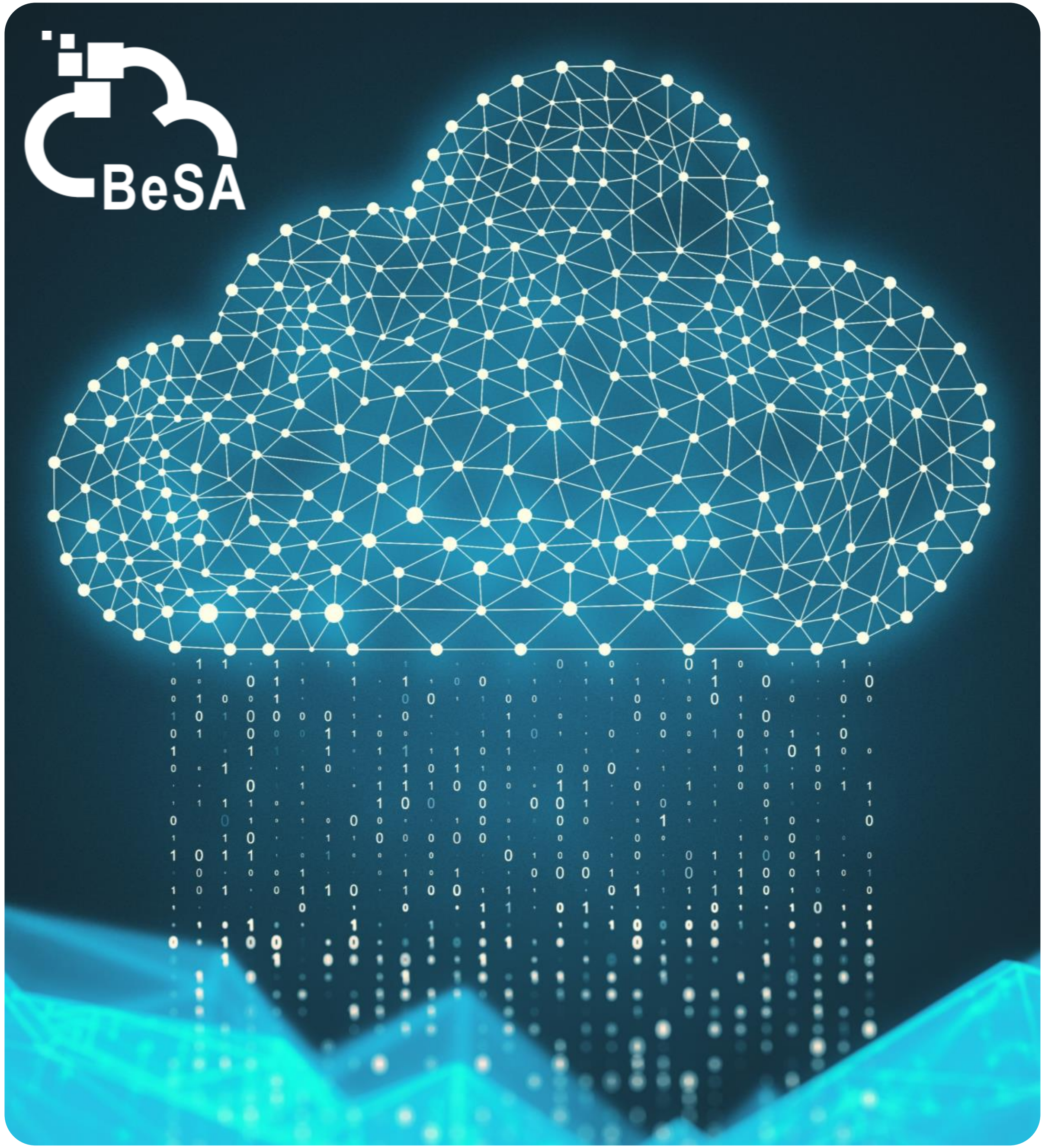
