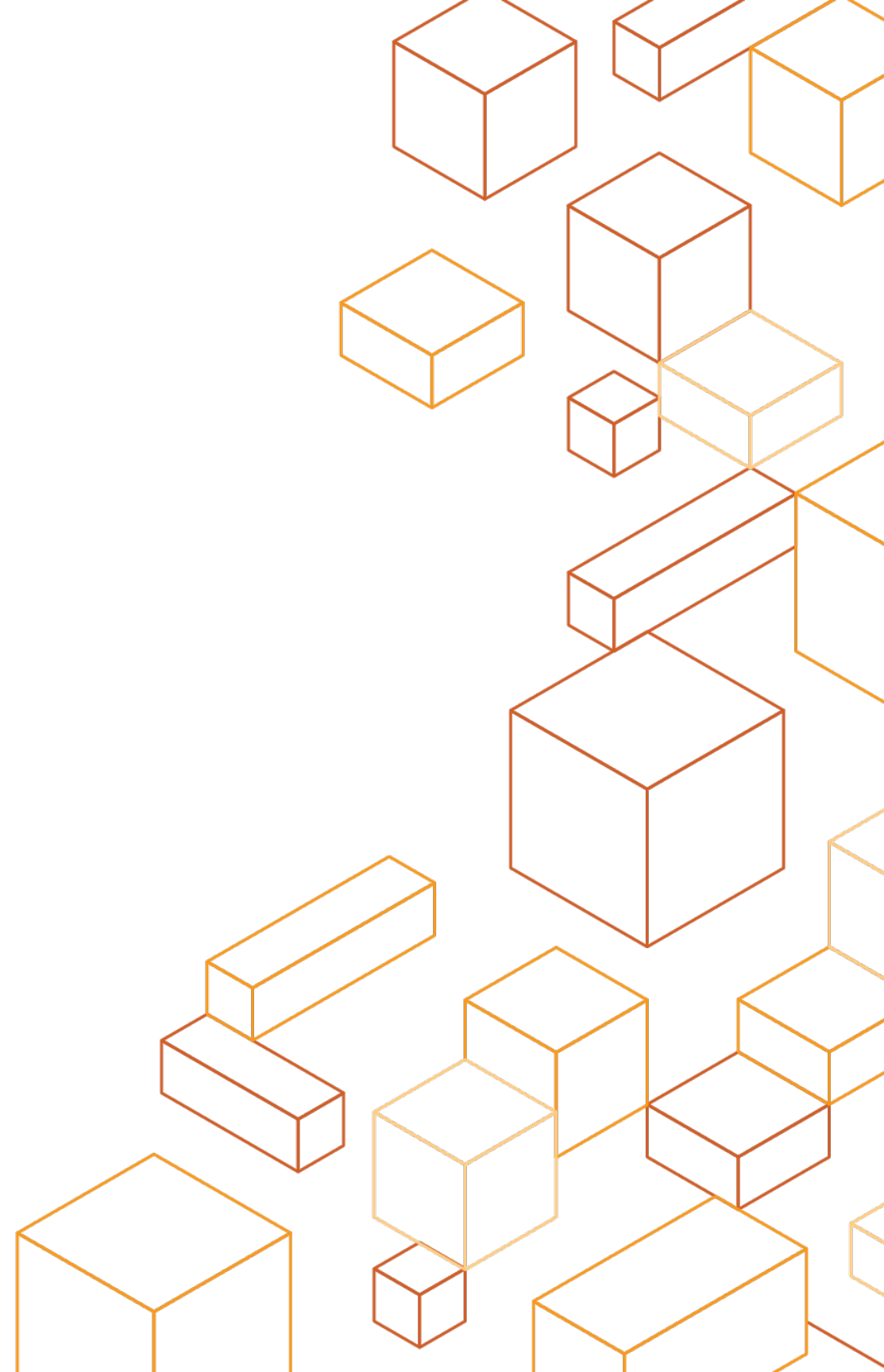


AWS VPC Overview



Agenda

- AWS Virtual Private Cloud
- Networking Concepts in AWS
- DNS
- Connectivity Features

Goals

- Understand how networking is implemented in AWS
- Discover features and functionality of VPC
- Learn how to connect other networks

Outcomes

- Decision on the number of VPC's and the relation between AWS Accounts and VPC's
- Decision on IP CIDR ranges
- Decision on DNS (Amazon DNS vs Self-managed AD)
- Decision on connectivity (Internet Gateway/Direct Connect/VPN)

Virtual Private Cloud (VPC)

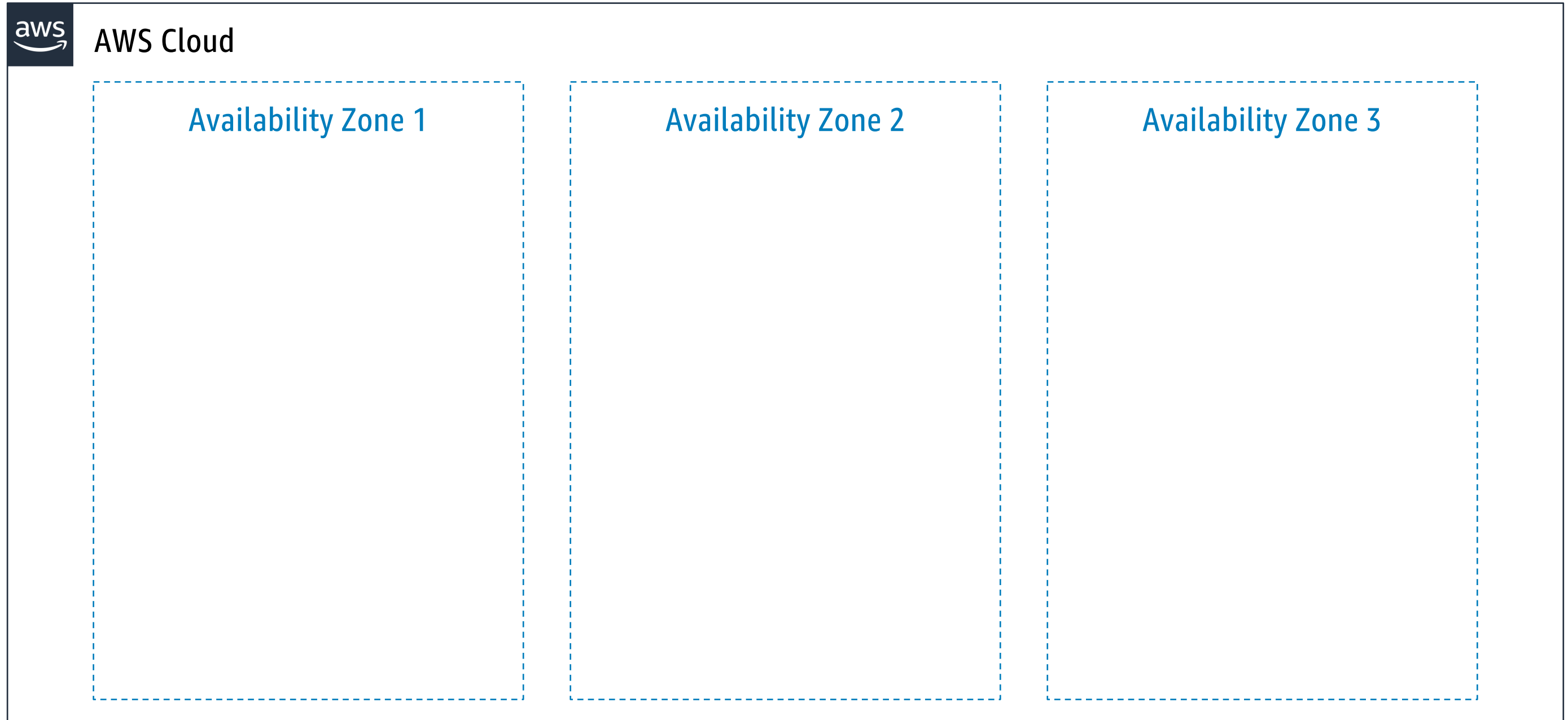
VPC Overview

What is a Virtual Private Cloud?

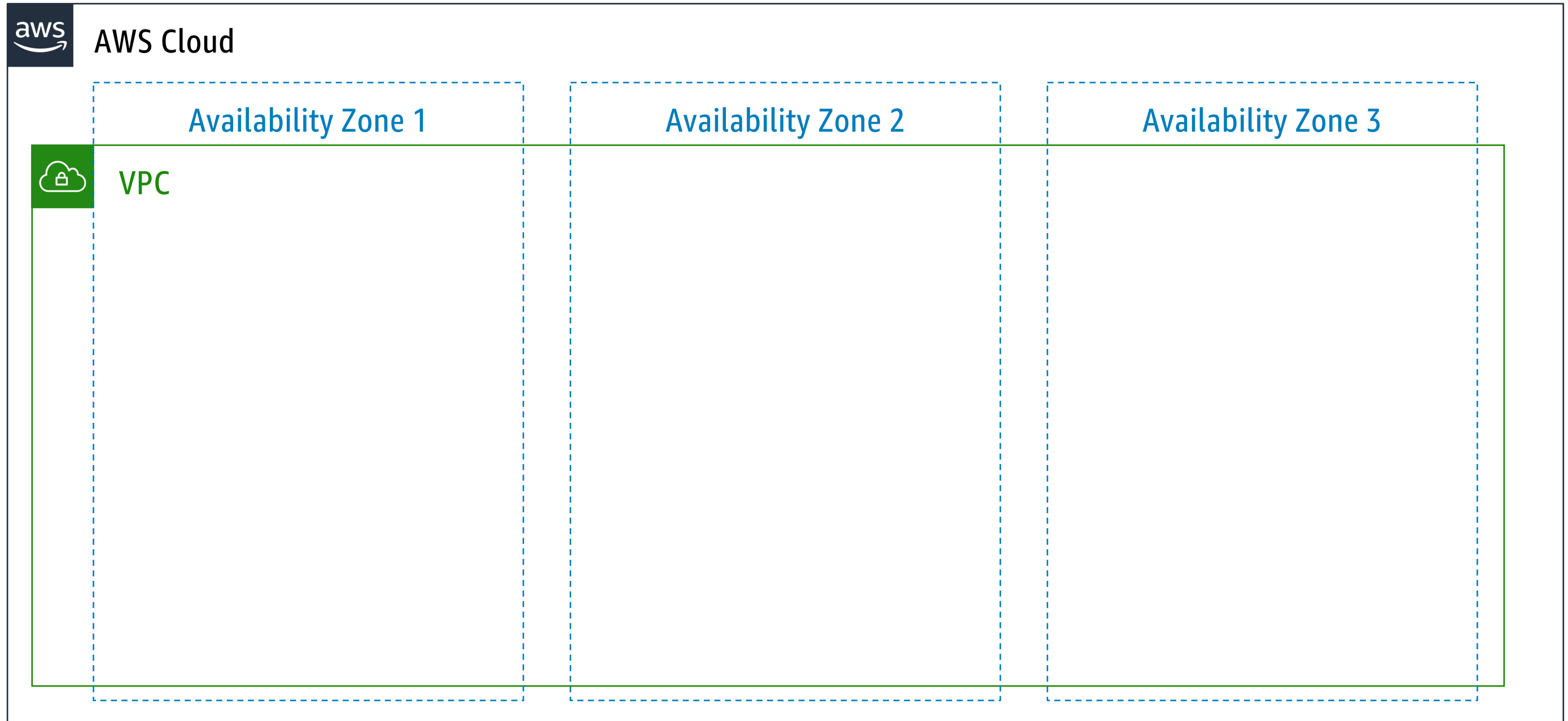


- Software-defined network
- Logically isolated
- Complete control
- Secure
- VPN & Internet connectivity
- Connect your on-premises IT environment

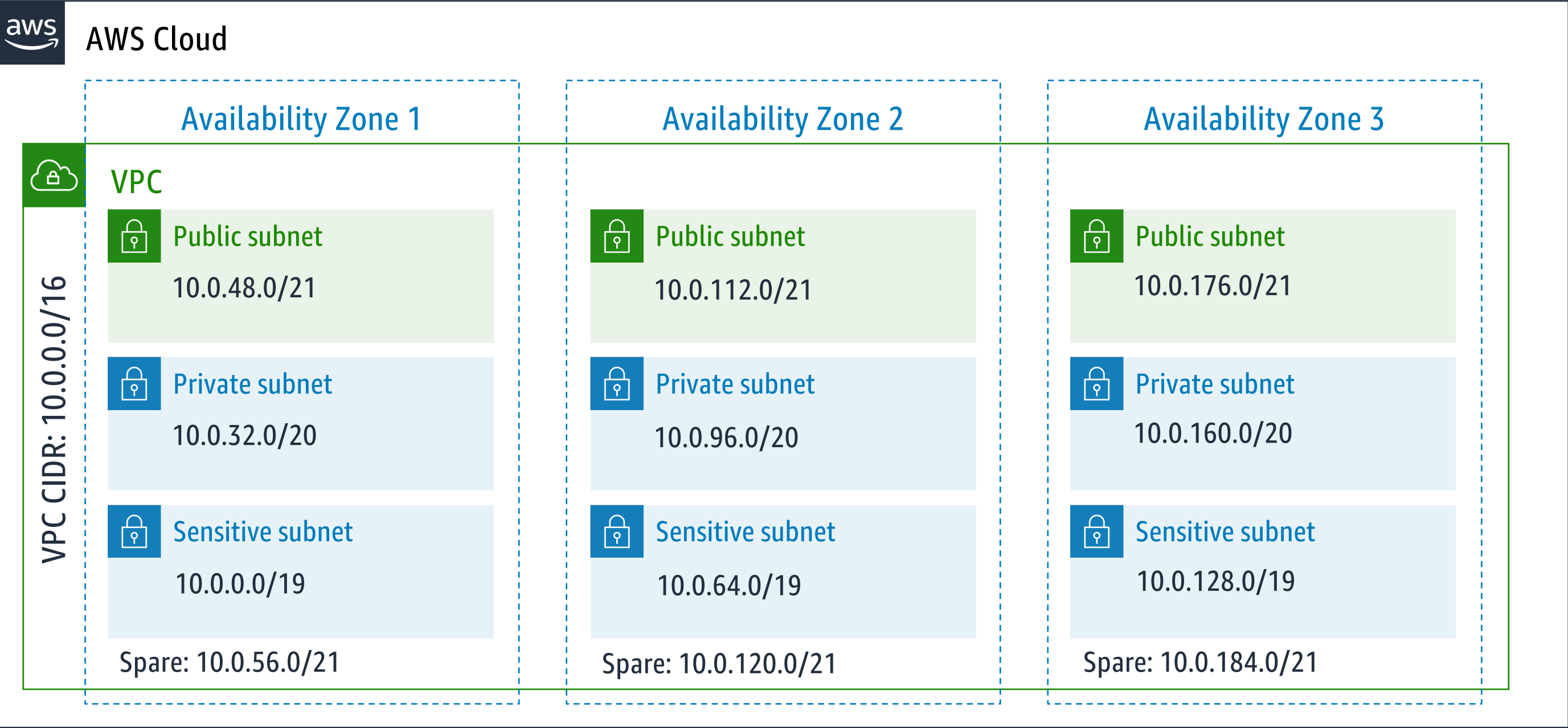
Each AWS Region has multiple Availability Zones



