AWS Certified Solutions Architect — Associate (SAA-C01)

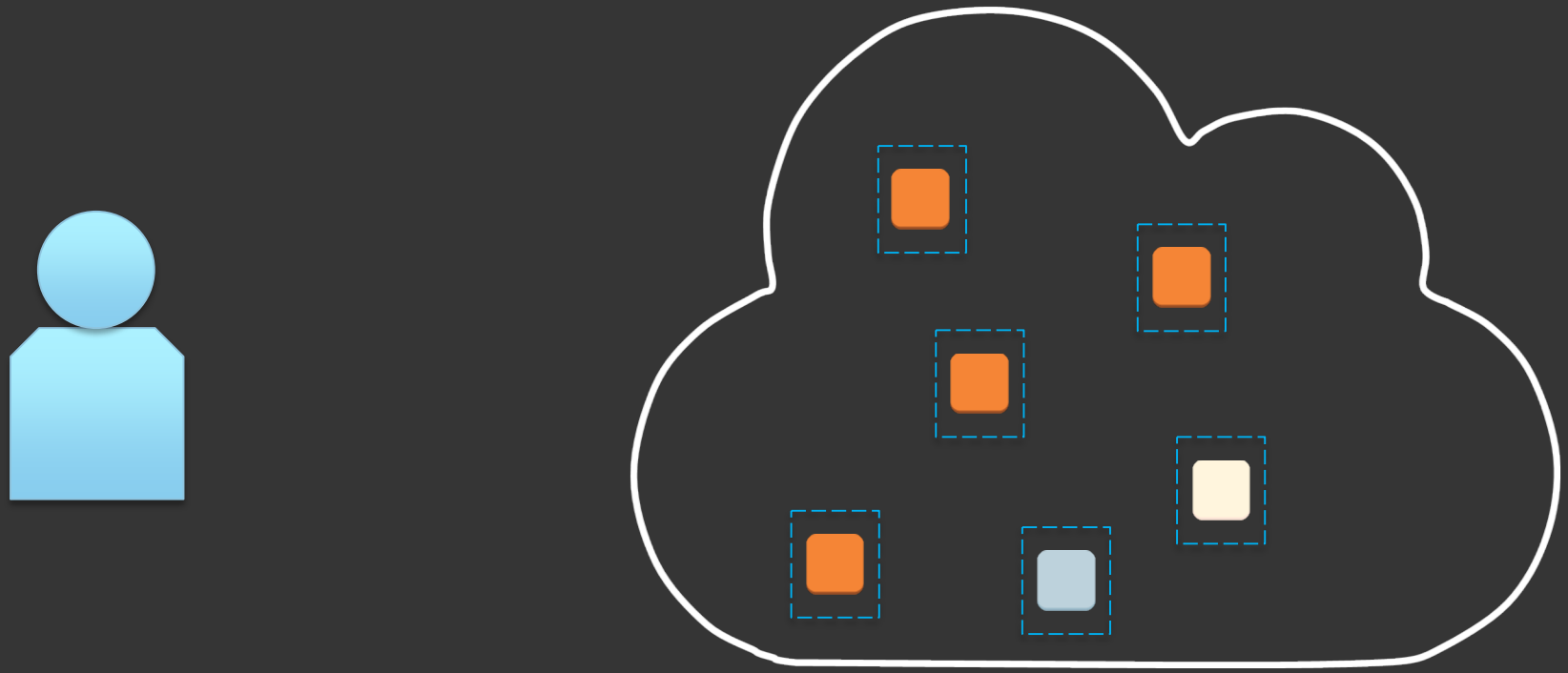
Module 8

Virtual Private Cloud (VPC)

Agenda

- Life Before VPC
- VPC Concepts & Architecture
- Networking Basics – IP Addressing
- VPC Routing
- VPC Endpoints
- VPC Security & Logging
- Labs

