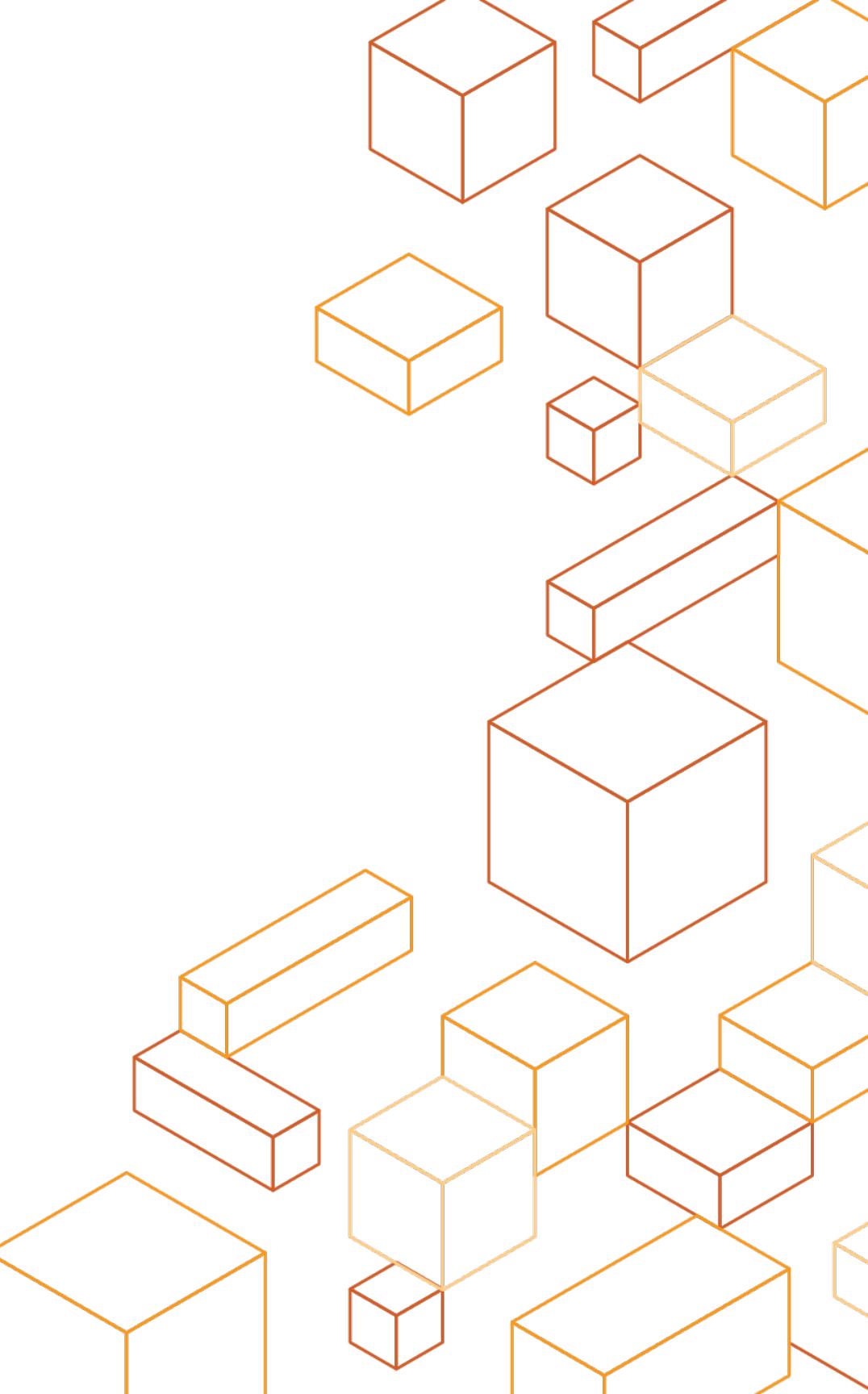




AWS VPC Overview



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



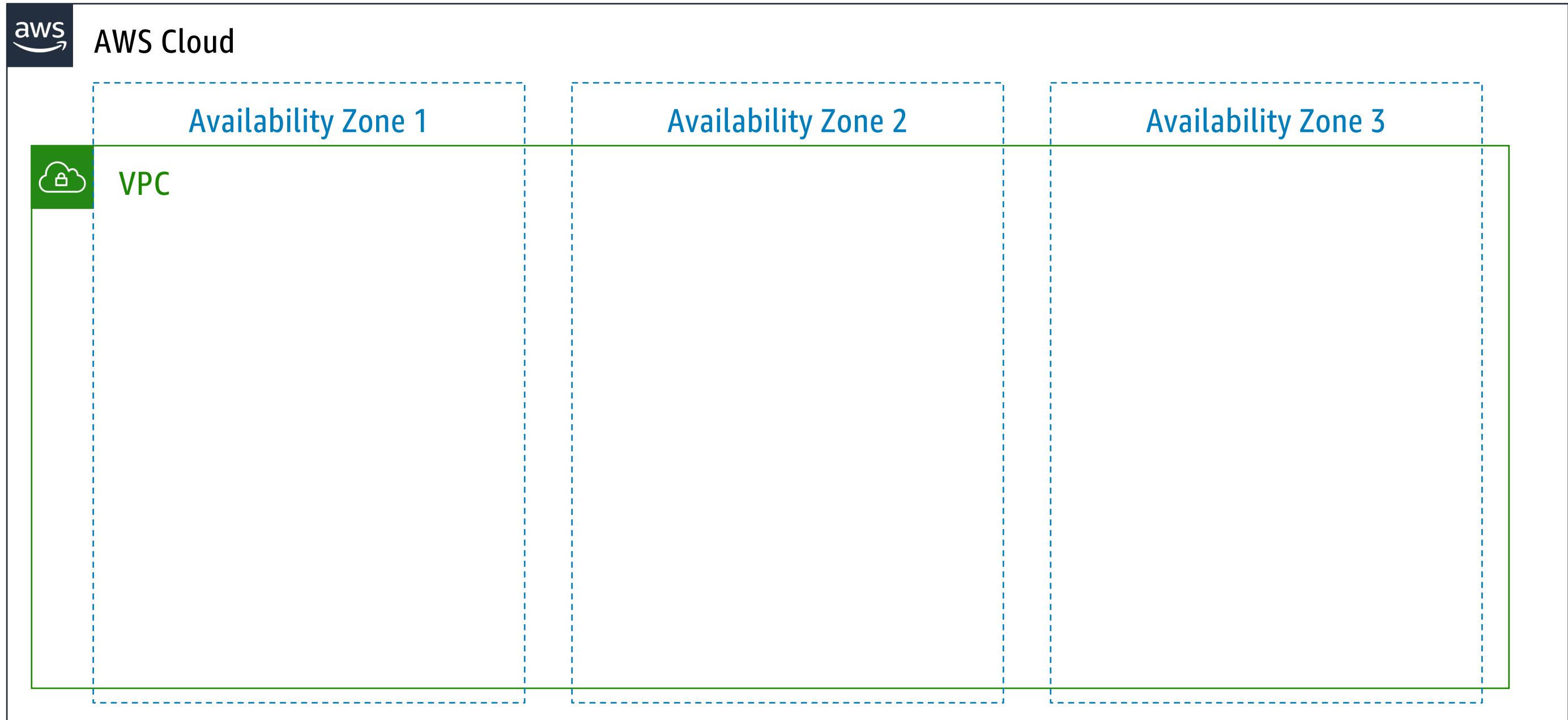
AWS Cloud

Availability Zone 1

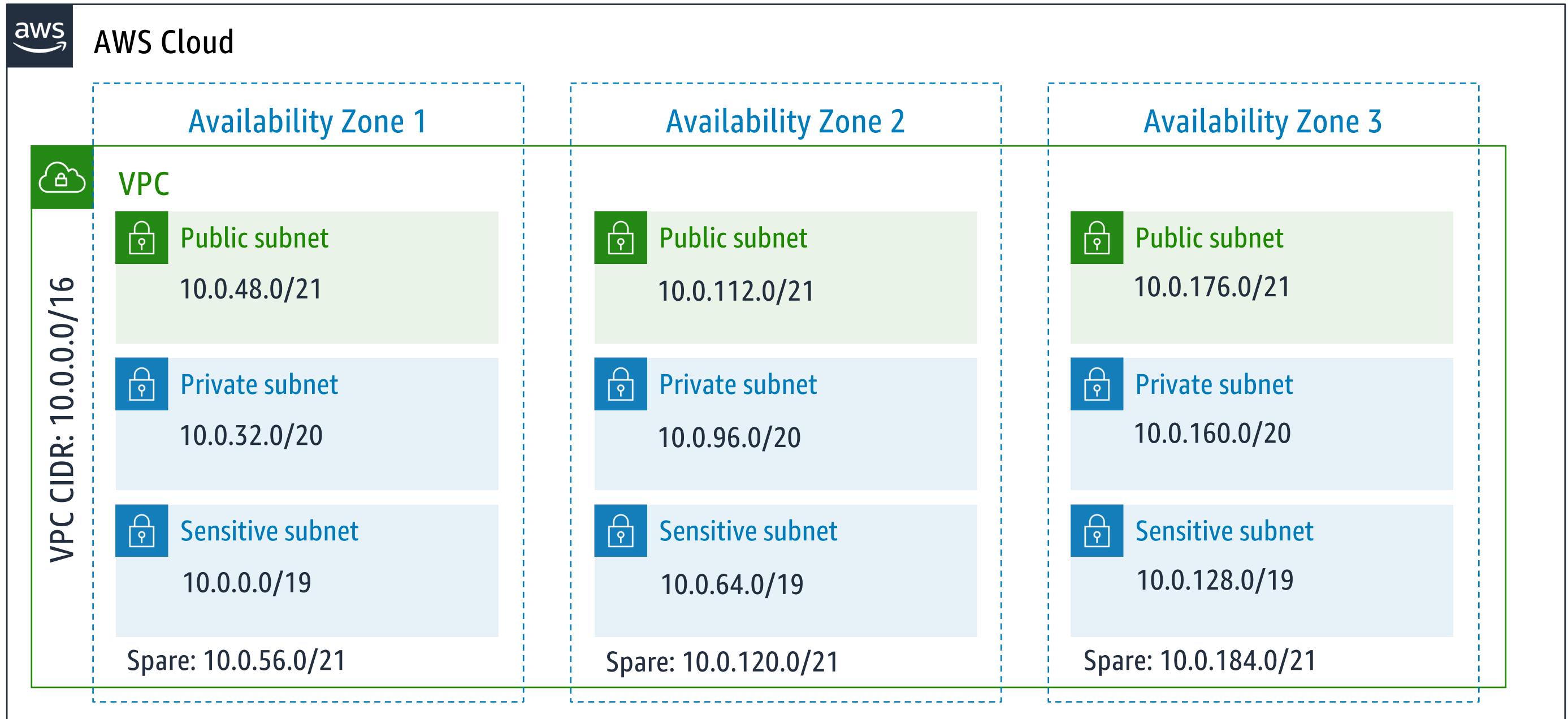
Availability Zone 2

Availability Zone 3

A VPC spans every Availability Zone in a Region



Subnets



Customers have full control over their VPC's



AWS Cloud

Availability Zone 1



VPC

Choose your VPC address range

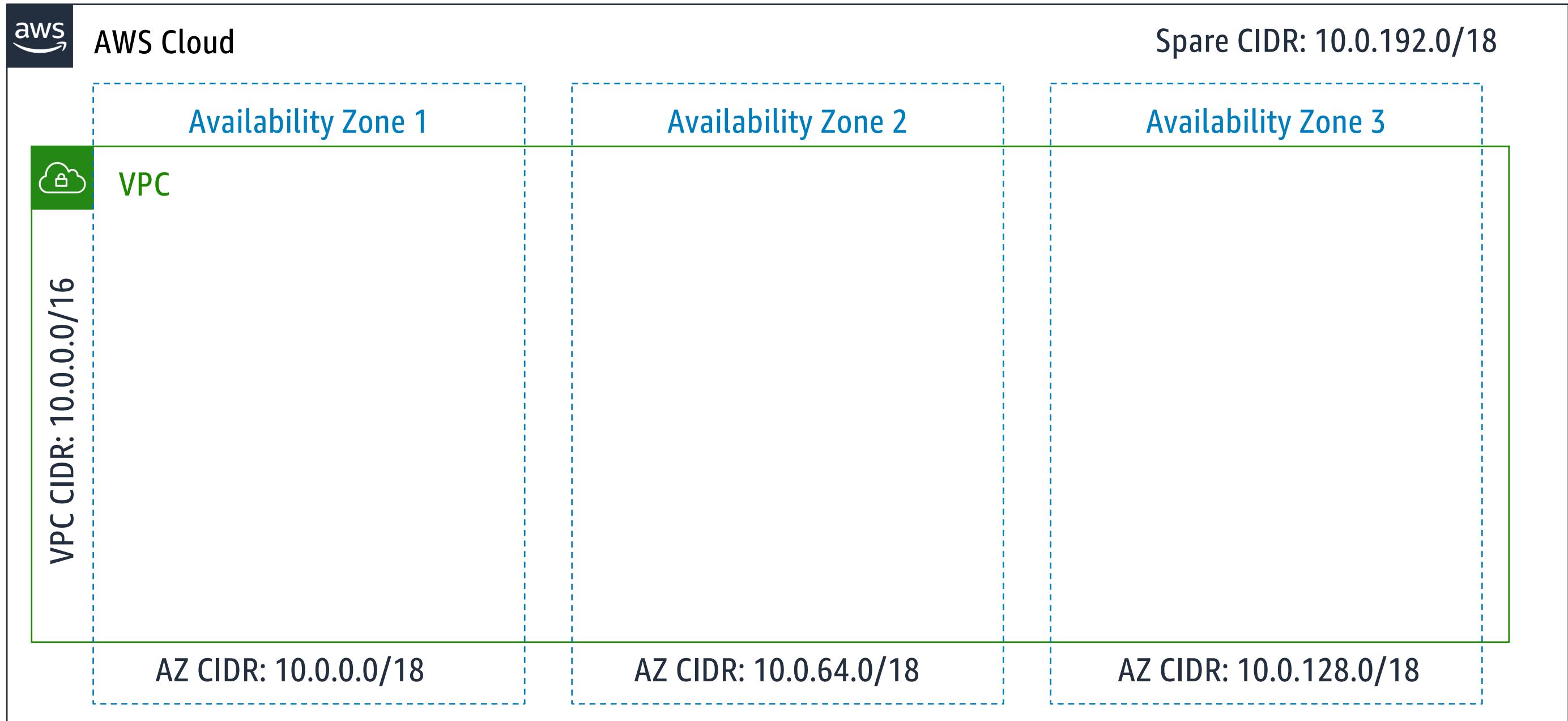
- Every VPC has a private IP address space (RFC1918 is recommended, but publicly routable IPv4 CIDR ranges are also supported)
- The VPC CIDR block size can be from /16 to /28
- Can associate additional IPv4 address blocks
- Can associate IPv6 address block

