IAAS ACADEMY

AWS Virtual Private Cloud (VPC) – Part 2

Amazon Web Services

Amazon VPC - Features

Security

Amazon VPC comes with advance levels of security option to configure. Features include Security Groups as well as Network Access Control Lists to enable inbound and outbound filtering at both the instance level as well as the subnet level.

Security Groups

Security Groups are virtual **Stateful** firewalls that control inbound and outbound traffic to AWS instances. Each instance must be attached to a security group. Key points to note:

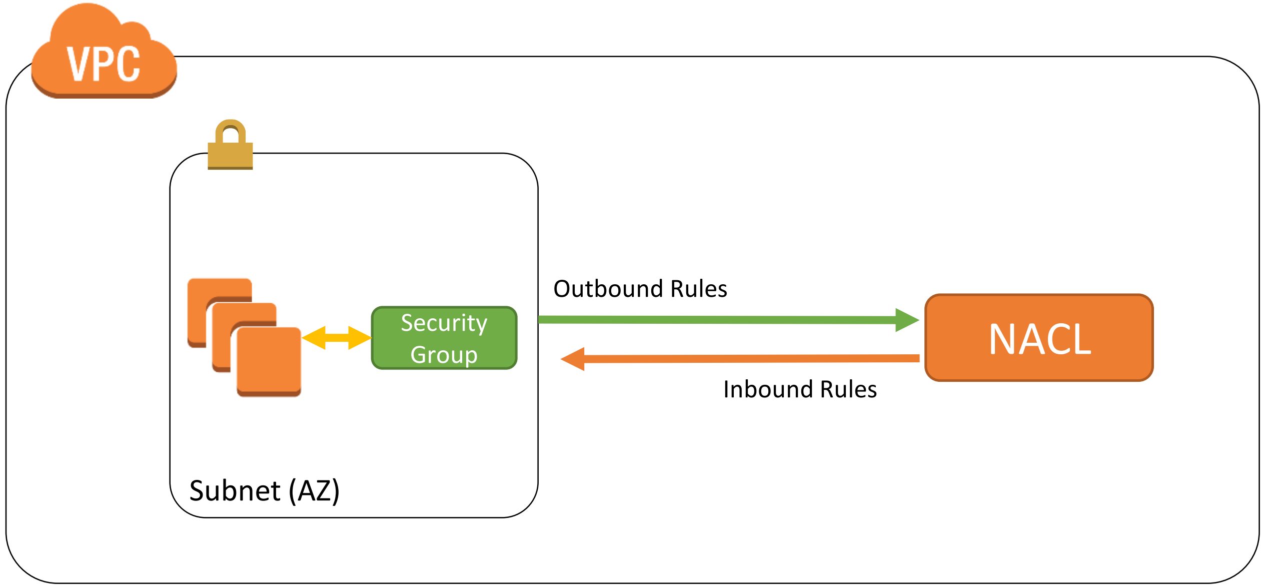
- By default no inbound traffic allowed until you add inbound rules
- By default new groups have outbound rule to allow all outbound traffic
- Supports only Allow Rules – You cannot have an explicit Deny Rule

Amazon VPC - Features

Security

Network Access Control Lists (NACL)