Life before VPC

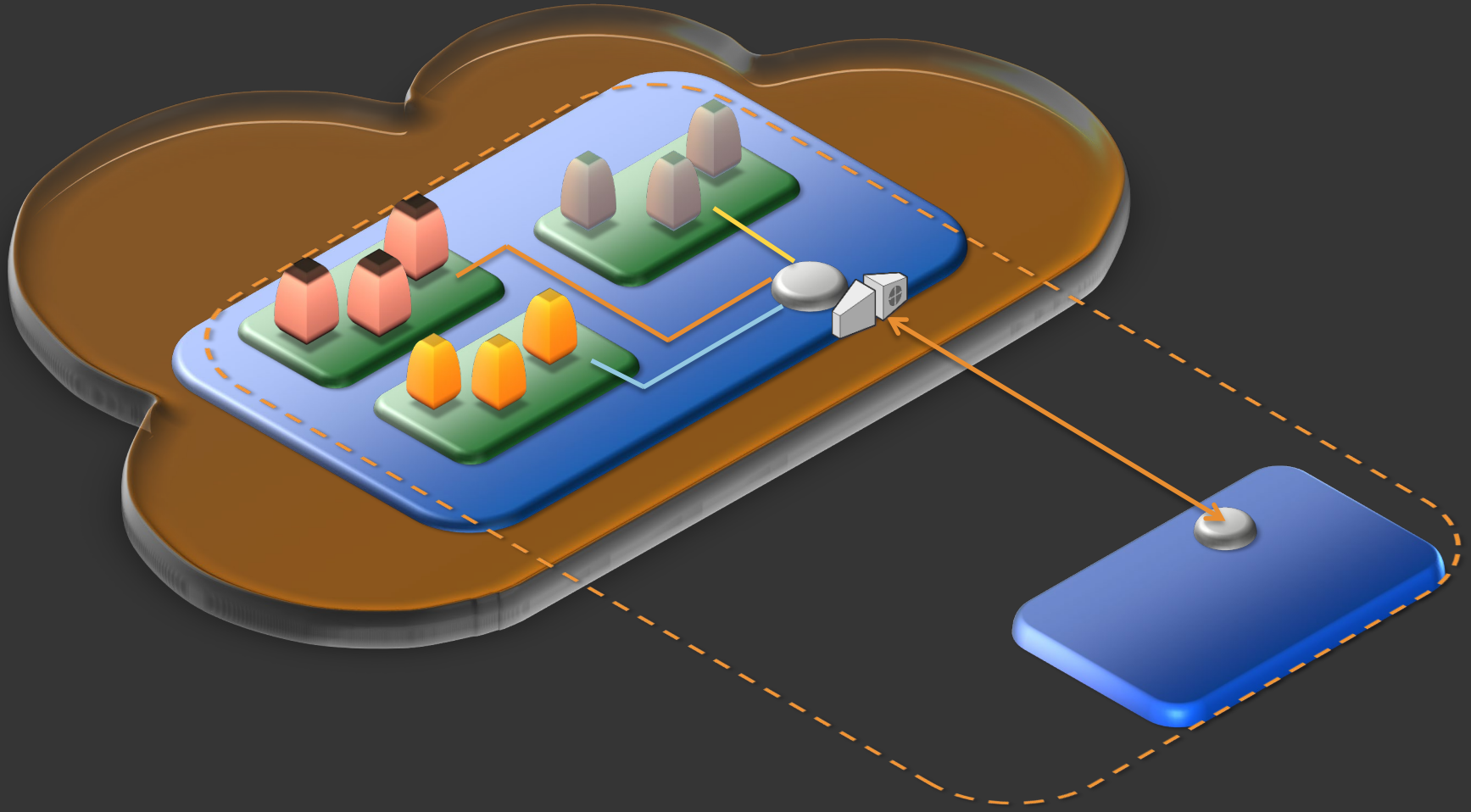


VPC

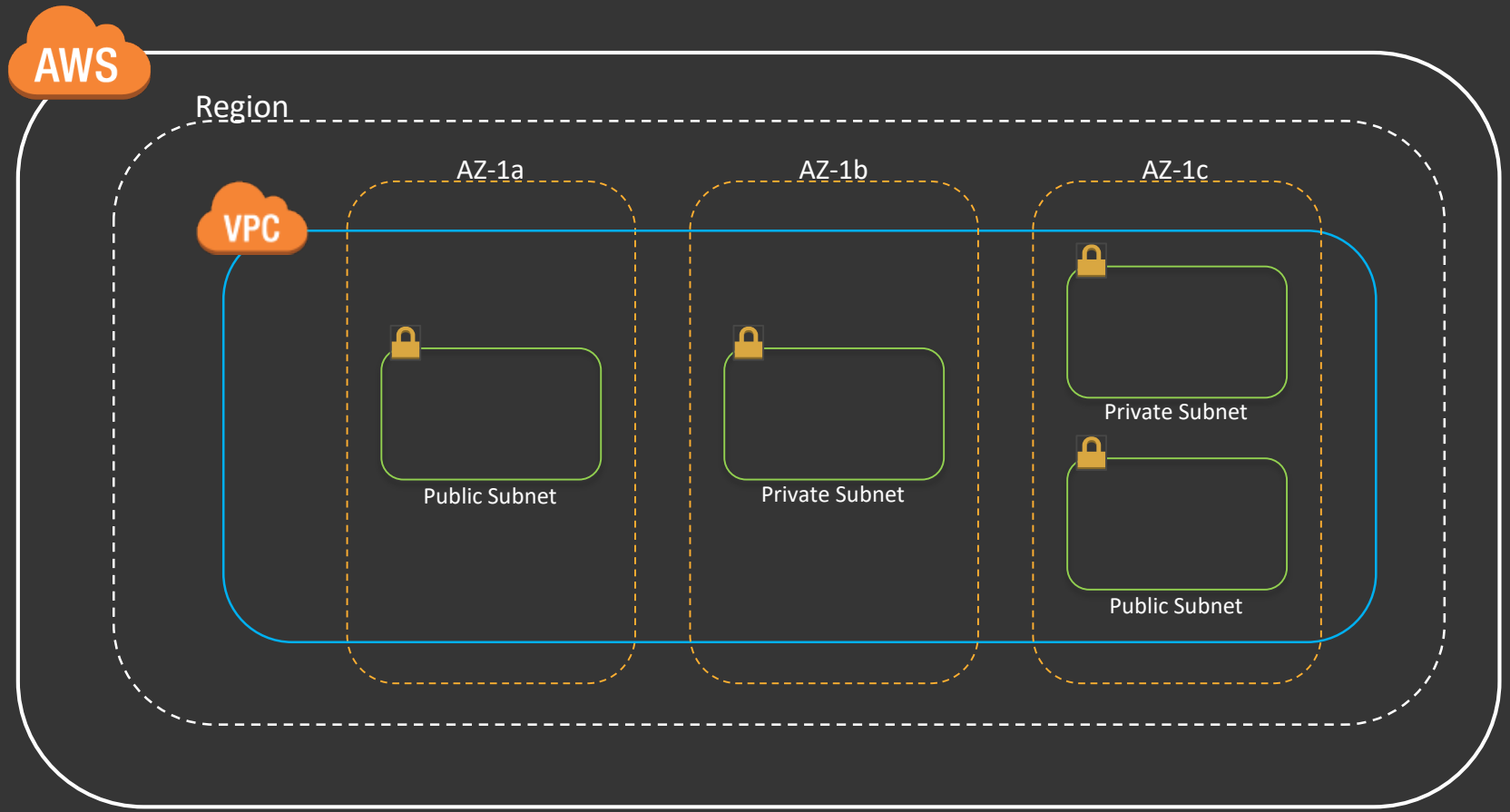
Virtual Private Cloud

Isolated Cloud Network

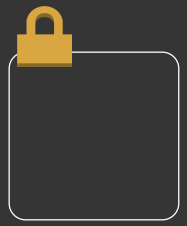
- Create user defined virtual networks (IPv4/v6)
- Allows control of the networking environment
- Can be connected to existing datacenters over VPN or Direct Connect
- Can be peered with other VPCs in AWS



VPC Architecture



Components of VPC



Subnet

Route Table

Router

Elastic IP

Elastic Network Interface (ENI)