Availability Zone 2

Select IP addressing strategy

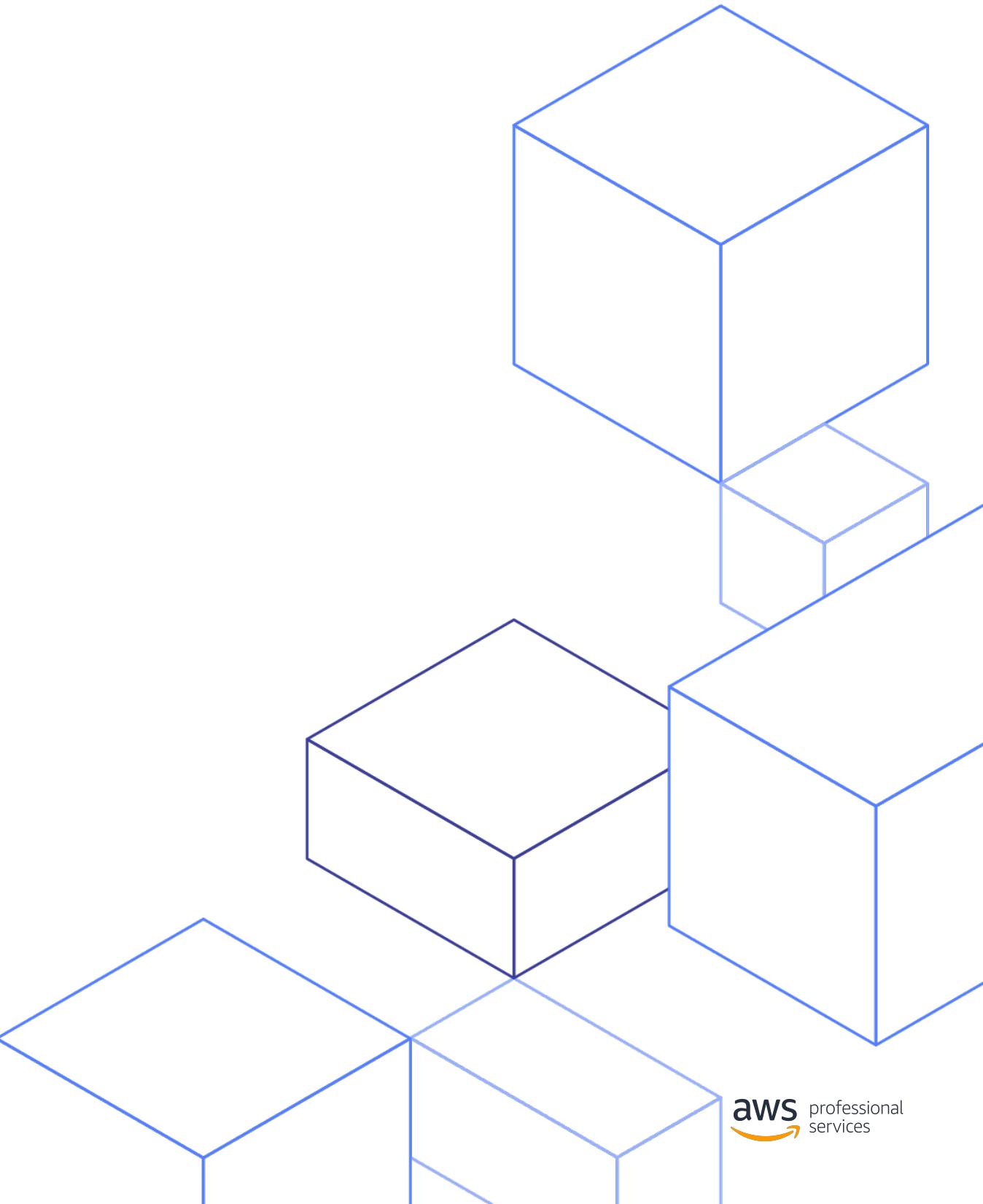
- Primary VPC CIDRs cannot be modified once created, additional space can be added
- Recommendation is to only use RFC1918 addresses or public IP space you own to prevent routing issues
- Consider address overlaps with other networks before committing to a CIDR
- Do not waste address space, but do not constrain growth either