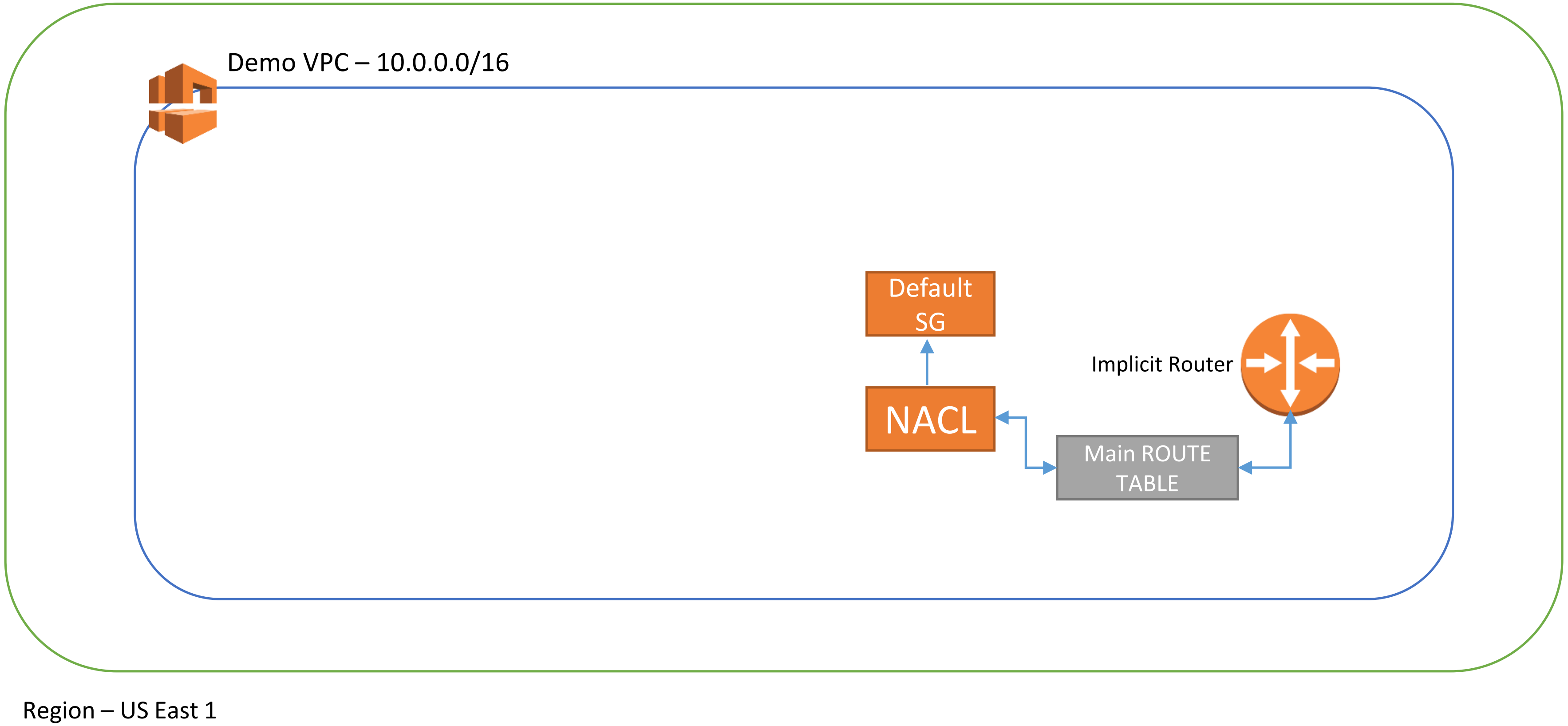
Network ACLs are **stateless** firewalls on the subnet level. Rules on an network ACL are evaluated in order, starting with the lowest numbered rule to determine if traffic will flow into and out of the subnet.



- NACL are stateless
- Supports allow and deny rules
- Rules are applied by order of priority, where the lowest number is the highest priority
- Automatically applied to all instances in a subnet
- One subnet can only be associated with one NACL

Amazon VPC – Components

VPC can span availability zones but not regions.



Amazon VPC – Components

Route Tables

Logical route configuration within a VPC contains rules which can be applied to each subnet. Route Tables enable traffic to flow within a subnet, between subnets, to the Internet via an Internet Gateway or NAT and to private VPN gateways. Route Tables will contain a default route called a local route.

