Architecting on AWS

Amazon Virtual Private Cloud

1 What is Amazon VPC?

2 Subnets, gateways, and routes

3 Advanced Features

VPC | What is Amazon VPC?

1

What is Amazon VPC?

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a **virtual network** that you've defined.

VPC |What is Amazon VPC?

Specify your own private IP address range from any ranges you choose

VPC | What is Amazon VPC?

Divide your private IP address range into one or more public or private subnets.

Specify your own private IP address range from any ranges you choose

VPC | What is Amazon VPC?

Divide your private IP address range into one or more public or private subnets.

Specify your own private IP address range from any ranges you choose

Control Inbound and outbound access to and from individual

Architecting With AWS

VPC | What is Amazon VPC?

Divide your private IP address range into one or more public or private subnets.

Specify your own private IP address range from any ranges you choose

Control Inbound and outbound access to and from individual

Assign multiple IP address and attach multiple ENIs and EIPs to EC2 instances

VPC |What is Amazon VPC?

Divide your private IP address range into one or more public or private subnets.

Specify your own private IP address range from any ranges you choose

Control Inbound and outbound access to and from individual

Bridge your VPC and your onsite IT infrastructure with an encrypted VPN connection

Assign multiple IP address and attach multiple ENIs and EIPs to EC2 instances

VPC |What is Amazon VPC?

Divide your private IP address range into one or more public or private subnets.

Specify your own private IP address range from any ranges you choose

Control Inbound and outbound access to and from individual

Only cost is optional hardware VPN ($0.05/hr)

Bridge your VPC and your onsite IT infrastructure with an encrypted VPN connection

Assign multiple IP address and attach multiple ENIs and EIPs to EC2 instances

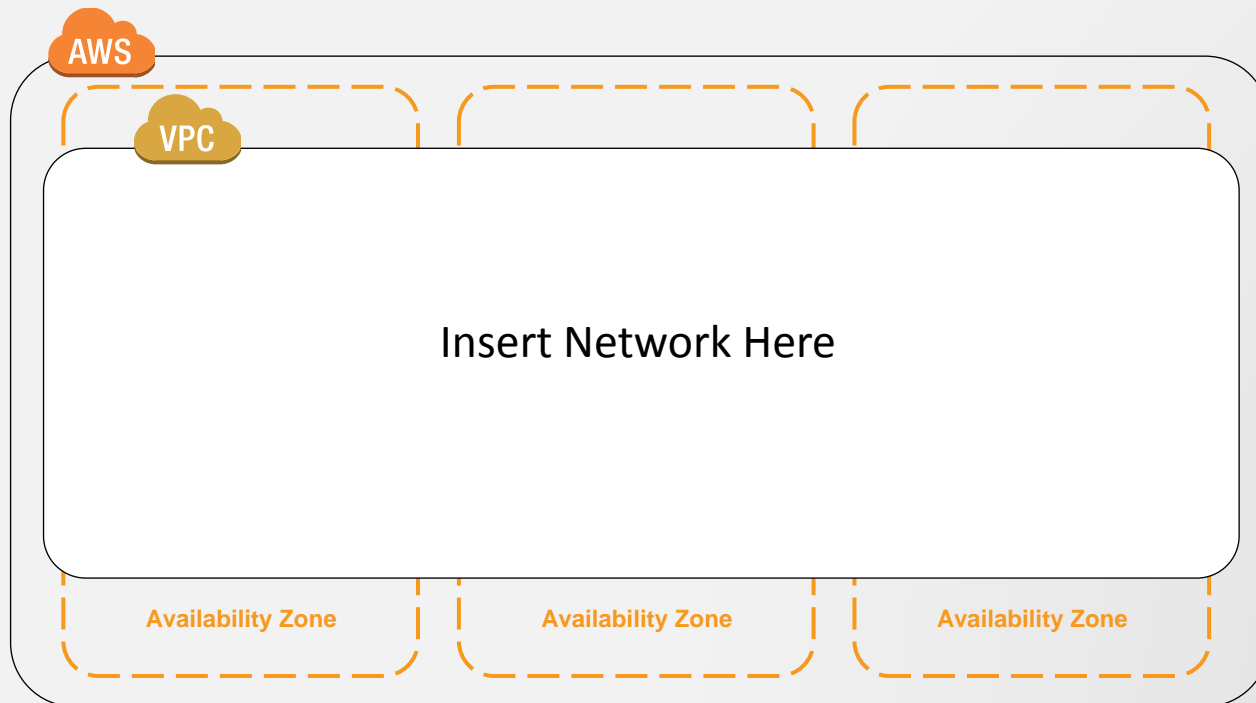**VPC |** Subnets, Gateways, and Routes

2

Subnets, gateways, and routes

With Amazon VPC, you can define a virtual network topology that closely resembles a traditional network that you might operate in **your own data center**.

Select an AWS region for your VPC

AWS

VPC

Insert Network Here

Availability Zone   **Availability Zone**   **Availability Zone**

VPC | Subnets, Gateways and routes

Select an AWS region for your VPC

- Specify the size of our network with a **CIDR block**

AWS

VPC

10.0.0.0/16

Availability Zone   **Availability Zone**   **Availability Zone**

VPC | **Subnets, Gateways and routes**
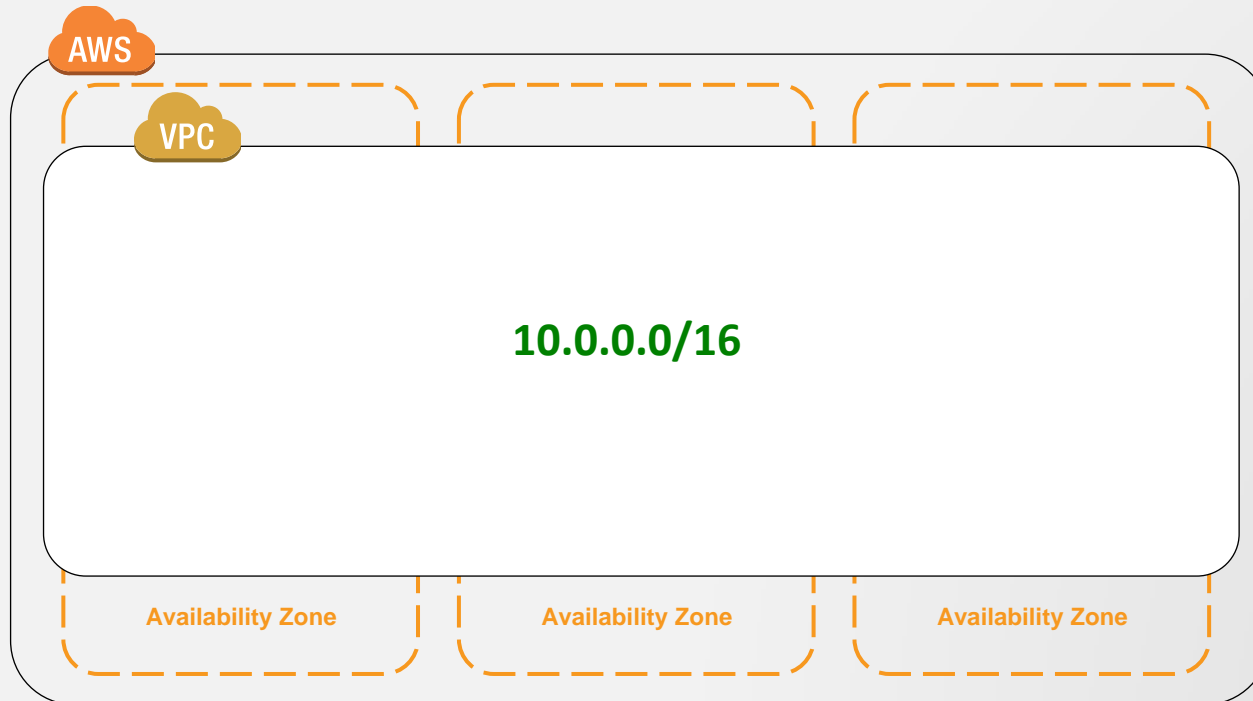
Create subnets inside the VPC

- Subnets do not span Availability Zones
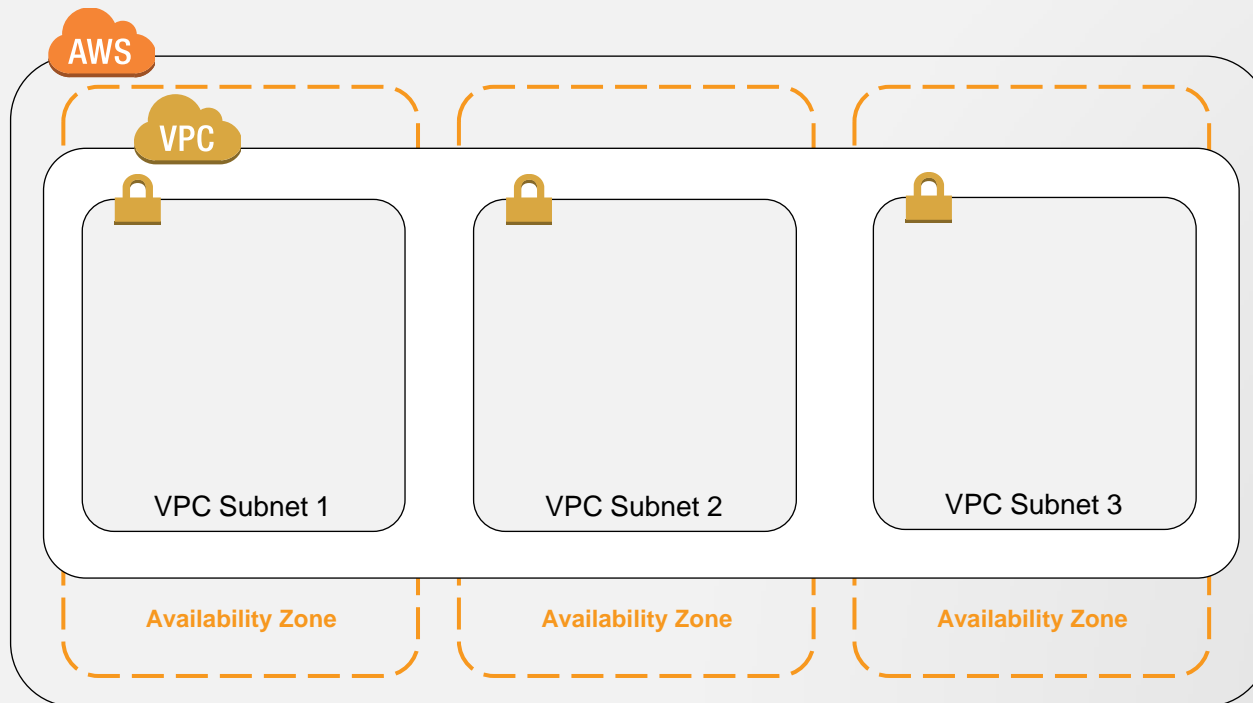
Create subnets inside the VPC