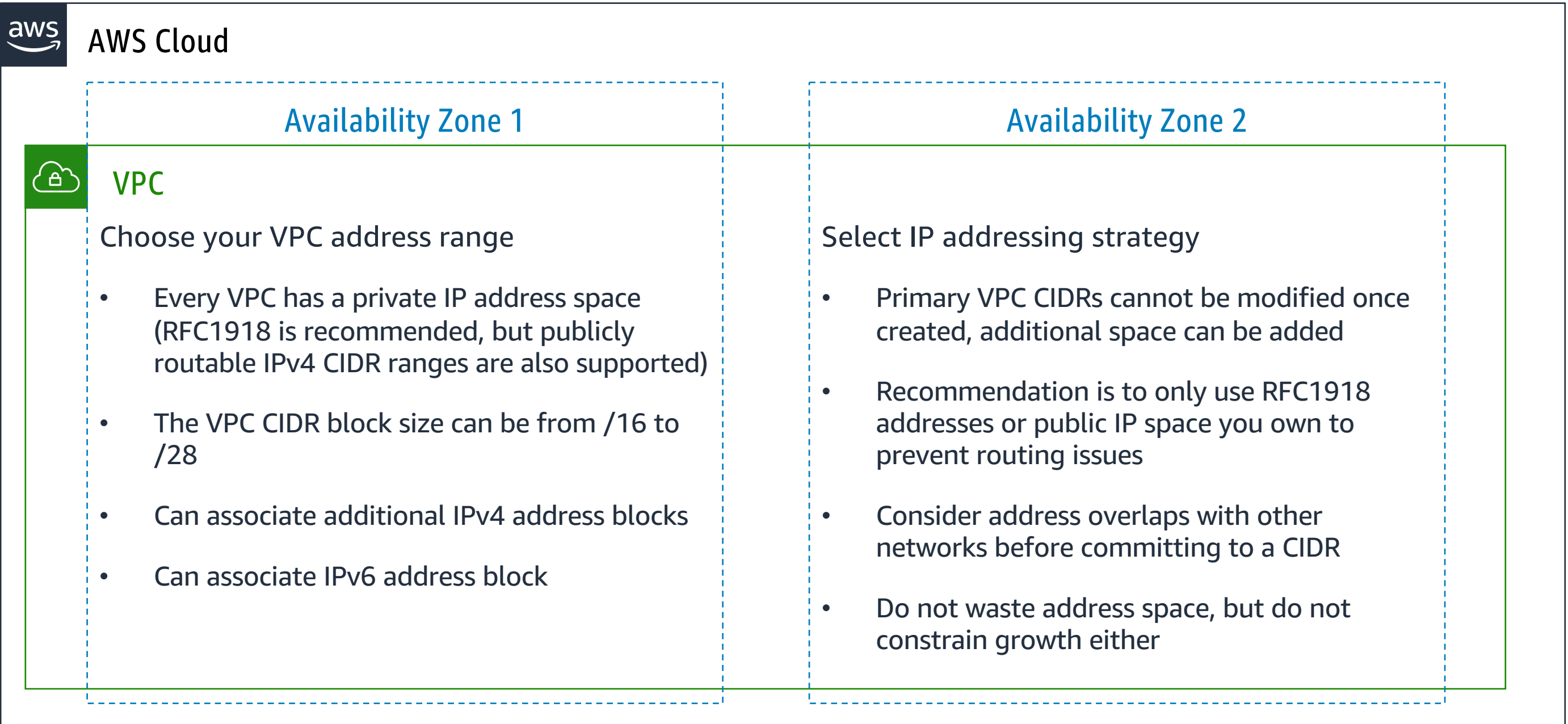
A VPC spans every Availability Zone in a Region



