* Directing Traffic Between VPC Resources
  + Route Tables:
    - Determine where network traffic is routed
    - Main (default) and custom route tables
    - All route tables include a local route entry
      * The local route entry cannot be deleted
    - Only one route table per subnet
    - USE CUSTOM ROUTE TABLES FOR EACH SUBNET
  + Security Groups
    - Stateful applications that act as virtual firewalls controlling inbound and outbound traffic for one or more instances
      * Stateful means both ways. Allow people that connect to receive
    - Deny all incoming traffic by default and use allow rules that can filter based on network protocols (TCP, UDP, and ICMP protocols)
    - Use a CIDR block or security group to create layers of security to define access to assets
    - If your inbound request is allowed, the outbound response is allowed automatically (stateful)
    - Use security groups to control traffic into, out of, and between resources
    - By default all newly created security groups allow all outbound traffic to all destinations
    - Most organizations create security groups with inbound rules for each functional tier (web/app/data) within an application
  + Network ACLs
    - A network ACL is a virtual firewall that controls traffic in and out of a subnet
    - Allow all incoming/outgoing traffic by default and use stateless rules to allow or deny traffic
    - Stateless rules inspect all inbound and outbound traffic and do not keep track of connections
      * Need to make 2 rules, one for incoming and one for outgoing
    - An allow rule must be explicitly created
* Directing Traffic to Your VPC
  + Internet gateways:
    - Allow communication from internet into VPC
    - Are horizontally scaled, redundant, and highly available by default
    - Provide a target in your subnet route tables for internet-routable traffic
  + To enable access to or from the internet for instances in a VPC subnet you must:
    - Attach an internet gateway to your VPC
    - Ensure that your subnet’s route table points to the internet gateway
    - Ensure that instances in your subnet have public IP address or Elastic IP addresses
    - Ensure that your network ACLs and security groups allow the relevant traffic to flow to and from your instance
* Outbound Traffic from Private Instances
  + Network Address Translation (NAT) services:
    - Enable instances in the private subnet to initiate outbound traffic to the internet or other AWS services
    - Prevent private instances from receiving inbound traffic from the internet
    - Two primary options:
      * Amazon EC2 instance set up as a NAT in a public subnet
      * NAT gateway