- Subnets do not span Availability Zones

- Each subnet has a CIDR range

10.0.100.0/24

10.0.150.0/24

10.0.200.0/24

Availability Zone   **Availability Zone**   **Availability Zone**

Attach Gateway Devices to Network

AWS

VPC

10.0.100.0/24

10.0.150.0/24

10.0.200.0/24

Availability Zone

Availability Zone

Availability Zone
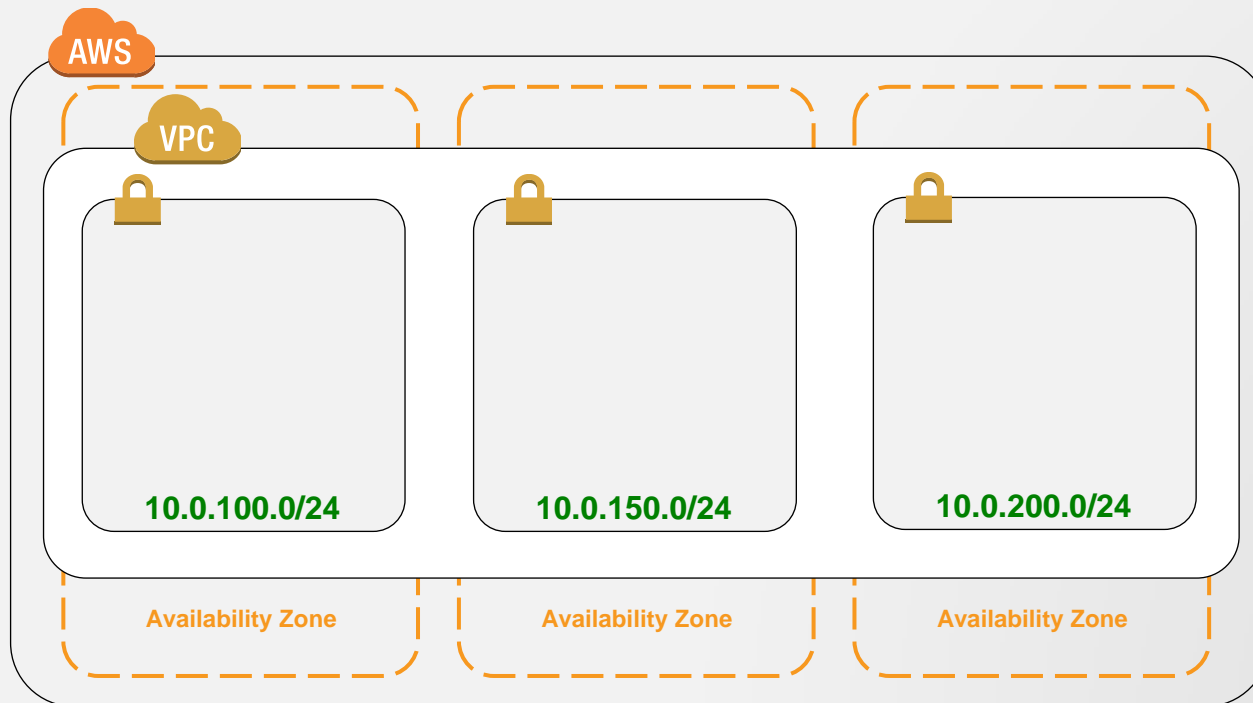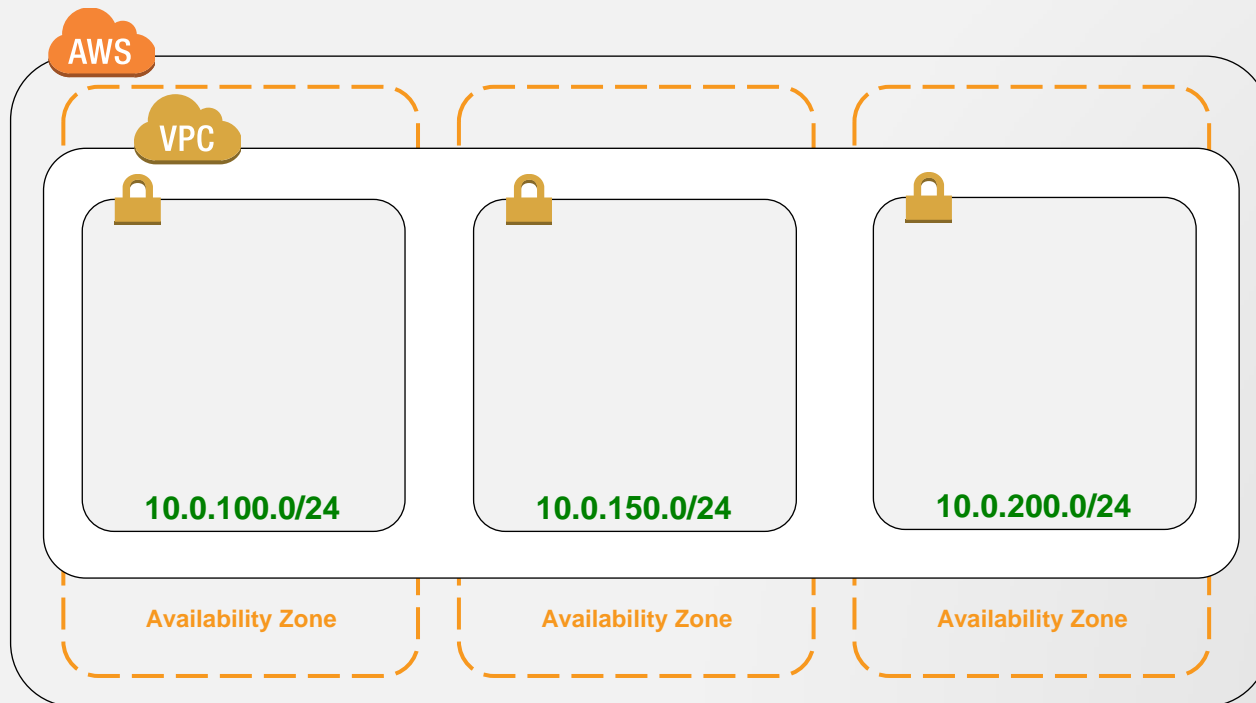
Attach Gateway Devices to Network

- **Internet Gateway (IGW)** allows subnet(s) to route to public Internet

10.0.100.0/24

10.0.150.0/24

10.0.200.0/24

Availability Zone

Availability Zone

Availability Zone
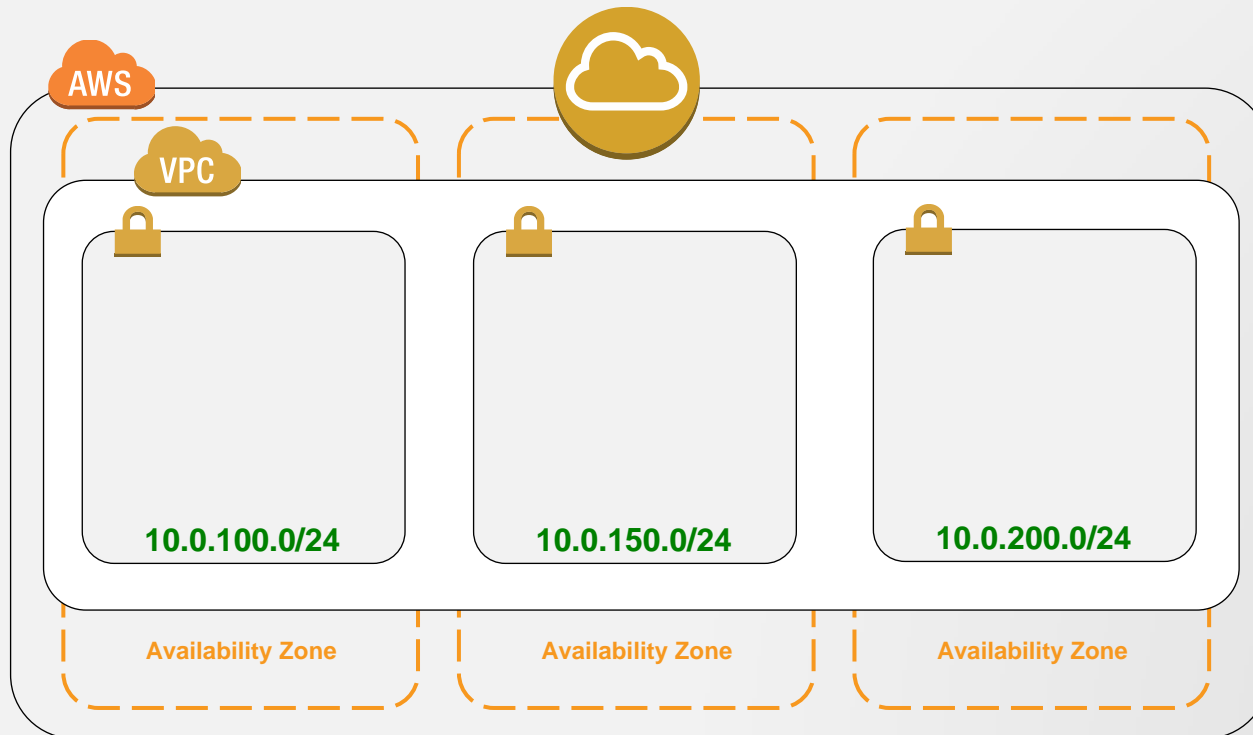
Attach Gateway Devices to Network