Key Points to Note:

- Your VPC has an implicit router
- Your VPC will have a main route table – by default this only contains one route to enable traffic to flow internally only
- You can create custom routes – for example routes to the Internet and VPG. For best practice create a separate route table for public Internet routes.
- Each subnet must be associated with a route table. If you don’t specify a route table, the subnet is automatically associated with the main route table

Amazon VPC – Components

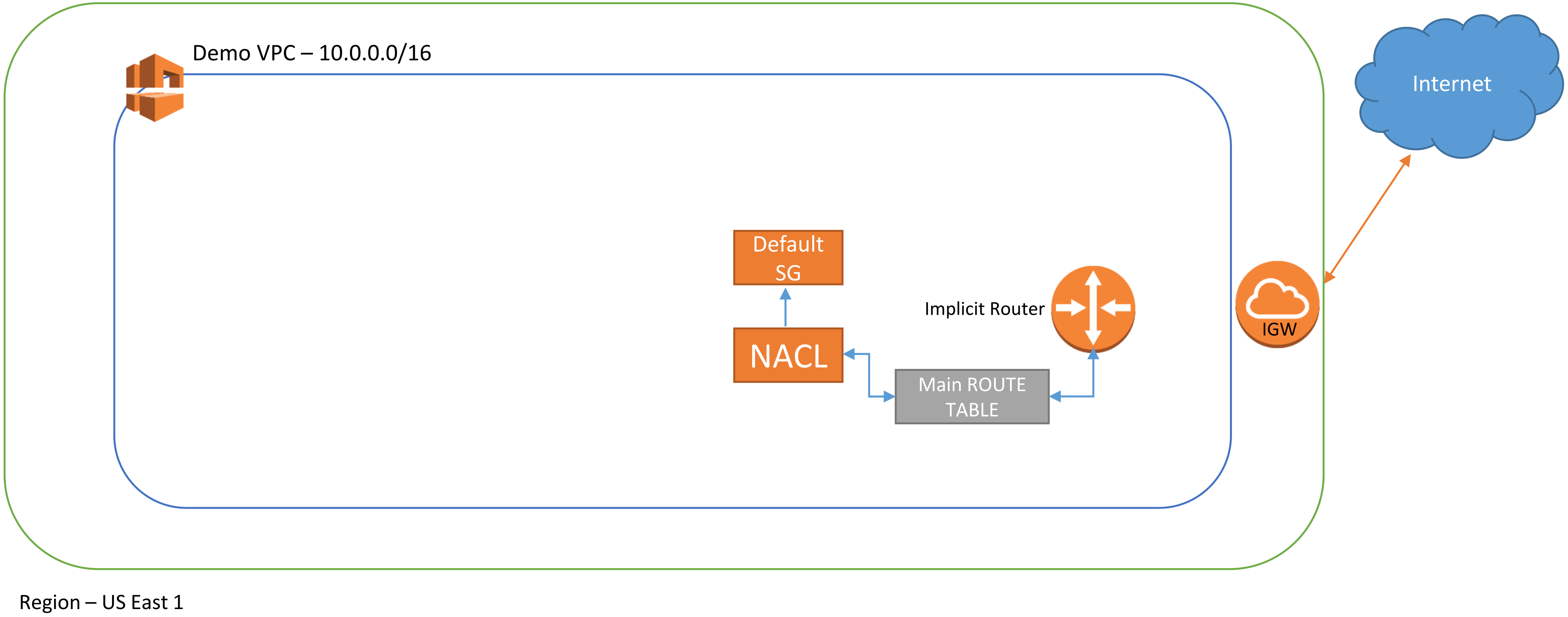
Internet Gateway

Internet Gateways can be attached to a VPC to enable specific subnets and instances contained within them access to the Internet.

- Note you can only have one Internet Gateway per VPC.