Logically allocate CIDR space for each AZ

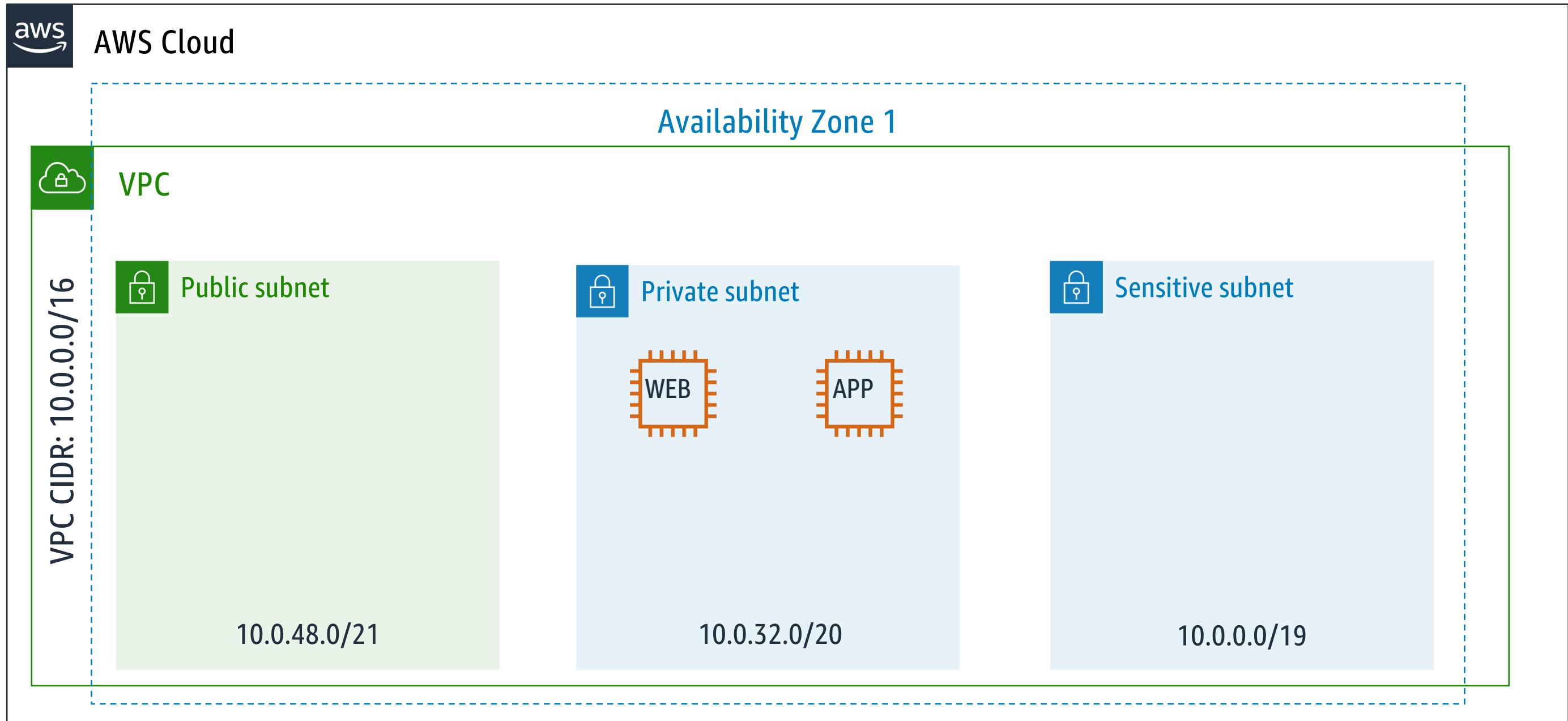


Security Groups

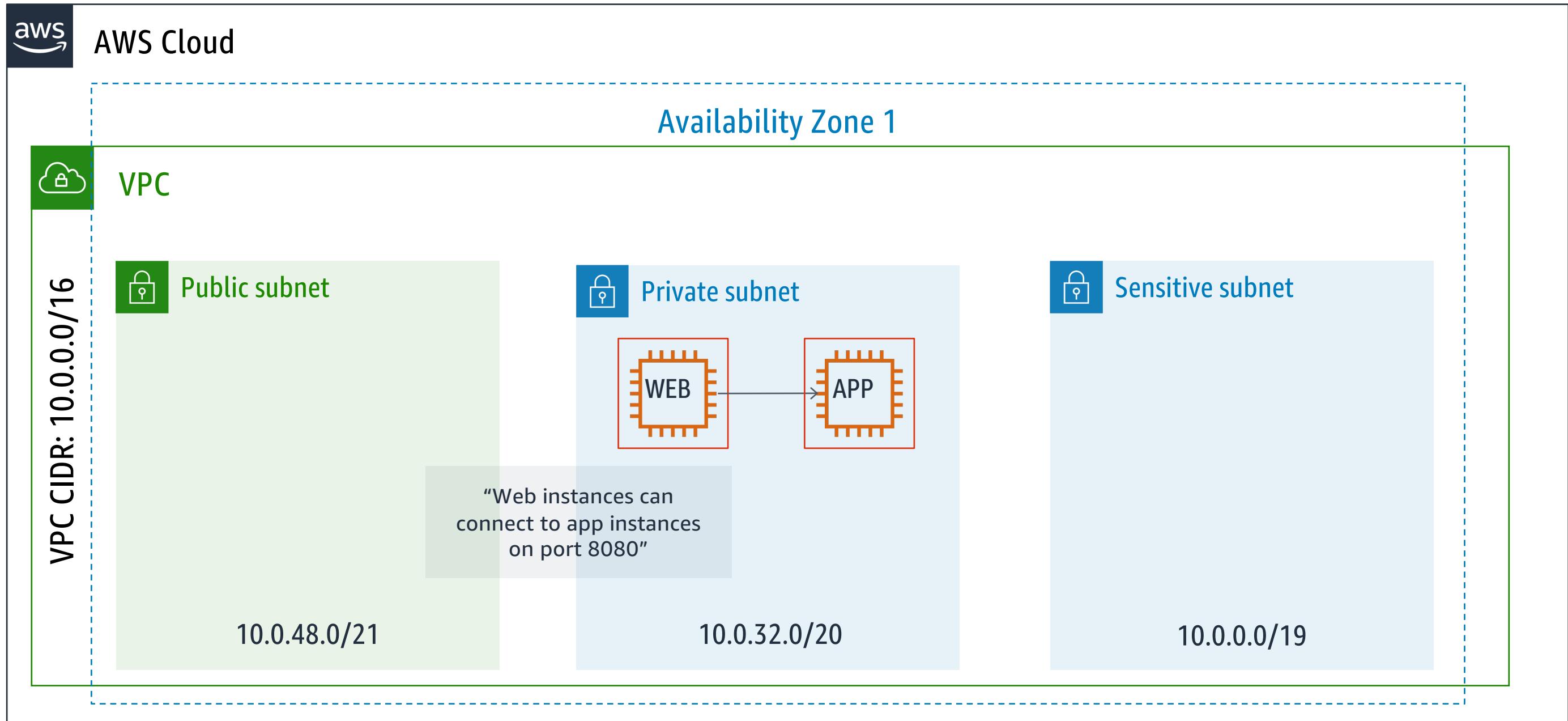
VPC Overview



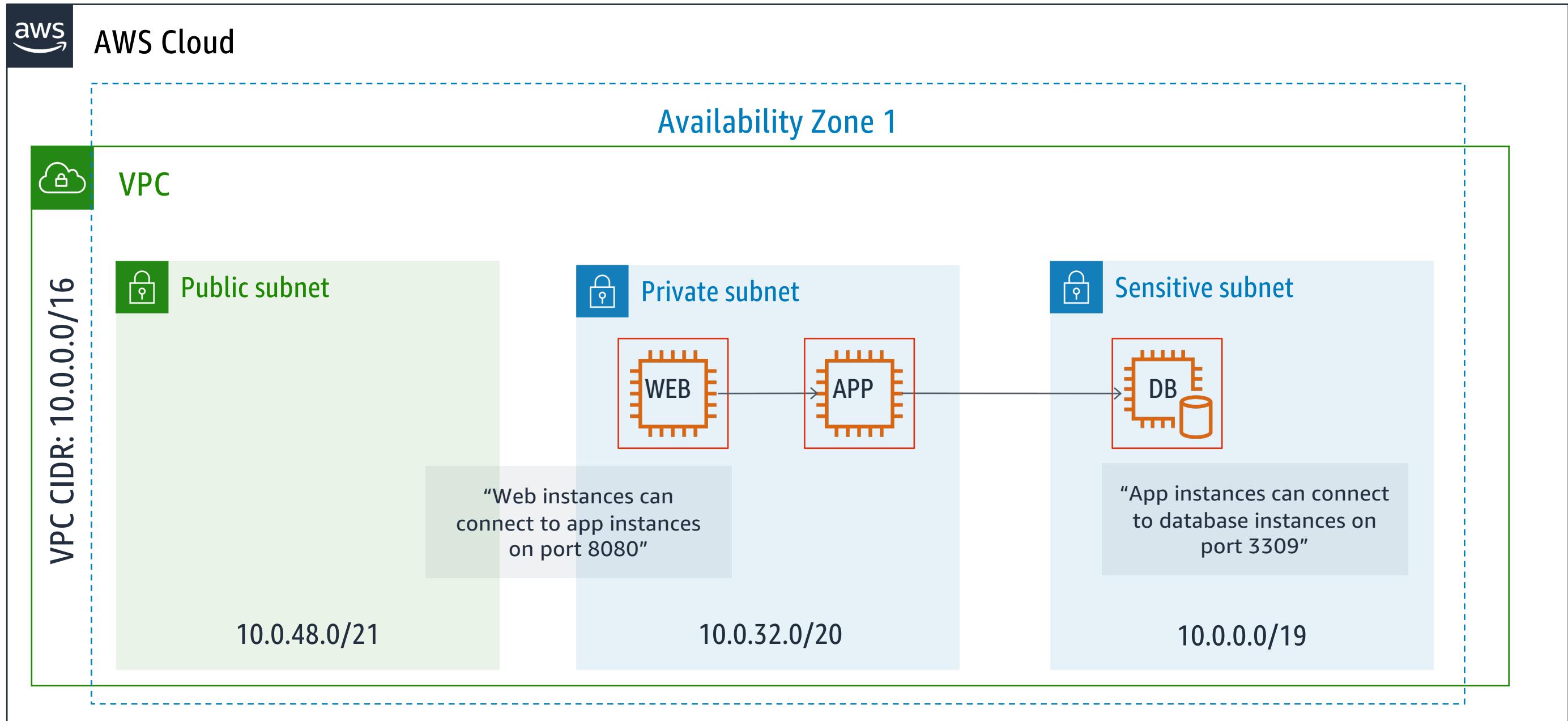
Security Groups – Stateful Firewall



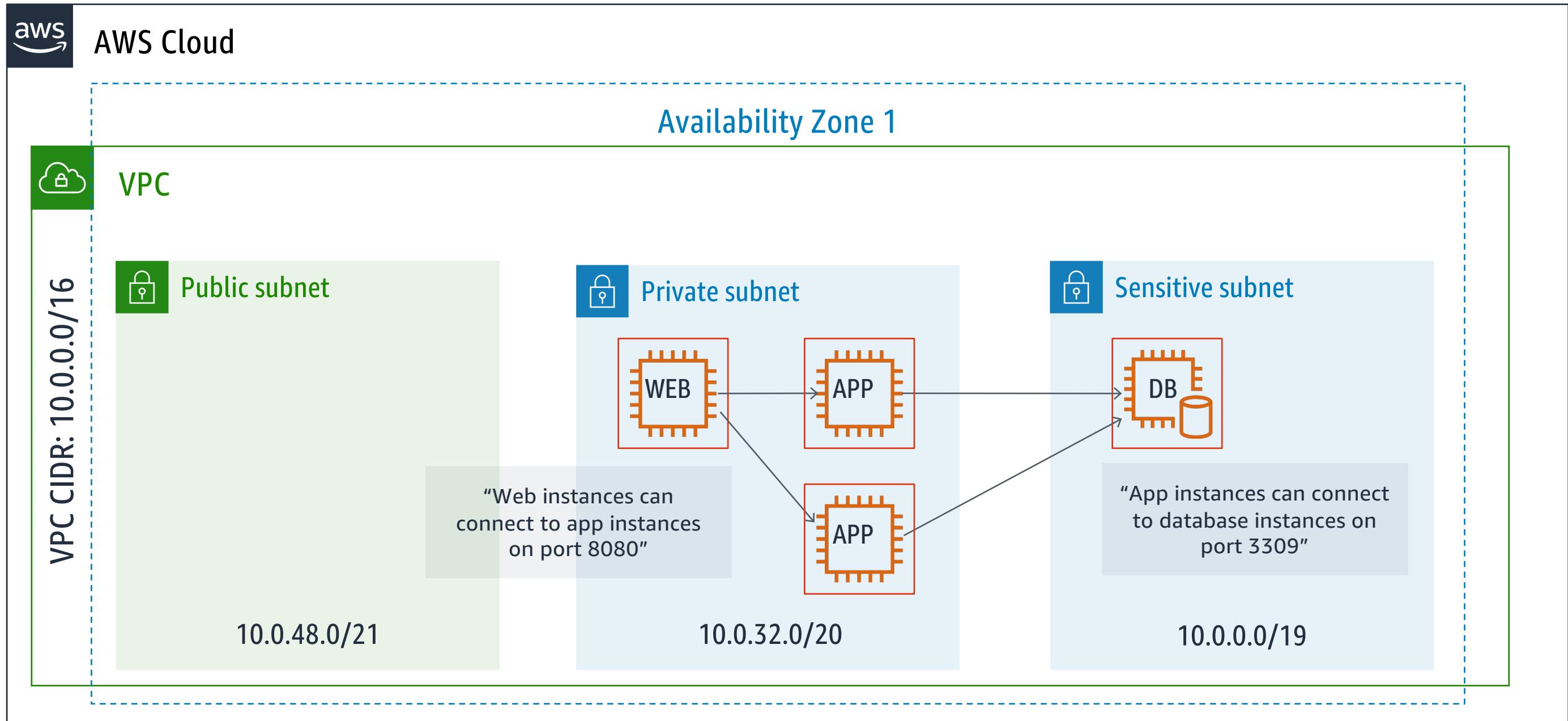
Security Groups – Stateful Firewall



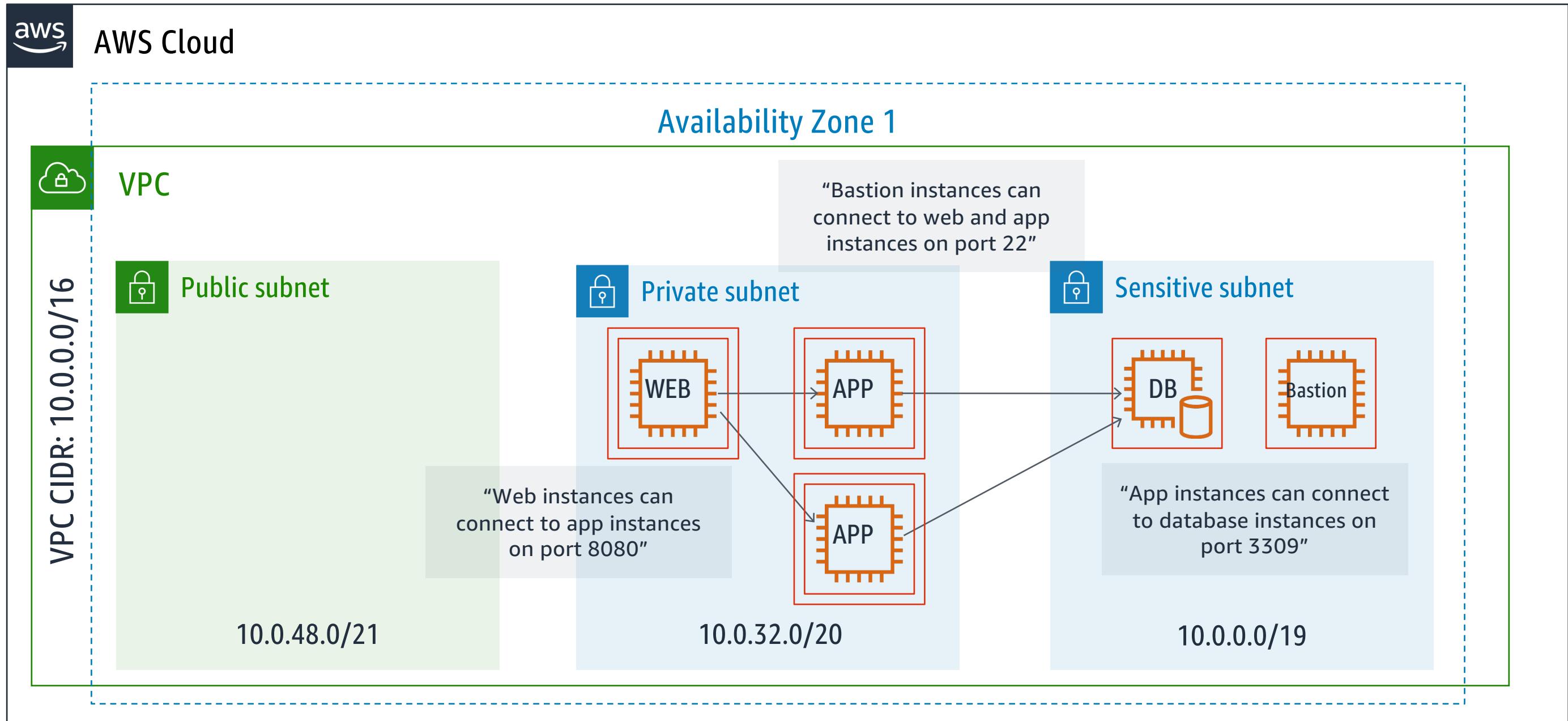
Security Groups – Stateful Firewall