Internet Gateway

Customer Gateway

VPN Connection

Virtual Private Gateway

VPC Peering

VPC Endpoints

NAT Gateway

IP Address & Subnets

8 + 8 + 8 + 8 = 32 bits

192 . 168 . 100 . 201

Octet = 8bits

IP CIDR Range: 10 . 0 . 0 . 0 / 16

10 . 0 . 0 . 0 – 10 . 0 . 255 . 255

Private IP Addresses

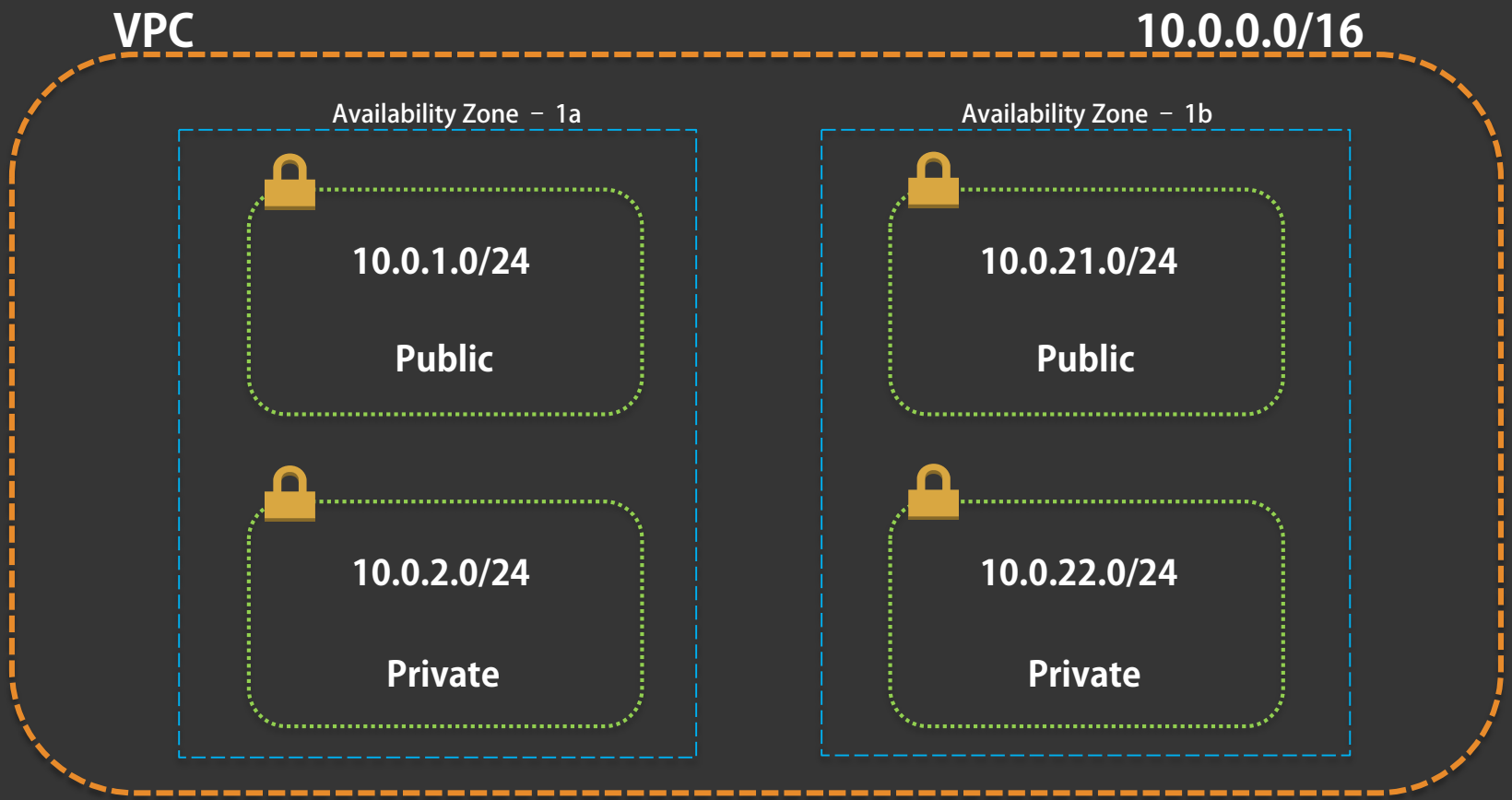
RFC1918 Standard

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