Amazon VPC – Components

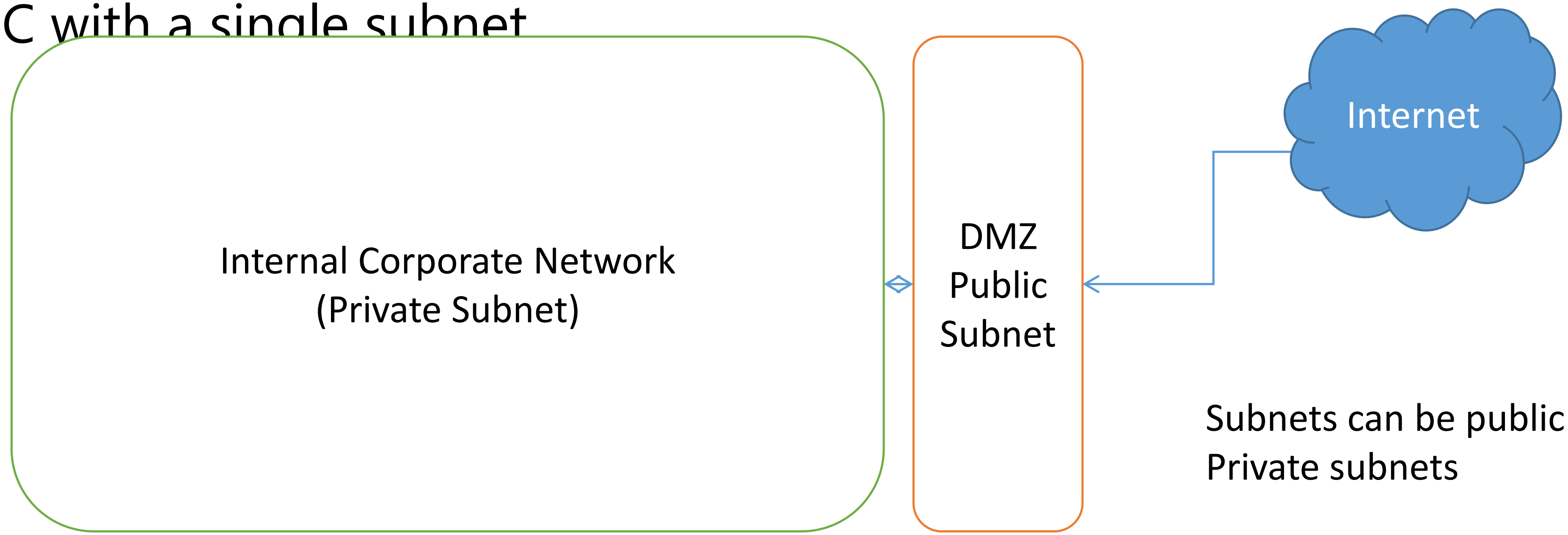
Attaching an Internet Gateway



Amazon VPC – Components

Subnets

Subnets allows you to create segments of your network where you can launch EC2 instances, Amazon RDS databases and other AWS resources. A Subnet will usually consist of a small block of IP Address range when compared to the VPC size but can extend the entire VPC as in the case of a VPC with a single subnet