Security Groups – Stateful Firewall

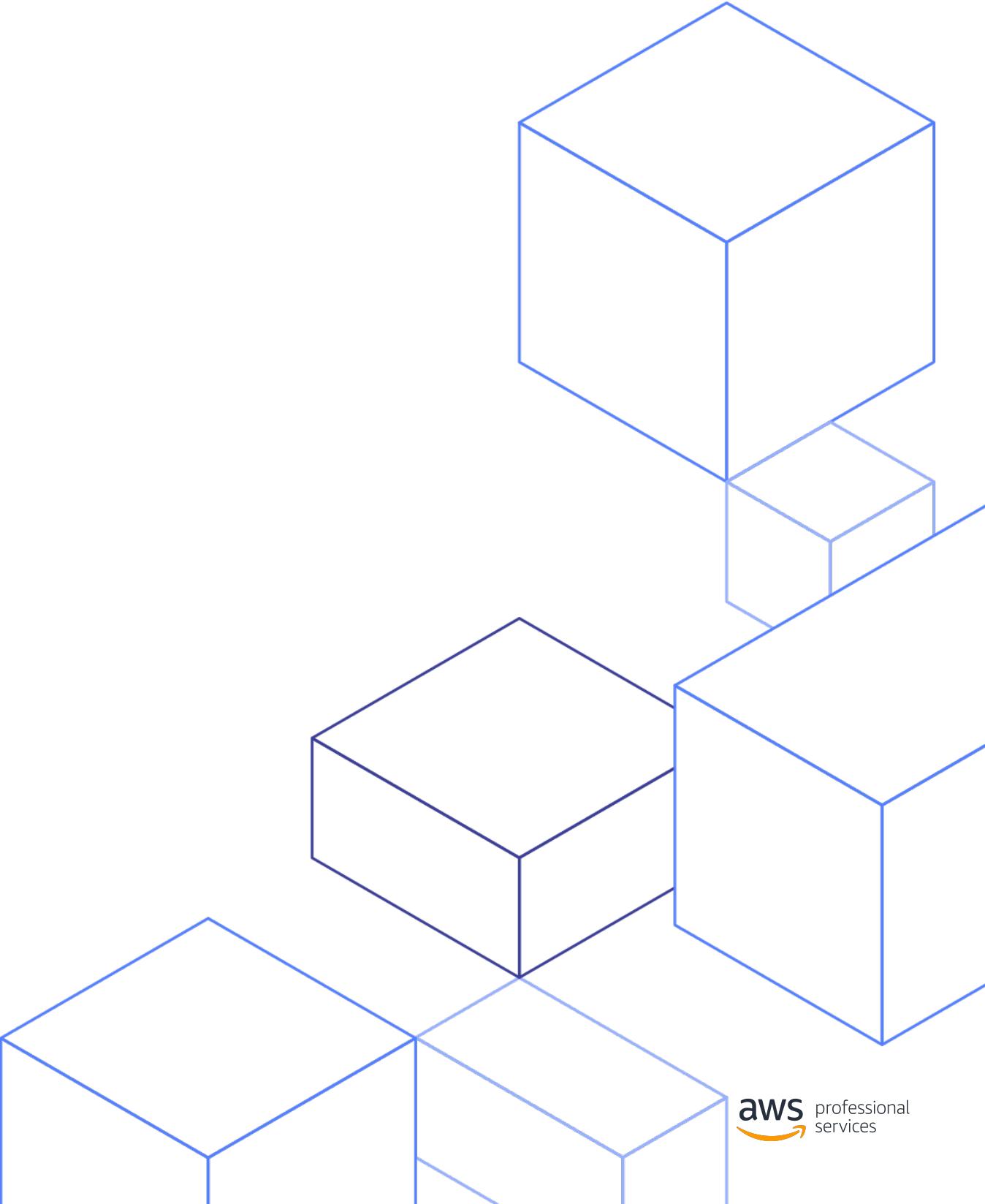


Security Groups – Stateful Firewall

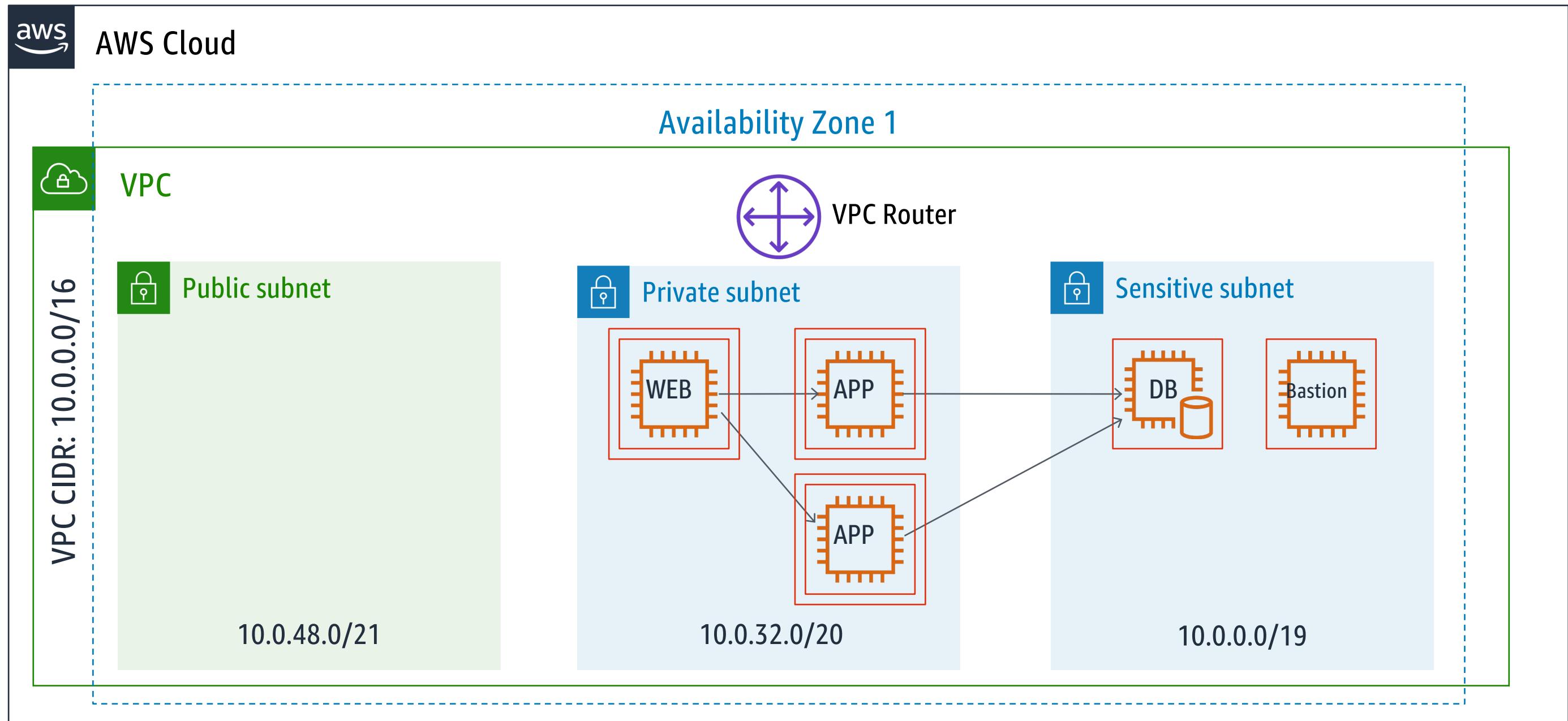


Routing, NACL's, and Load Balancing

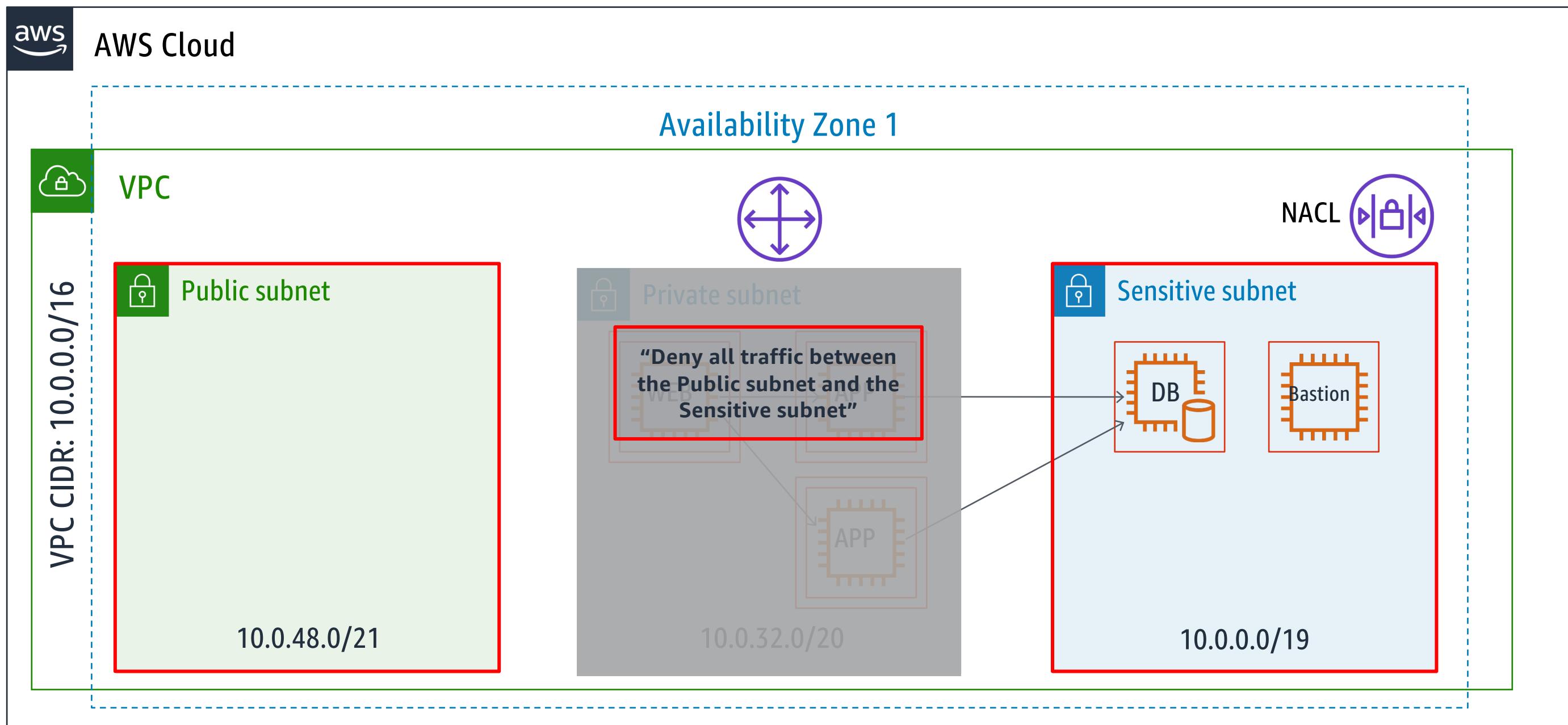
VPC Overview



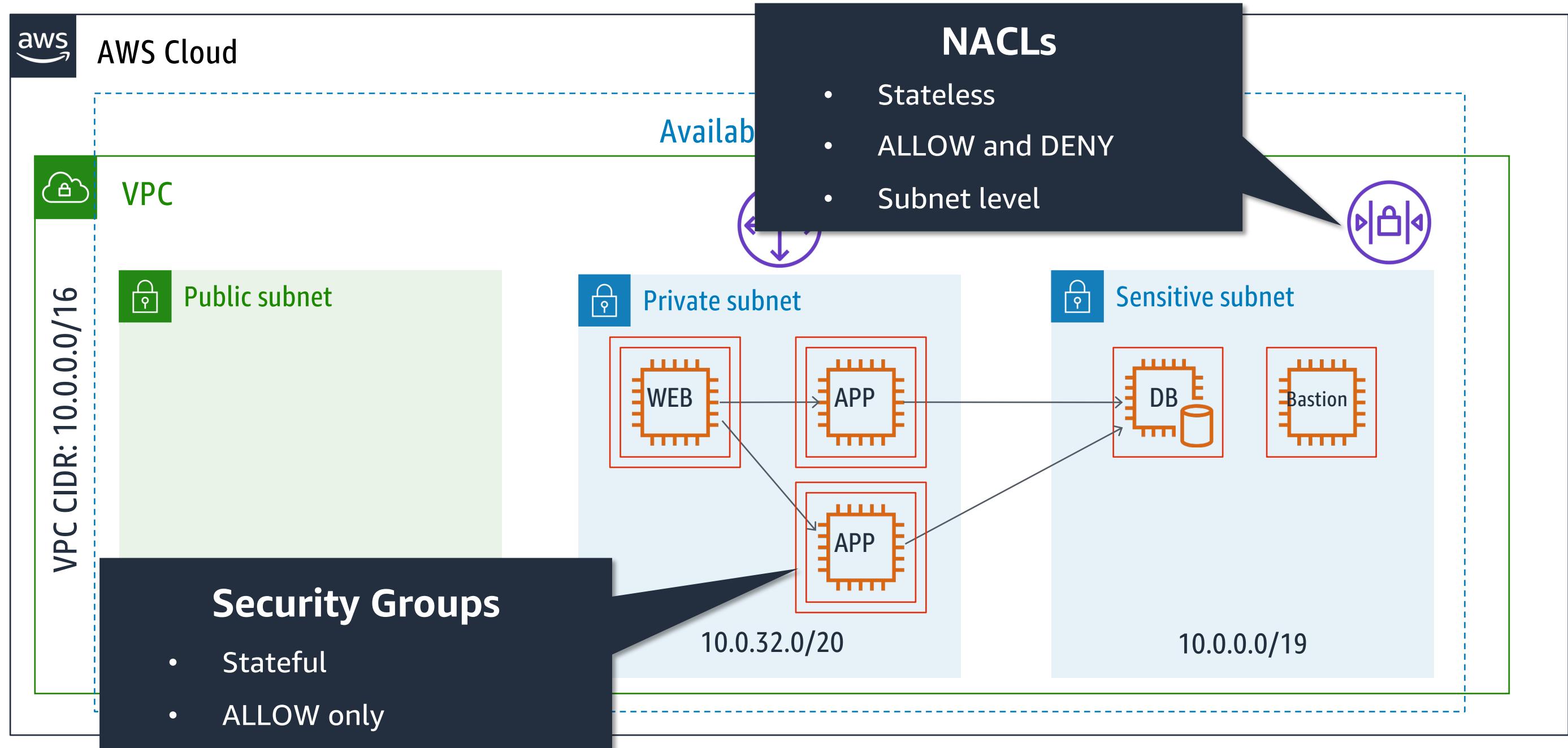
Routing



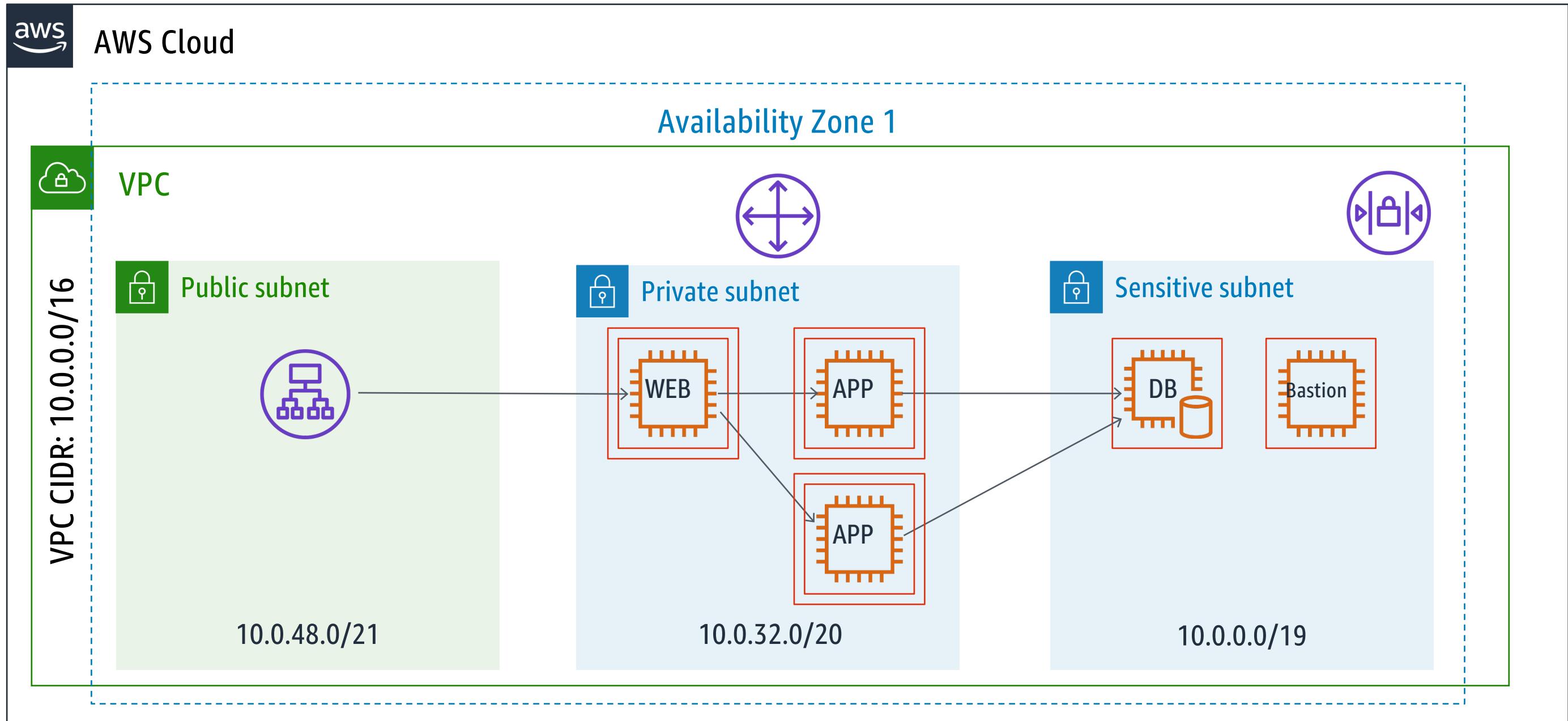
Network Access Control List (NACL)