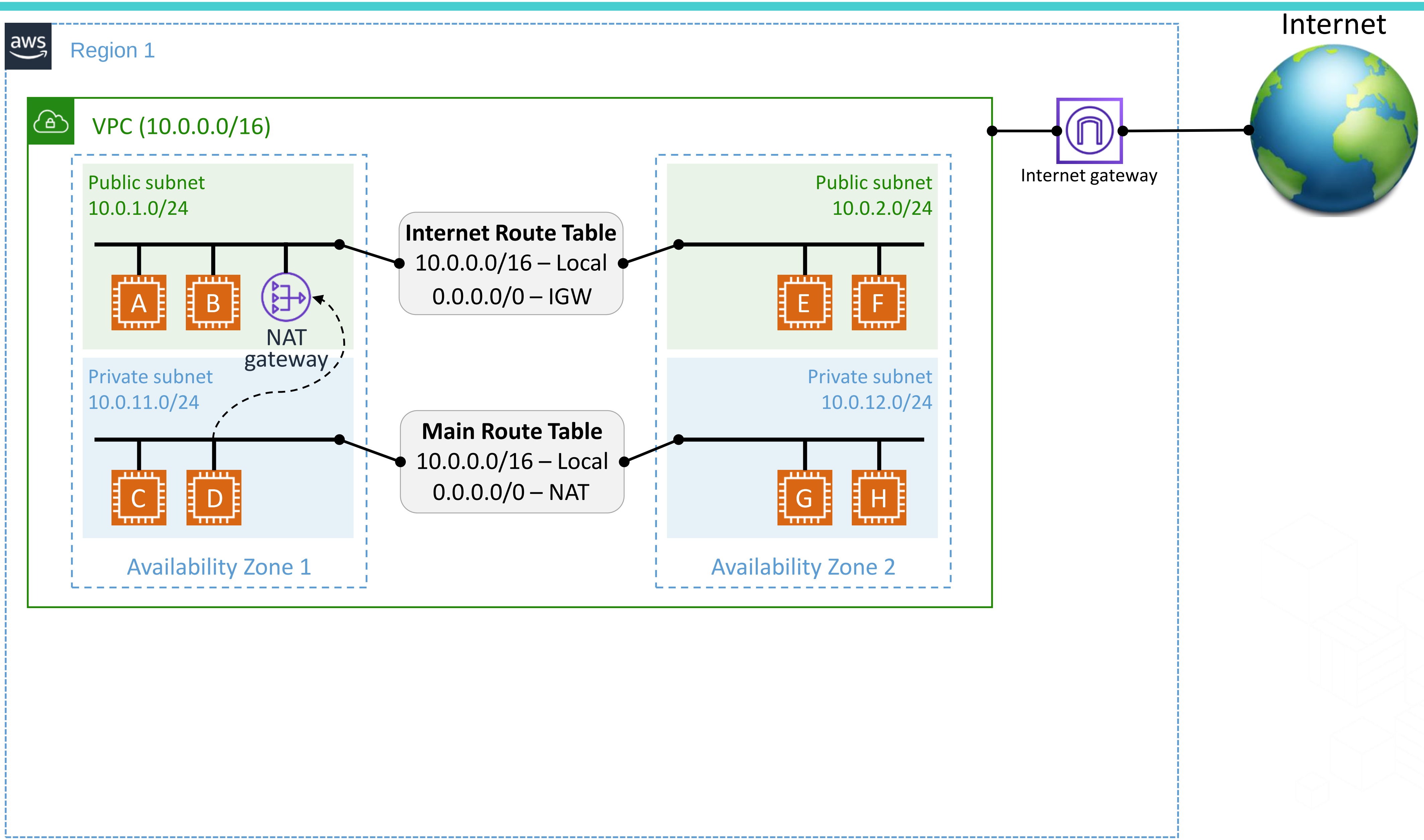