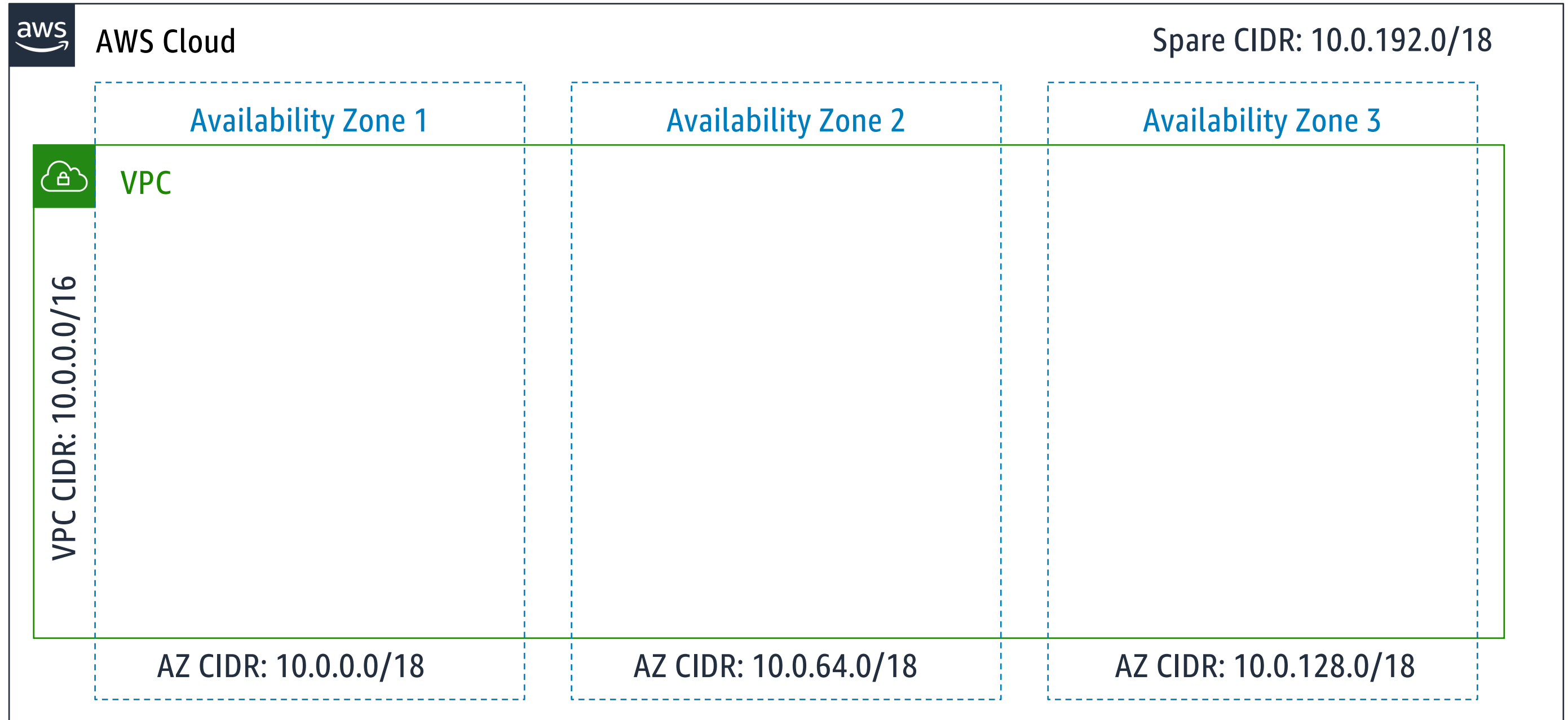
Subnets



Customers have full control over their VPC's

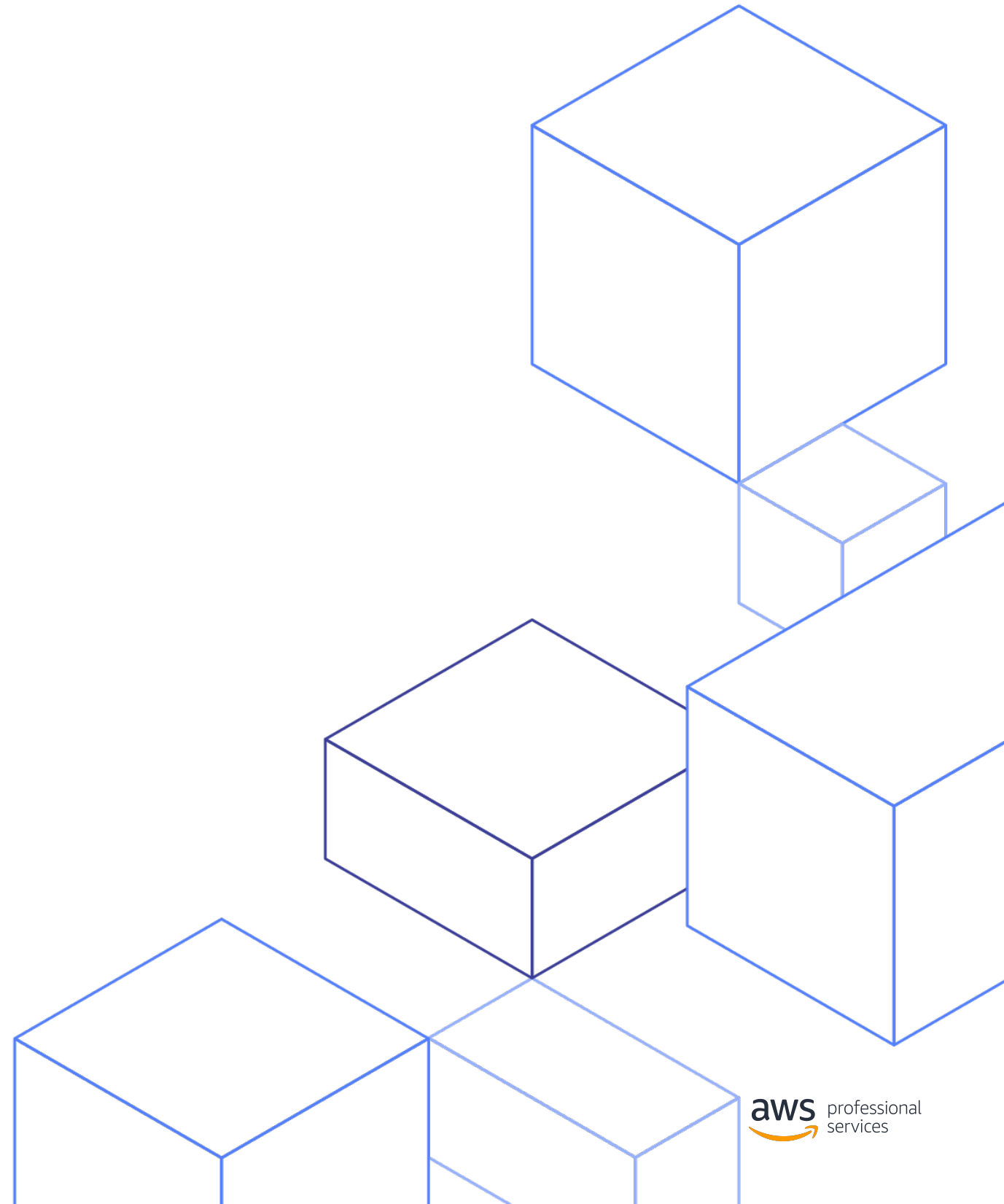


Logically allocate CIDR space for each AZ

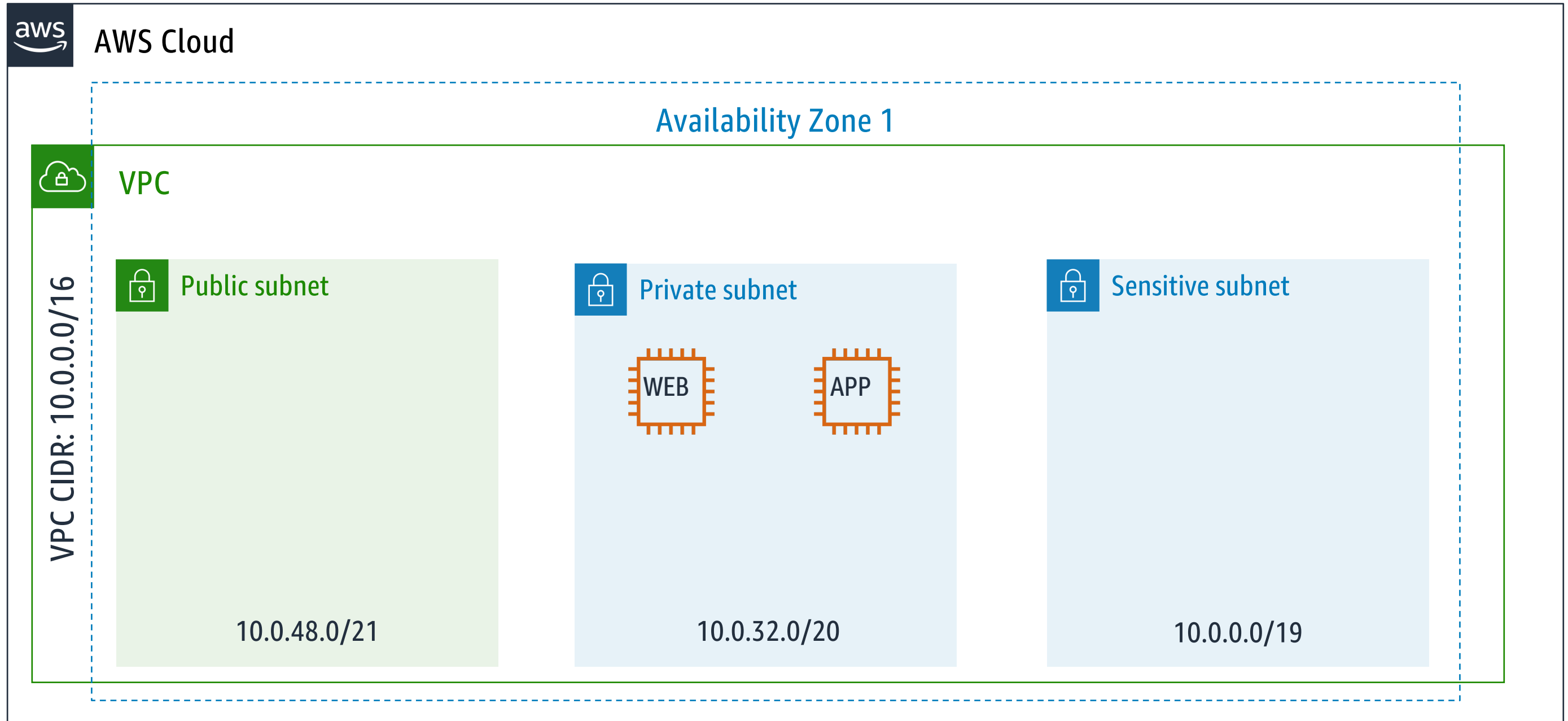


Security Groups

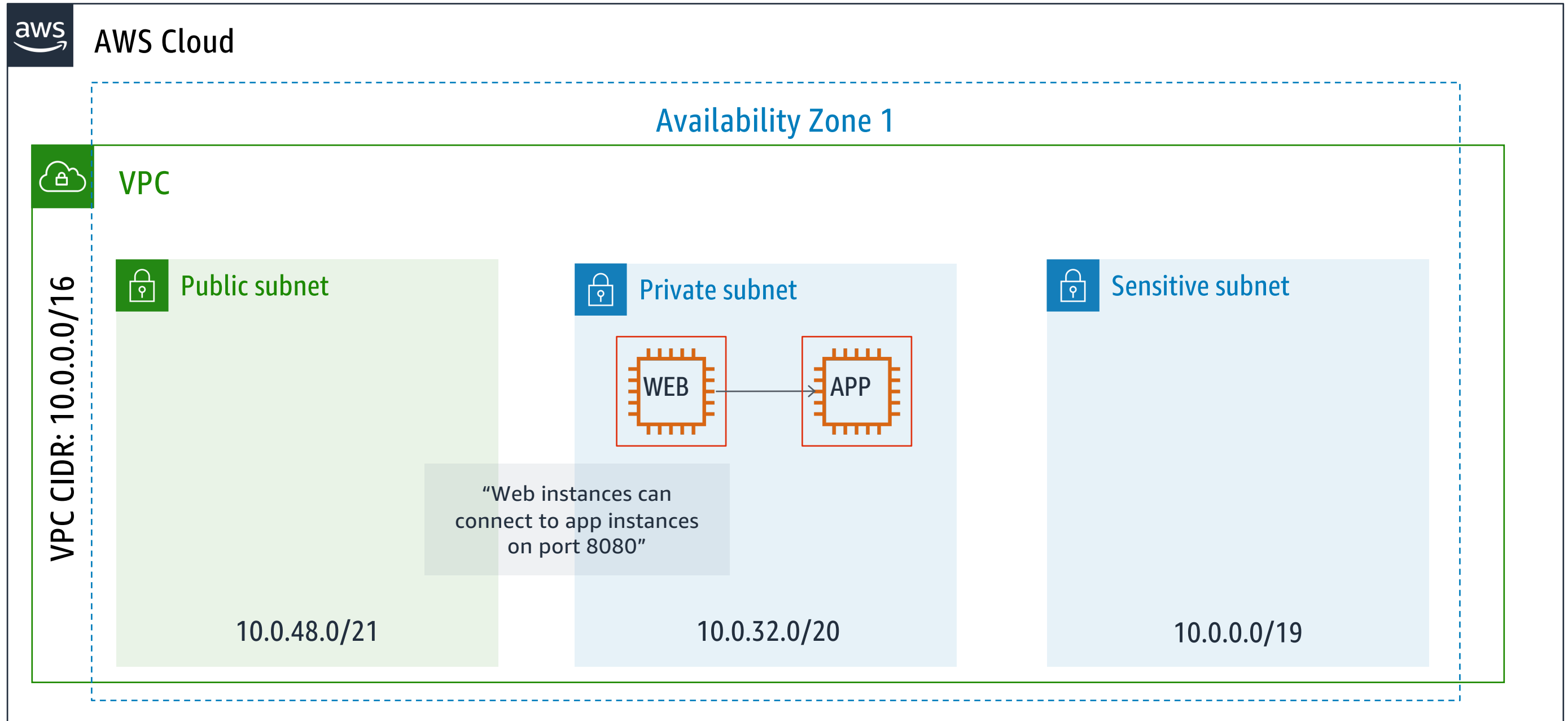
VPC Overview



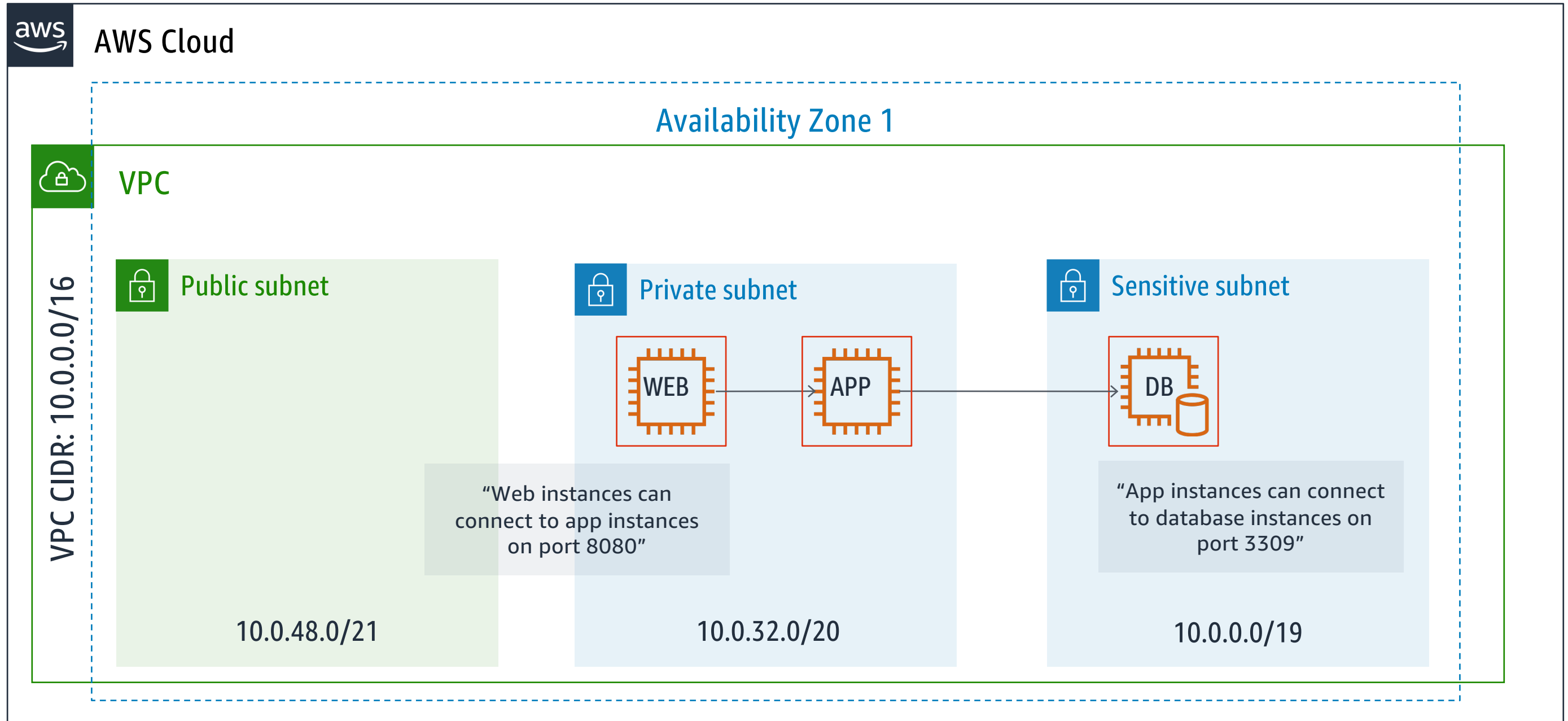
Security Groups – Stateful Firewall



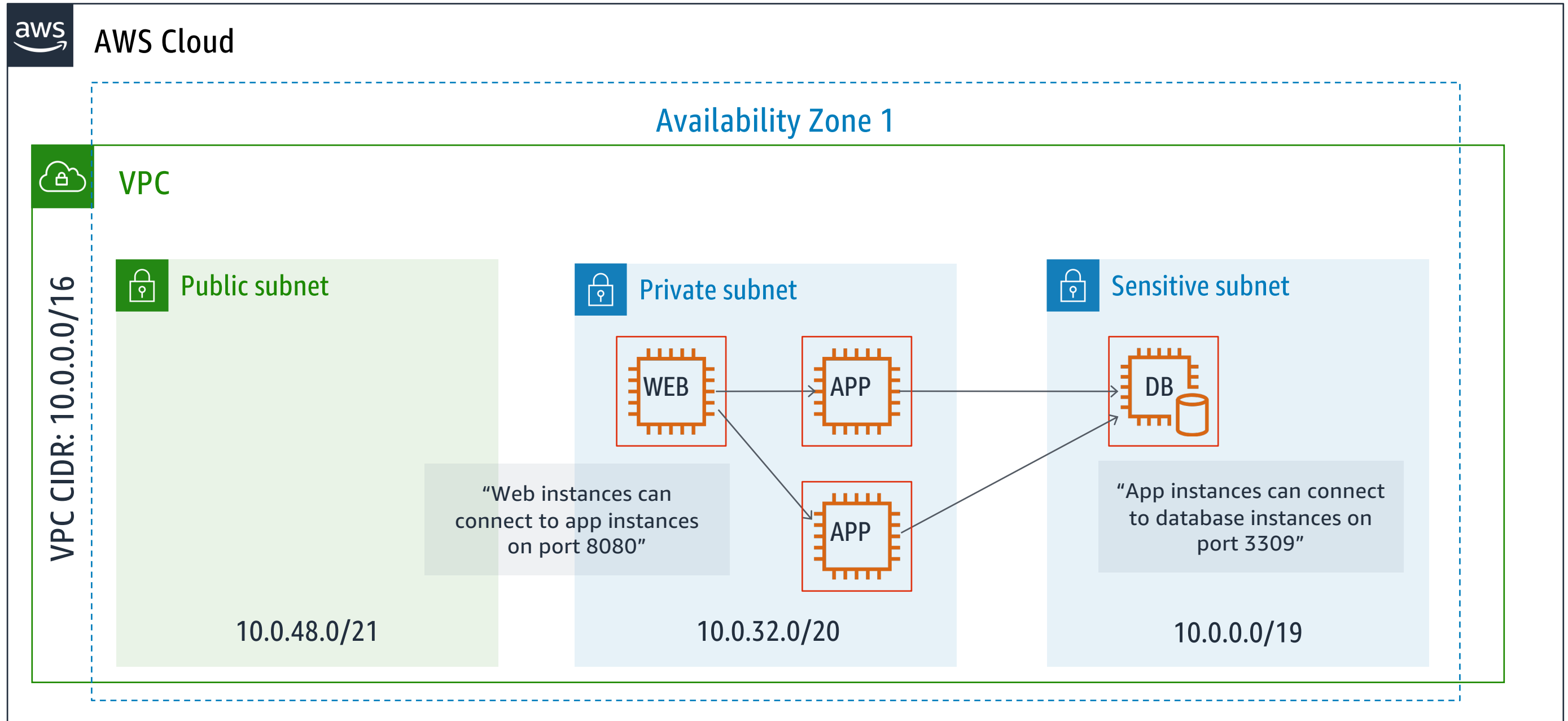