- **VPN Gateway (VGW)** allows subnet(s) to route to on-premises network over IPSEC VPN
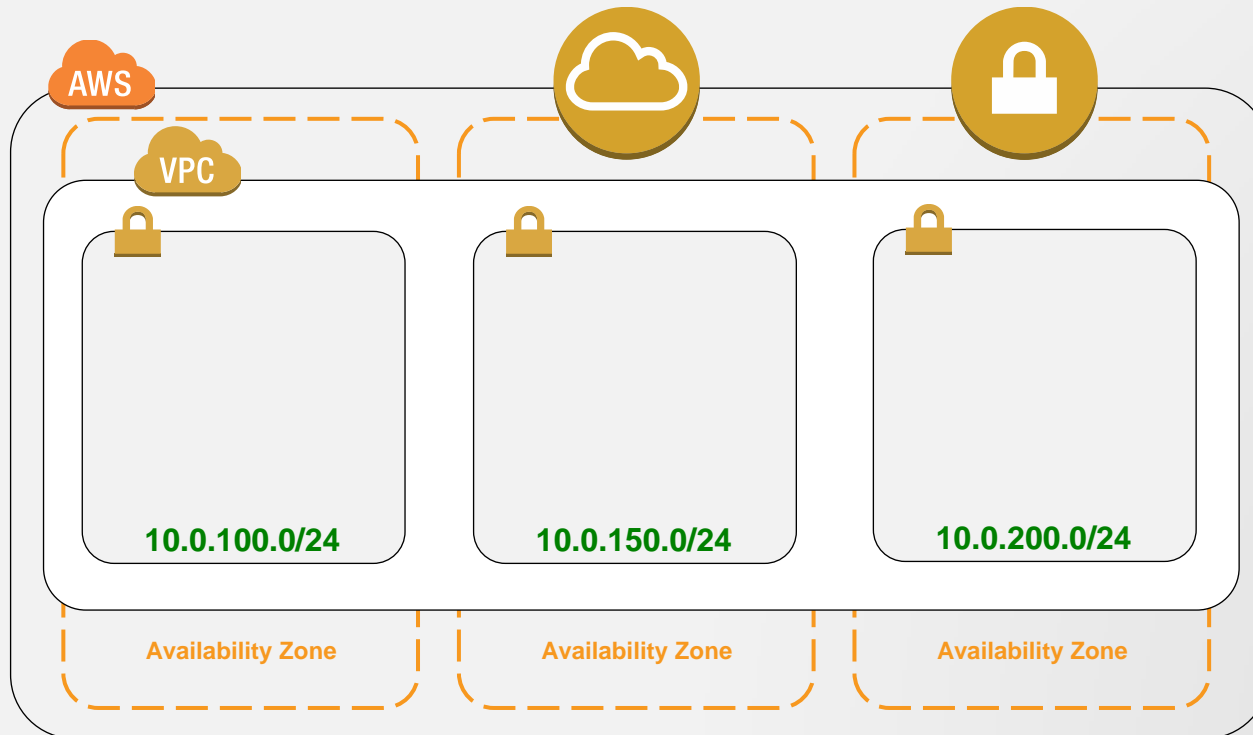
Define custom routing rule(s) for each subnet

AWS

VPC

10.0.100.0/24

10.0.150.0/24

10.0.200.0/24

Availability Zone

Availability Zone

Availability Zone
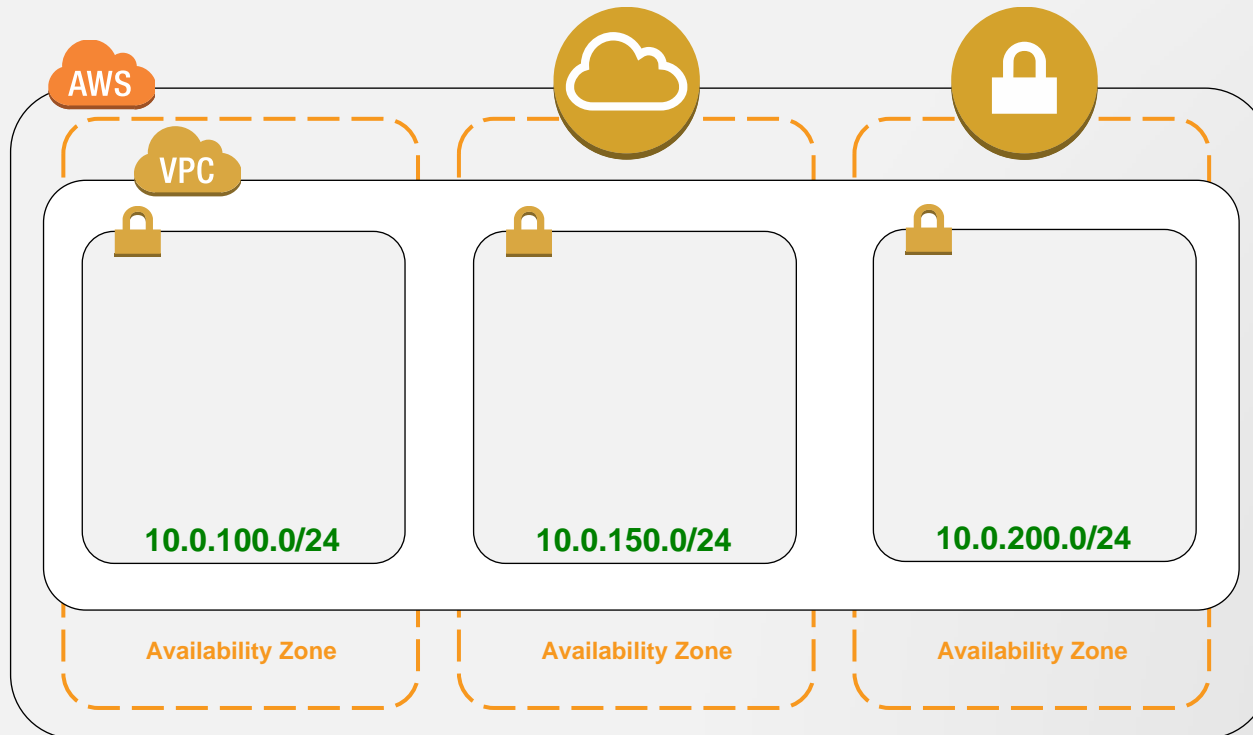
Private subnet with IPSEC VPN to corporate datacenter via VGW

AWS

VPC

10.0.100.0/24

10.0.150.0/24

10.0.200.0/24

Route Table	
Destination	Target
172.16.0.0/16	VGW

Availability Zone

Availability Zone

Availability Zone

Corporate Data center

VPC | **Subnets, Gateways and routes**
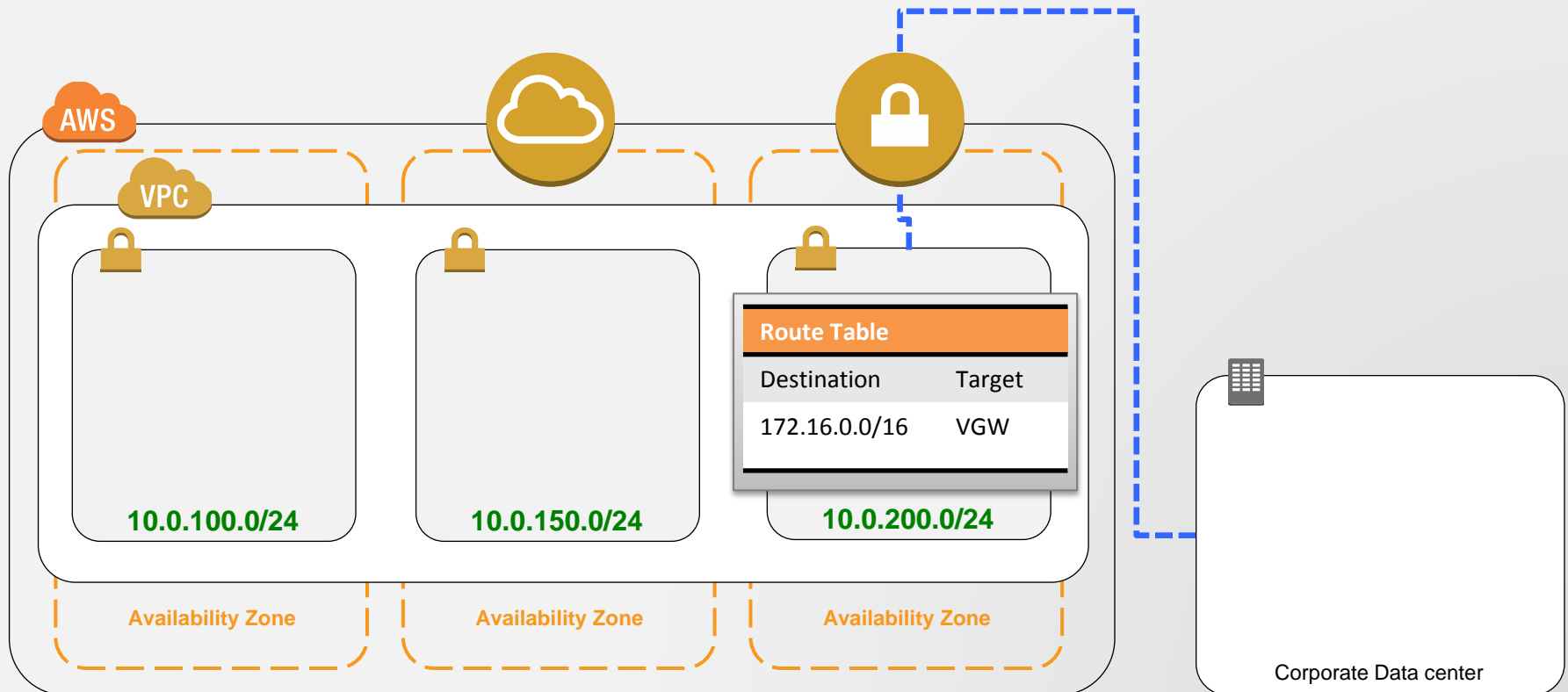
Public subnet with inbound/outbound Internet connectivity via IGW