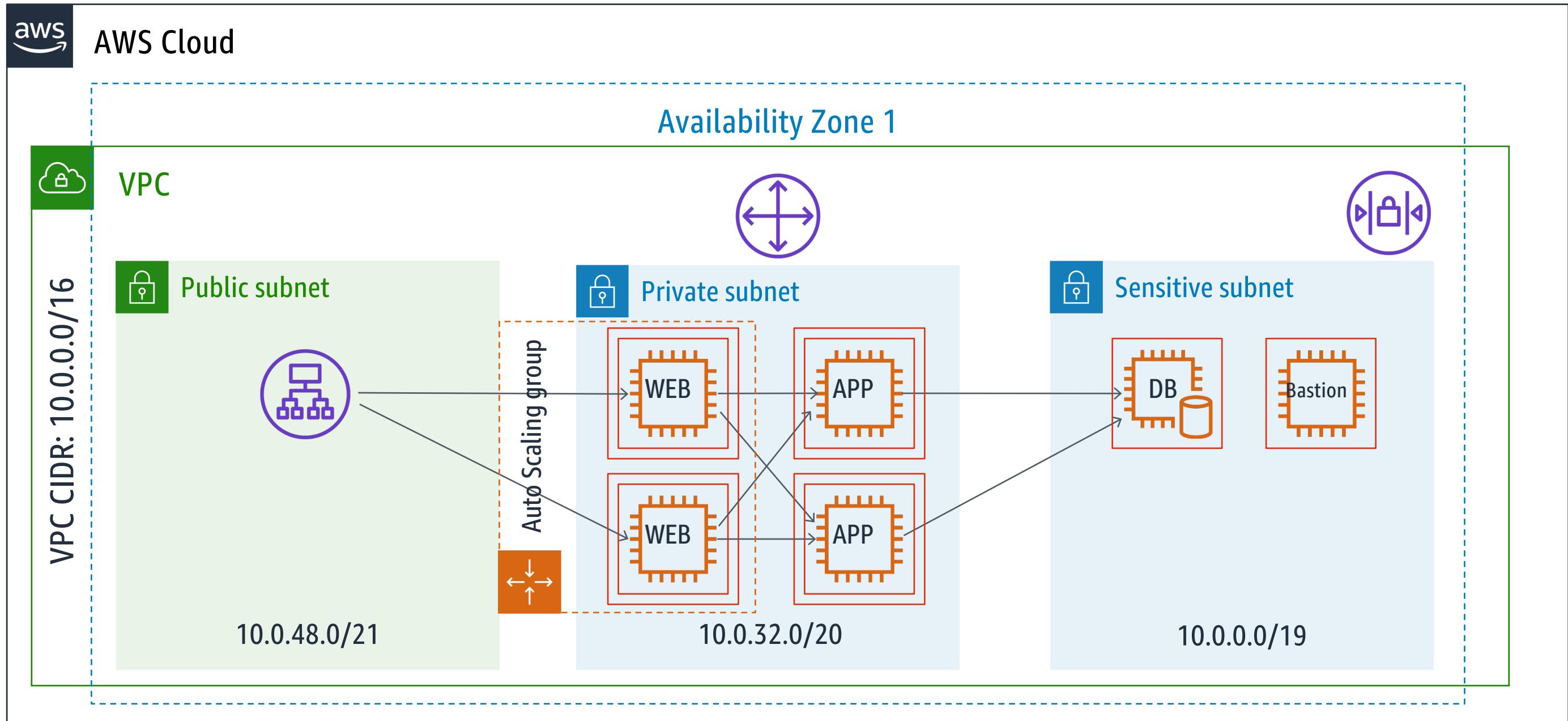
NACLs and Security Groups



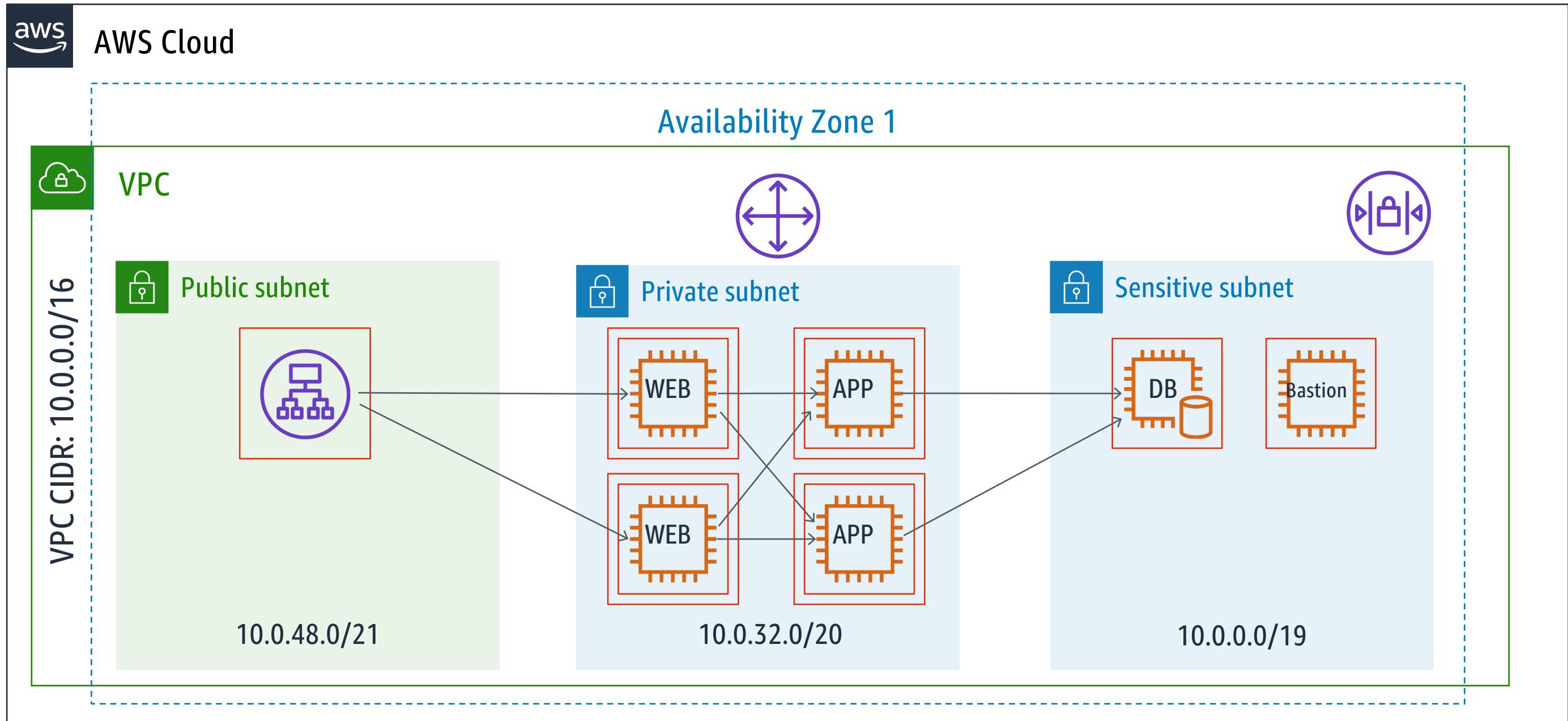
Load Balancing



Load Balancing



Load Balancing



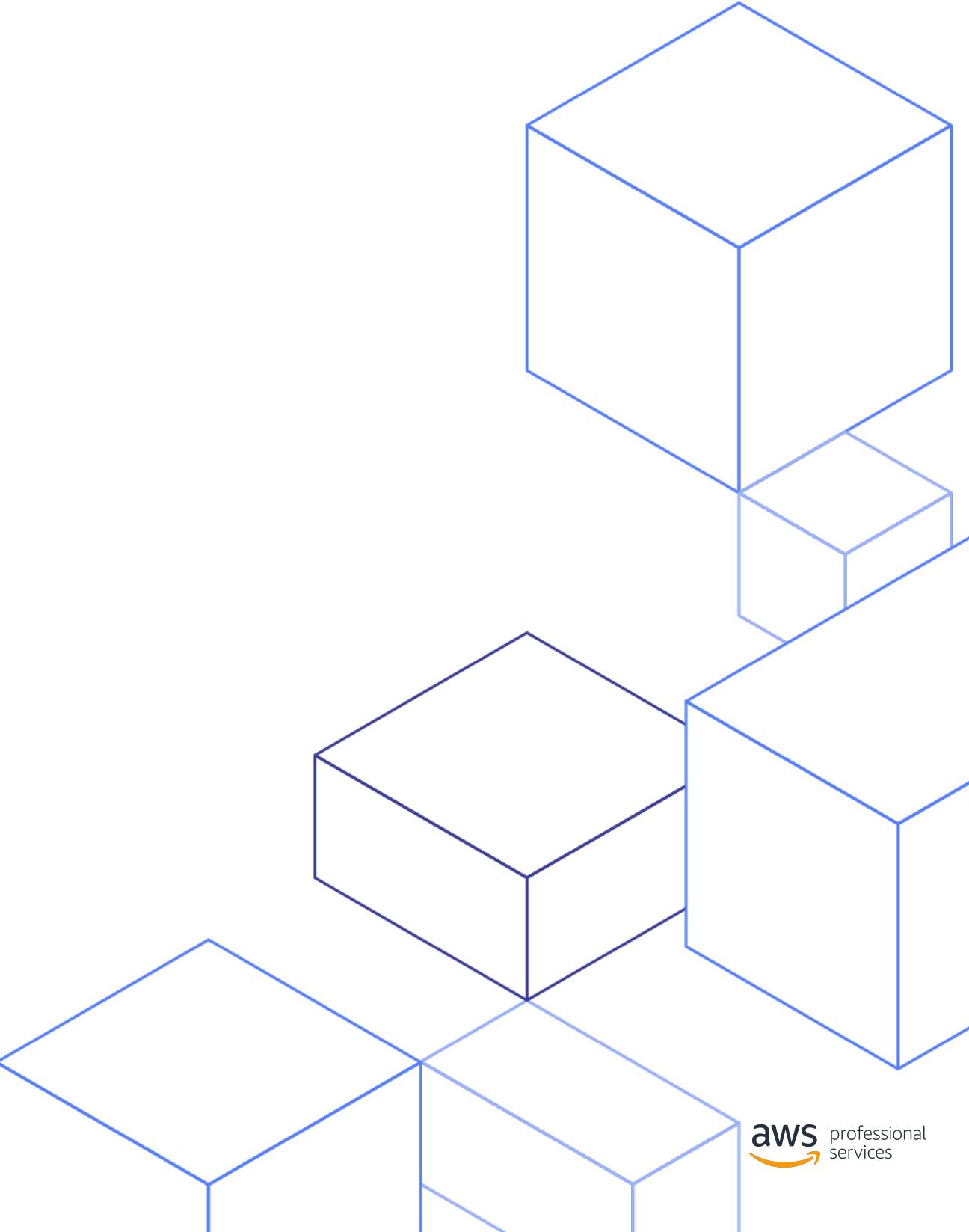
Load Balancing – ELB Types

	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	✓	✗	✗	✗

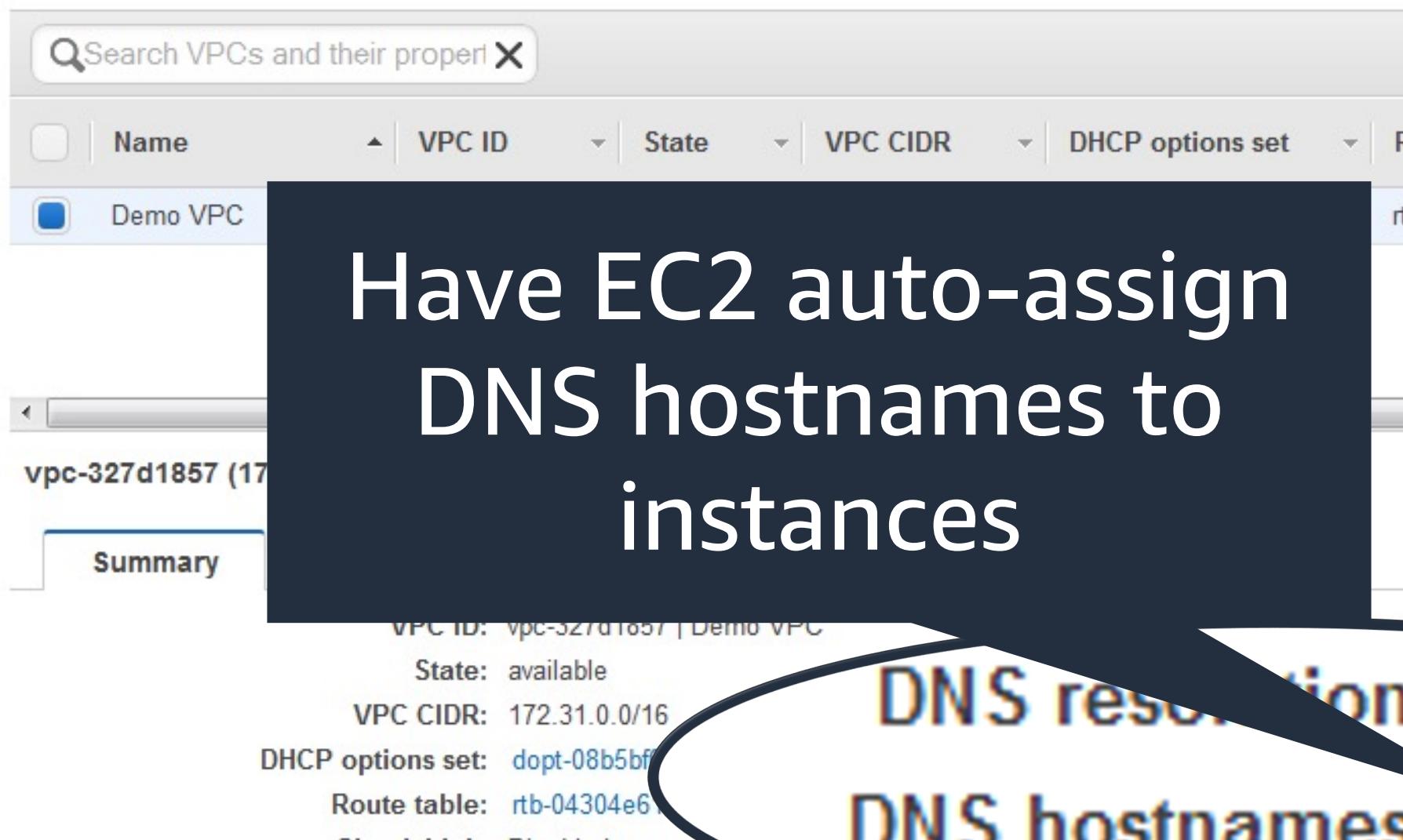
<https://aws.amazon.com/elasticloadbalancing/features/>

DNS

VPC Overview



VPC DNS Options



Use
Amazon
DNS server

EC2 DNS Hostnames

Internal DNS
hostname: Resolves
to Private IP address

Description	Status Checks	Logs
Instance ID	i-a34...	
Instance state	running	
Instance type	t2.micro	
Private DNS	ip-172-31-0-201.eu-west-1.compute.internal	
Private IPs	172.31.0.201	
Secondary private IPs		
VPC ID	vpc-327d1857	

External DNS name:
Resolves to...

...eu-west-1.compute.amazonaws.com



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
```

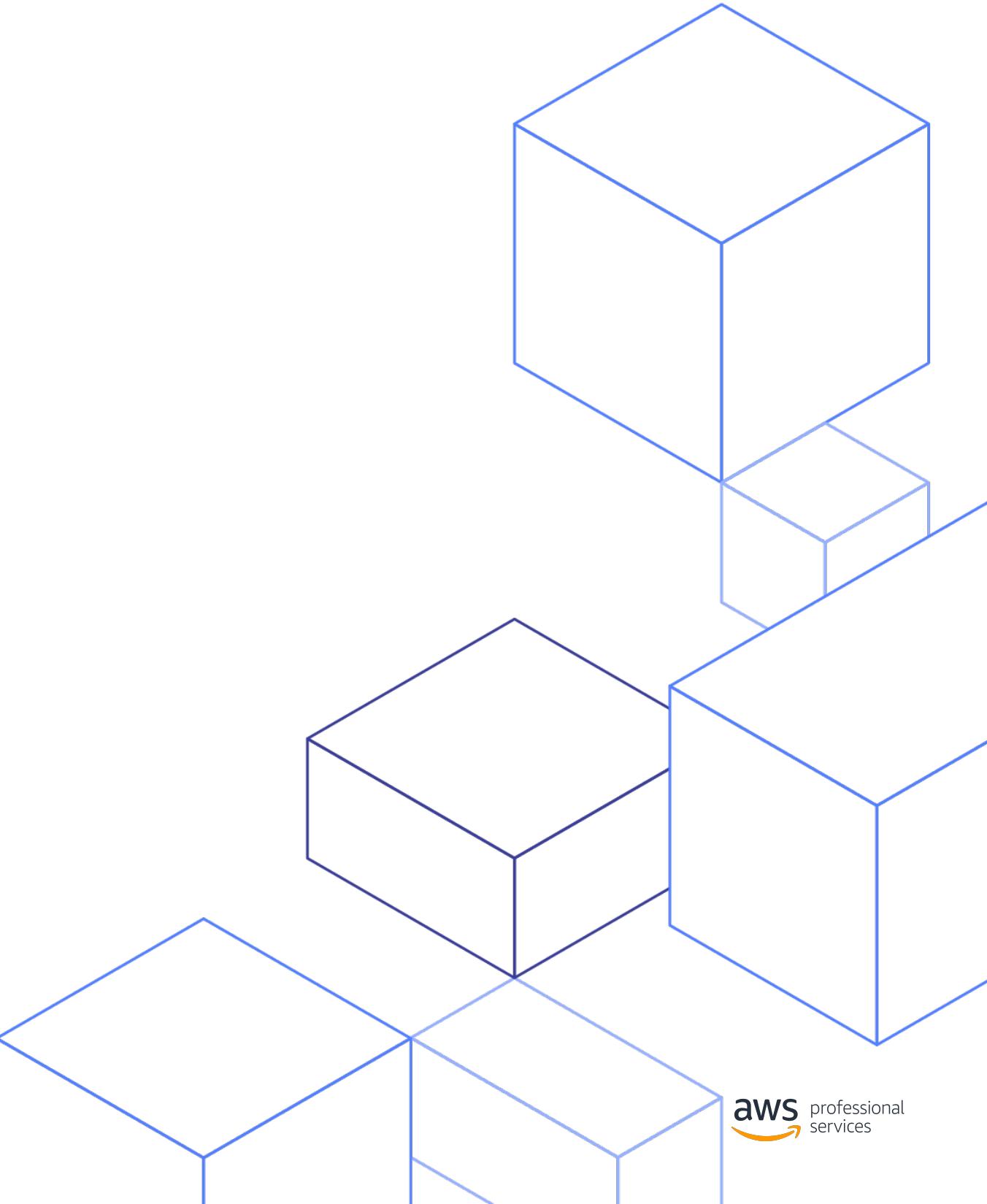
```
;; ANSWER SECTION:  
ec2-52-18-10-57.eu-west-1.compute.amazonaws.com. 60 IN A 172.31.0.137
```

