Virtual Private Cloud (VPC)

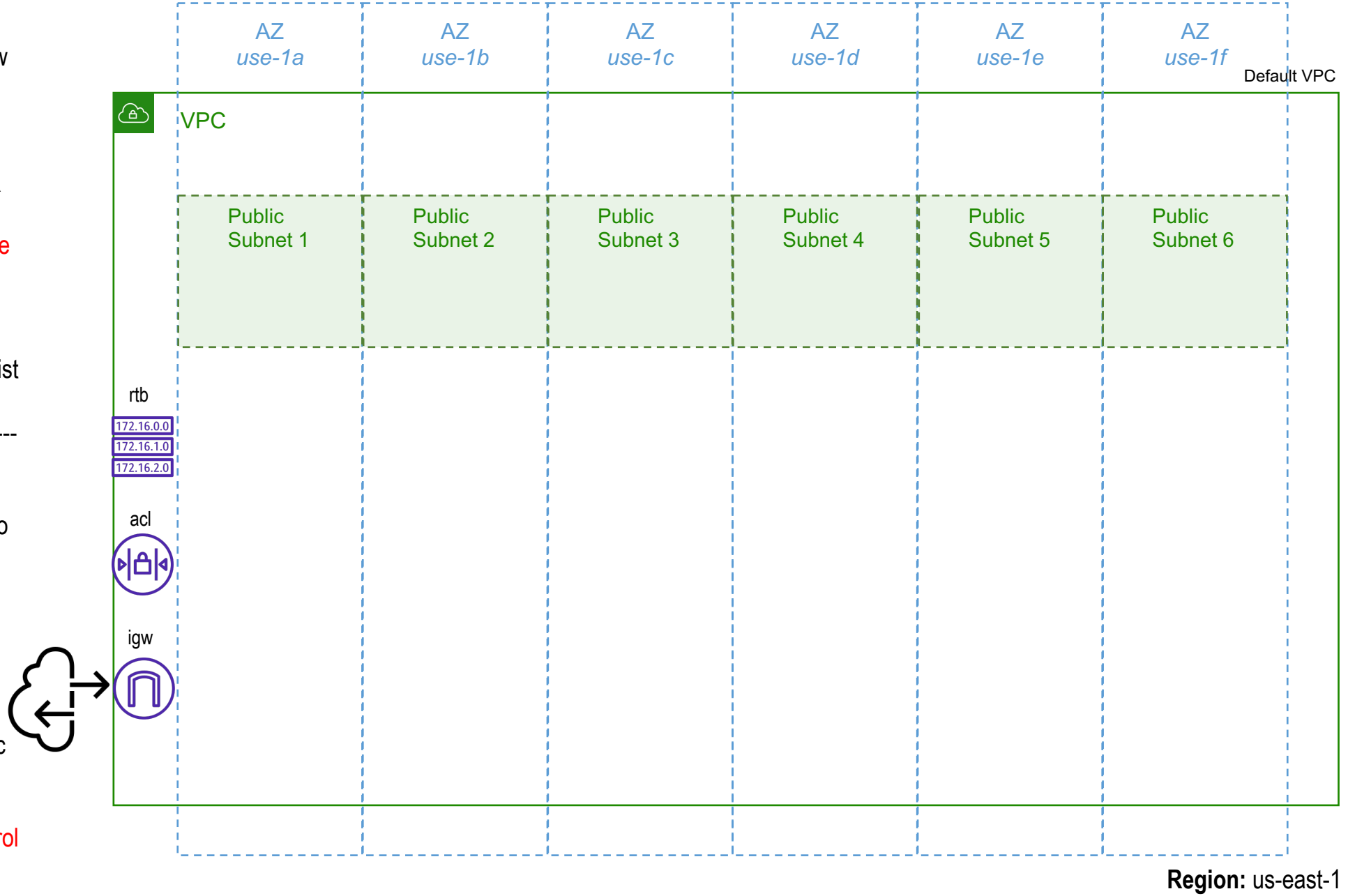
Overview | Deploying w/CloudFormation

Default VPC

- Created automatically w/new account
- /16 CIDR[1] (- 5 reserved)
  - 16K IP Addresses
- *N* Subnets – Each /20 CIDR
  - 4K IP Addresses
  - 1 per Availability Zone
  - Public
- 1 Default Route Table (rtb)
- 1 Internet Gateway (igw)
- 1 Network Access Control List (acl)

Essentially:

- Subnets are public because they have two-way access to the internet via the ***igw***.
- Subnets use the default ***rtb*** which routes all VPC traffic locally and all other traffic (0.0.0.0/0) to the internet.
- The VPC's ***acl*** allows all inbound and outbound traffic from 0.0.0.0/0
- Complex architectures generally require more control