Security Groups – Stateful Firewall



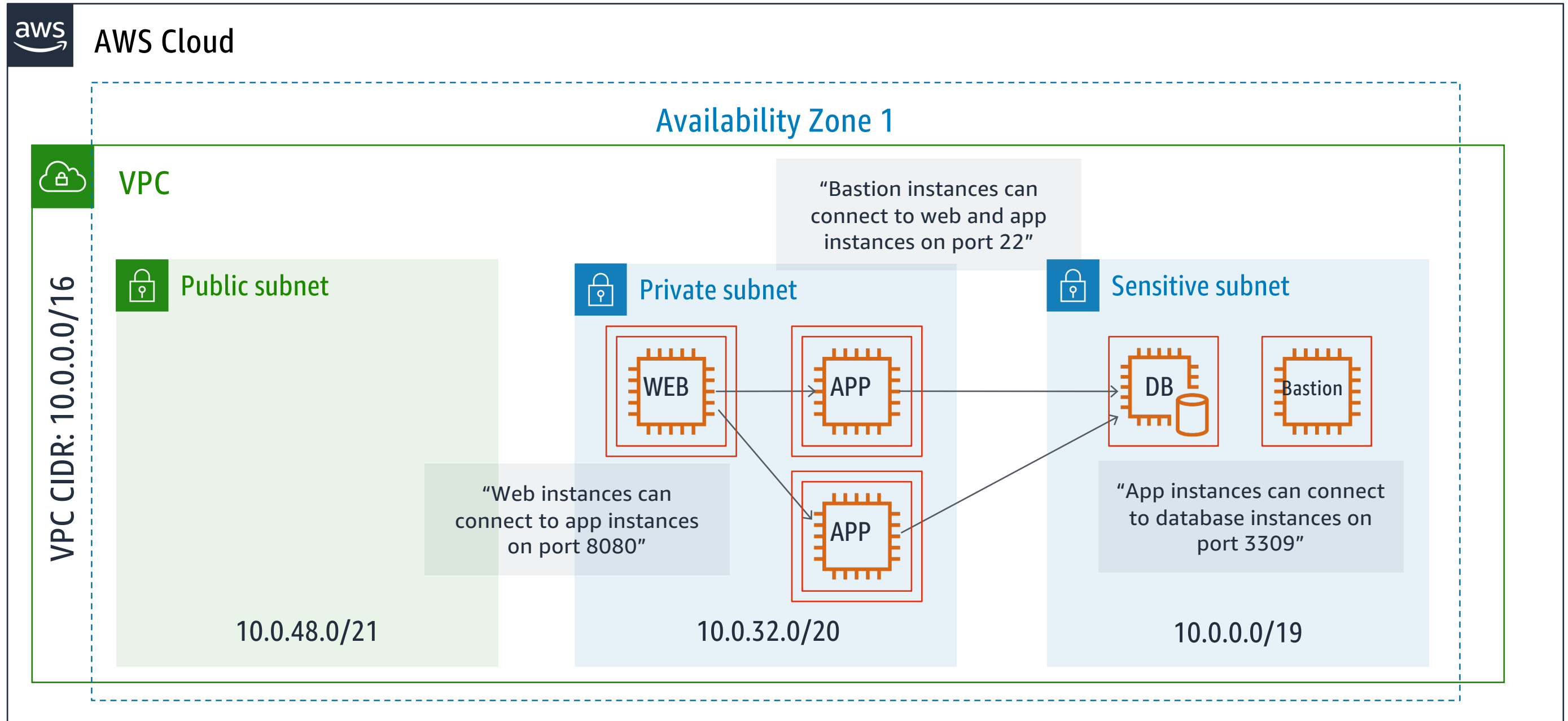
Security Groups – Stateful Firewall



Security Groups – Stateful Firewall



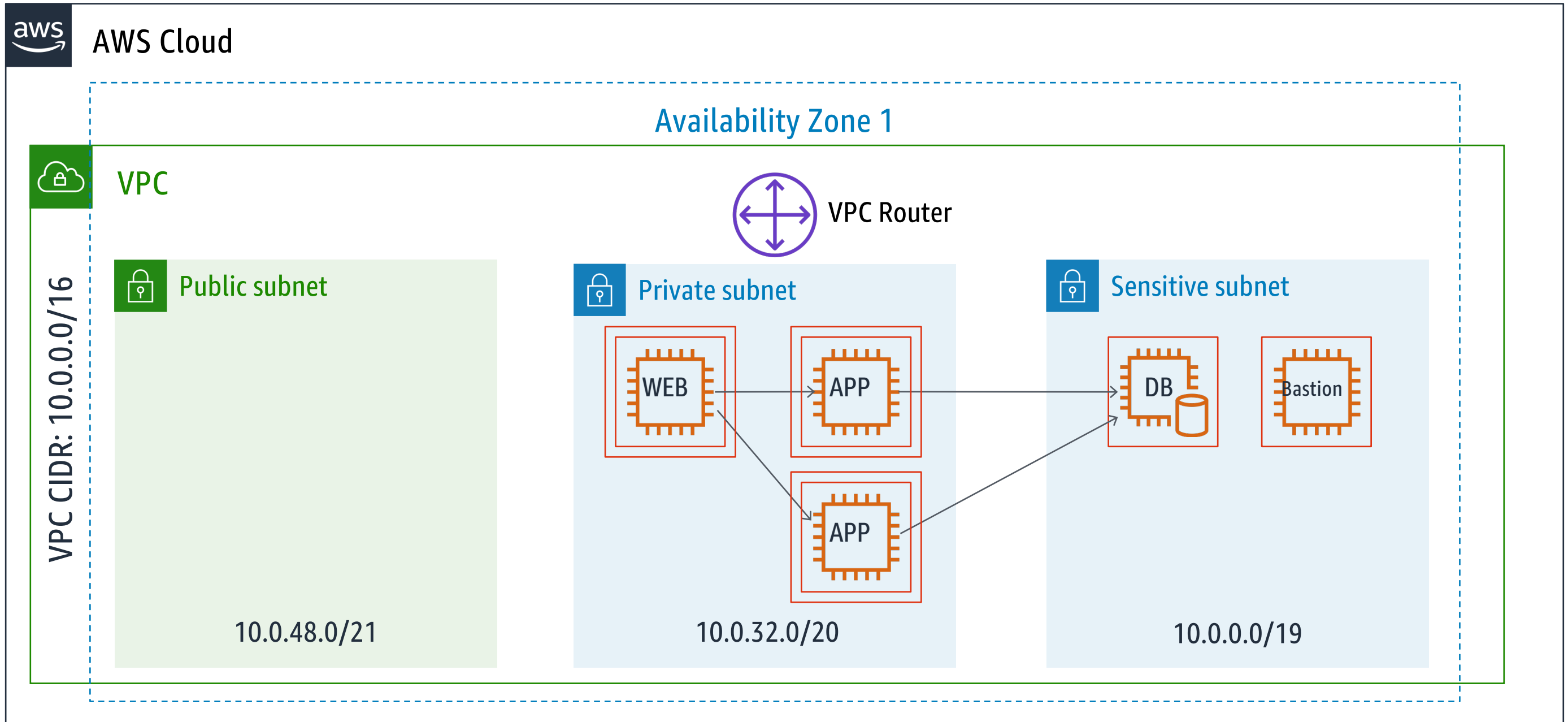
Security Groups – Stateful Firewall



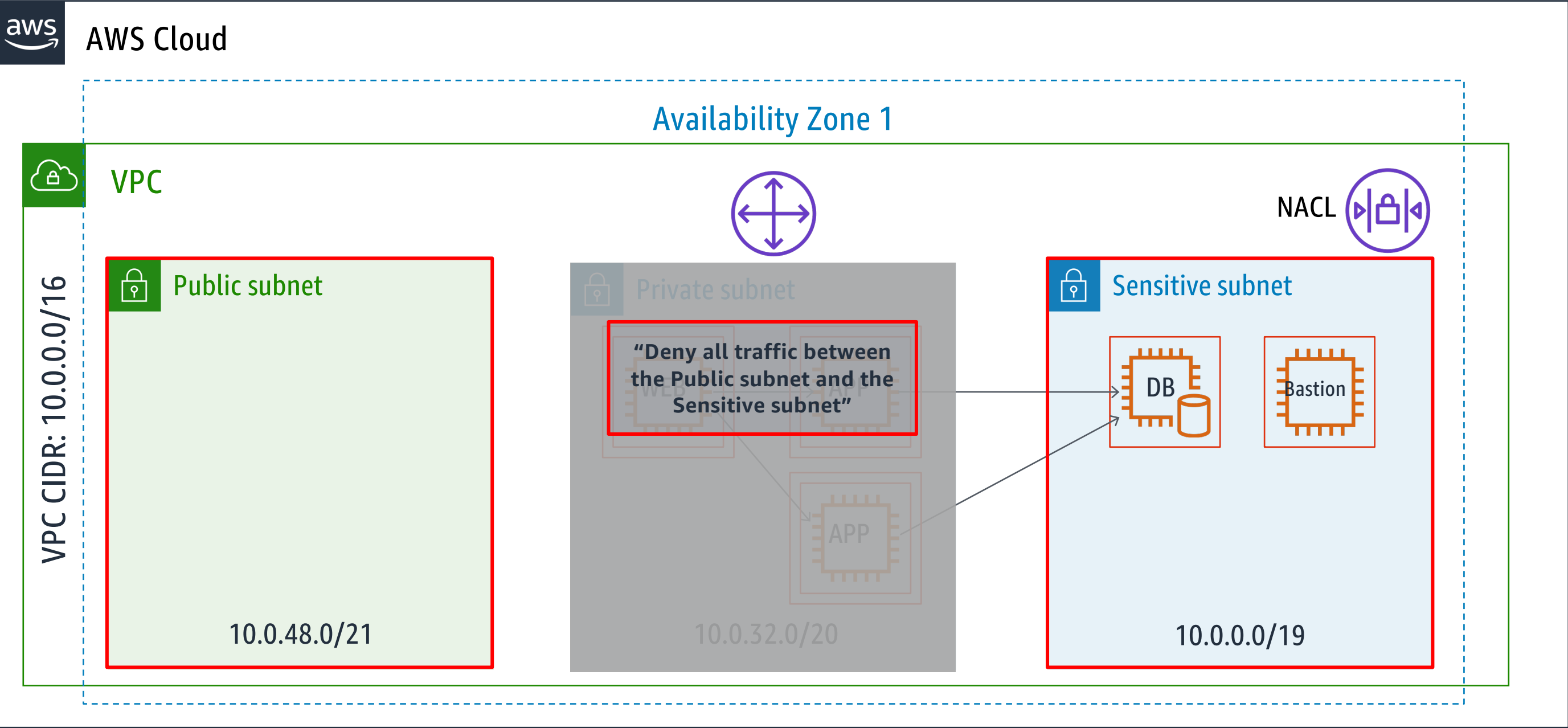
Routing, NACL's, and Load Balancing

VPC Overview

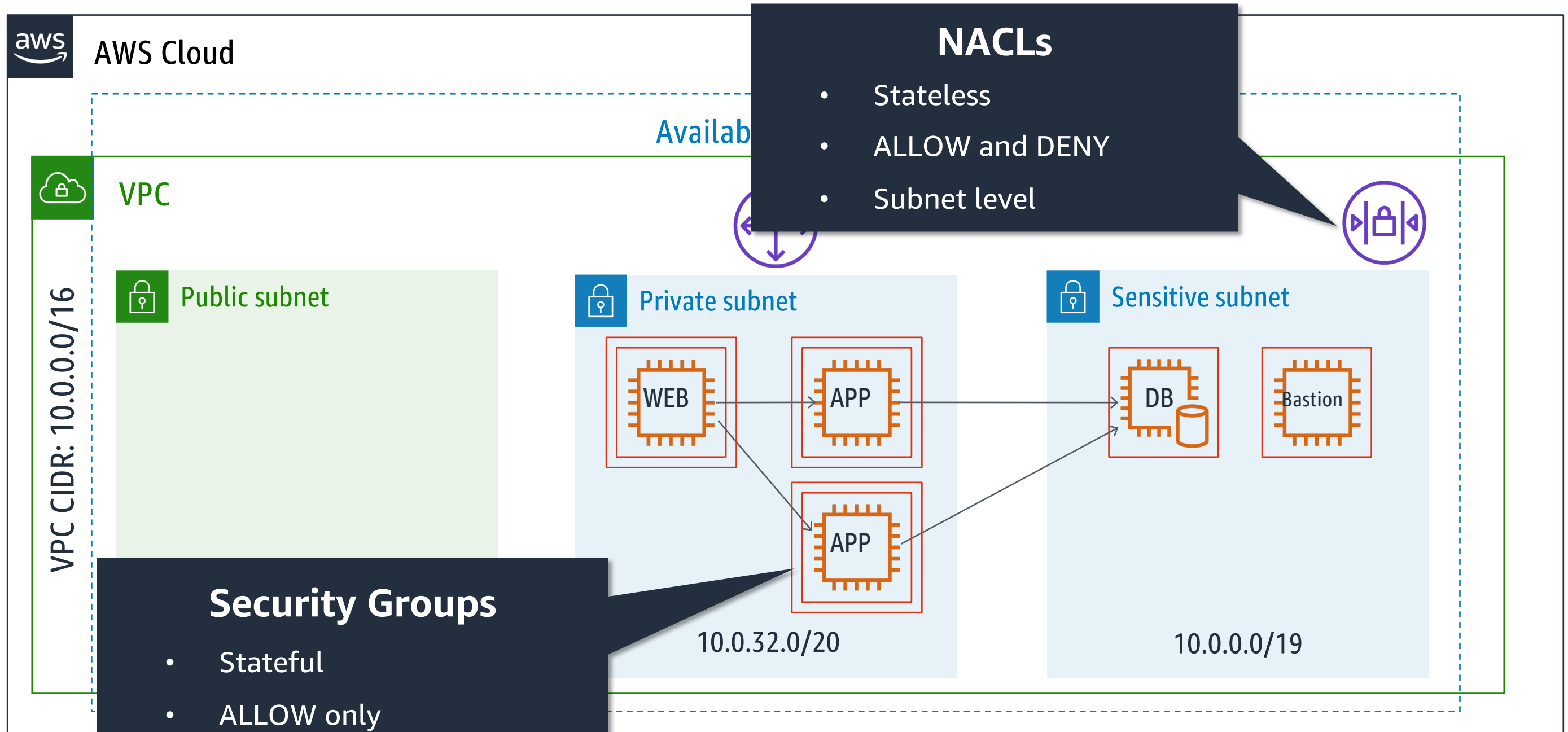
Routing



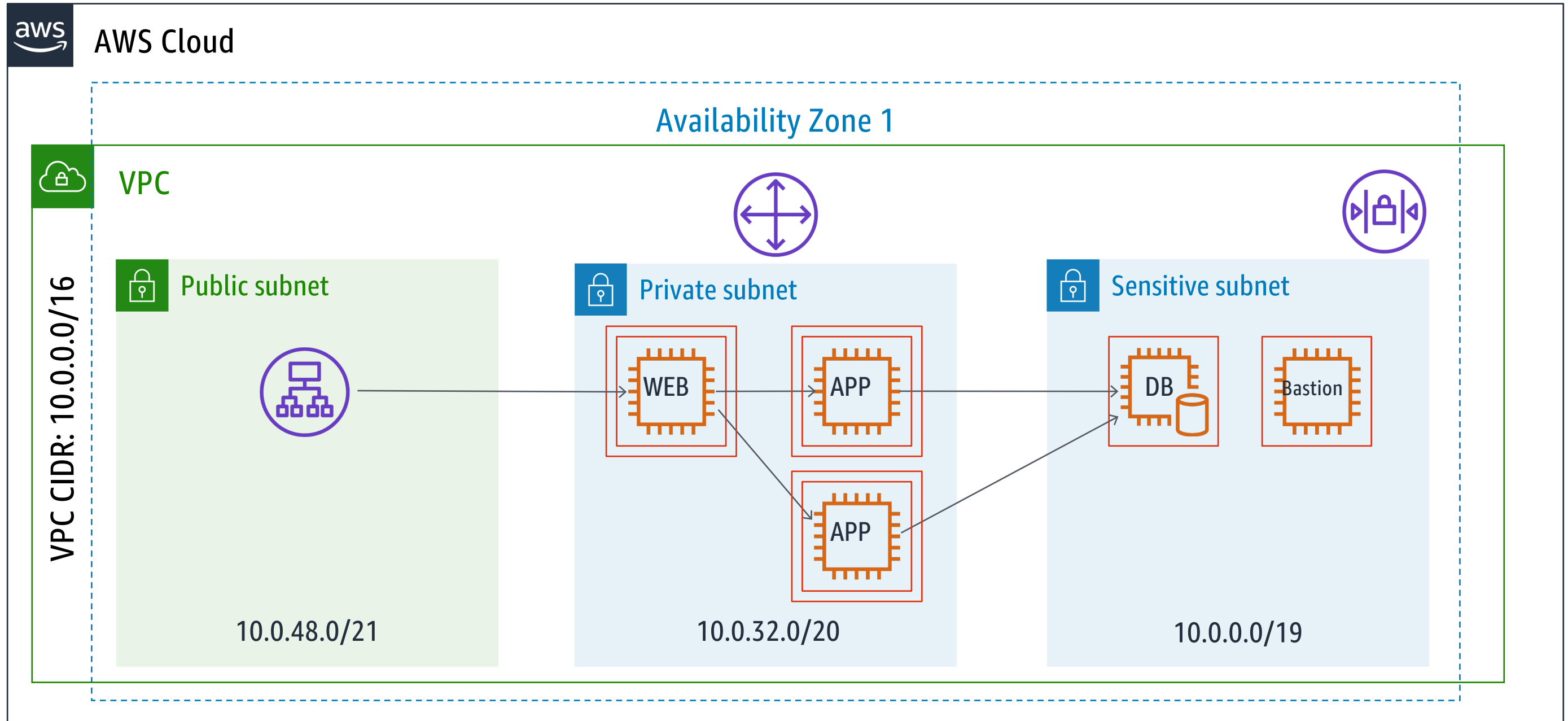
Network Access Control List (NACL)