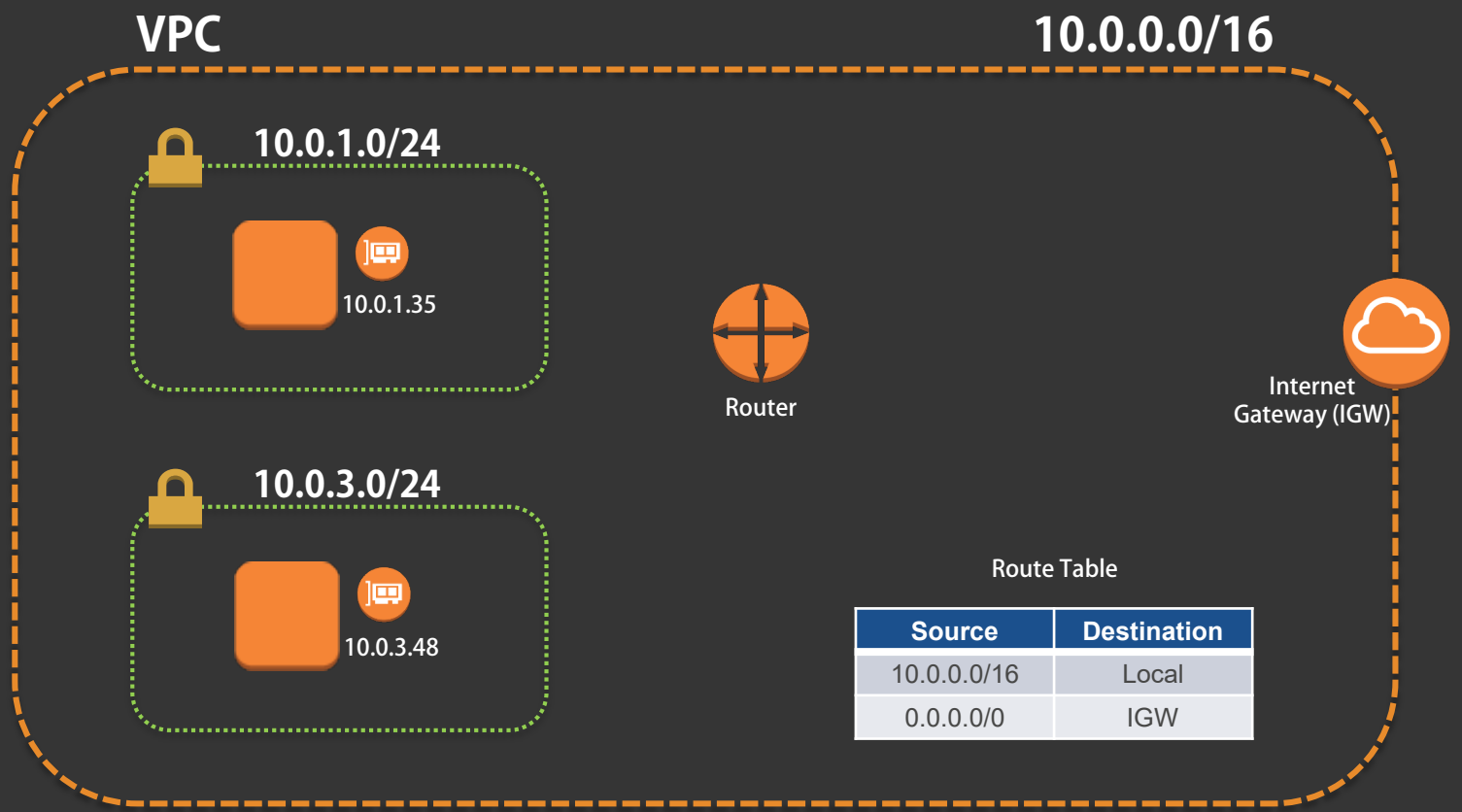
Reserved IP Addresses

- 10.0.0.0: Network address.
- 10.0.0.1: Reserved by AWS for the VPC router.
- 10.0.0.2: Reserved by AWS. The IP address of the DNS server
- 10.0.0.3: Reserved by AWS for future use.
- 10.0.0.255: Network broadcast address. Broadcast is not supported in a VPC, therefore this address is reserved.