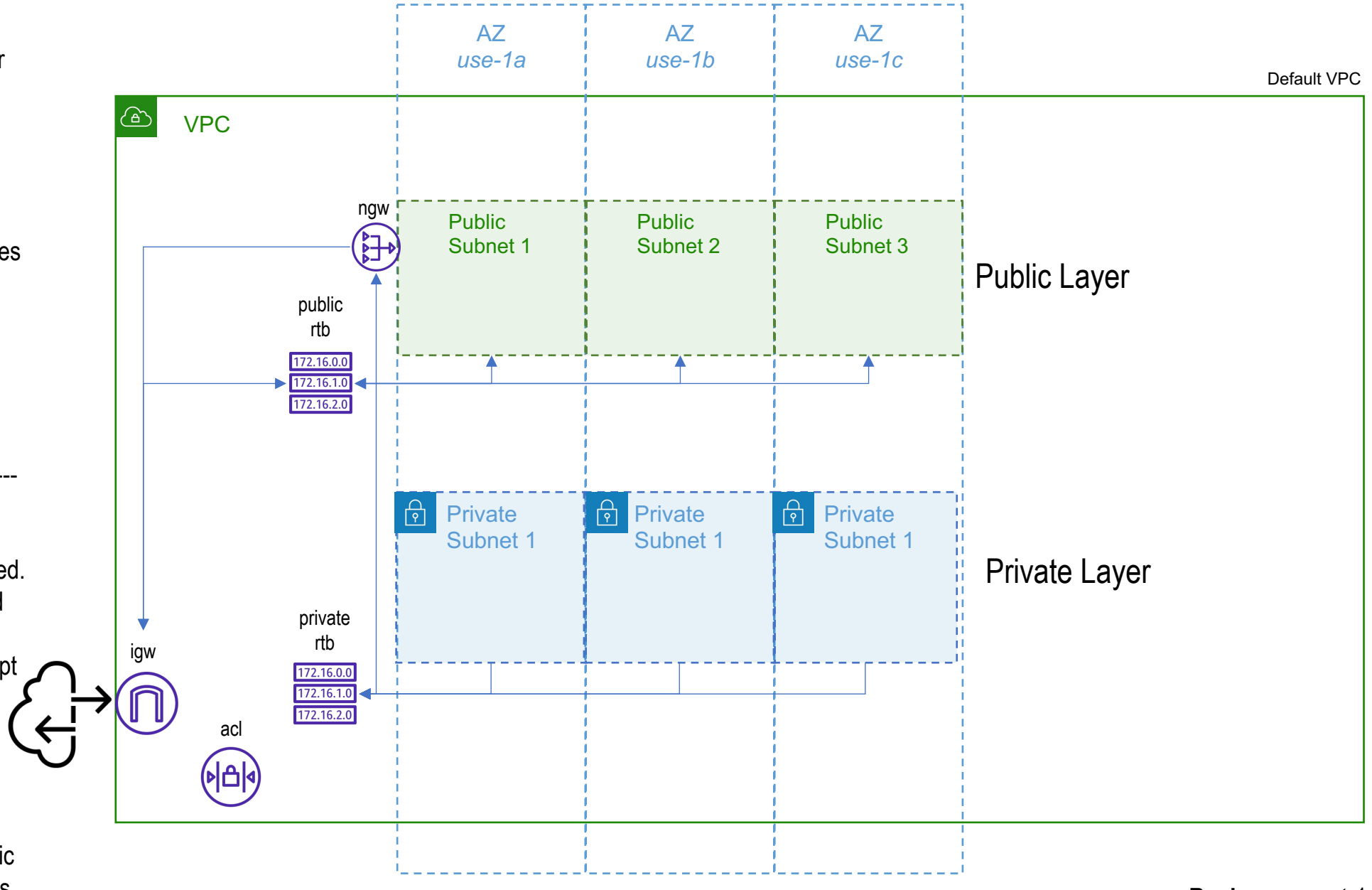
1. https://www.ripe.net/about-us/press-centre/IPv4CIDRChart_2015.pdf

Nondefault VPC

- Created via Console, CLI, or programmatically
- You specify configuration
- Subnets used to organize application layers
  - Public subnets for internet facing services
  - Private subnets for back-end services
- Tools
  - ACLs
  - Security Groups
  - NAT Gateways

Essentially:

- You'll need to manually add rtbs, acls, and igw as required.
- Subnets use specific rtb and acl to control traffic
- Private subnets do not accept inbound internet traffic
  - Use NAT Gateway (**ngw**) for outbound access
- Use Security Groups (sg) to limit inbound traffic to specific resources like EC2 instances



Note: A NAT Gateway is attached to a Public Subnet

Amazon Virtual Private Cloud
(Amazon VPC)

Public subnet

Private subnet

Availability Zone

VPC

Internet gateway

NAT gateway

Network access
control list

Your Account

aws AWS Cloud

Route table

Router

Note: I use Route Table and Router symbols interchangeably.

Region