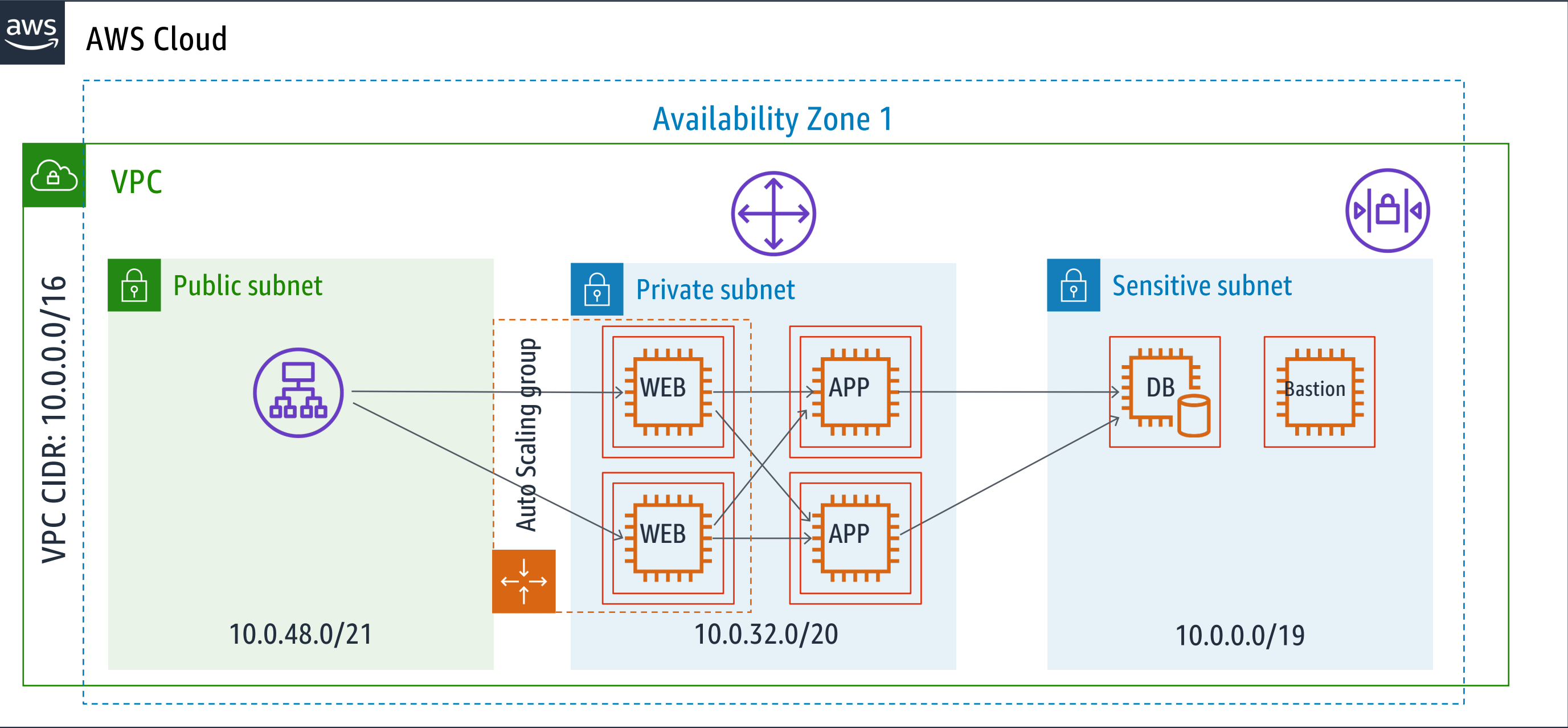
NACLs and Security Groups



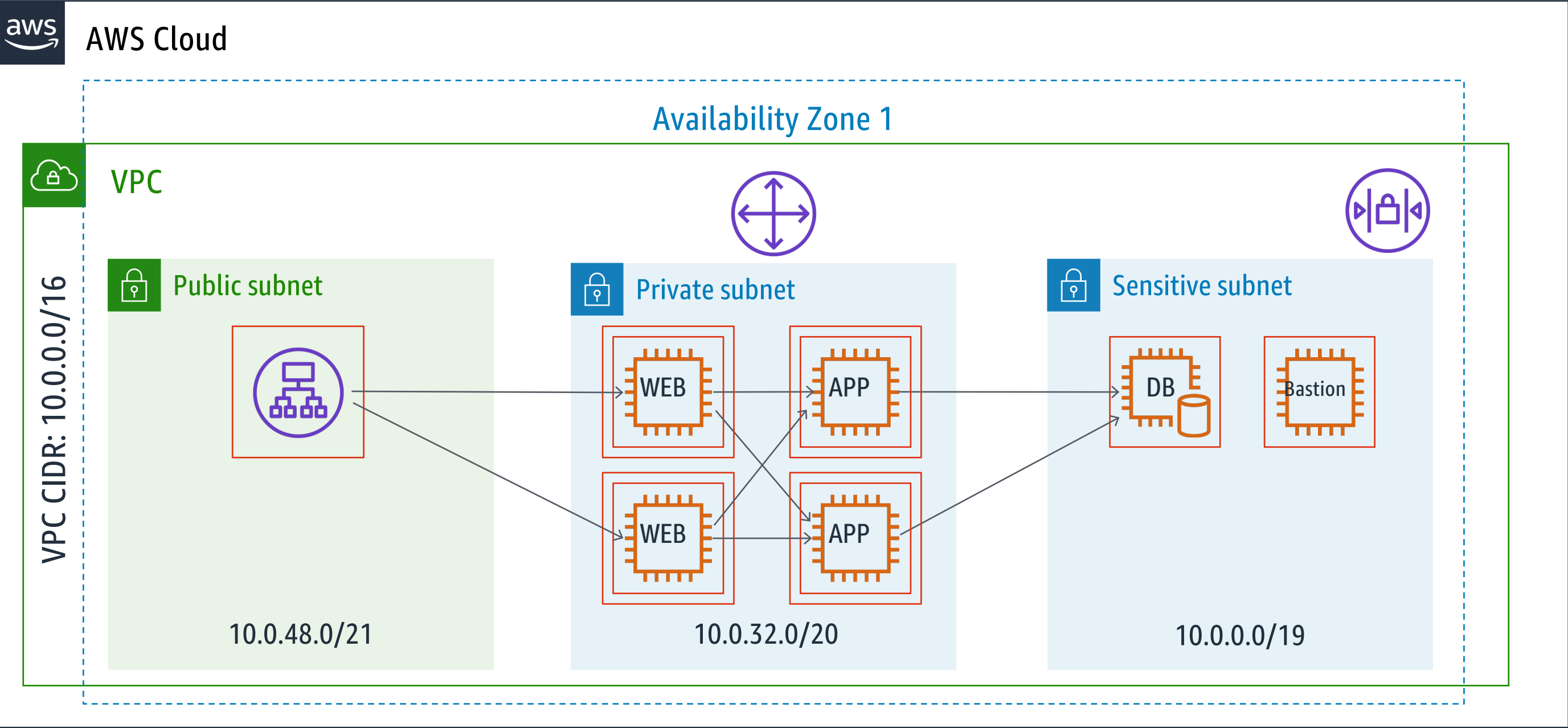
Load Balancing







Load Balancing



Load Balancing



Load Balancing – ELB Types

	Classic Load Balancer 	Application Load Balancer 	Network Load Balancer 	Gateway Load Balancer 
Protocols	TCP, SSL/TLS, HTTP, HTTPS	HTTP, HTTPS	TCP, TLS	GENEVE
Network Layer	L4 – L7	L7	L4	L3 – L4
IP address as a target	✗	✓	✓	✓
Lambda function as a target	✗	✓	✗	✗
Server Name Indication (SNI)	✗	✓	✗	✗
Preserve Source IP address	✗	✓	✓	✓
Static IP	✗	✗	✓	✗(only available as VPC service endpoint)
User authentication	✗	✓	✗	✗
Back-end TLS authentication based on public-key	✓	✗	✗	✗

<https://aws.amazon.com/elasticloadbalancing/features/>

DNS

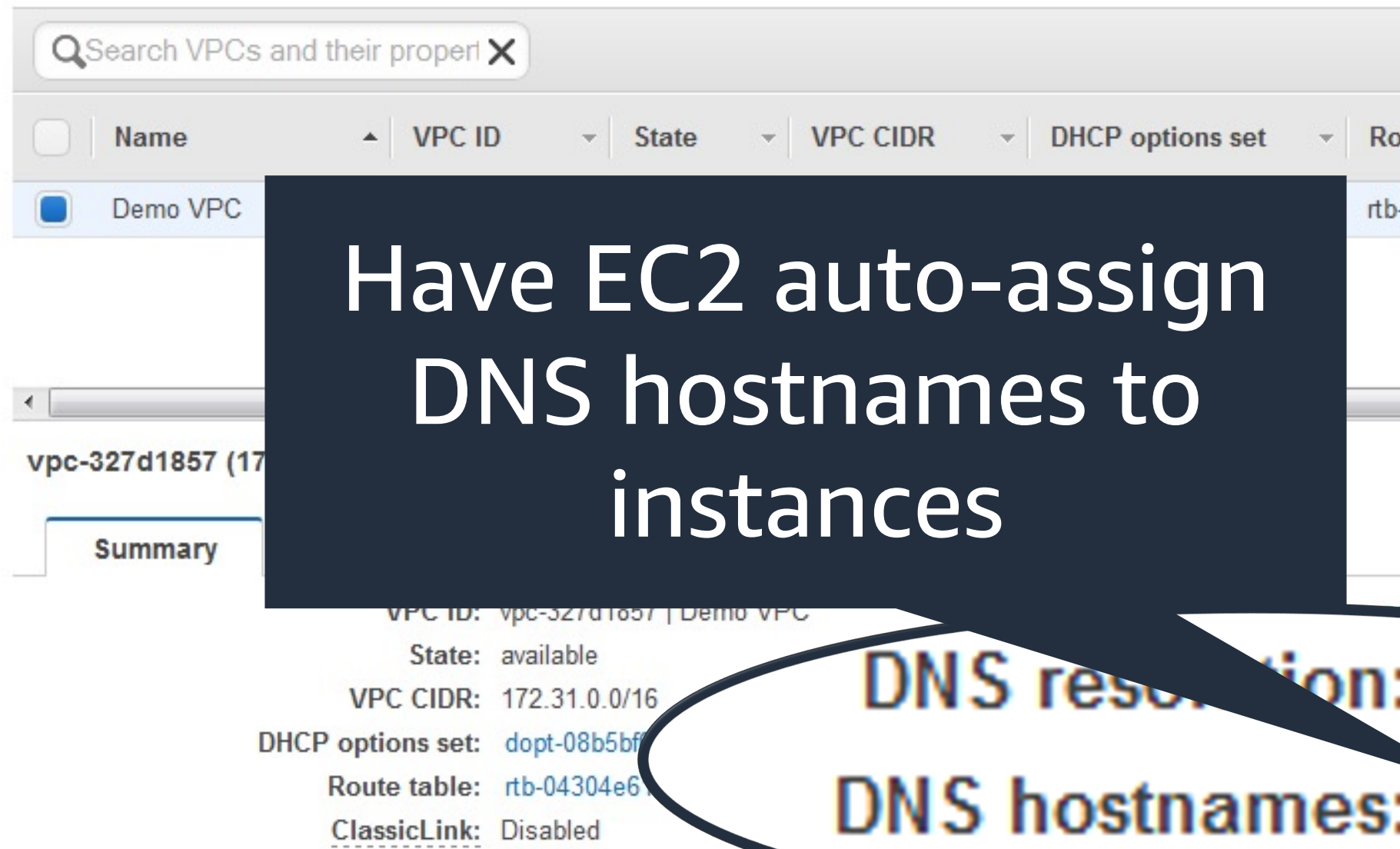
VPC Overview

AWS Professional Services Security Workshop v6.0

VPC Overview

© 2022, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

VPC DNS Options



The screenshot shows the AWS Management Console interface for a VPC named 'Demo VPC'. The console displays various attributes of the VPC, including its ID, state, CIDR block, DHCP options set, and route table. A large dark blue callout box is overlaid on the console, containing the text 'Have EC2 auto-assign DNS hostnames to instances'. Another dark blue callout box points to the 'DNS hostnames' option in the 'Summary' section, which is set to 'yes'.

Name	VPC ID	State	VPC CIDR	DHCP options set	Route table
Demo VPC	vpc-327d1857	available	172.31.0.0/16	dopt-08b5b5f1	rtb-04304e61

Summary

- VPC ID: vpc-327d1857 | Demo VPC
- State: available
- VPC CIDR: 172.31.0.0/16
- DHCP options set: dopt-08b5b5f1
- Route table: rtb-04304e61
- ClassicLink: Disabled
- DNS resolution: yes
- DNS hostnames: yes

Use
Amazon
DNS server

EC2 DNS Hostnames

Internal DNS
hostname: Resolves
to Private IP address

External DNS name:
Resolves to...

Description		eu-west-1.compute.amazonaws.com	
Instance ID	i-a34...	Public DNS	ec2-52-19-188-57.eu-west-1.compute.amazonaws.com
Instance state	running	Public IP	52.19.188.57
Instance type	t2.micro	Elastic IP	-
Private DNS	ip-172-31-0-201.eu-west-1.compute.internal	Availability zone	eu-west-1a
Private IPs	172.31.0.201	Security groups	default . view rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-327d1857	AMI ID	amzn-ami-hvm-2015.03.1.x86_64-gp2 (ami-e4d18e93)

EC2 DNS Hostnames from outside the VPC

```
C:\>nslookup ec2-52-18-10-57.eu-west-1.compute.amazonaws.com
```

Non-authoritative answer:

Name: ec2-52-18-10-57.eu-west-1.compute.amazonaws.com

Address: 52.18.10.57

Outside your VPC:
Public IP address

EC2 DNS Hostnames from inside the VPC

```
[ec2-user@ip-172-31-0-201 ~]$ dig ec2-52-18-10-57.eu-west-1.compute.amazonaws.com
```

```
;; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.30.rc1.38.amzn1 <<>> ec2-52-18-10-  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36622  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
```

```
;; QUESTION SECTION:  
;ec2-52-18-10-57.eu-west-1.compute.amazonaws.com. IN A
```

```
;; ANSWER SECTION:  
ec2-52-18-10-57.eu-west-1.compute.amazonaws.com. 60 IN A 172.31.0.137
```

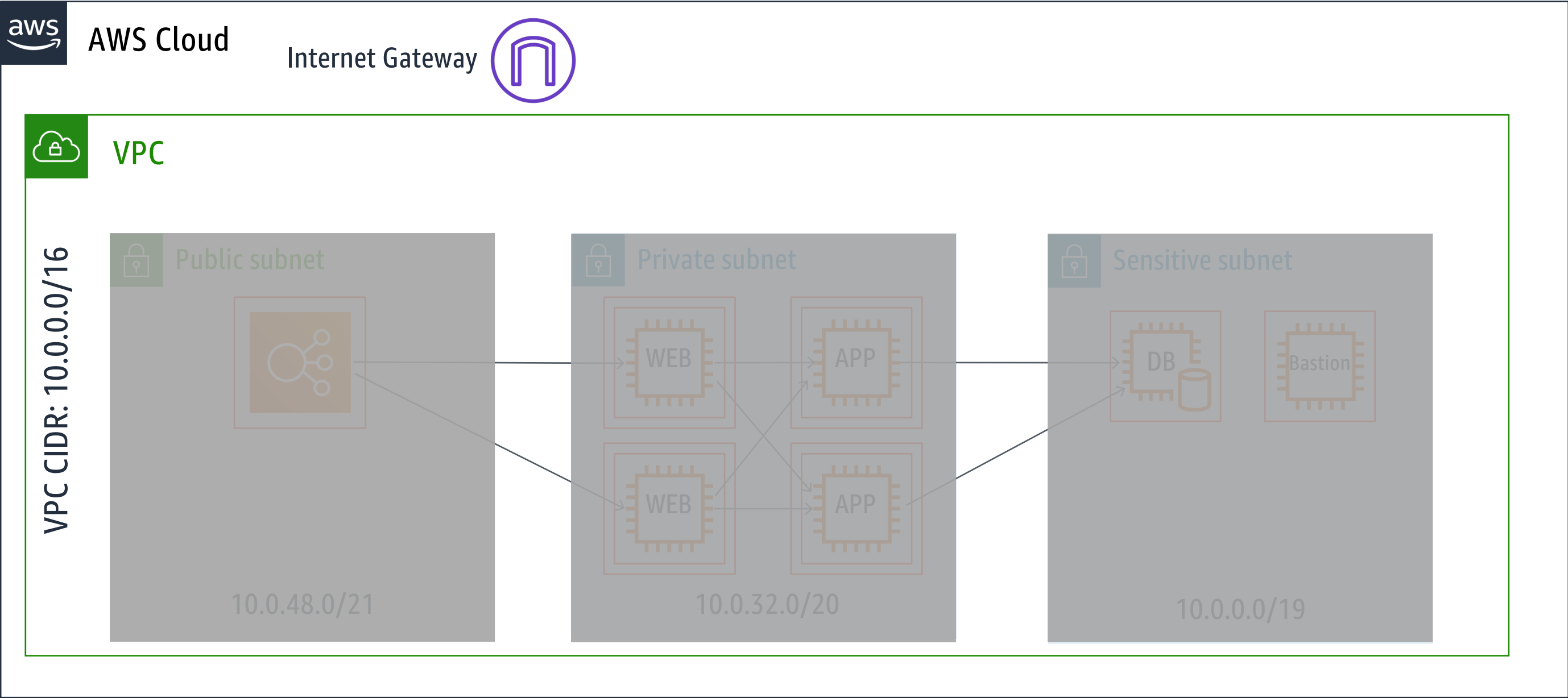
```
;; Query time: 2 msec  
;; SERVER: 172.31.0.2#53(172.31.0.2)  
;; WHEN: Wed Sep 9 22:32:56 2015  
;; MSG SIZE rcvd: 81
```