Route Table	
Destination	Target
0.0.0.0/0	IGW

10.0.100.0/24

10.0.150.0/24

10.0.200.0/24

AWS

VPC

Availability Zone

Availability Zone

Availability Zone

Corporate Data center
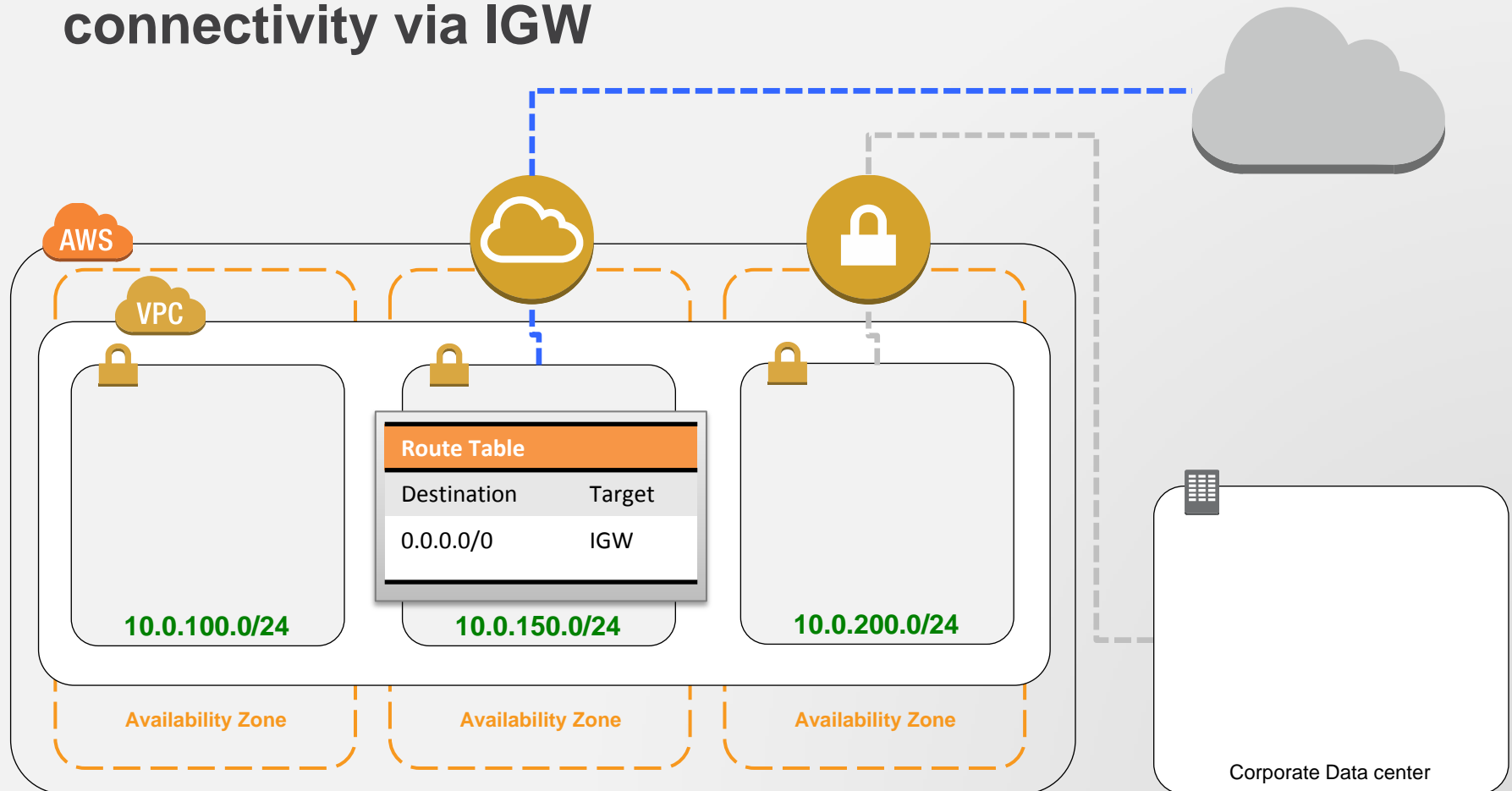
Private subnet with outbound Internet connectivity via EC2 Instance running NAT in public subnet

Route Table	
Destination	Target
0.0.0.0/0	i-123456

NAT Instance

10.0.100.0/24

10.0.150.0/24

10.0.200.0/24

AWS

VPC

Availability Zone

Availability Zone

Availability Zone

Corporate Data center
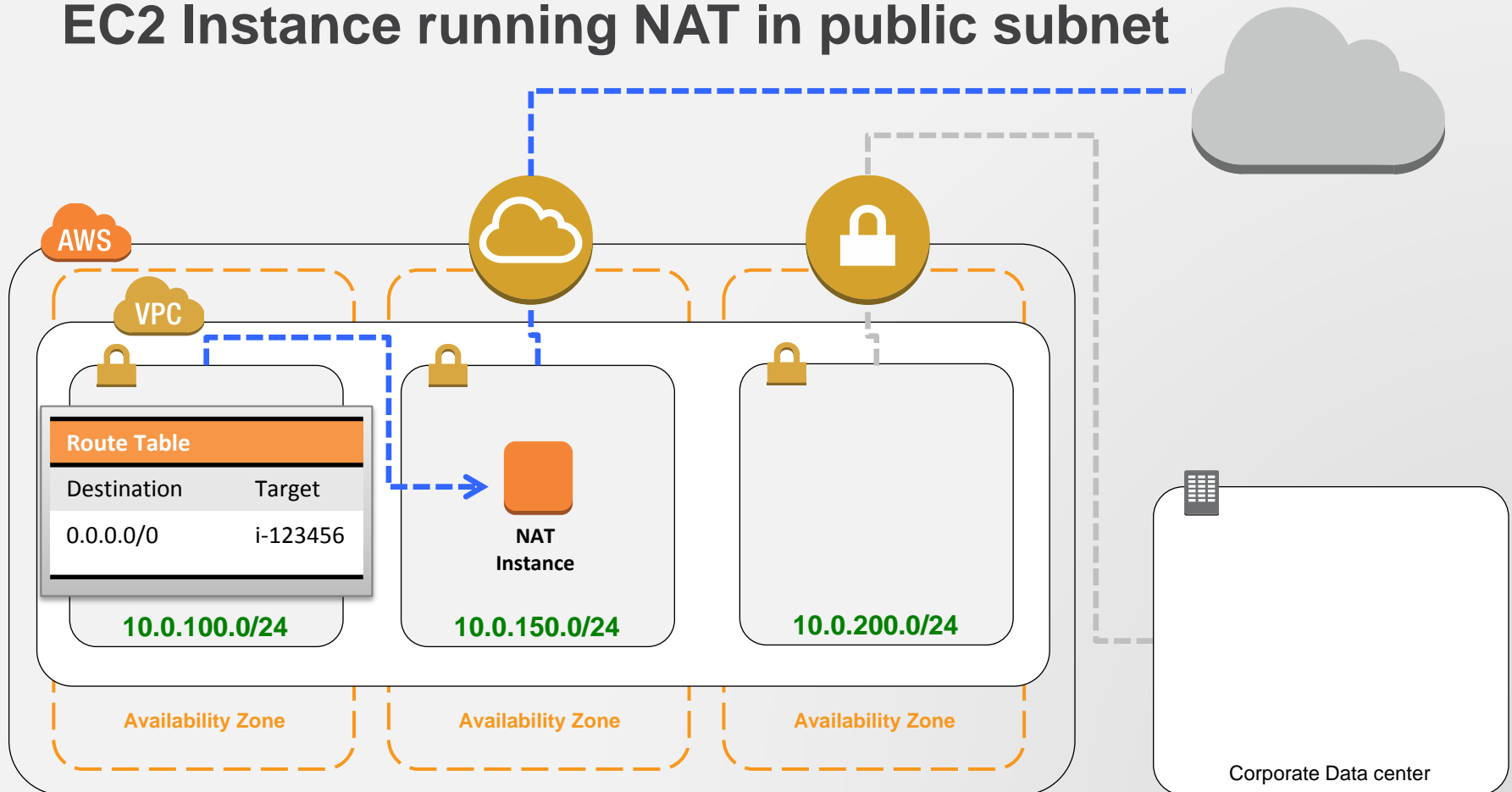
Network Access Control Lists allow or deny traffic entering or existing the subnet

AWS

VPC

SSH

NAT Instance

10.0.100.0/24

10.0.150.0/24

10.0.200.0/24

Availability Zone

Availability Zone

Availability Zone

Corporate Data center

RDP

VPC | Advanced Features

3
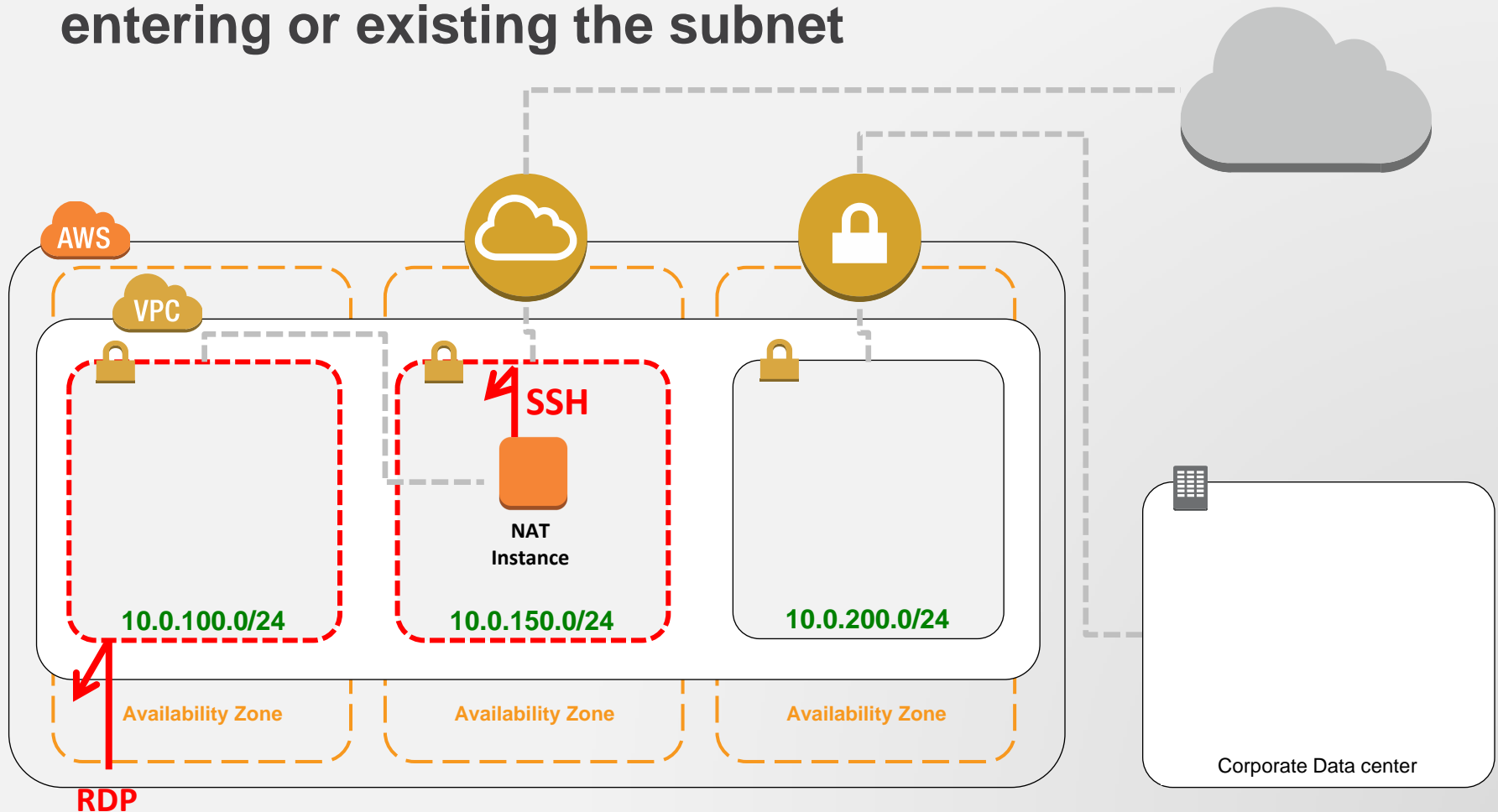
Advanced Features

Amazon Virtual Private Cloud (Amazon VPC) includes features such as security groups, network access control lists, and Elastic Network Interfaces (ENIs).