Subnets can be public subnets or Private subnets

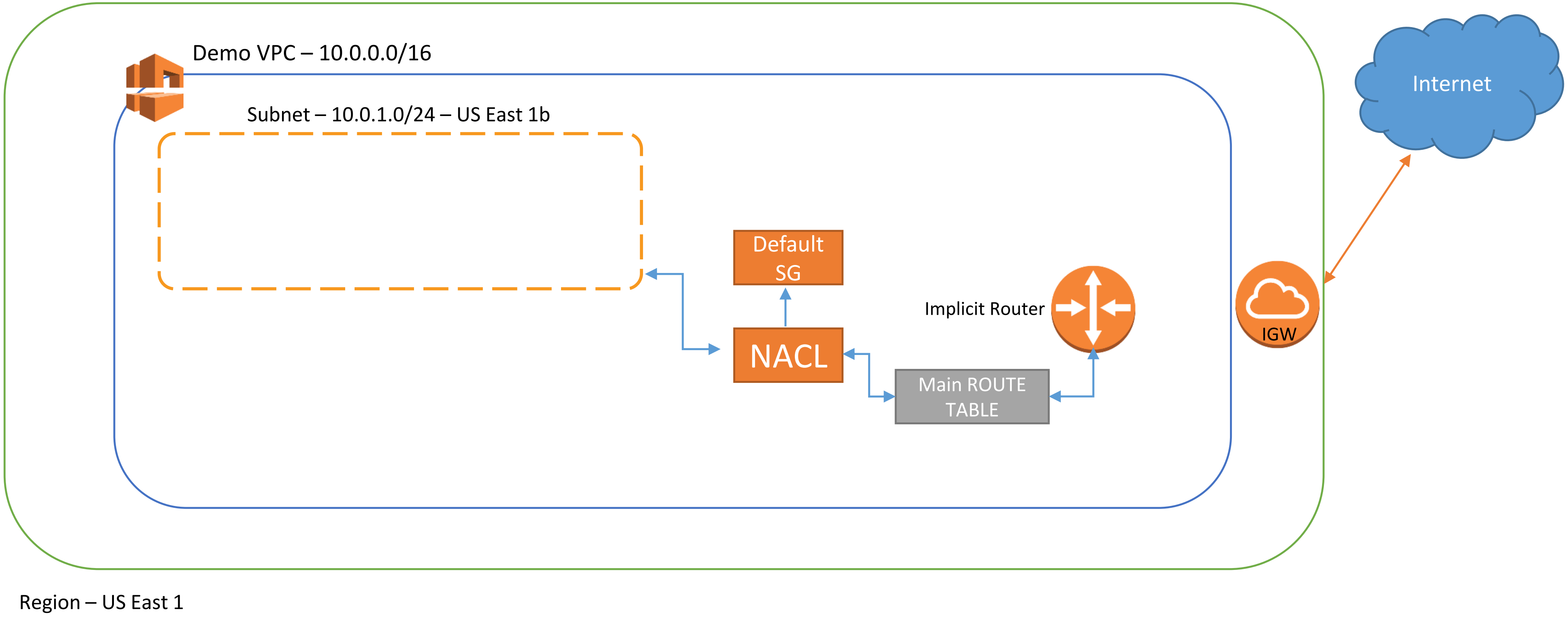
Amazon VPC – Components

Private, Public & Elastic IP Addresses

- Private IP Address
- Public IP Address
- Elastic IP Address
  - Amazon Web Services maintain a pool of static public IP Addresses which you can lease for workloads on your account that need a static public IP. EIPs remain static and is yours to use as long as you want. Key Points to Note:
    - You must allocate an EIP for use within a VPC and then assign it to an instance
    - EIPs are region specific
    - One to One relations between network interfaces and EIPs
    - You can move an EIP from one instance to another, or between VPCs as long as its in the same region
    - EIPs will remain associated unless you release them
    - You are charged for EIPs if you don't associate them with an instance
    - The default limit on number of EIPs is 5