Subnets



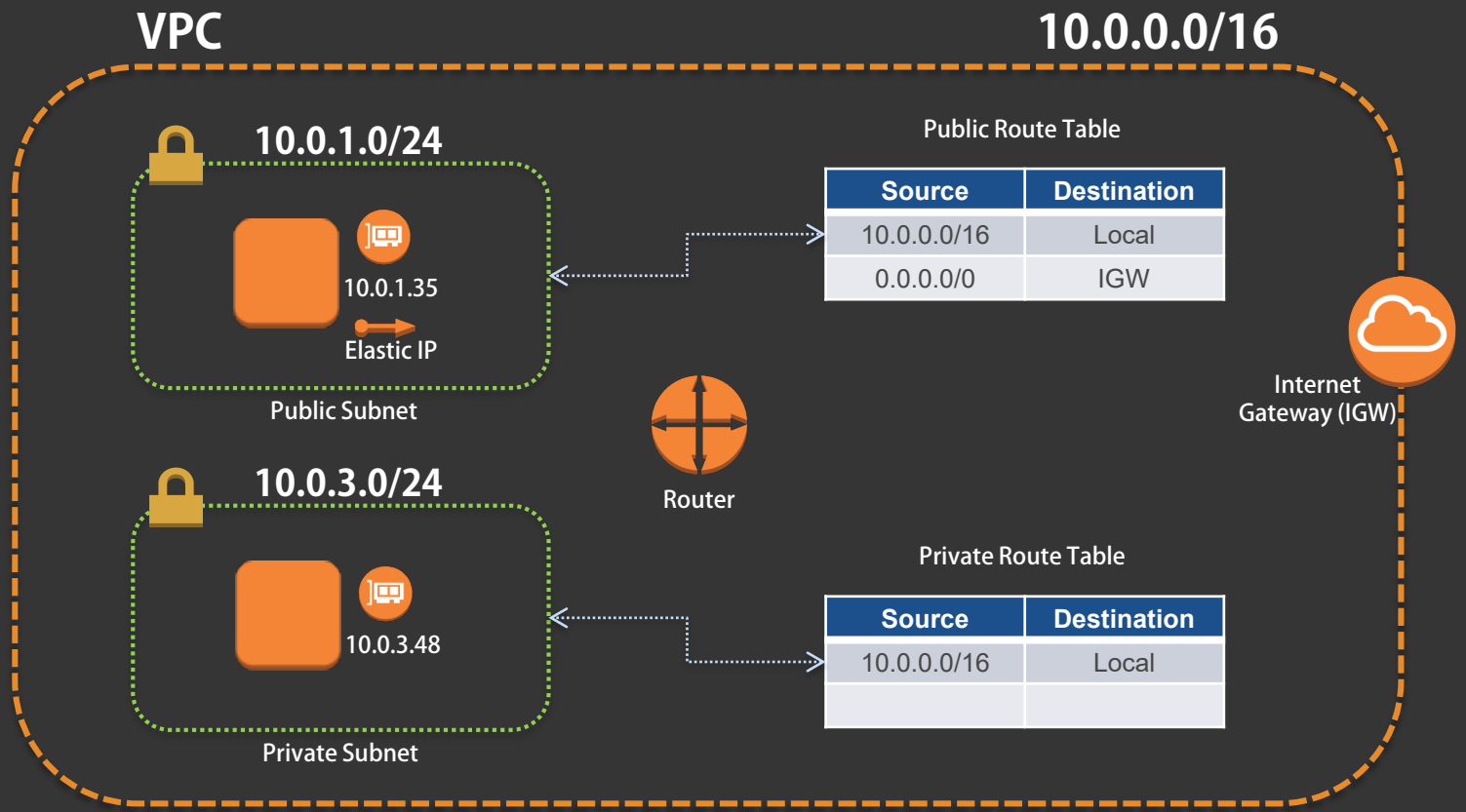
Routing



Route Table

Source	Destination
10.0.0.0/16	Local
0.0.0.0/0	IGW

Routing



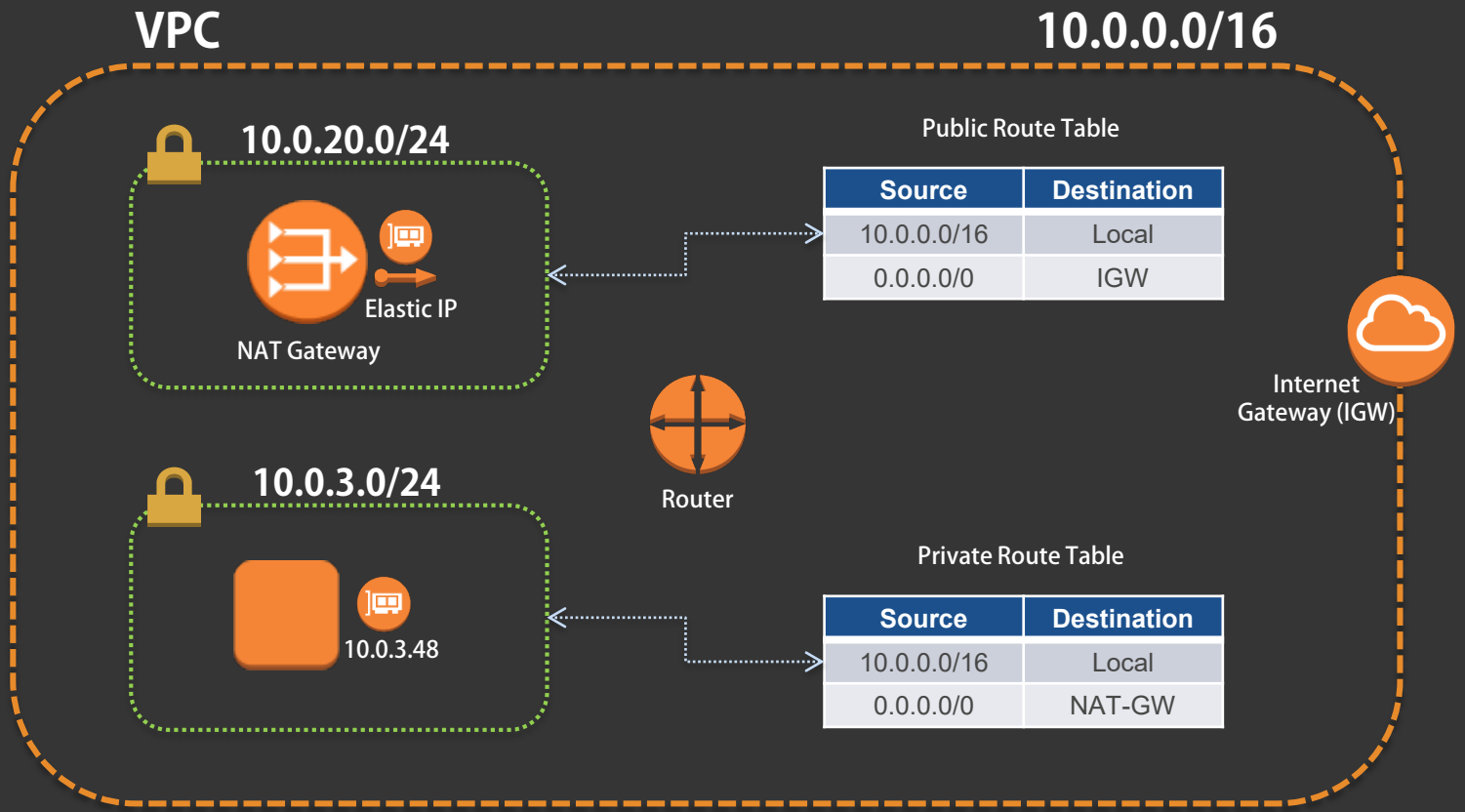
NAT Gateway

- An AWS managed Network Address Translation (NAT) gateway to enable instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection to those instances.

- Allows your instances to perform updates/patching whilst still being inside a private subnet