Inside your VPC:
Private IP address

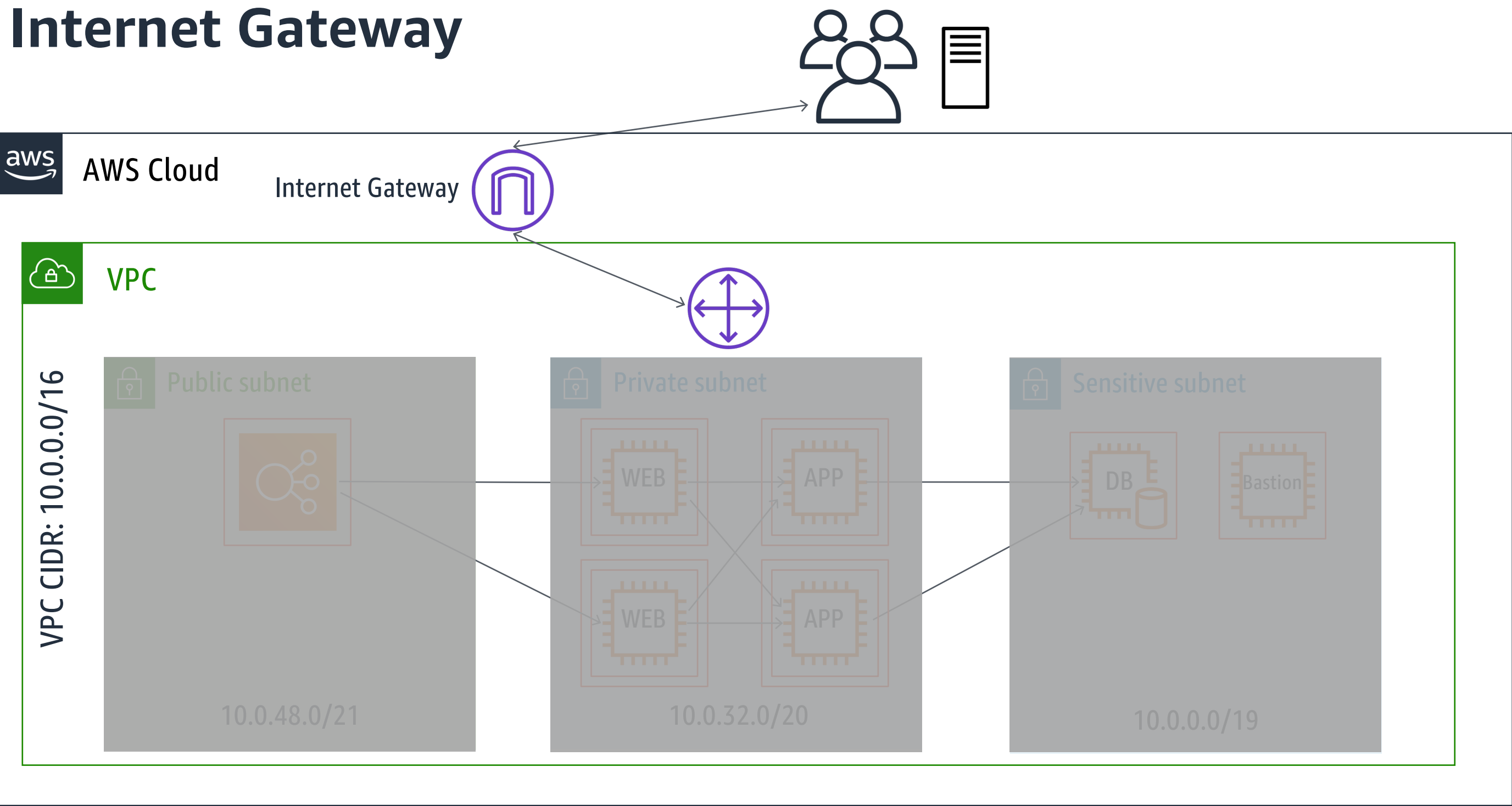
Connectivity

VPC Overview

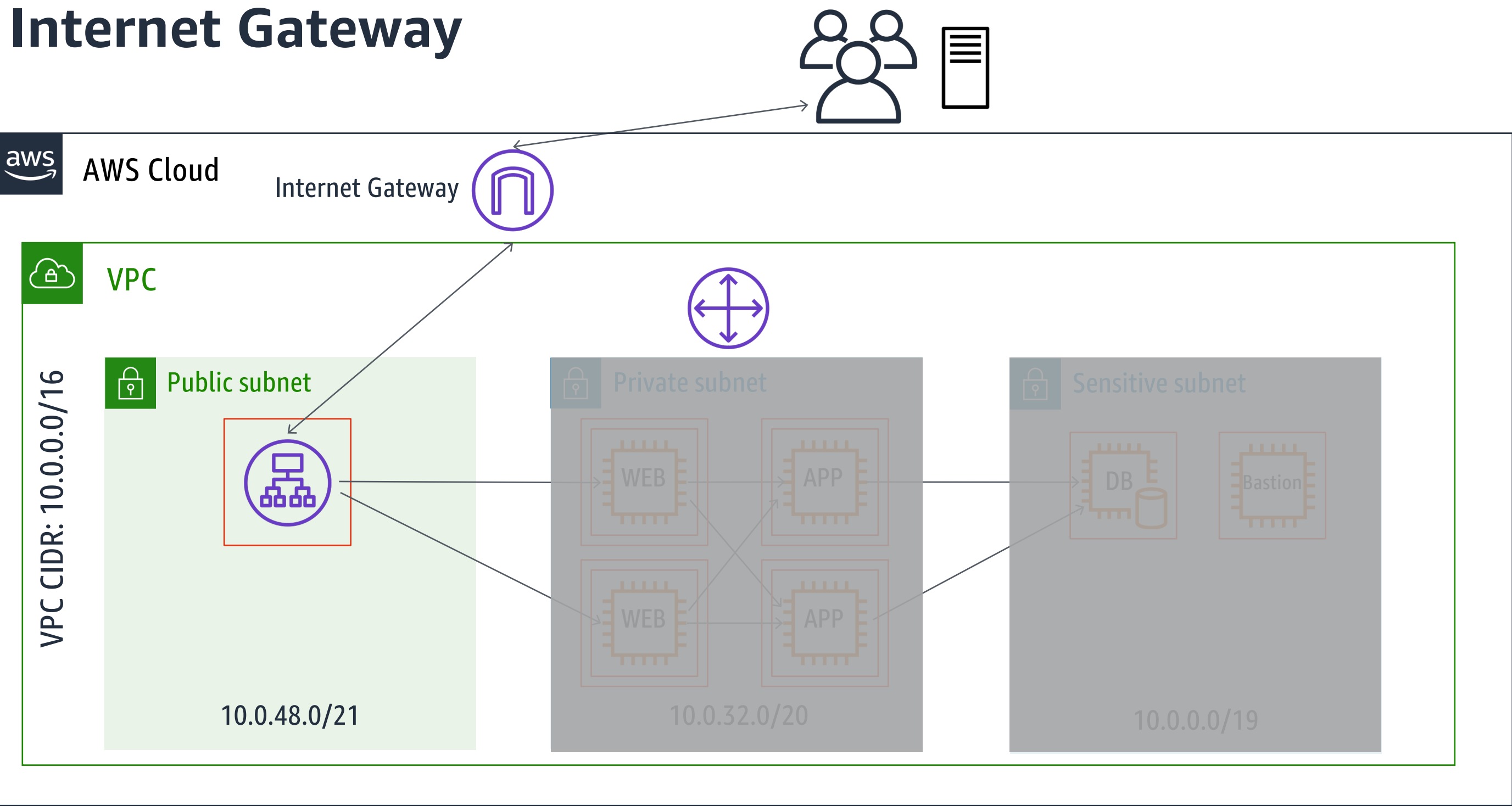
Internet Gateway



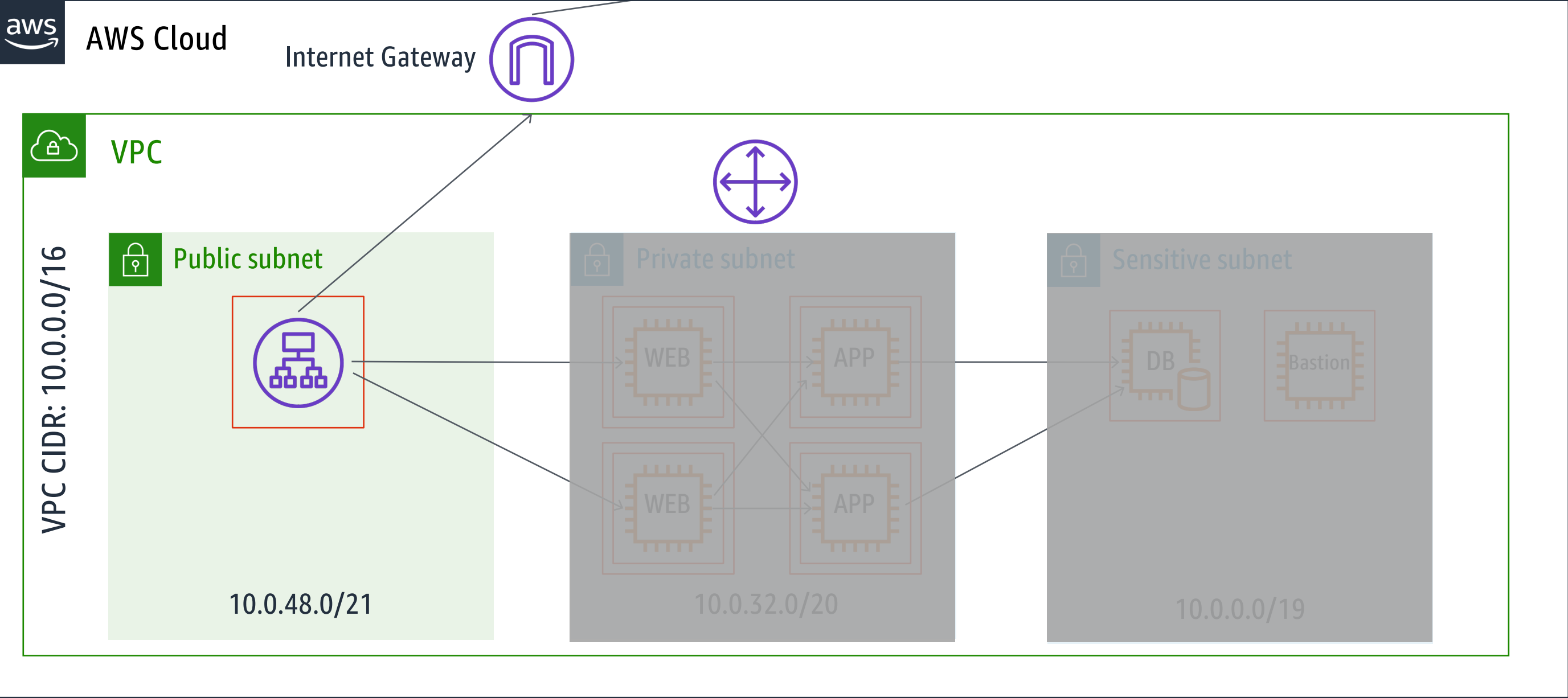
Internet Gateway



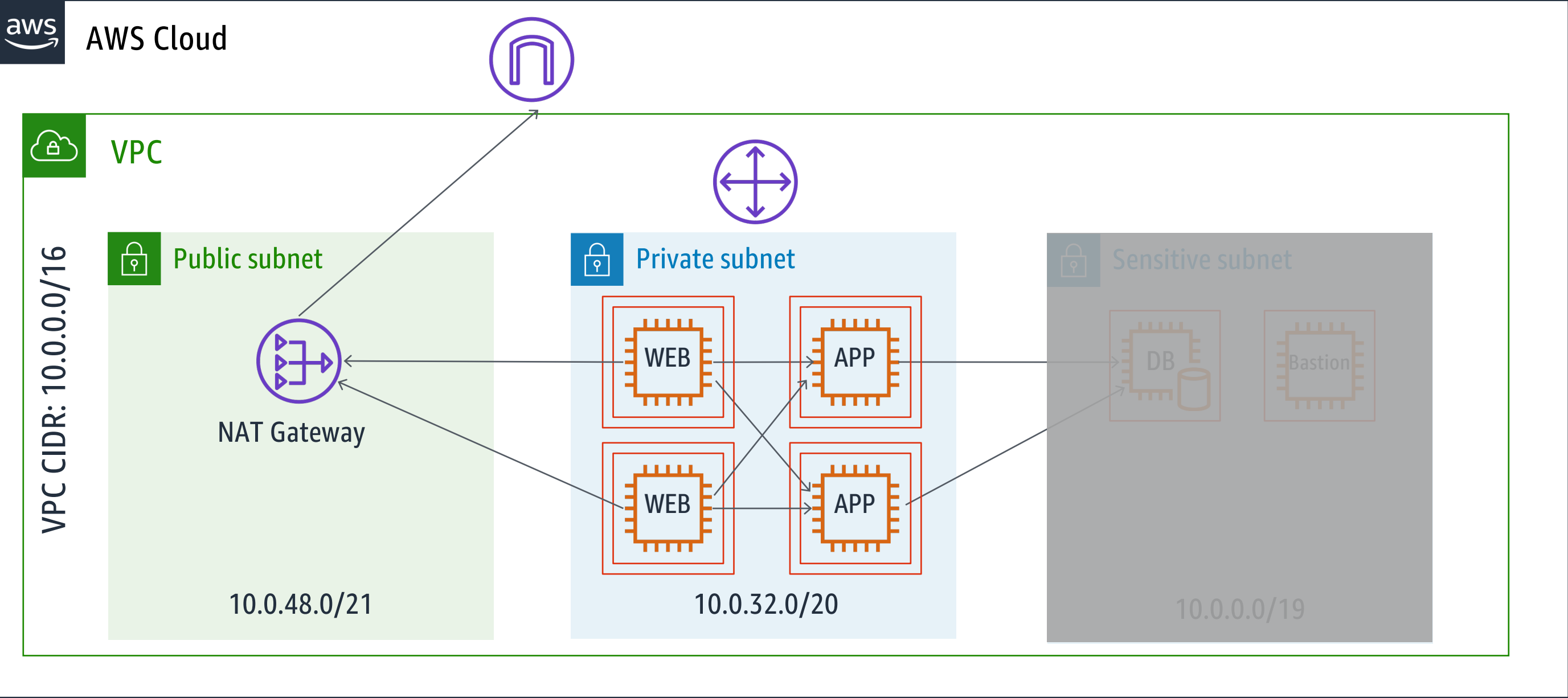
Internet Gateway



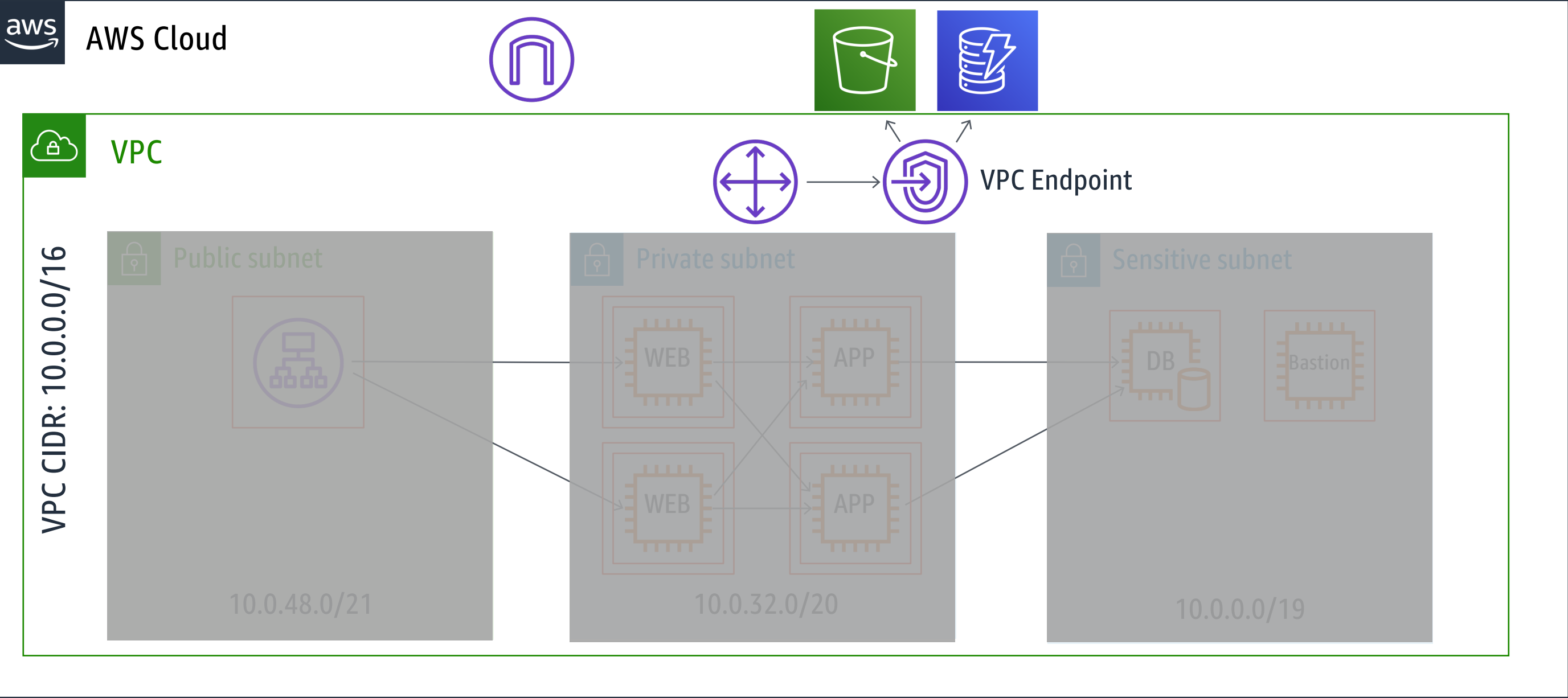