VPC | Advanced Features

Security Groups

Web (HTTP)

AWS

VPC

VPC Subnet 1

VPC Subnet 3

VPC Subnet 2

VPC Subnet 4

M

S

Availability Zone

Availability Zone
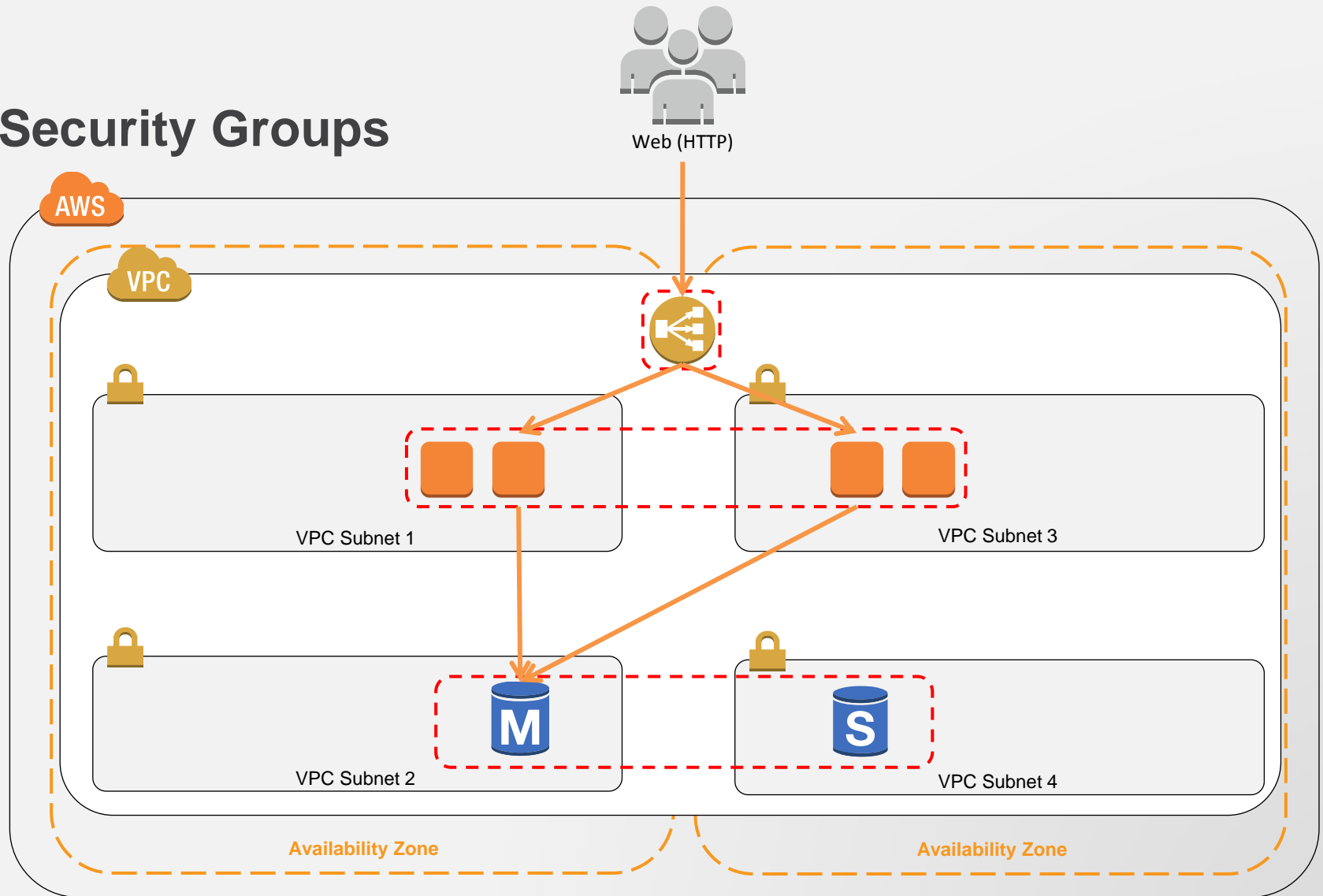
Network Access Control Lists

Elastic Network Interface (ENI)

AWS

VPC

VPC Subnet 1

eth0
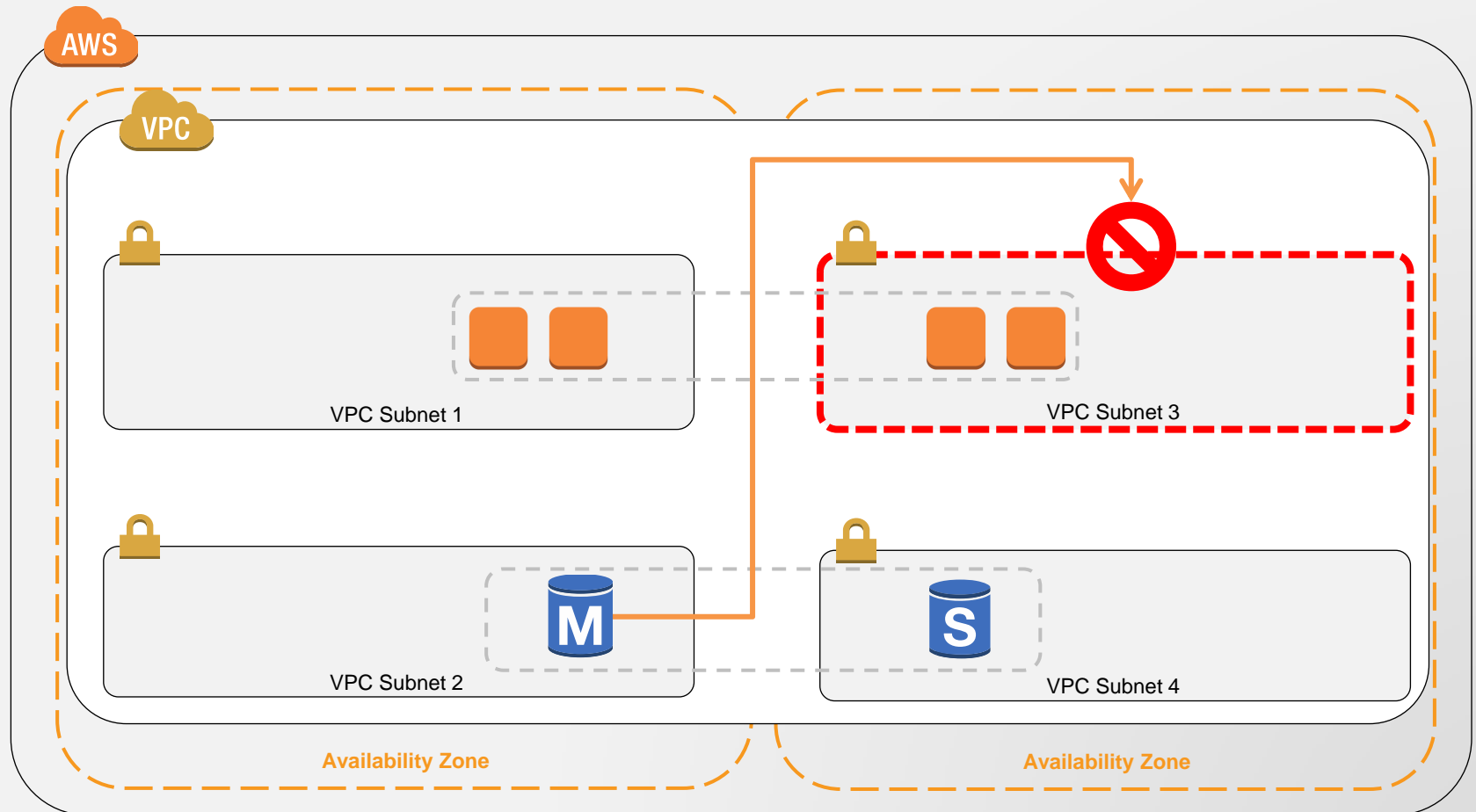
Every instance has a primary ENI

VPC Subnet 2

Availability Zone

Internet

Corporate Data center

Elastic Network Interface (ENI)

AWS

VPC

eth0

VPC Subnet 1

VPC Subnet 2

Availability Zone

Properties of an ENI:

- MAC address
- 1+ private IPs
- 1 Public EIP (optional)
- 1+ Security Groups
- Subnet
- DeleteOnTermination

Internet

Corporate Data center

Elastic Network Interface (ENI)

Properties of an ENI:

- *1a:dd:8b:a7:d8:e4*
- *10.0.0.135, 10.0.0.22*
- *54.236.244.12*
- *WebSecurityGroup*
- *subnet-5f9e7930*
- ***DeleteOnTermination=True***

AWS

VPC

eth0

VPC Subnet 1

VPC Subnet 2

Availability Zone

Internet

Corporate Data center

VPC |Advanced Features

Elastic Network Interface (ENI)

More than one ENI may be attached to an instance, and may exist in a different subnet

AWS

VPC

eth0

VPC Subnet 1

eth1

VPC Subnet 2

Availability Zone

Internet

Corporate Data center

Elastic Network Interface (ENI)

AWS

VPC

eth0

VPC Subnet 1

eth1

VPC Subnet 2

Availability Zone

Properties of eth1:

- *1c:de:2a:c2:b6:aa*
- *10.0.99.6*
- *No public IP (private subnet)*
- *ManagementSecurityGroup*
- *subnet-9a3075f*
- ***DeleteOnTermination=False***