```
;; 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
```

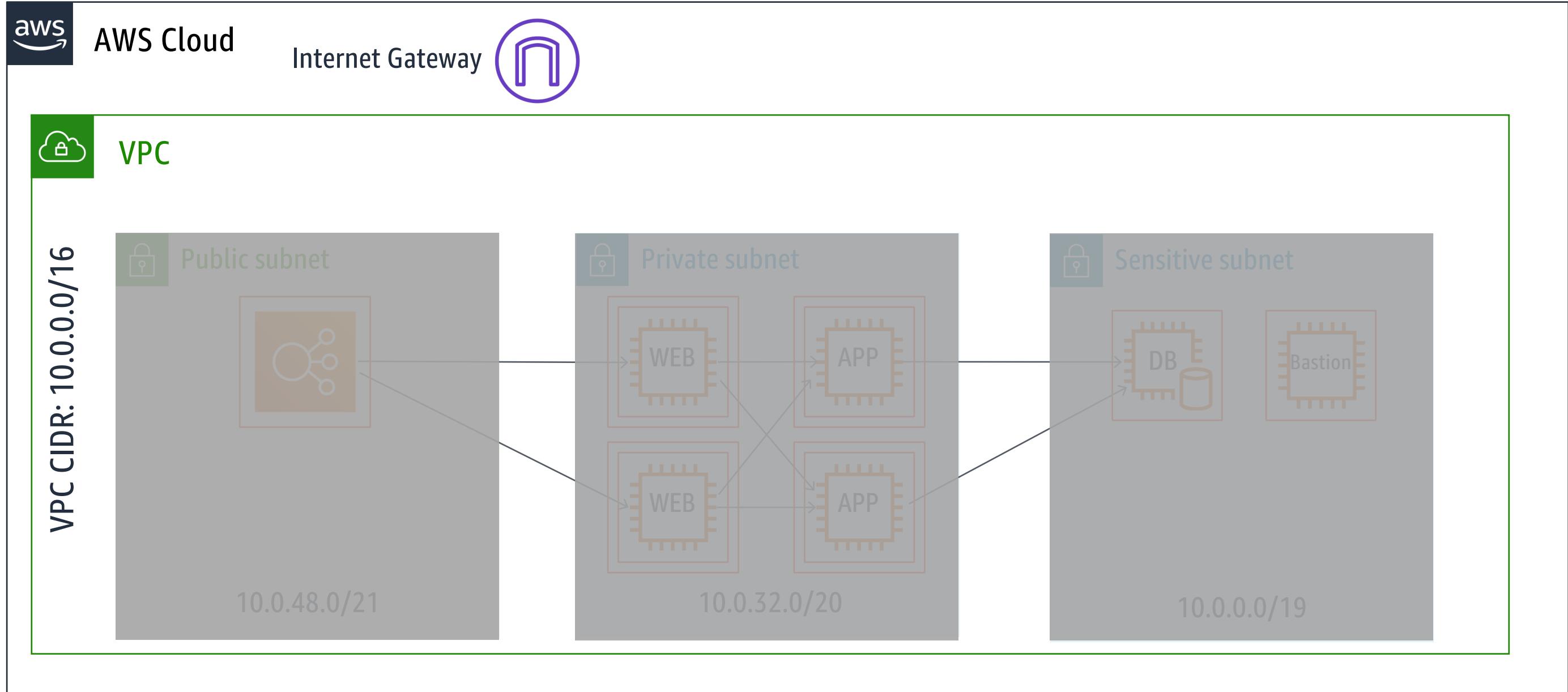
Inside your VPC:
Private IP address

Connectivity

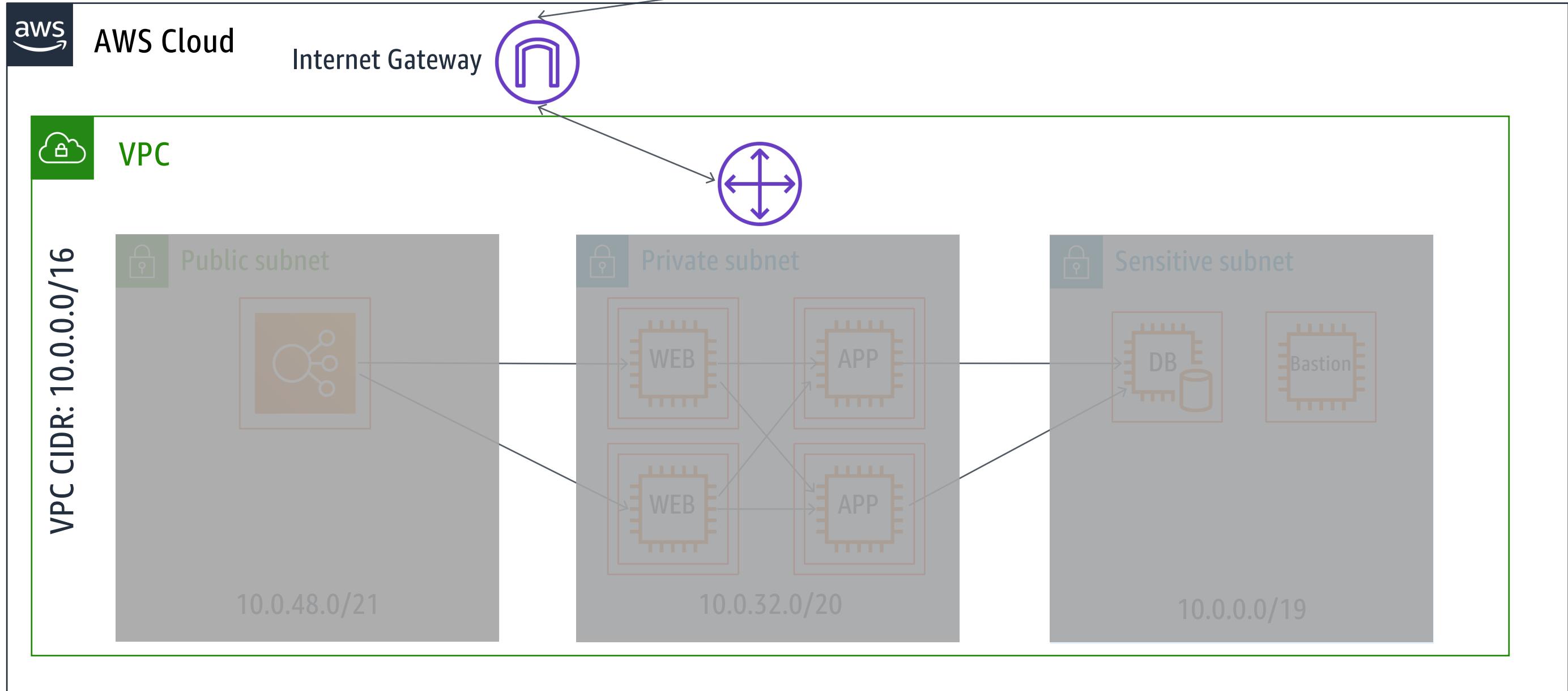
VPC Overview



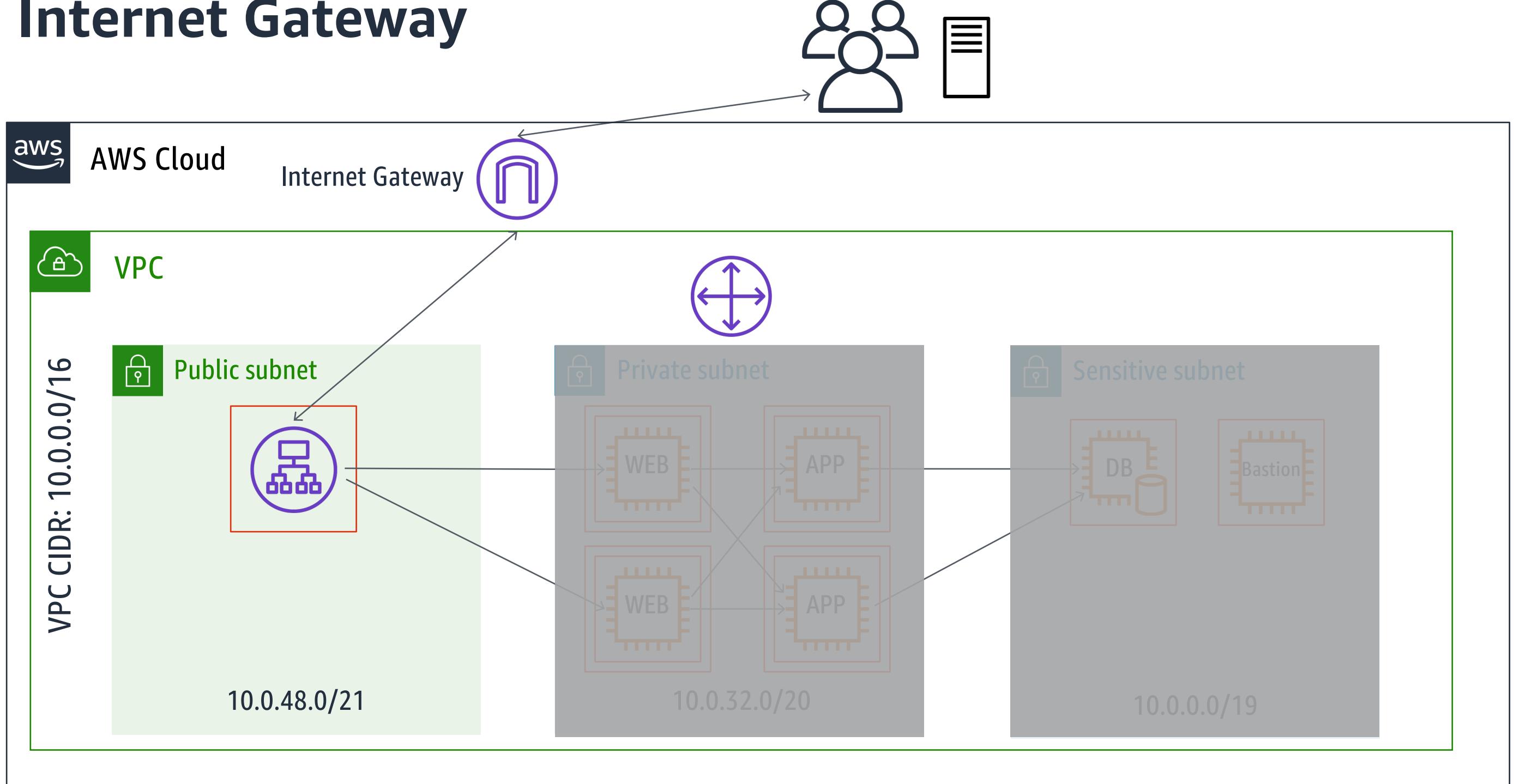
Internet Gateway



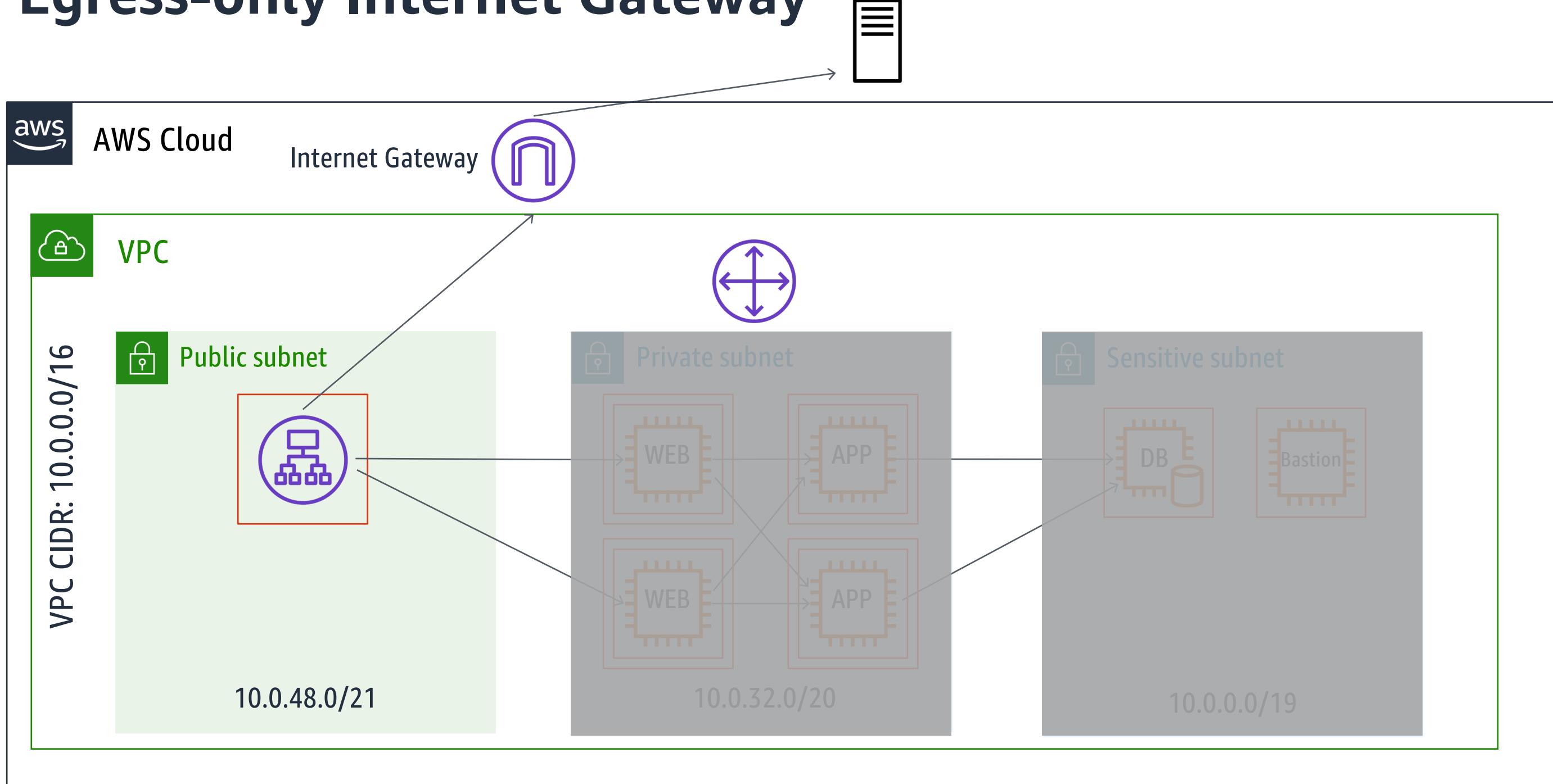
Internet Gateway