Egress-only Internet Gateway



NAT Gateway



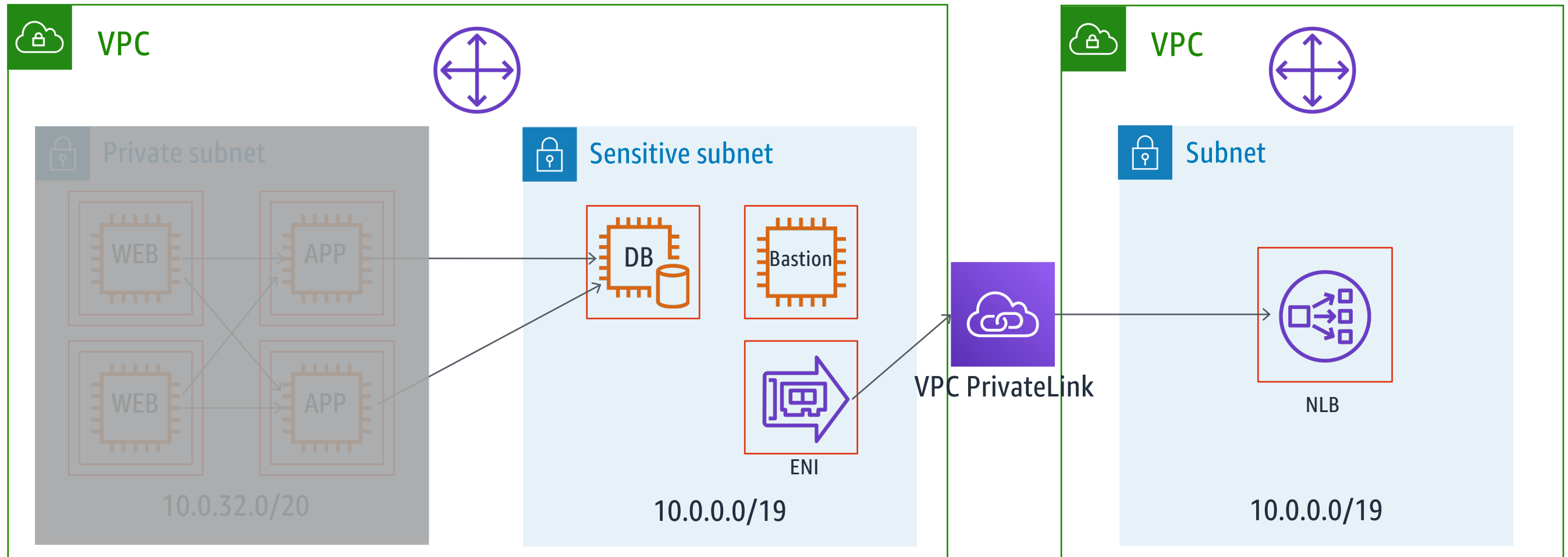
VPC Endpoints



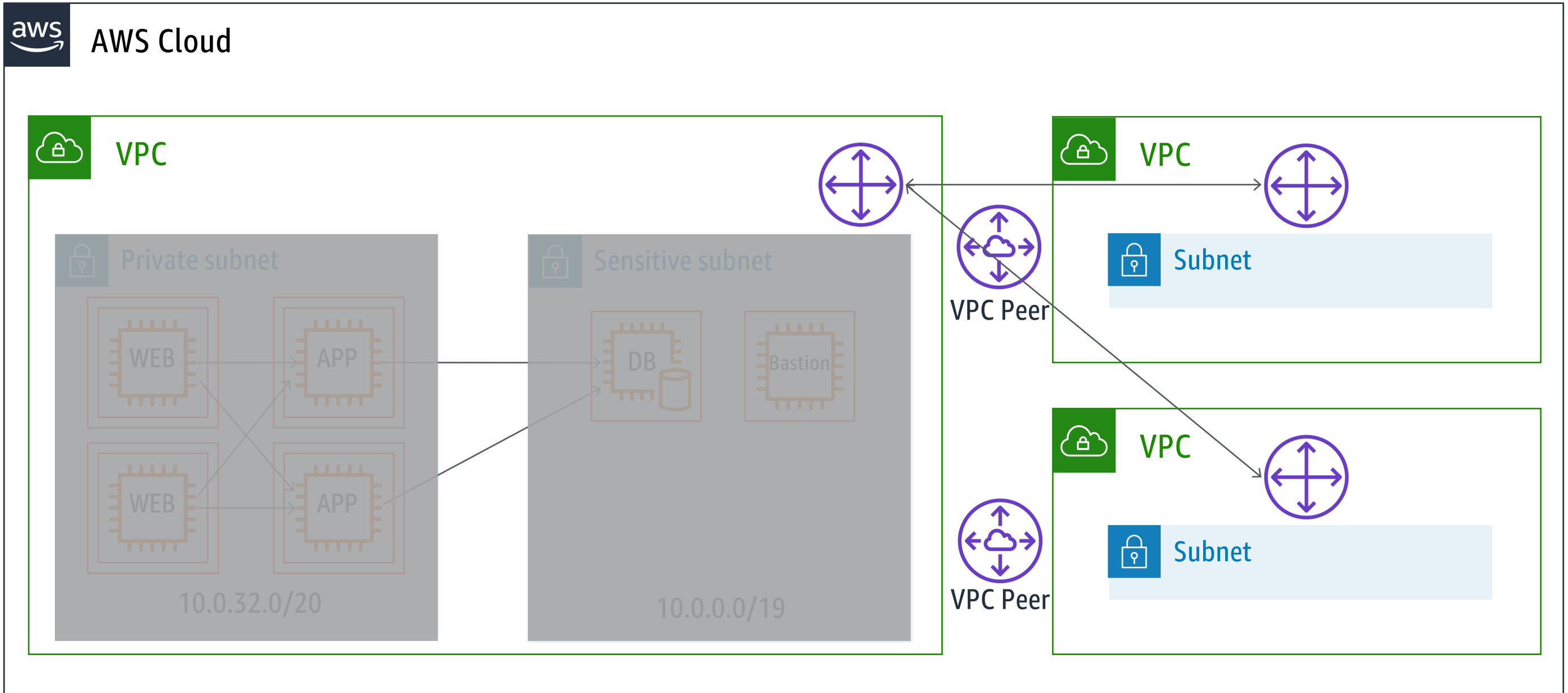
VPC PrivateLink



AWS Cloud



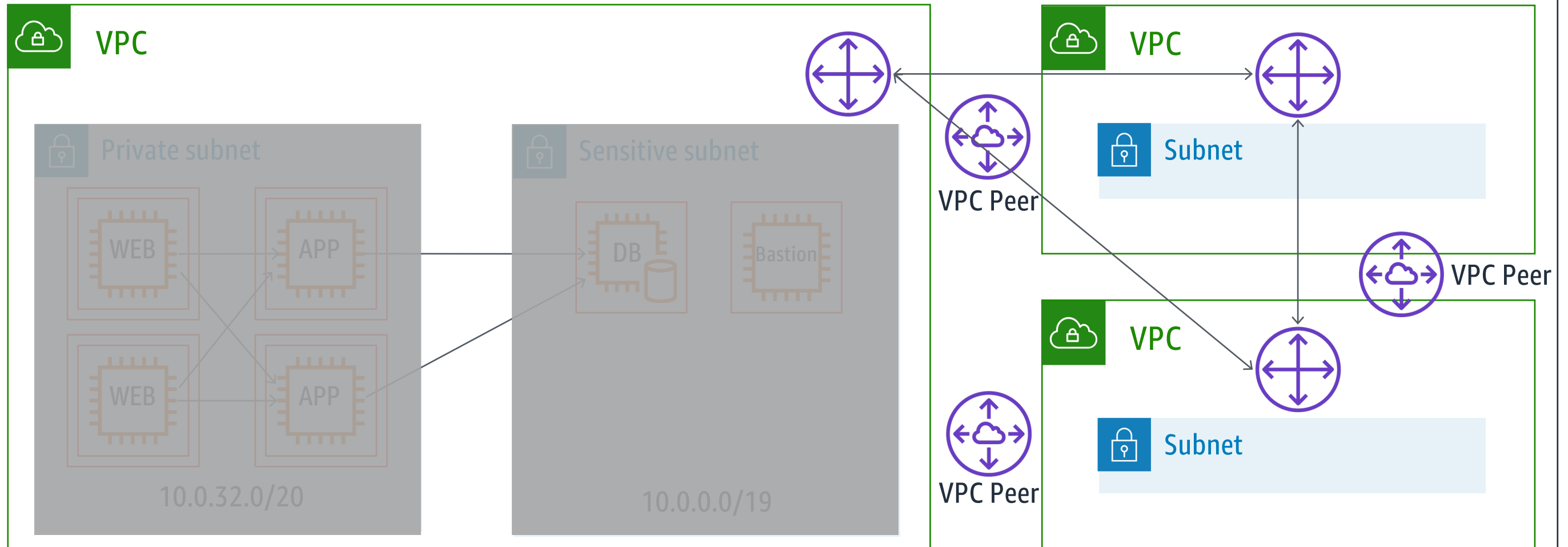
VPC Peering



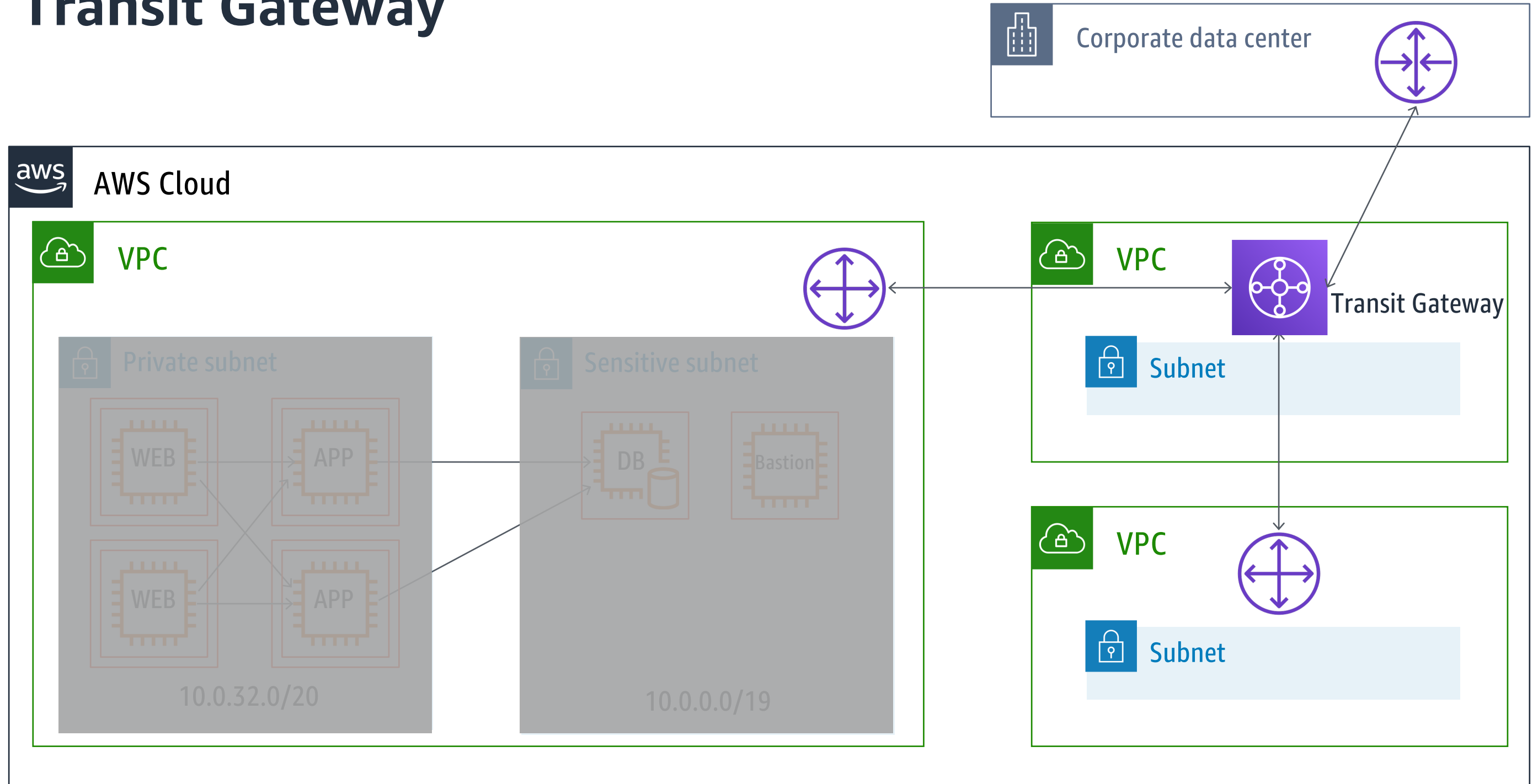
VPC Peering