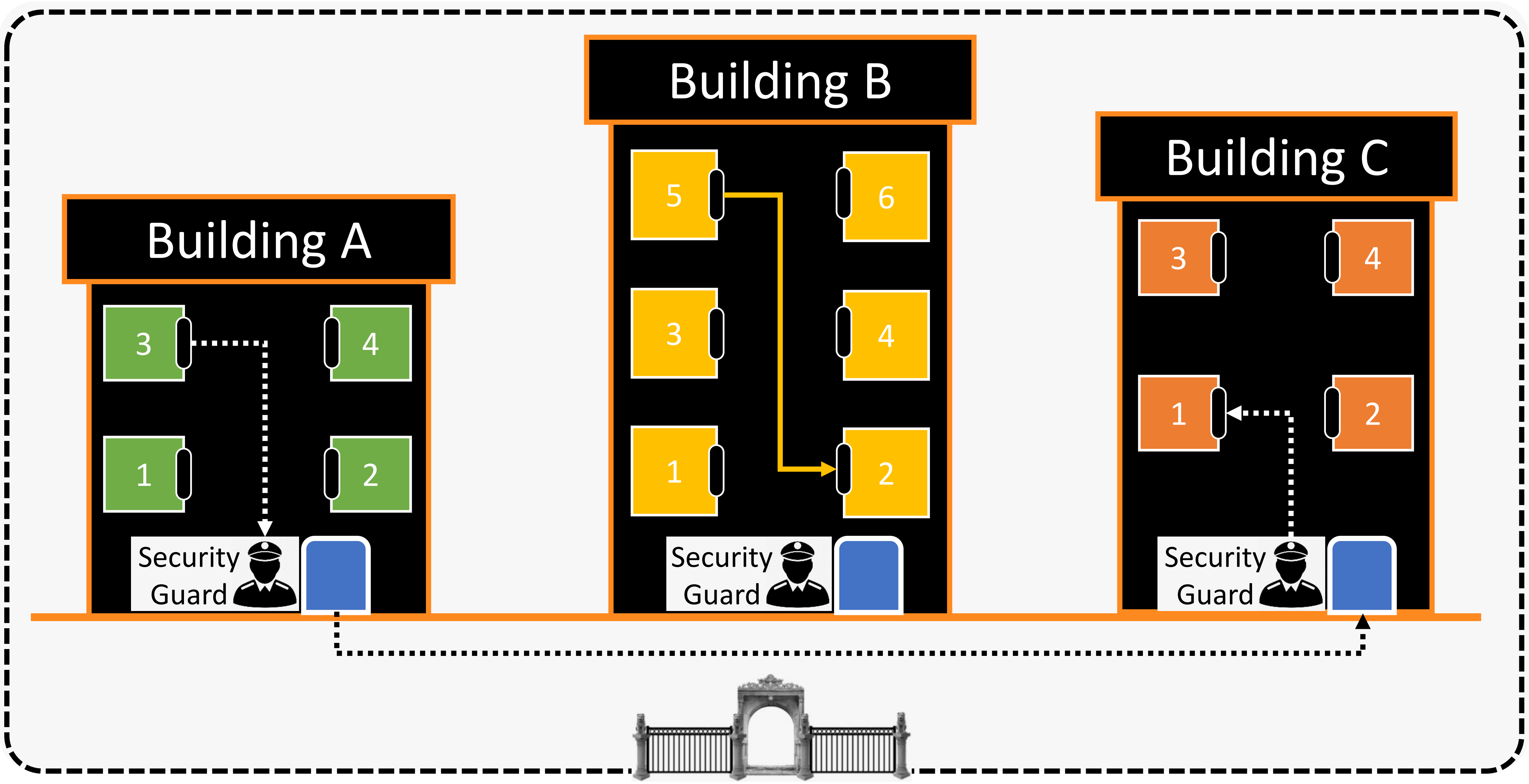
Hold the door

Security Group and Network ACL

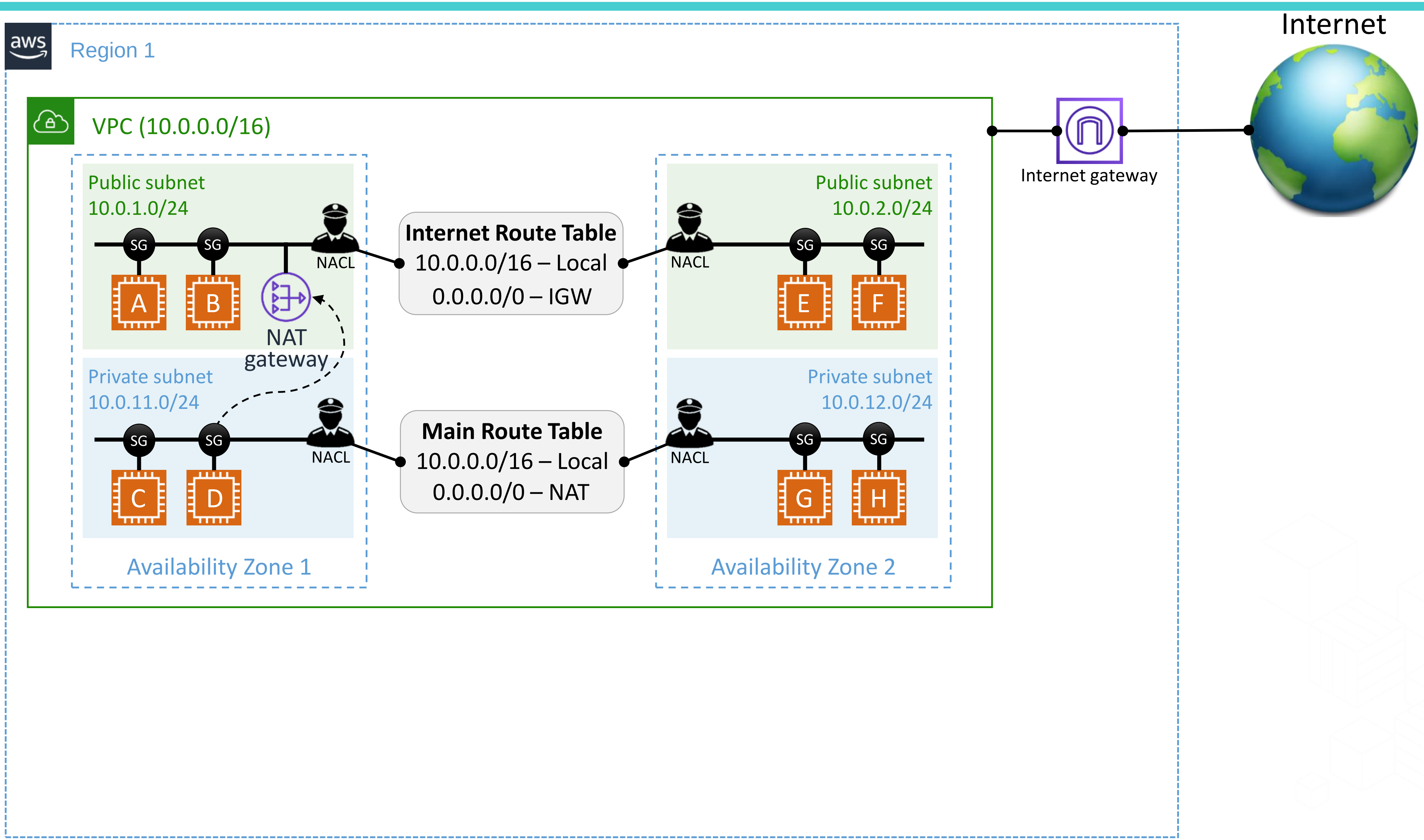
Amazon VPC


Internet
Region 1
VPC (10.0.0.0/16)
Internet gateway
Public subnet
10.0.1.0/24
A
B
NAT
gateway
Private subnet
10.0.11.0/24
C
D
Availability Zone 1
Internet Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – IGW
Main Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – NAT
Public subnet
10.0.2.0/24
E
F
Private subnet
10.0.12.0/24
G
H
Availability Zone 2

Security Group and Network ACL



Amazon VPC



Internet Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – IGW

Main Route Table
10.0.0.0/16 – Local
0.0.0.0/0 – NAT

Security Group vs. Network ACL

Security Group	Network ACL
Applied at Instance (ENI) Level	Applied at Subnet Level
Stateful - Response is always allowed	Stateless - Request and Response both have to be allowed

UK Immigration	India Immigration
IMMIGRATION OFFICER * UK * 11 FEB 2023 LONDON HEATHROW Stateful	PASSPORT CONTROL ARRIVAL 07-Dec-2022 DELHI 01/JH PASSPORT CONTROL DEPARTURE 10-Feb-2023 MUMBAI A0/21 Stateless

Security Group vs. Network ACL

Security Group	Network ACL
Applied at Instance (ENI) Level	Applied at Subnet Level
Stateful - Response is always allowed	Stateless - Request and Response both have to be allowed
Default Rules (For Default SG) - All inbound is allowed from the same SG - All outbound is Allowed Default Rules (For a new SG) - All Inbound is Deny - All outbound in Allowed	Default Rules (For Default NACL) - All inbound is Allowed - All outbound is Allowed Default Rules (For a new NACL) - All inbound is Deny - All outbound is Deny
1 Instance can have many SG assigned	1 Subnet can have only 1 NACL
Only allow statements	Allow and Deny both statements
Order is not important	Order is important (lower order rule is applied first)
Source - IP / IP Range / Port / SG-<xxxxxxx>	Source - IP / Port / IP Range