- Works only for IPv4. For IPv6, use Egress-only Internet Gateway

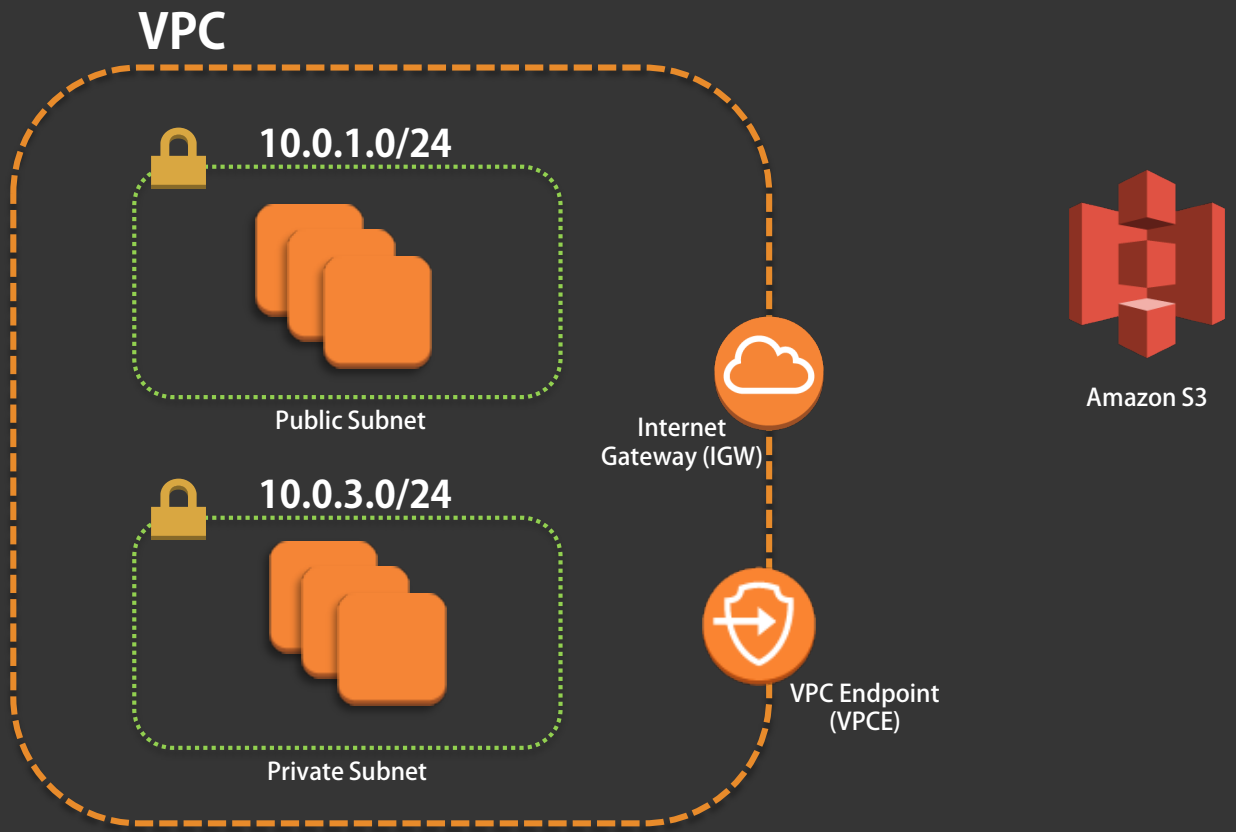
NAT Gateway



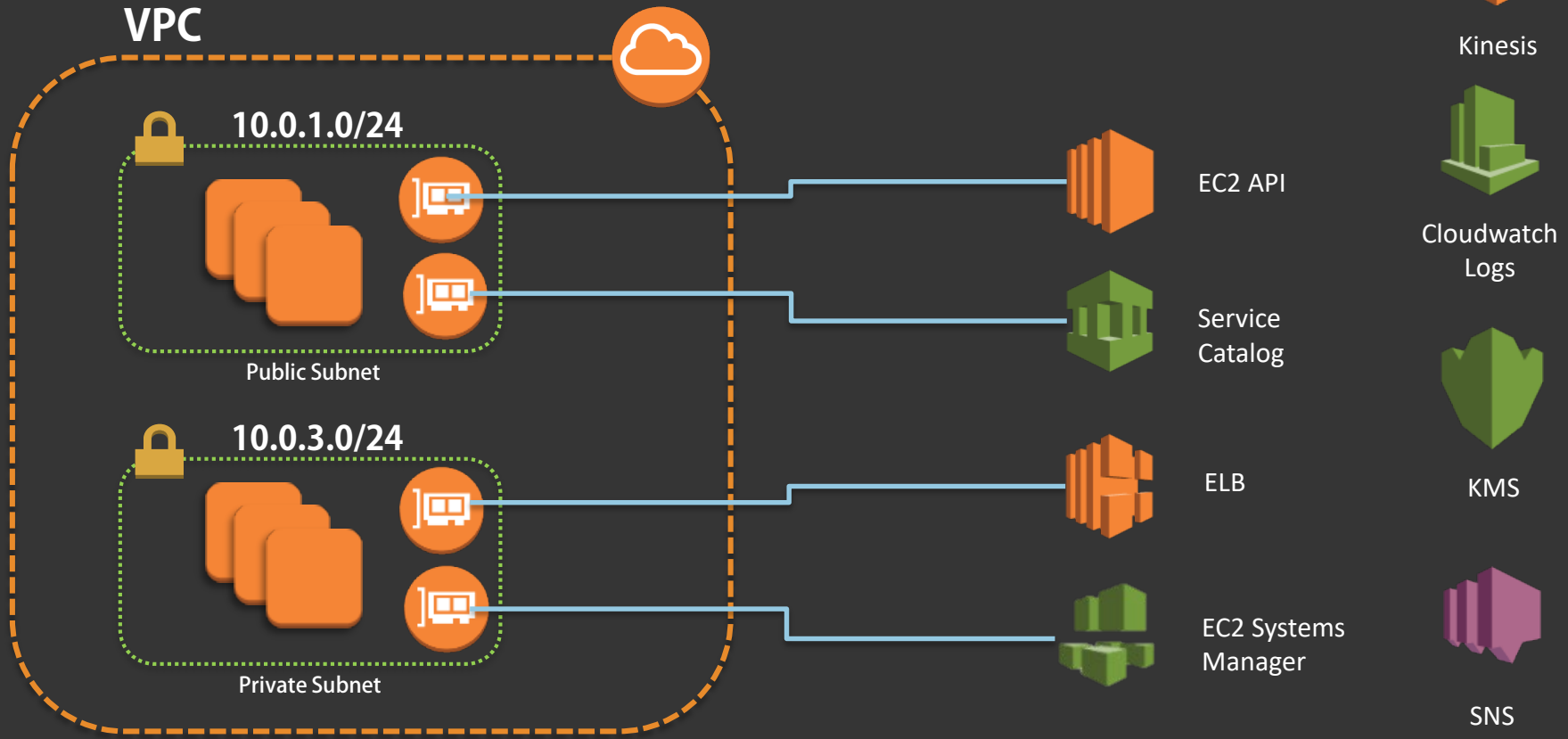
Key Points

- VPCs are limited to a region but stretch across AZs.
- Subnets can be Private or Public and are limited to a single AZ.
- Subnets must be associated with Route Tables.
- An Interget Gateway route must be added in the Route Rable rule for internet inbound/outbound.
- A NAT gateway can be used to simulate DMZs where inbound public access is blocked but external internet access is allowed.
- 5 IPs are un-usable/reserved – { .0 | .1 | .2 | .3 | .255 }