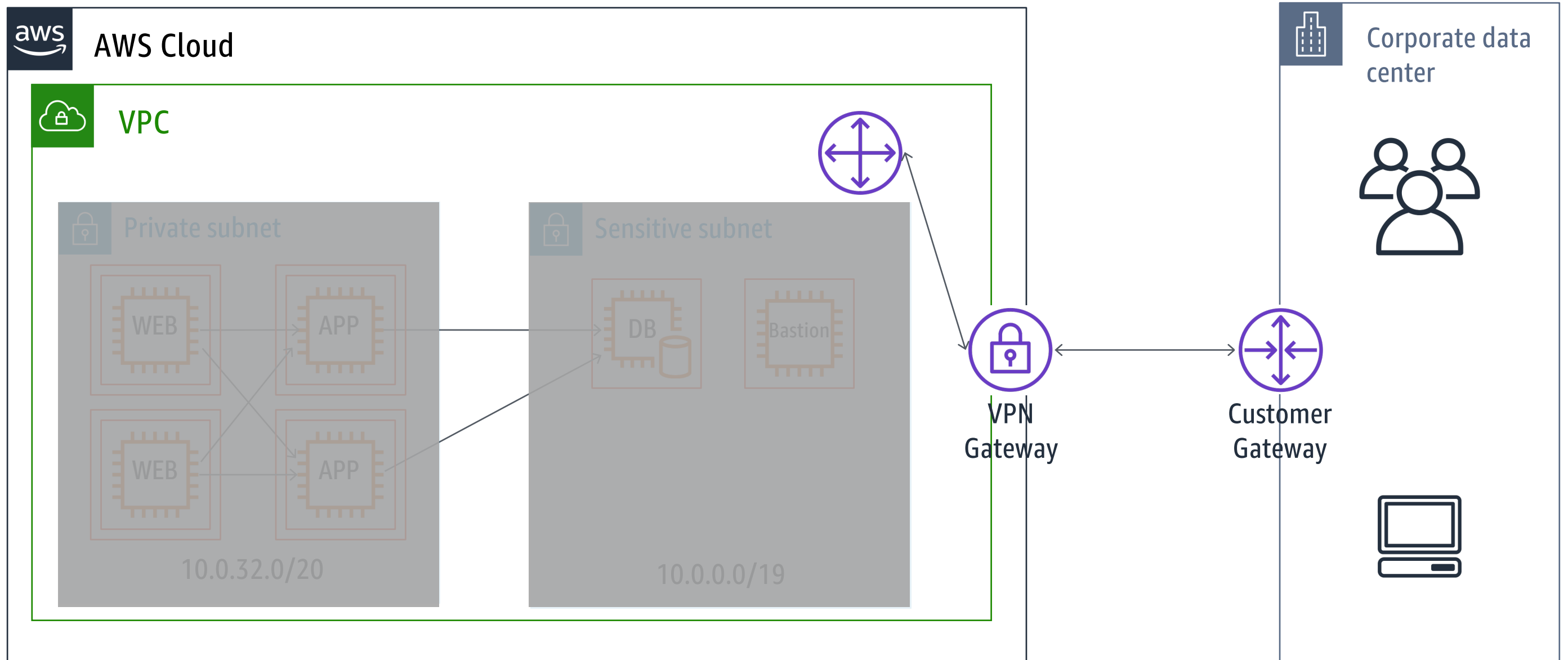
AWS Cloud



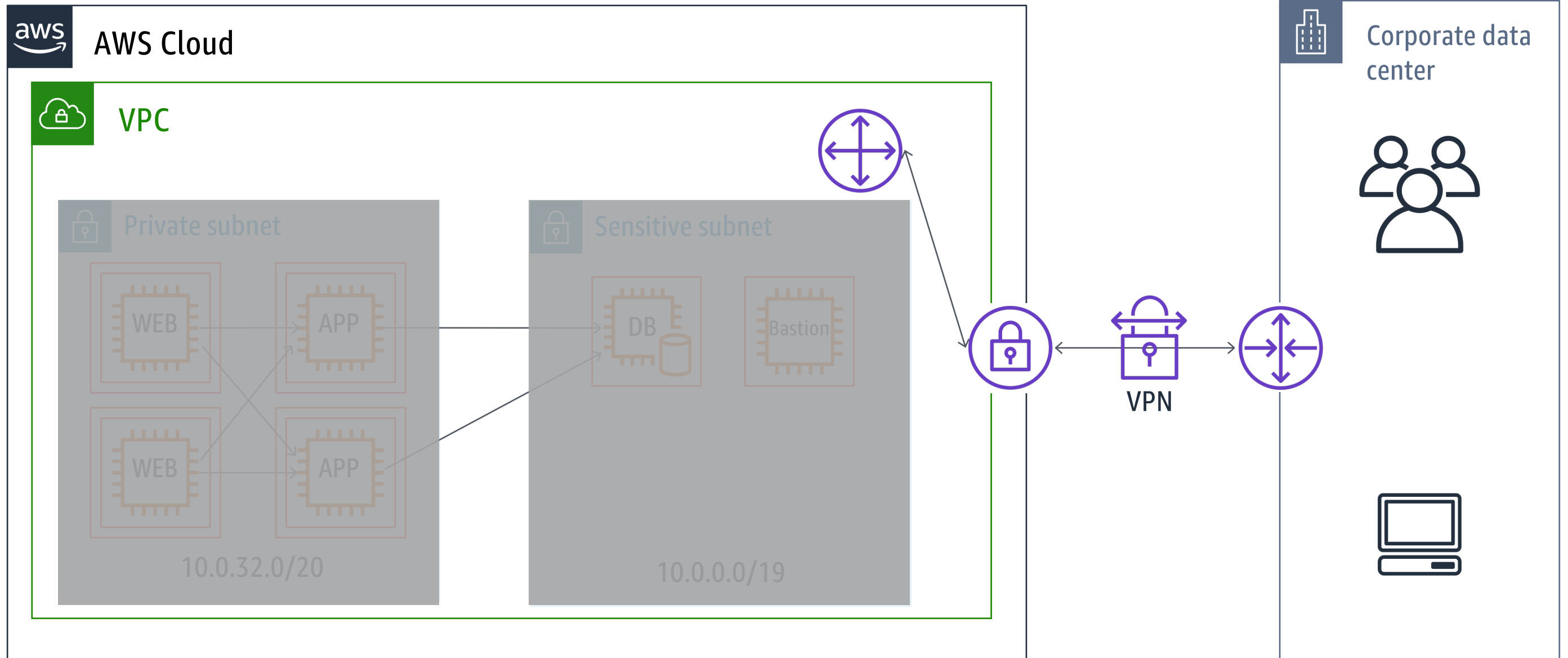
Transit Gateway



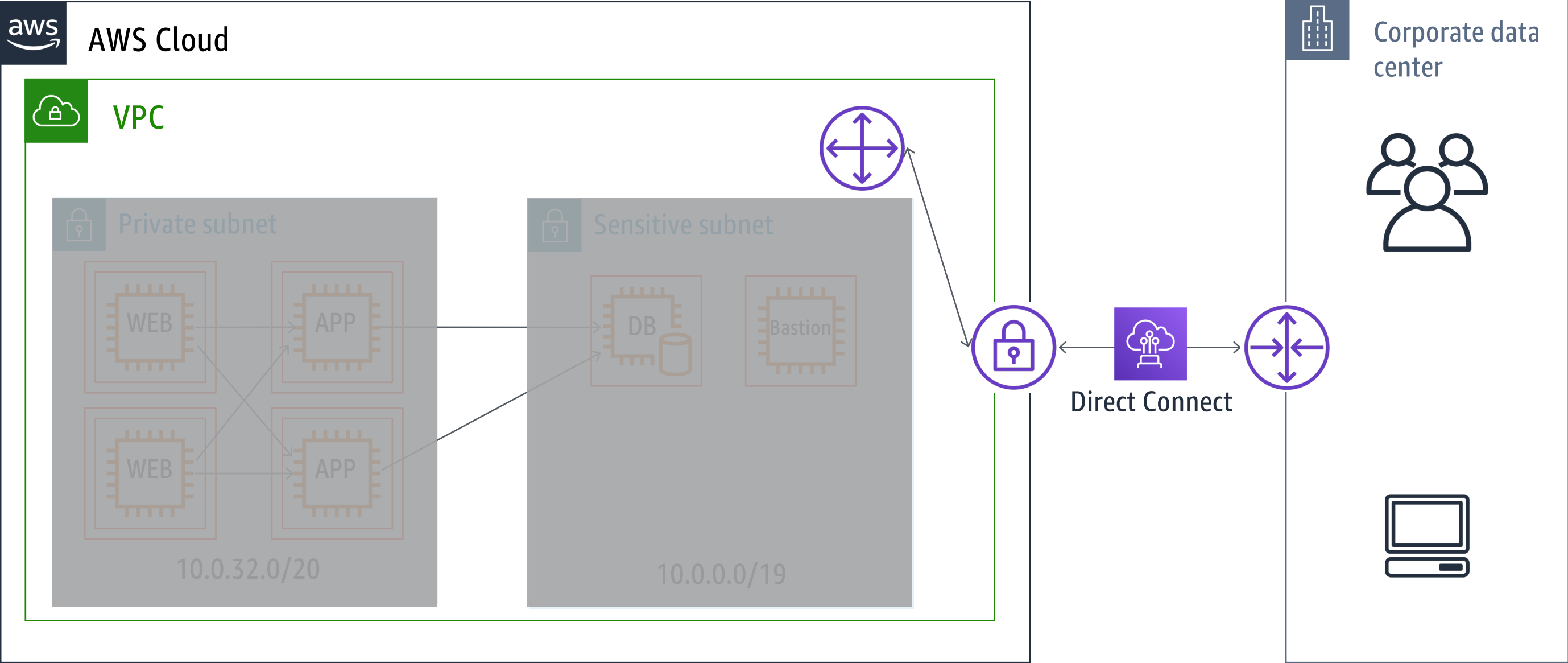
VPN



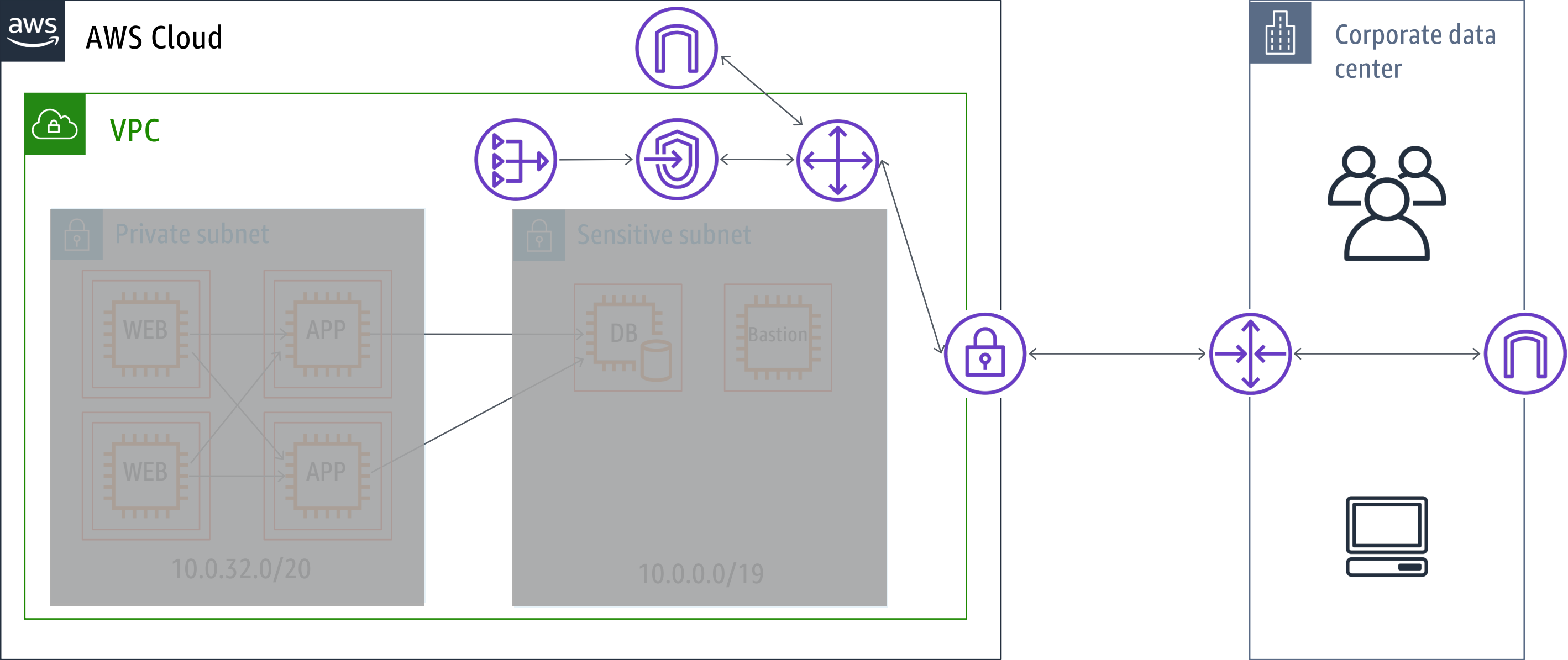
VPN



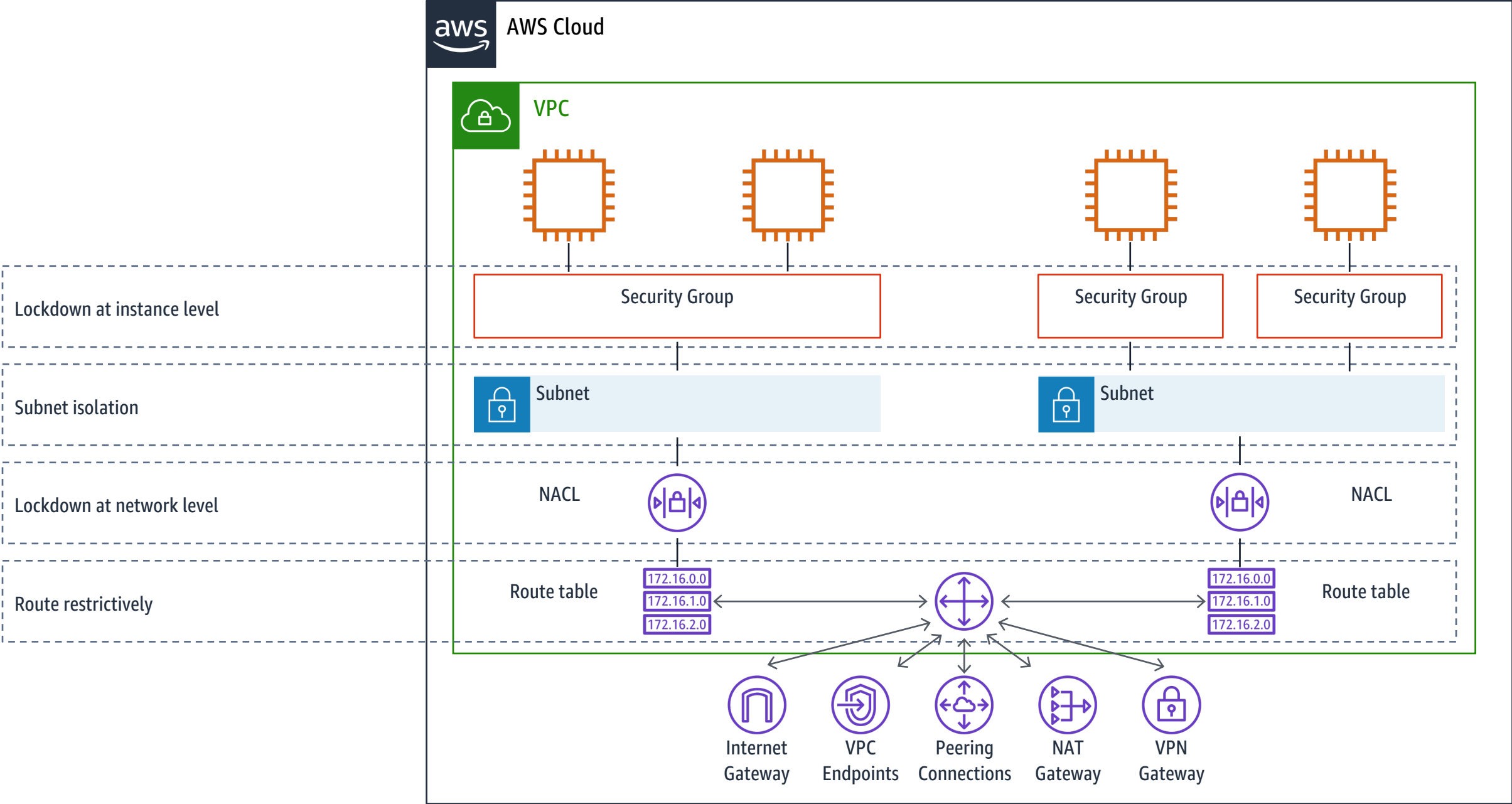
Direct Connect



Multiple Gateways



Network Defense in Depth



Questions?