Reference:

FAQs

Category:

Networking
and Content
Delivery

Amazon VPC

Complete book:

Click Here

Created by:

Ashish Prajapati

What?

- Amazon Virtual Private Cloud (Amazon VPC) enables you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you have defined.
- This virtual network closely resembles a traditional network that you would operate in your own data center.

Why?

- You can define your own network space, and control how your network and the Amazon EC2 resources inside your network are exposed to the Internet.
- You can also leverage more granular access to and from the Amazon EC2 instances in your virtual network.

When?

- You want to launch AWS resources in a logically isolated virtual network and spend less time setting up, managing, and validating your virtual network.
- You want to use multiple layers of security, including security groups and network access control lists.

Where?

- VPC is a regional entity and spans across all of the Availability Zones in the region.
- Each subnet must reside entirely within one Availability Zone and cannot span zones.
- You can launch AWS resources, such as EC2 instances, into a specific subnet.

Who?

- Your AWS resources are automatically provisioned in a ready-to-use default VPC or you can create additional VPCs.
- You can specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.

How?

- When you create a VPC, you must specify an IPv4 CIDR block for the VPC. Afterwards you can add subnets, route tables, security groups, network access control list, an internet gateway, and other gateways as necessary.

How much?

- There is no additional charge for using a VPC. There are charges for some VPC components, such as NAT gateways, Reachability Analyzer, and traffic mirroring. Usage charges for other Amazon Web Services, including Amazon EC2, still apply at published rates for those resources, including data transfer charges.