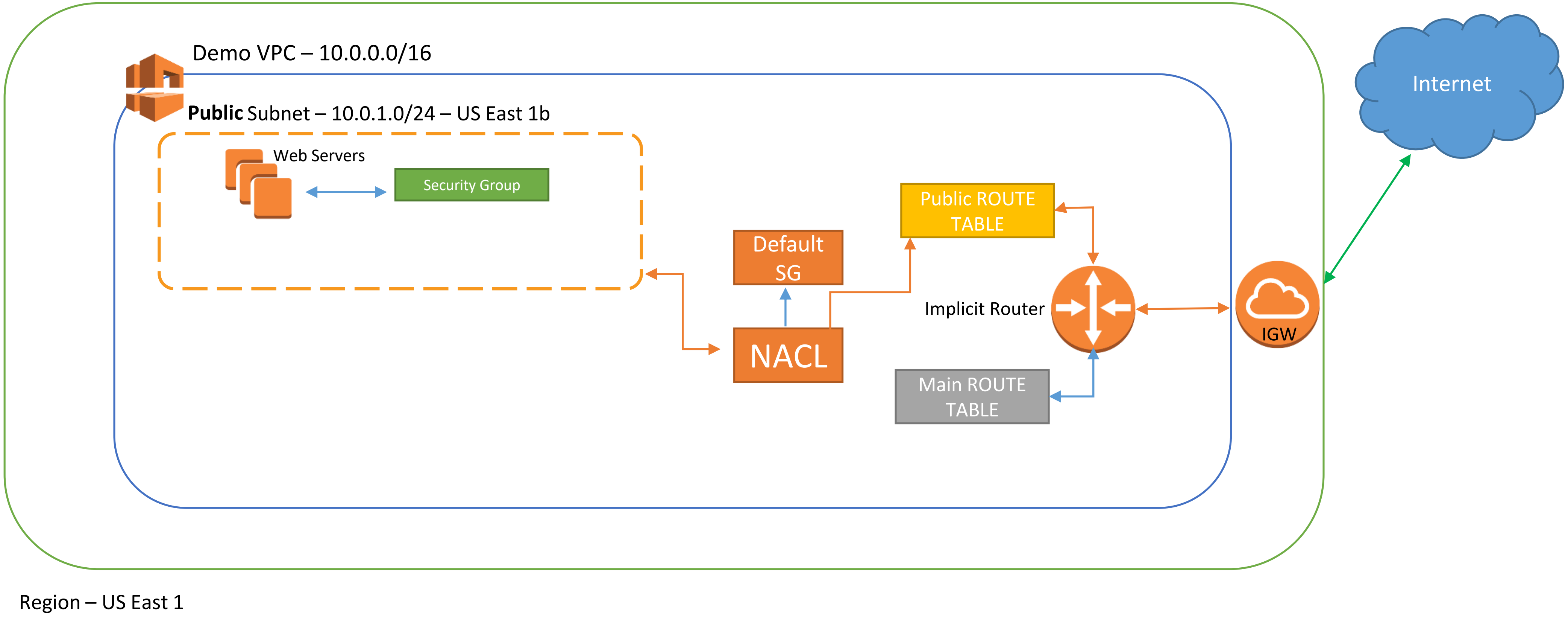
Amazon VPC – Components

Creating Subnets



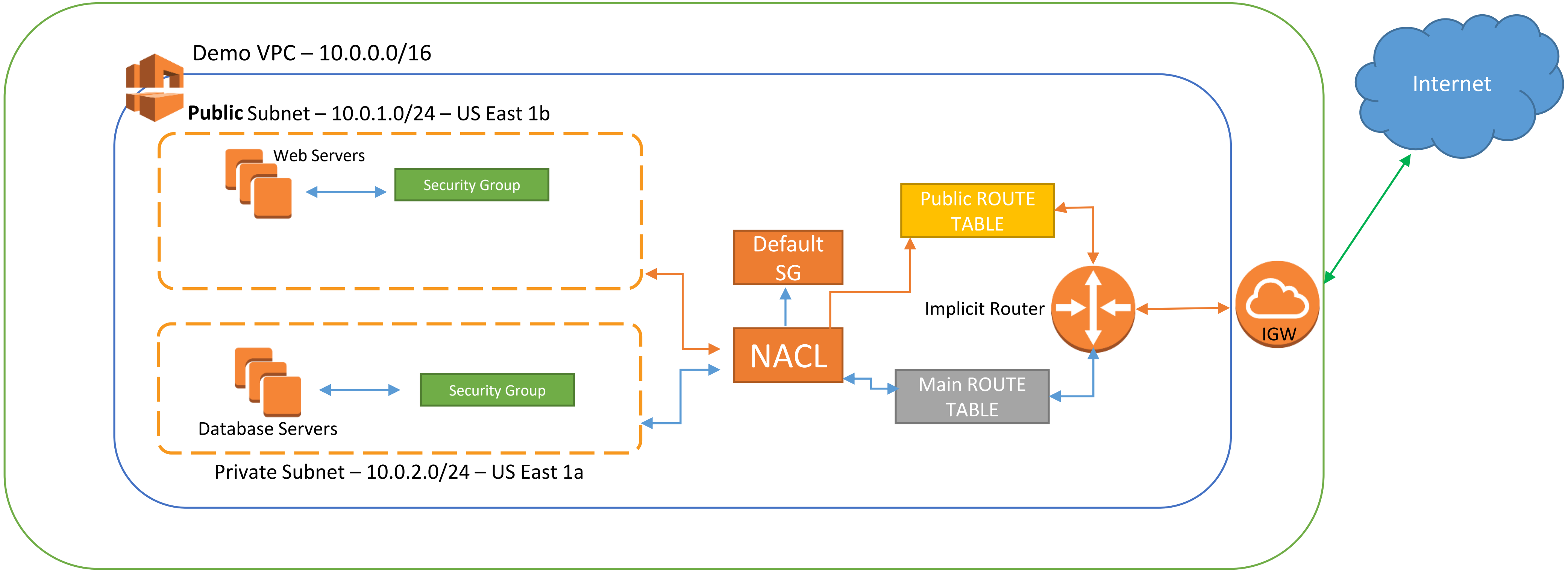
Amazon VPC – Components

Creating Subnets



Amazon VPC – Components

Creating Subnets



Region – US East 1

Amazon VPC – NAT Gateway

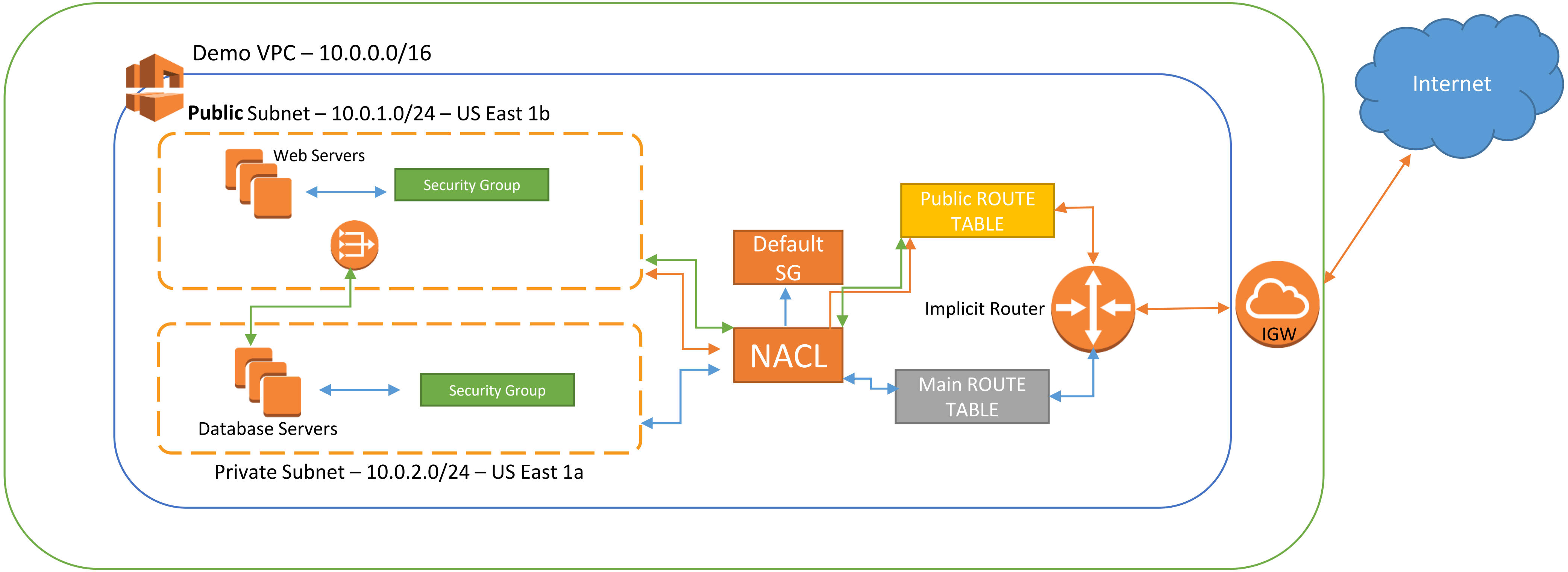
You can use a NAT device to enable instances in a private subnet to connect to the internet (for example, for software updates) or other AWS services, but prevent the internet from initiating connections with the instances. A NAT device forwards traffic from the instances in the private subnet to the internet or other AWS services, and then sends the response back to the instances.

Setup NAT Gateways:

- Configure Route Table associated with a private subnet to direct Internet bound traffic to the NAT gateway
- Allocate an EIP to the NAT gateway

Amazon VPC – Components

Creating Subnets



Region – US East 1

Next Video