Internet

Corporate Data center

VPC | **Advanced Features**
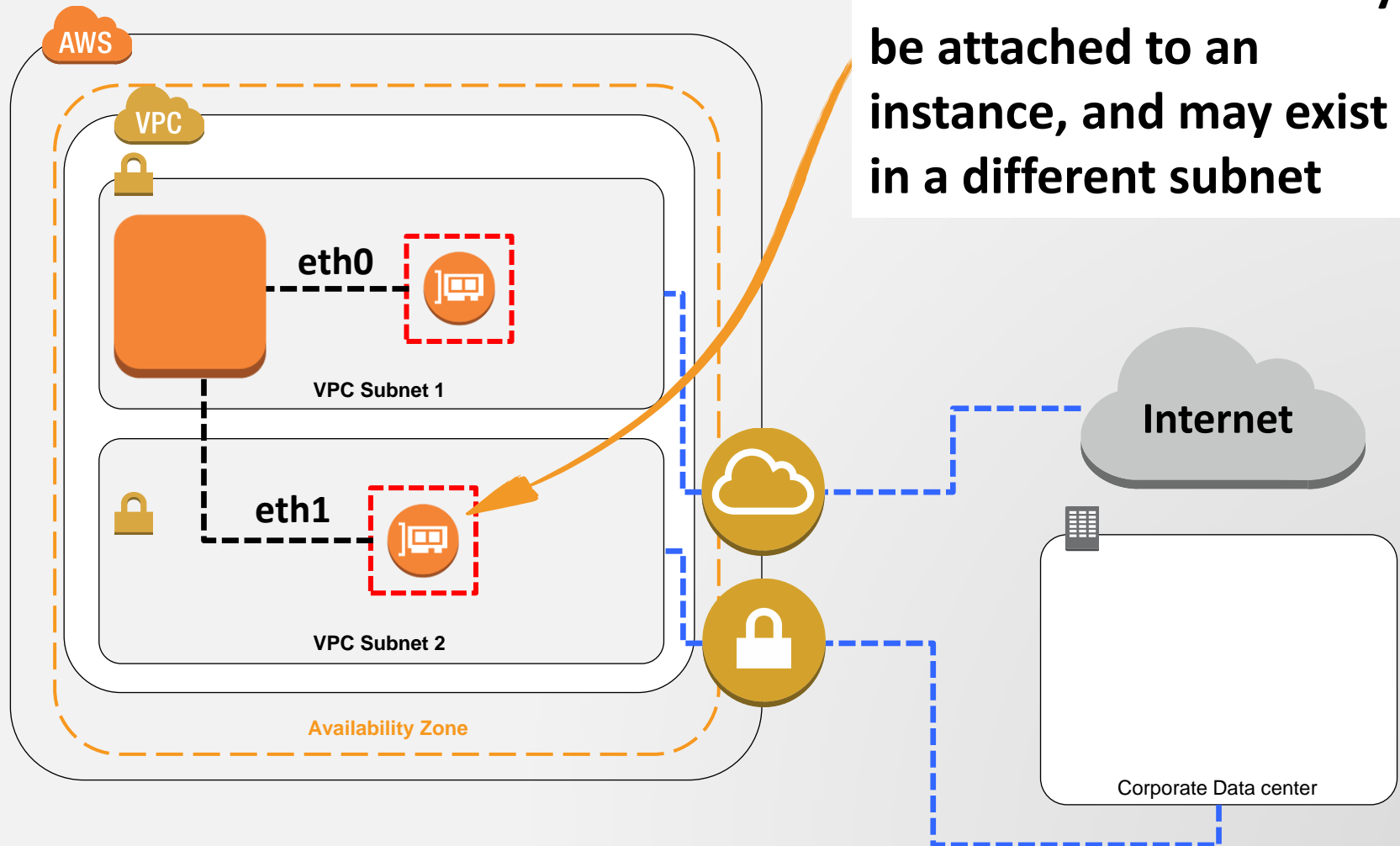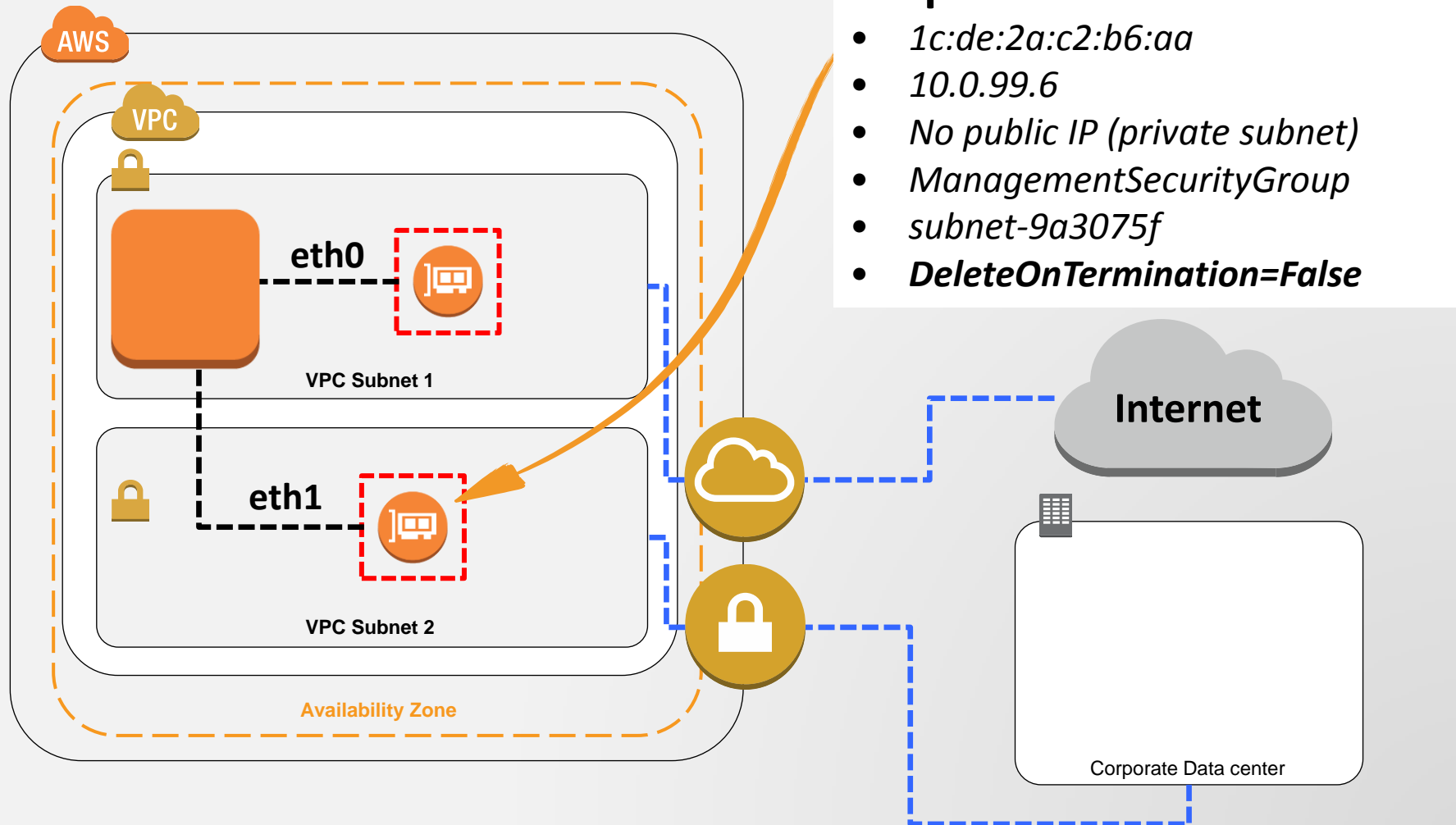
Elastic Network Interface (ENI)

