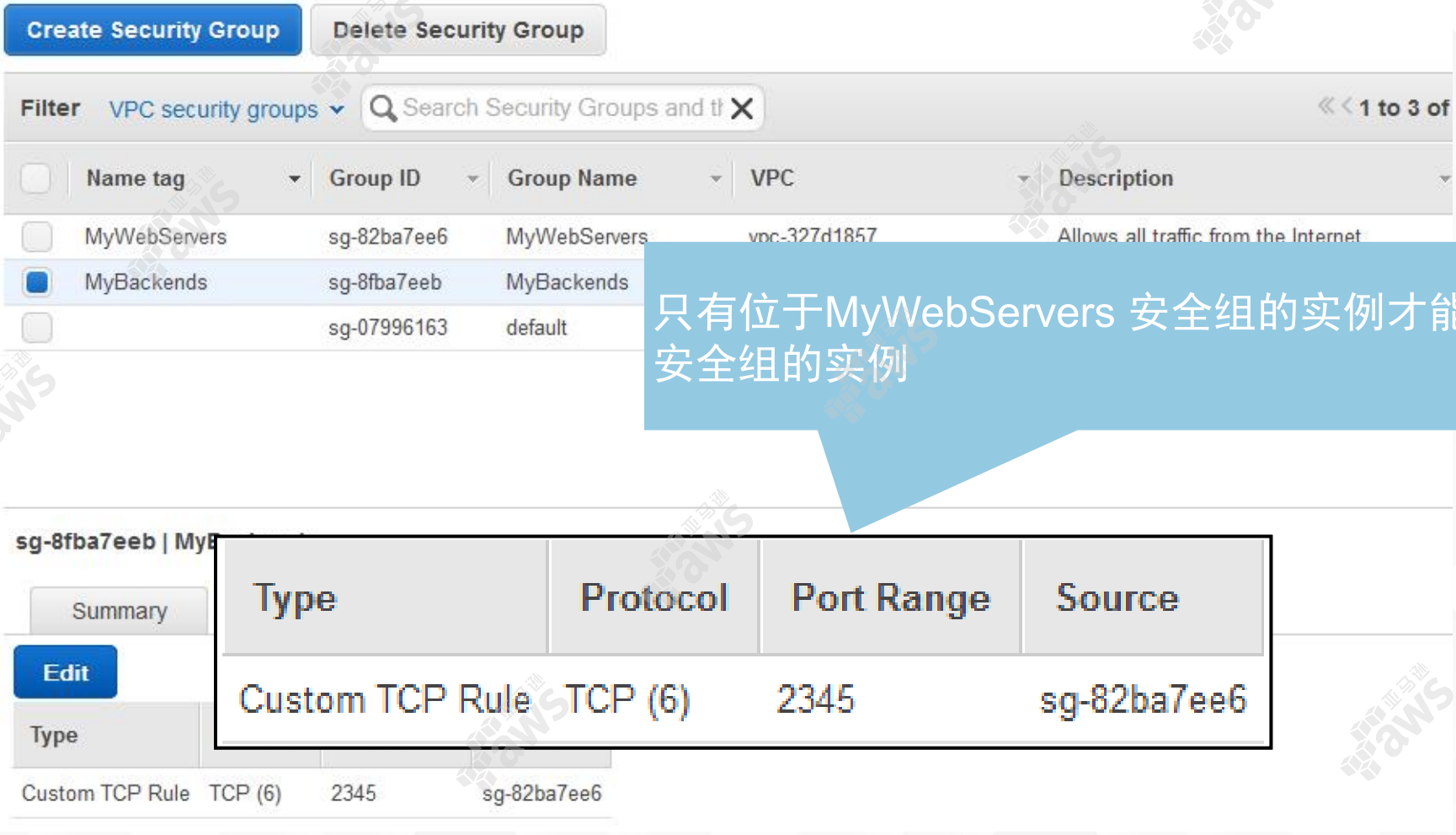
安全组遵循你应用的构架

安全组= 有状态防火墙



Type	Protocol	Port Range	Source
HTTP (80)	TCP (6)	80	0.0.0.0/0

安全组= 有状态防火墙



Type	Protocol	Port Range	Source
Custom TCP Rule	TCP (6)	2345	sg-82ba7ee6

VPC中安全组：附加的注意点

- VPC允许创立进出两个方向的安全组规则
- 最佳实践：只要可能，通过指定的规则允许流量联通
- 很多的应用构架通过安全组（谁可以联通我）和IAM 角色（我可以做什么）定义1对1的互相访问规则（谁可以联通我）

Thank You