VPC Endpoints



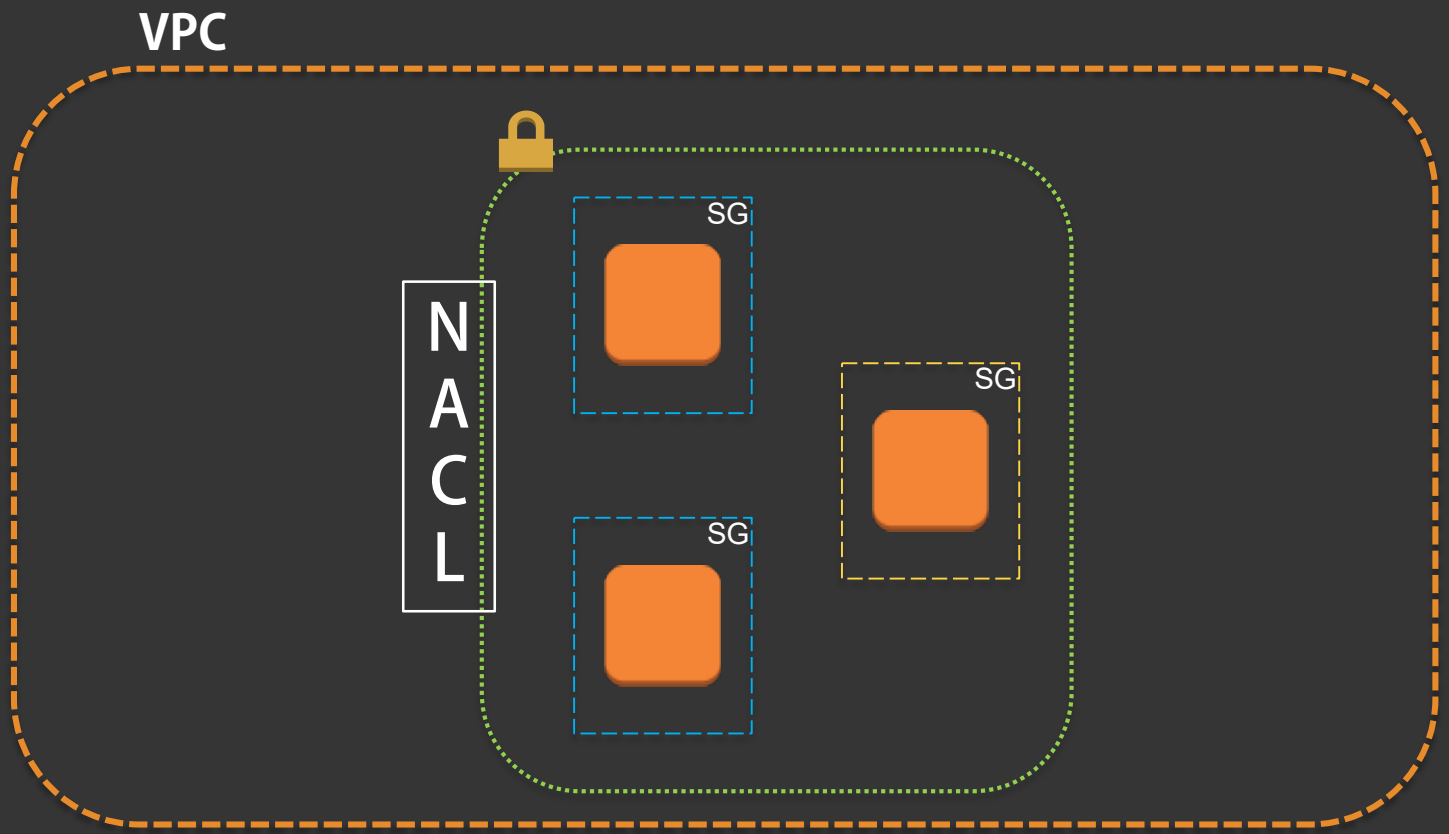
VPC Interface Endpoints



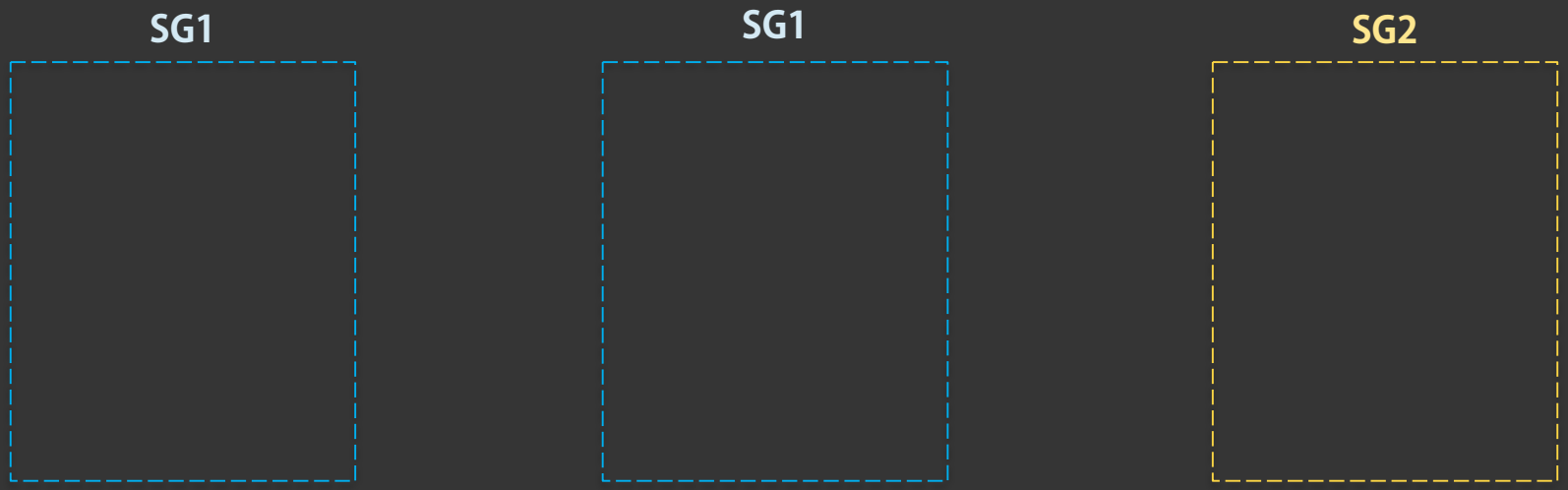
VPC Security & Logging

- NACLs
- Security Groups
- Flow Logs

NACLs & Security Groups



Security Groups



NACLs & Security Groups

Security Group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
All rules before deciding whether to allow traffic	Rules in number order when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets it's associated with (backup layer of defence, so you don't have to rely on someone specifying the security group)

VPC Labs