Terminate instance
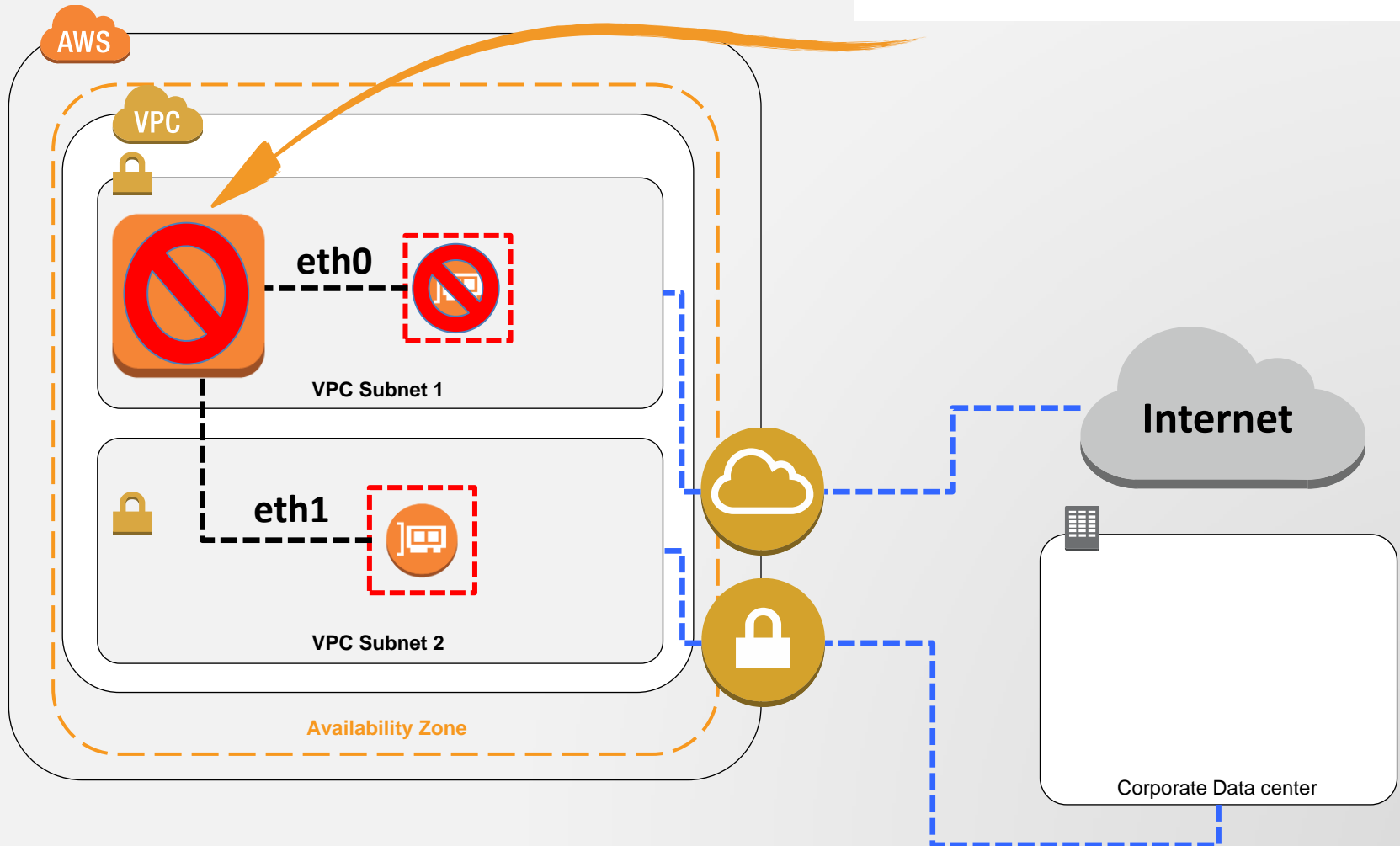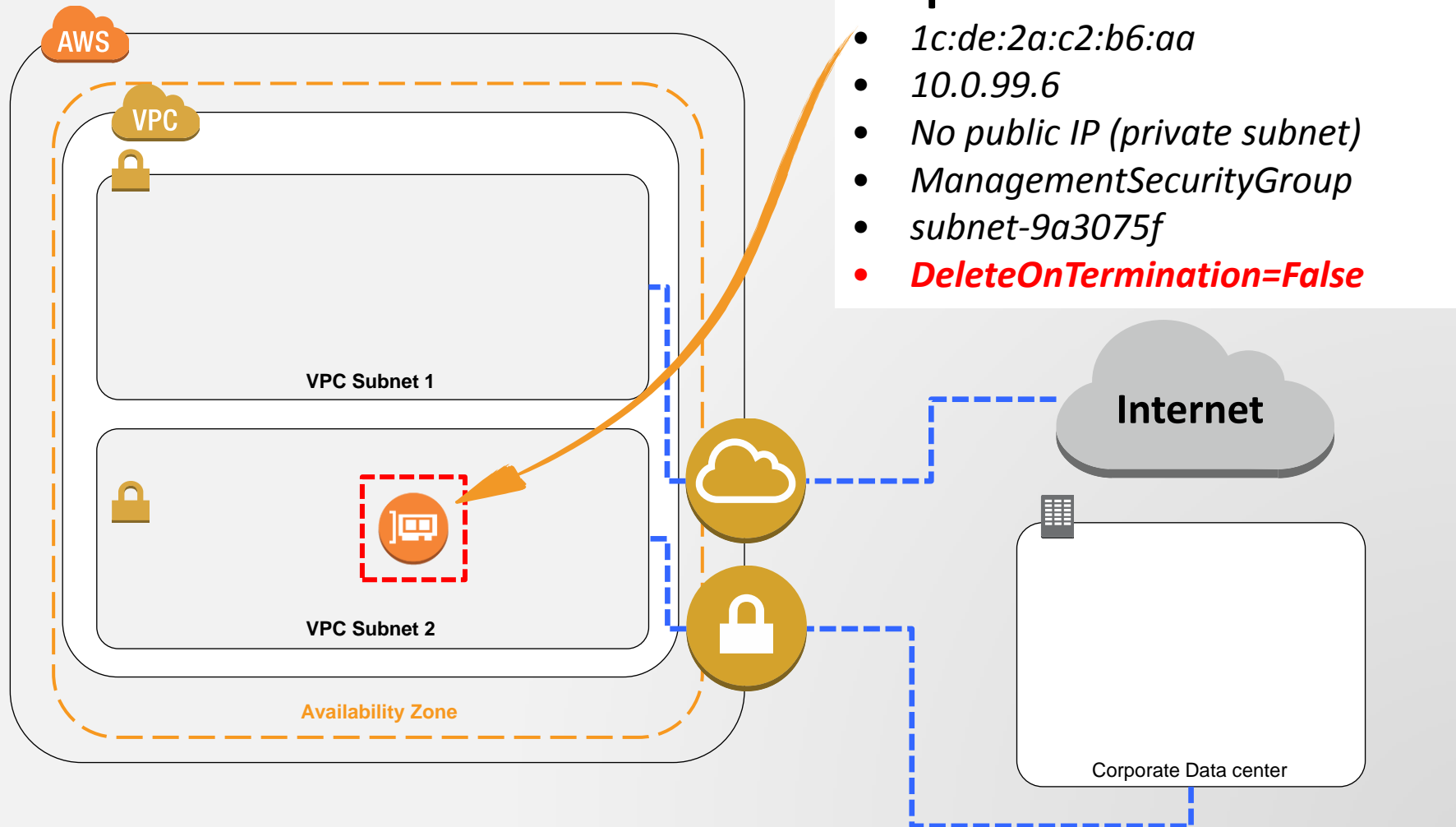
AWS

VPC

eth0

VPC Subnet 1

eth1

VPC Subnet 2

Availability Zone

Internet

Corporate Data center

VPC |Advanced Features

Elastic Network Interface (ENI)

AWS

VPC

VPC Subnet 1

VPC Subnet 2

Availability Zone

Internet

Corporate Data center

Properties of eth1:

- *1c:de:2a:c2:b6:aa*
- *10.0.99.6*
- *No public IP (private subnet)*
- *ManagementSecurityGroup*
- *subnet-9a3075f*
- ***DeleteOnTermination=False***

VPC | **Advanced Features**

Elastic Network Interface (ENI)

Launch new instance

AWS

VPC

eth0

VPC Subnet 1

VPC Subnet 2

Availability Zone

Internet

Corporate Data center

VPC |Advanced Features
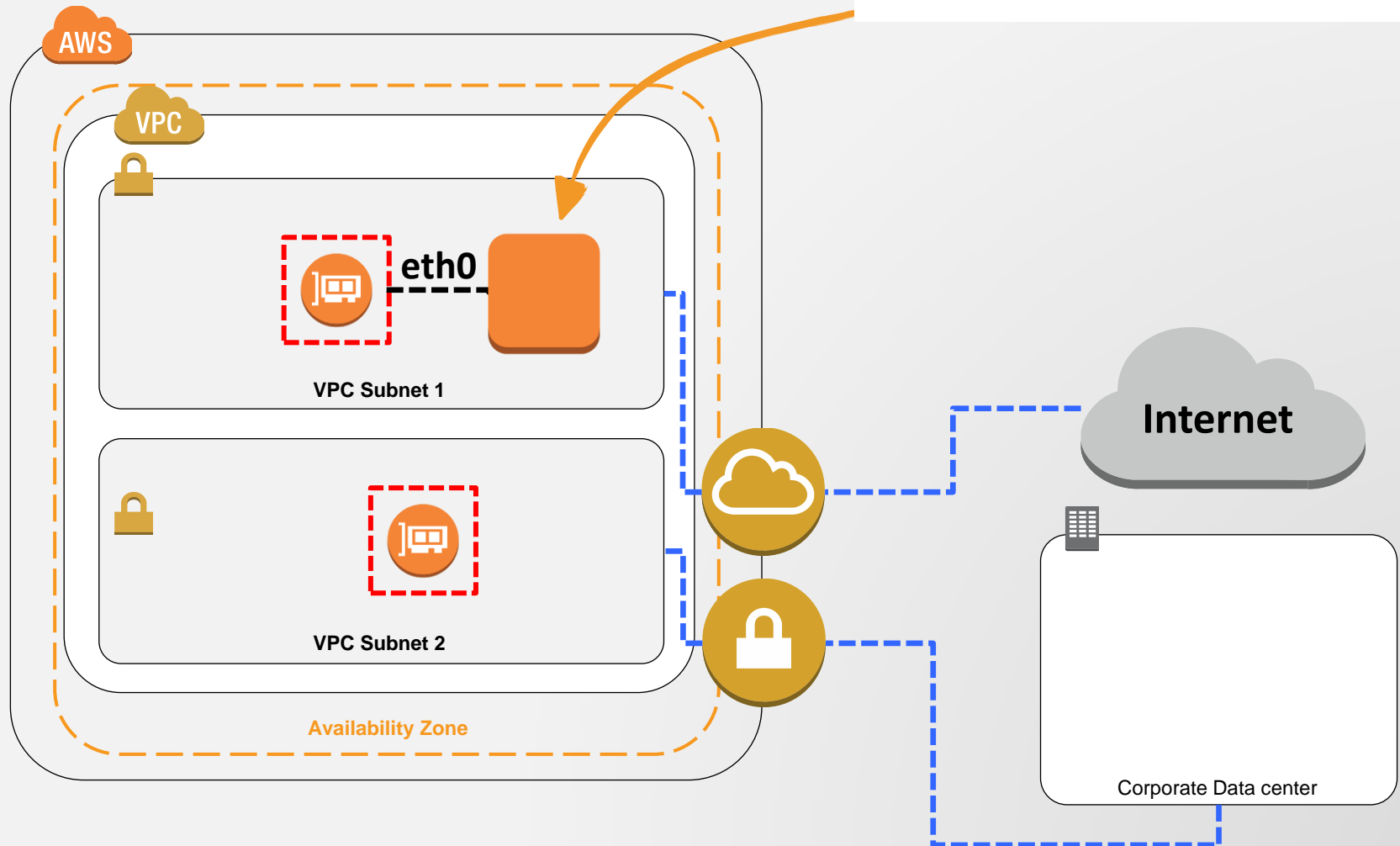
Elastic Network Interface (ENI)