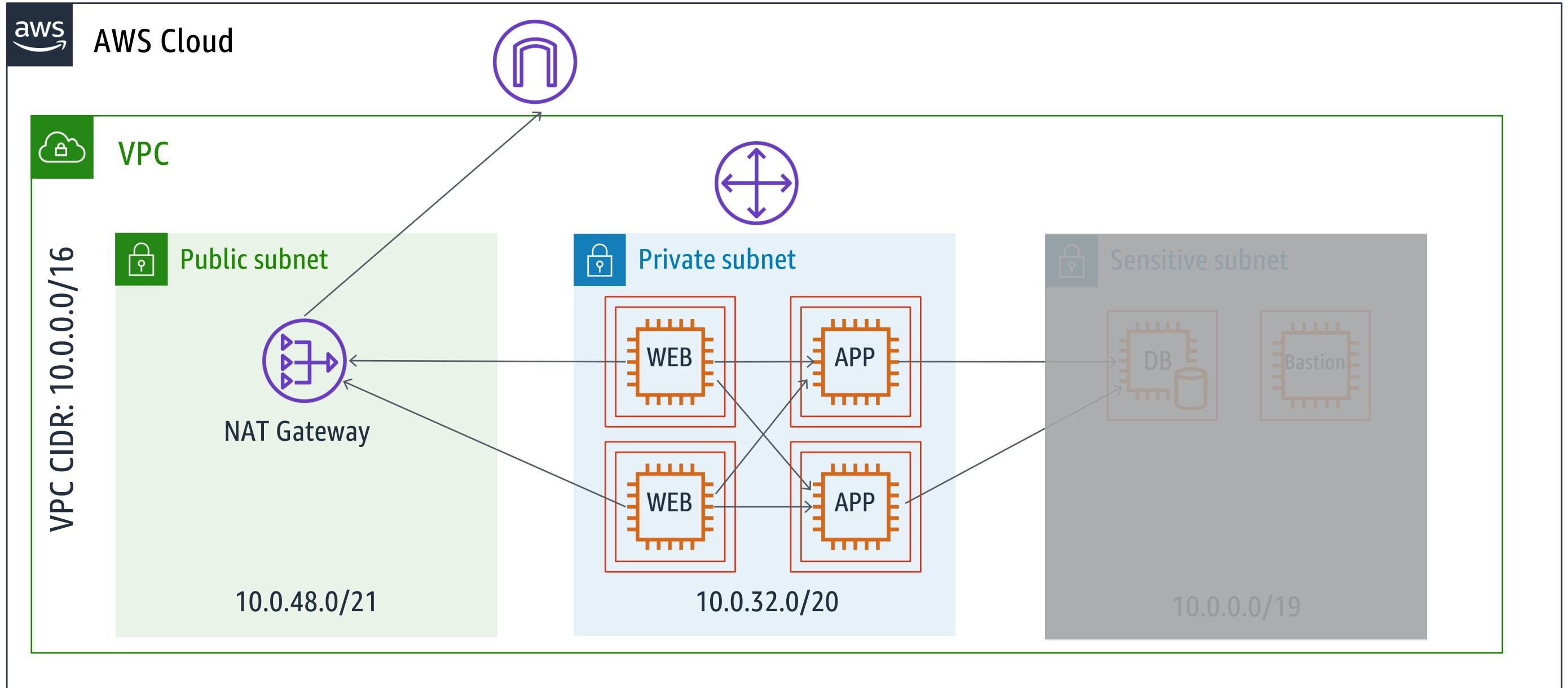
Internet Gateway



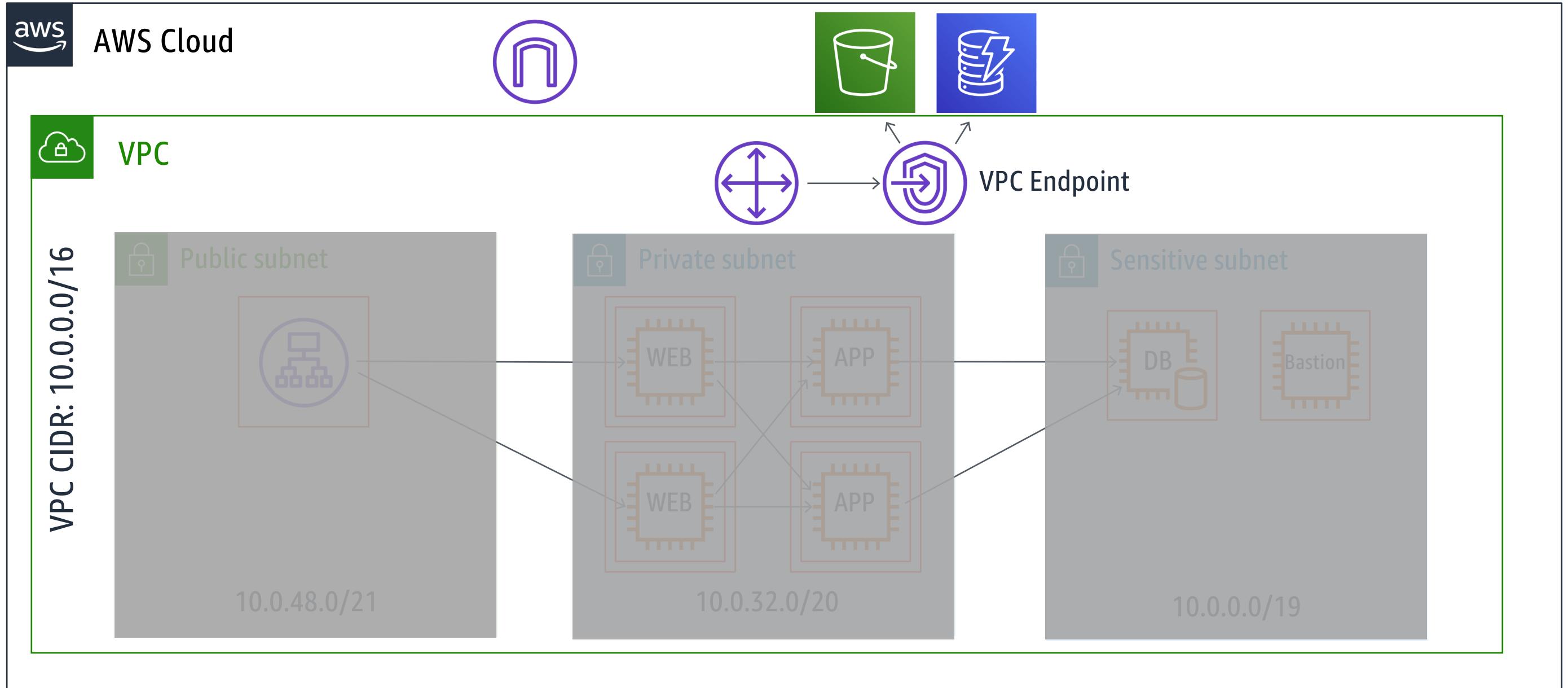
Egress-only Internet Gateway



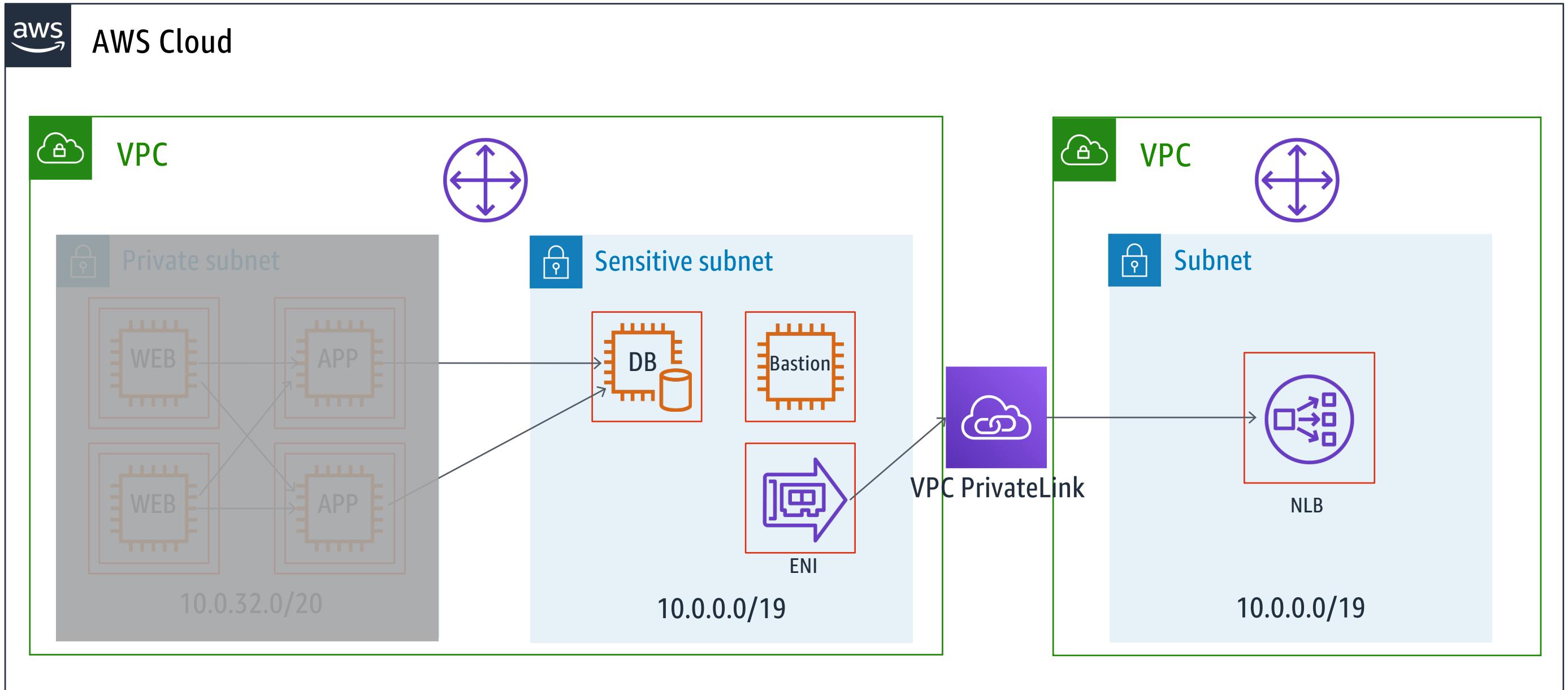
NAT Gateway



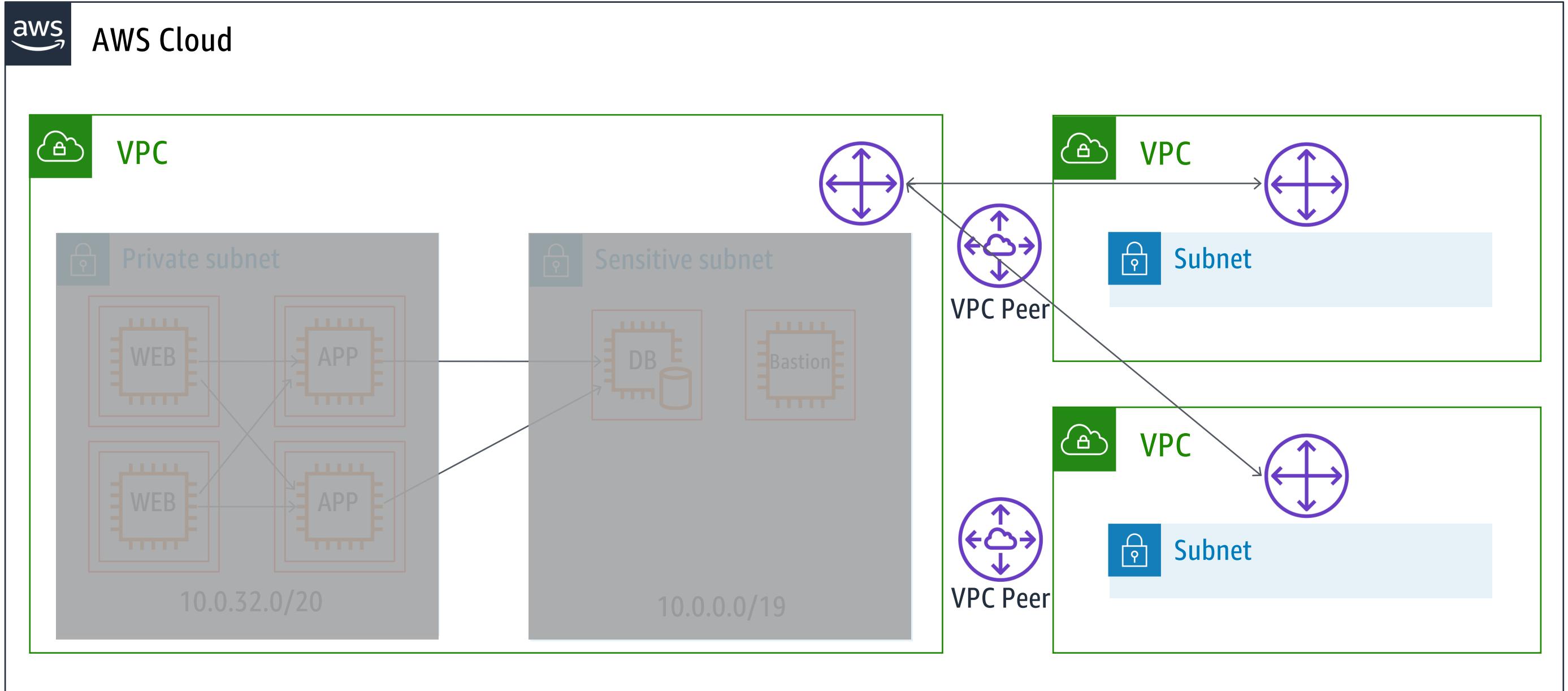
VPC Endpoints



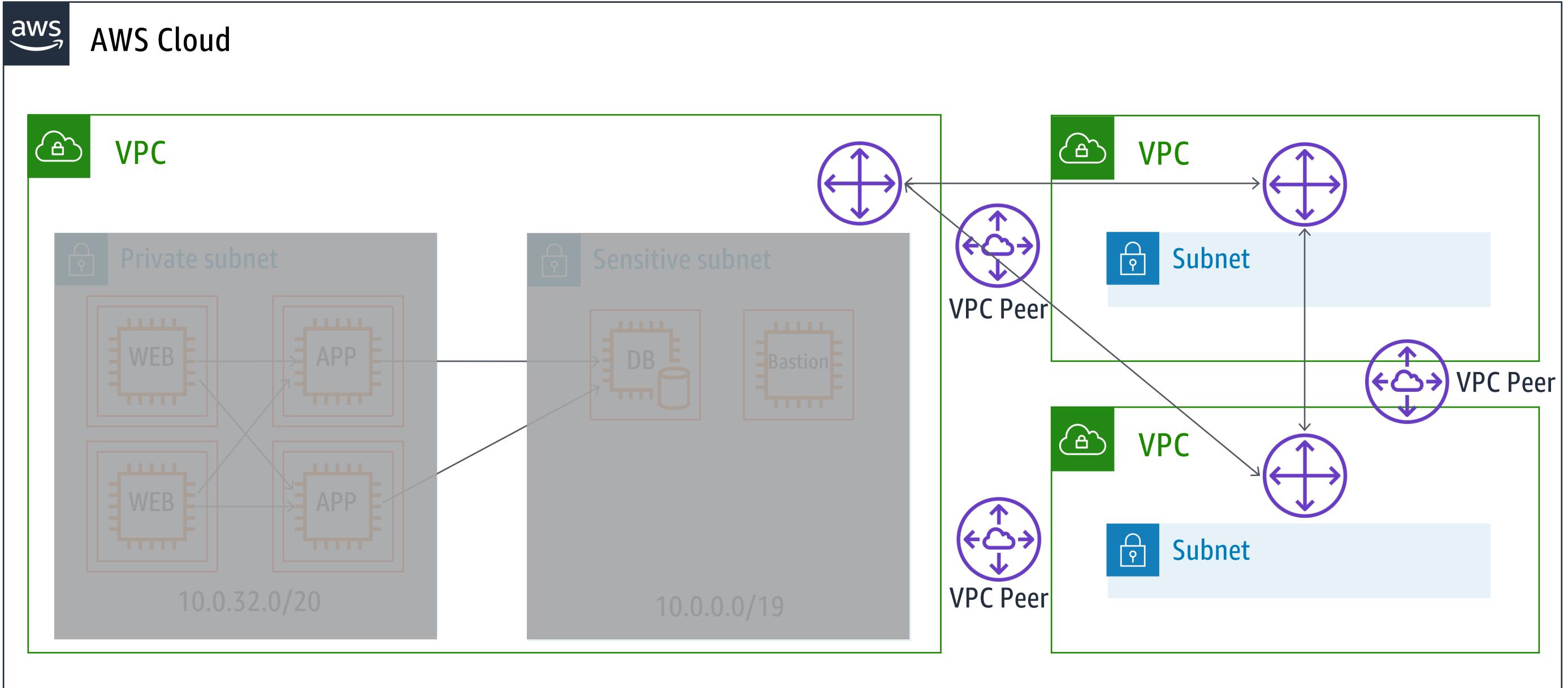
VPC PrivateLink



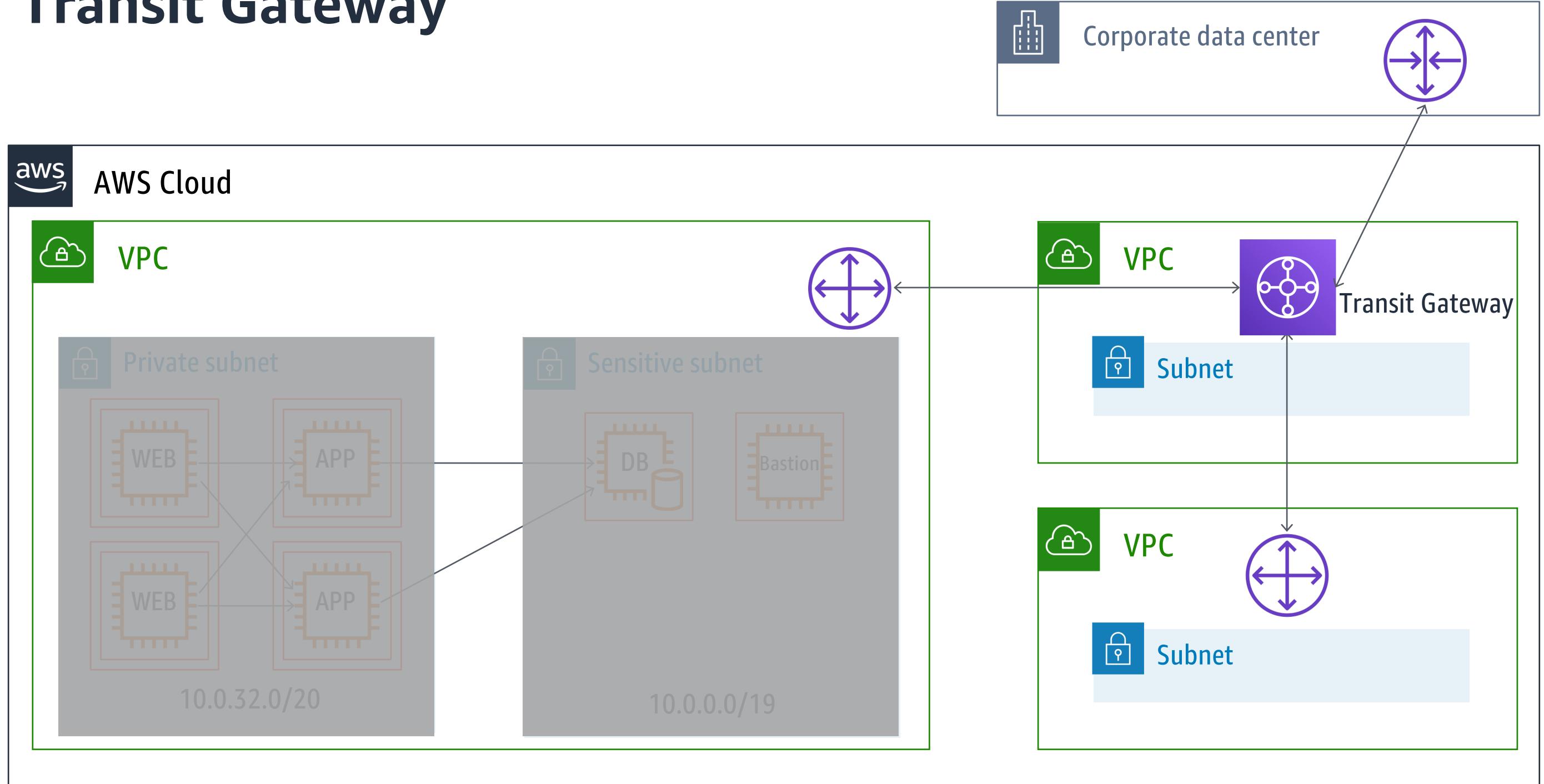