Launch new instance, attach existing ENI

AWS

VPC

eth0

VPC Subnet 1

eth1

VPC Subnet 2

Availability Zone

Internet

Corporate Data center
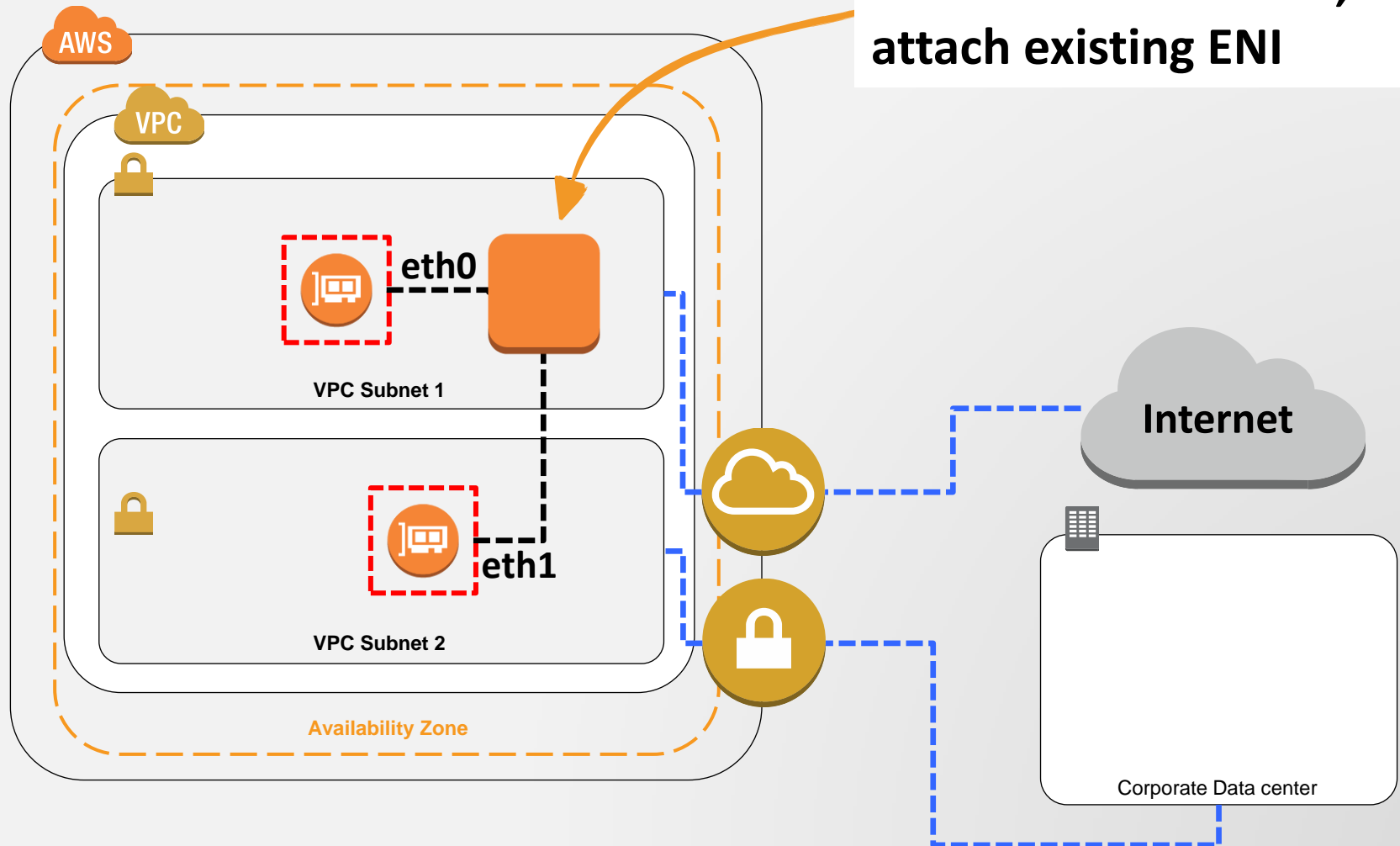
Load Balancing

Load Balancing

• External ELB

AWS

VPC

VPC Subnet 1

VPC Subnet 2

Availability Zone

Internet Gateway

VPN Gateway

Route Table
172.16.0.0
172.16.1.0
172.16.2.0

Route Table
172.16.0.0
172.16.1.0
172.16.2.0

Corporate Data center

VPC |Advanced Features
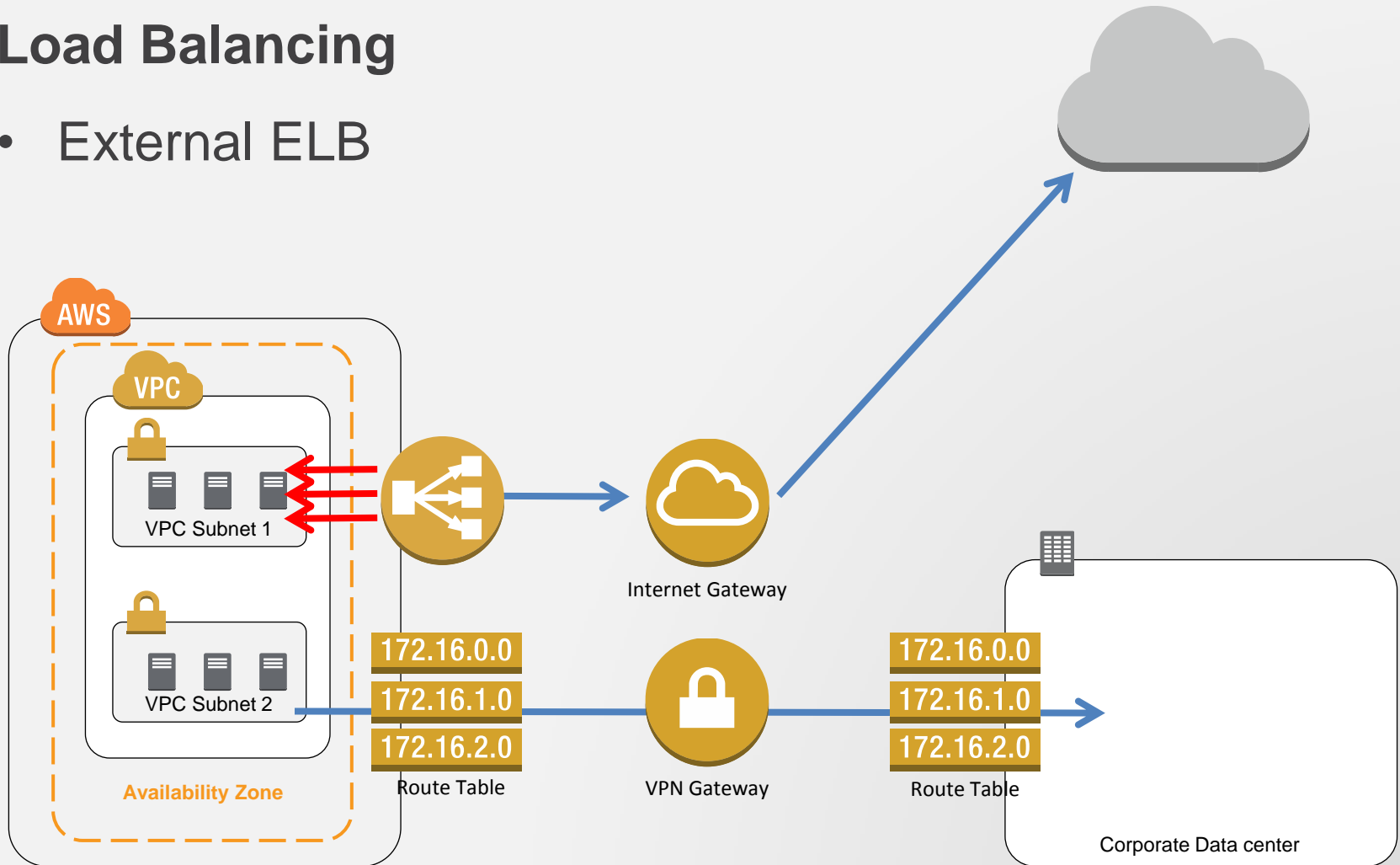
Load Balancing

- External ELB

- Mid-tier ELB

AWS

VPC

VPC Subnet 1

VPC Subnet 2

Availability Zone

Internet Gateway

VPN Gateway

Route Table

| 172.16.0.0 |
| 172.16.1.0 |
| 172.16.2.0 |

Route Table

| 172.16.0.0 |
| 172.16.1.0 |
| 172.16.2.0 |

Corporate Data center

VPC |Advanced Features
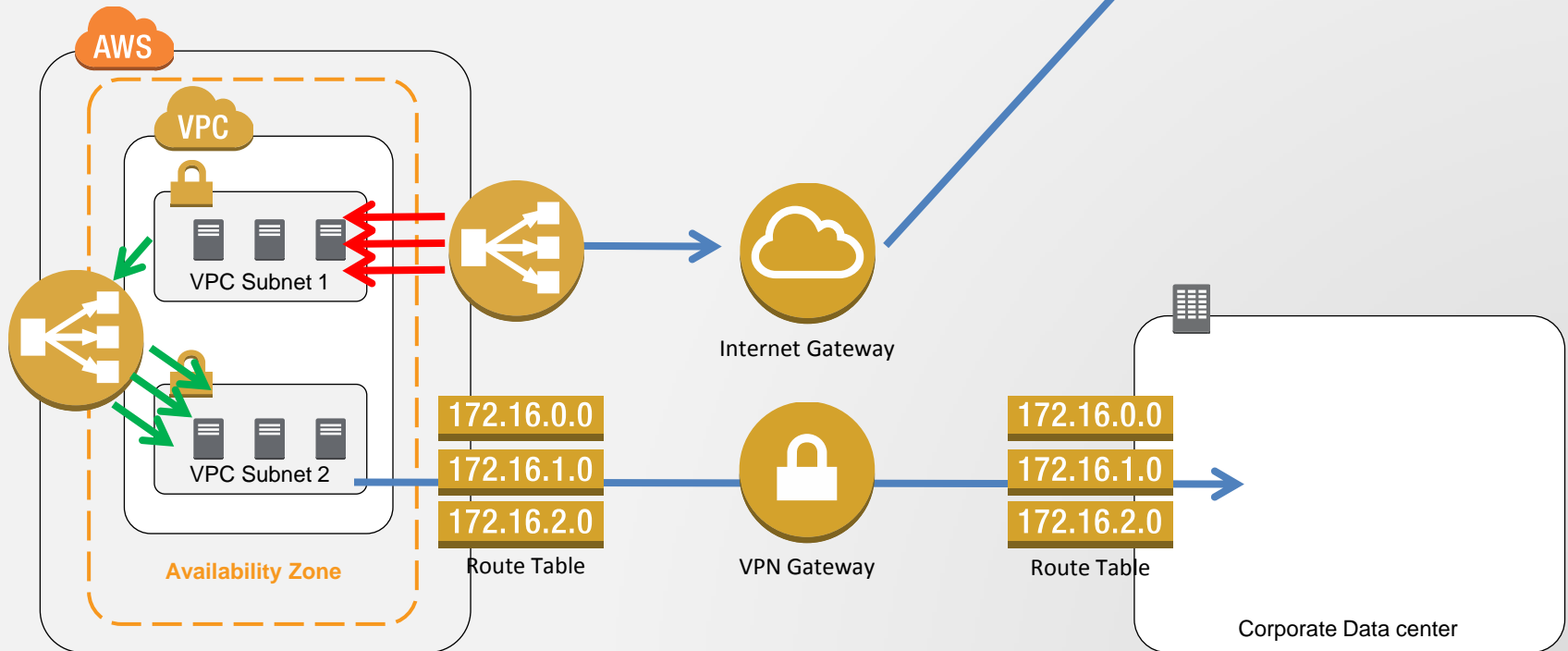
Load Balancing

- Intranet-facing ELB

Appendix

Internet

Customer Network
172.16.0.0/8

AWS

VPC

**Amazon EC2
API endpoint**

**Amazon S3
API endpoint**

**Web Server
10.0.0.5**
198.51.100.1 (EIP)

**NAT
10.0.0.8**
198.51.100.4 (EIP)

Internet
Gateway

VPN
Gateway

**DB Server
10.0.1.5**

**DB Server
10.0.1.7**

**Web Server
10.0.0.6**
198.51.100.2 (EIP)

**Web Server
10.0.0.7**
198.51.100.3 (EIP)

R

VPC
10.0.0.0/16

**DB Server
10.0.1.6**

Main Route Table

Destination	Target
10.0.0.0/16	local
172.16.0.0/8	Virtual Private Gateway
0.0.0.0/0	NAT Instance

Public Subnet
10.0.0.0/24

Private Subnet
10.0.1.0/24

Custom Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	Internet Gateway