VPC Peering



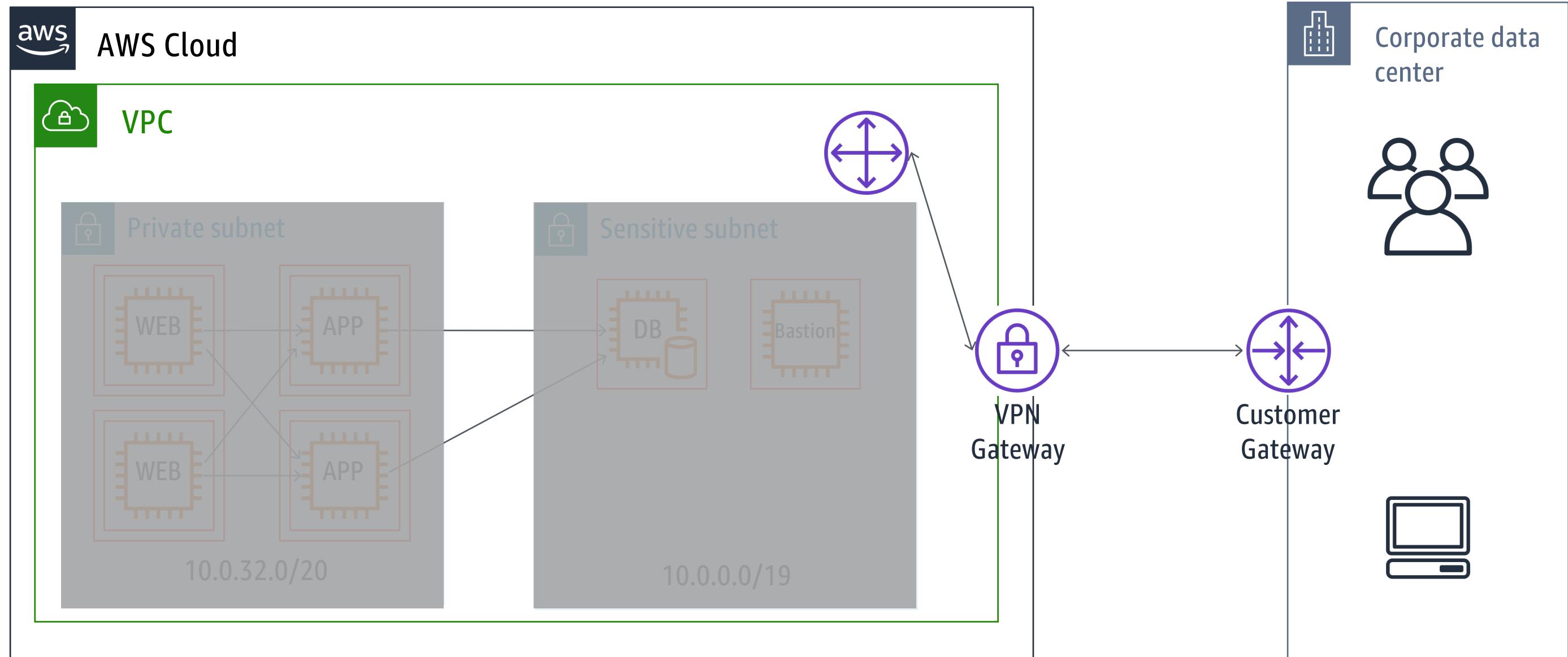
VPC Peering



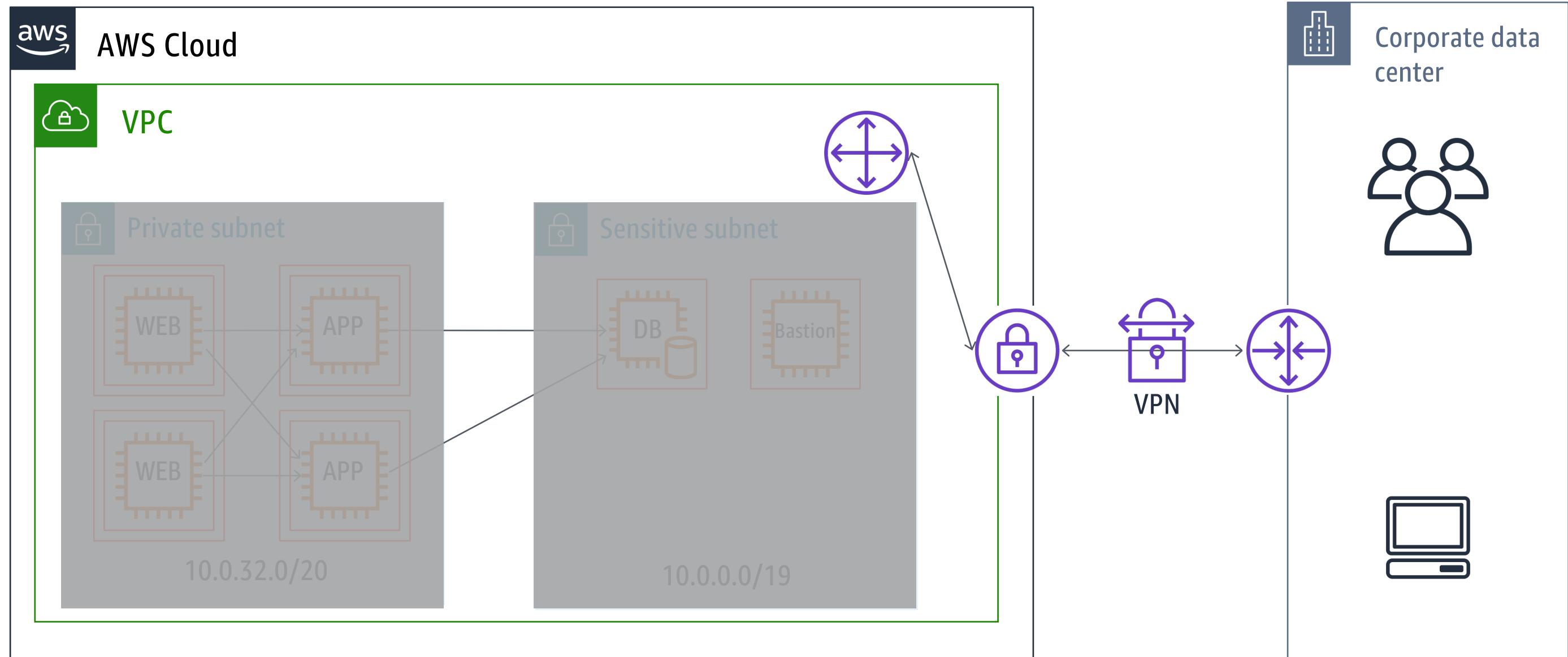
Transit Gateway



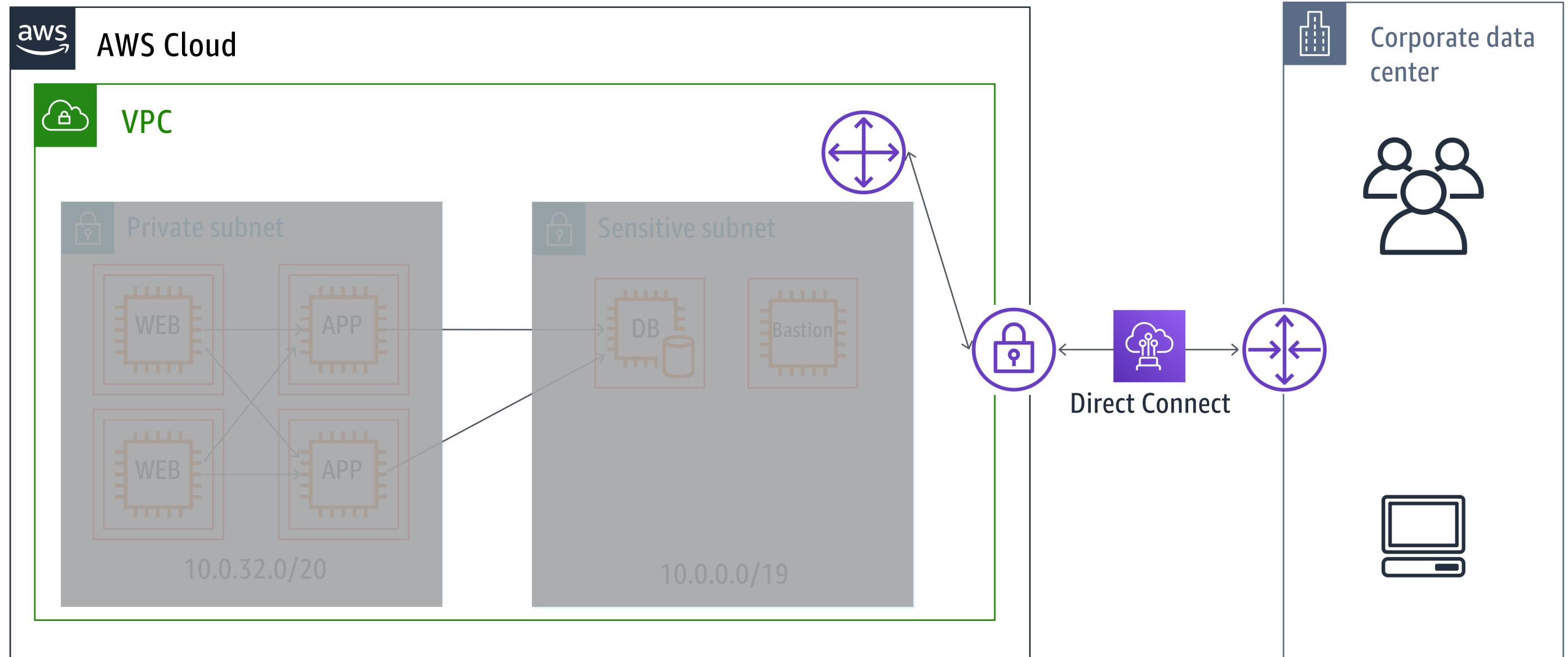
VPN



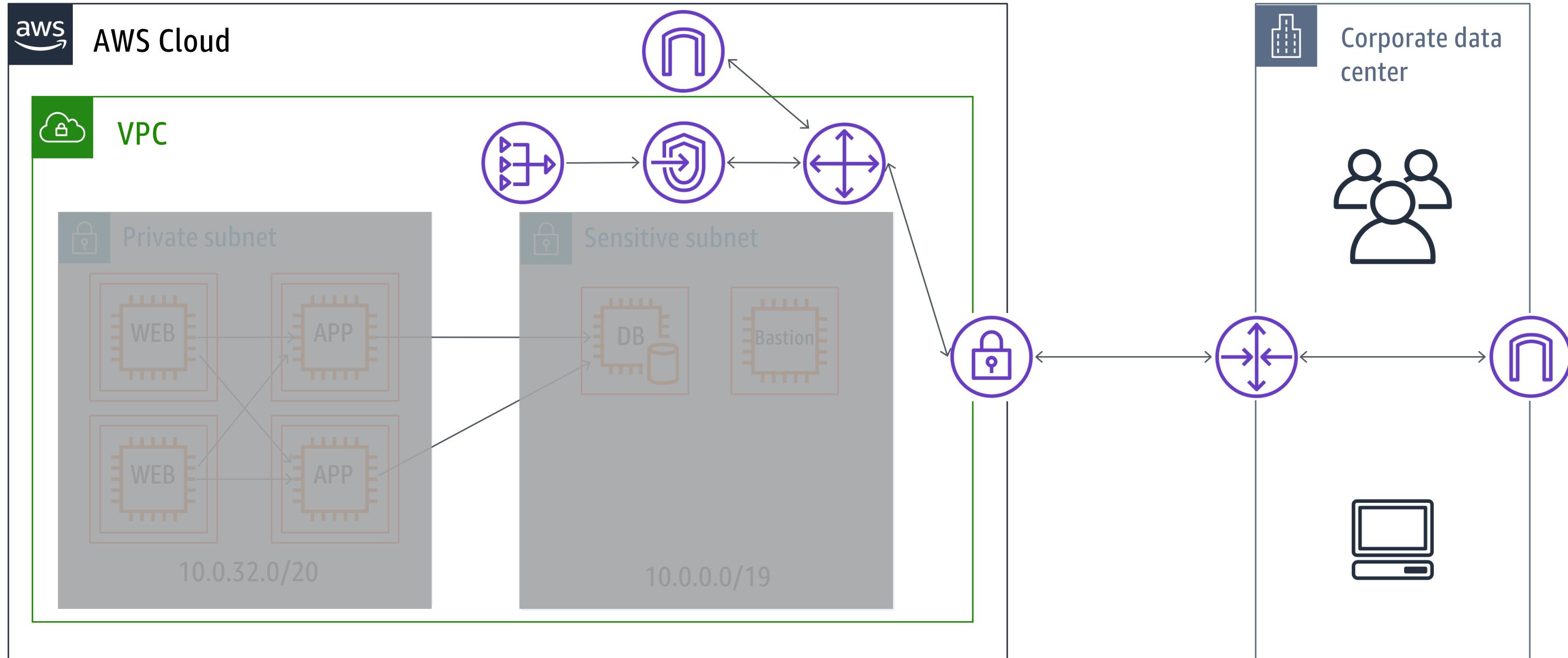
VPN



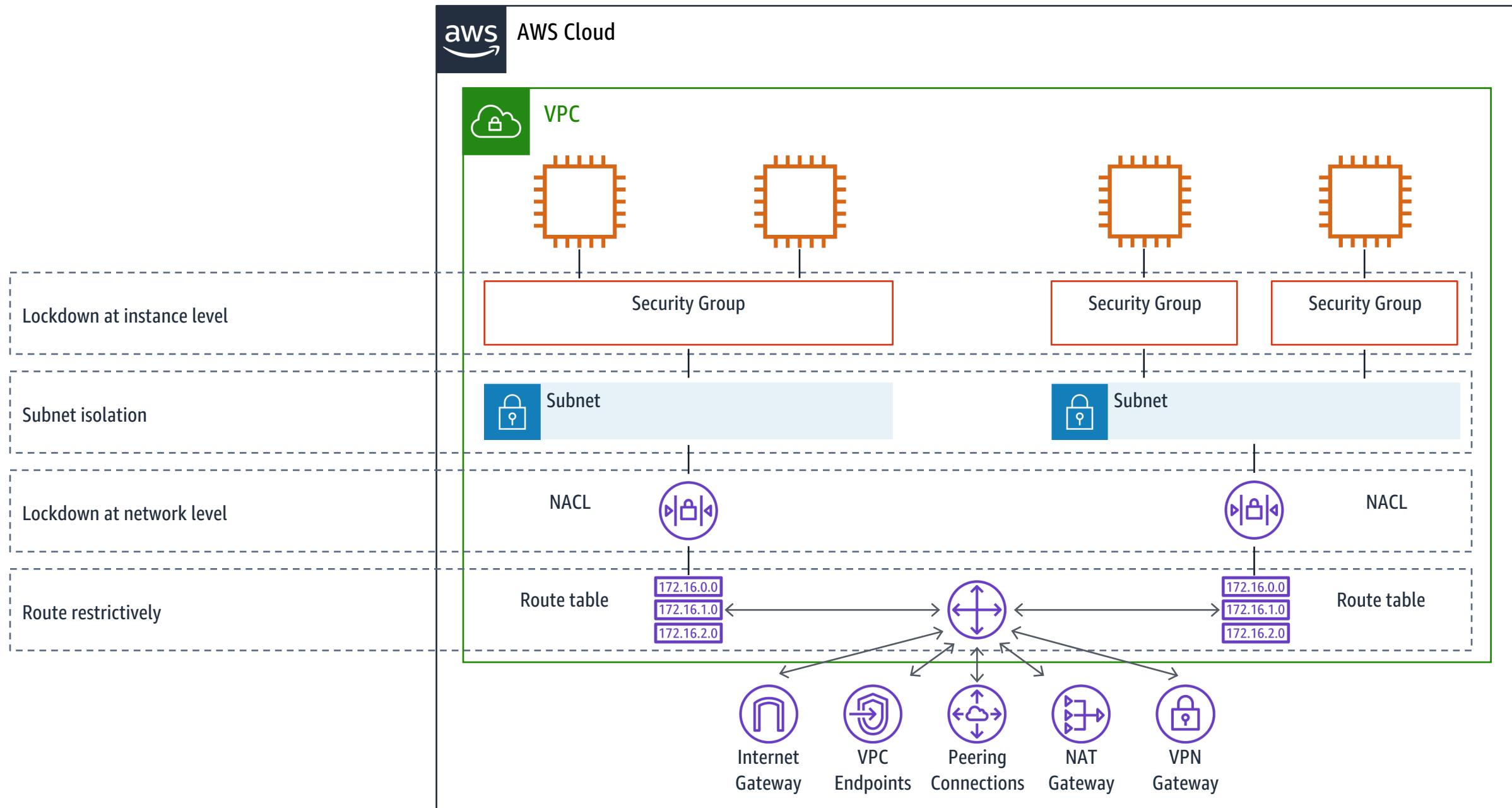
Direct Connect



Multiple Gateways



Network Defense in Depth





Questions?

