Overview of Virtual Private Cloud

AWS Security Workshop

Agenda

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

Goals

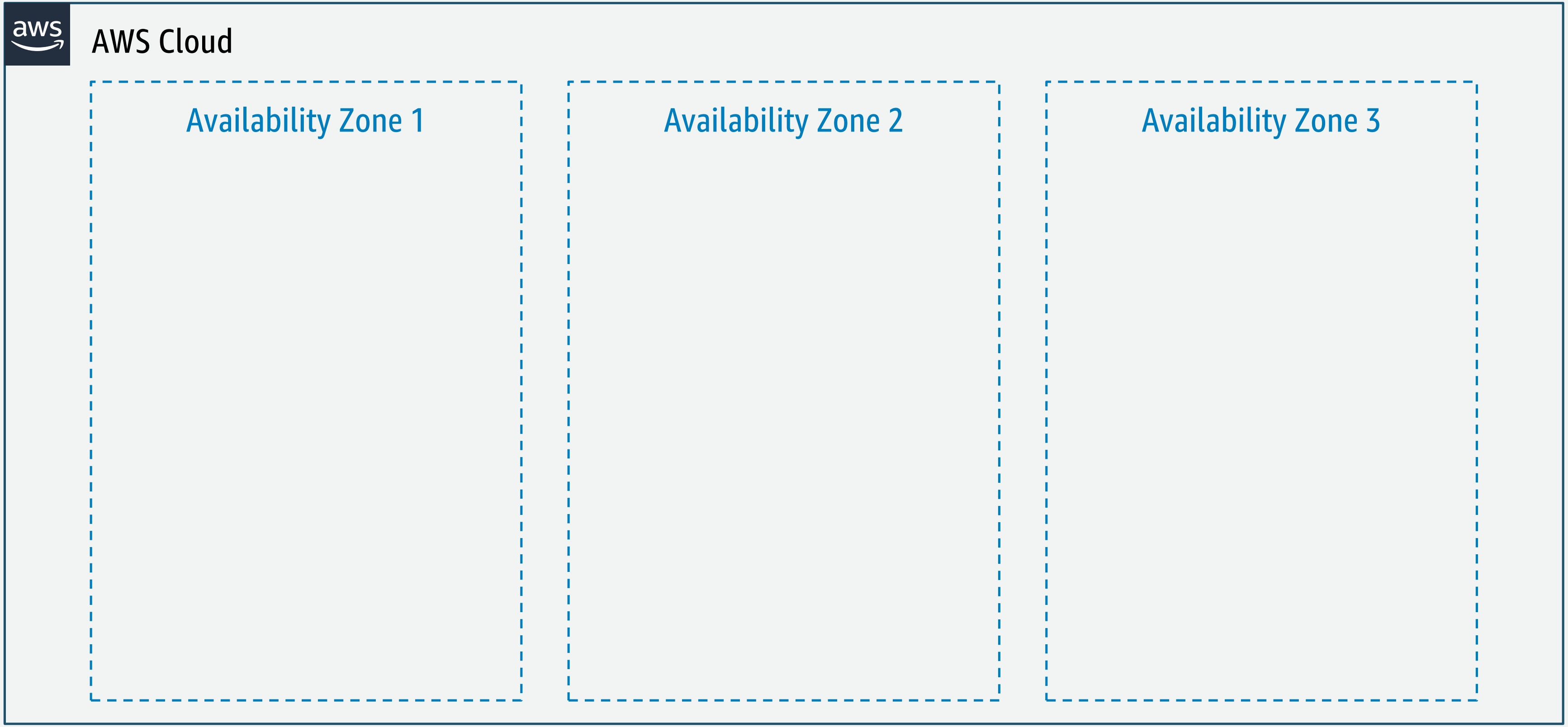
- Understand how networking is implemented in AWS
- Discover features and functionality of VPC
- Learn how to connect other networks

Virtual Private Cloud (VPC)

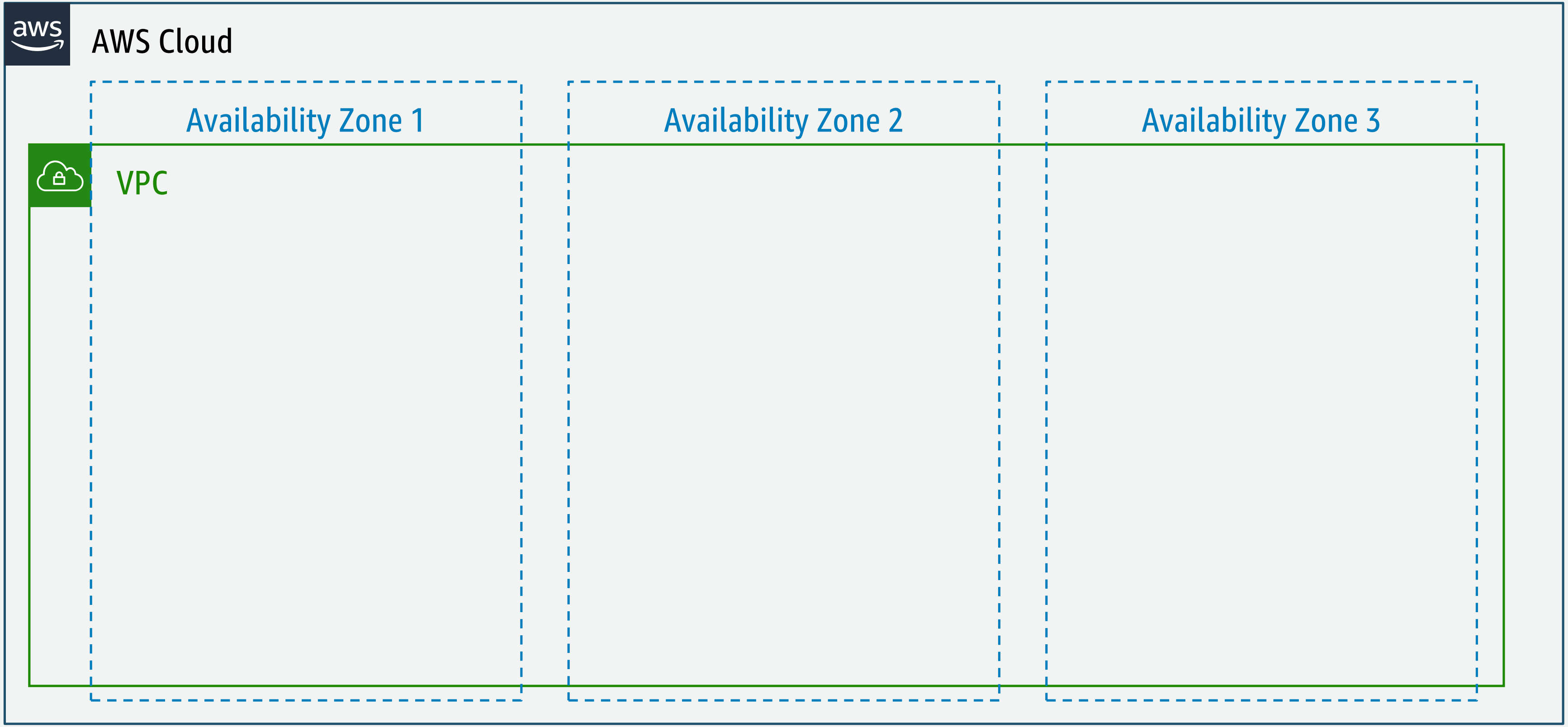
What is a Virtual Private Cloud?

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

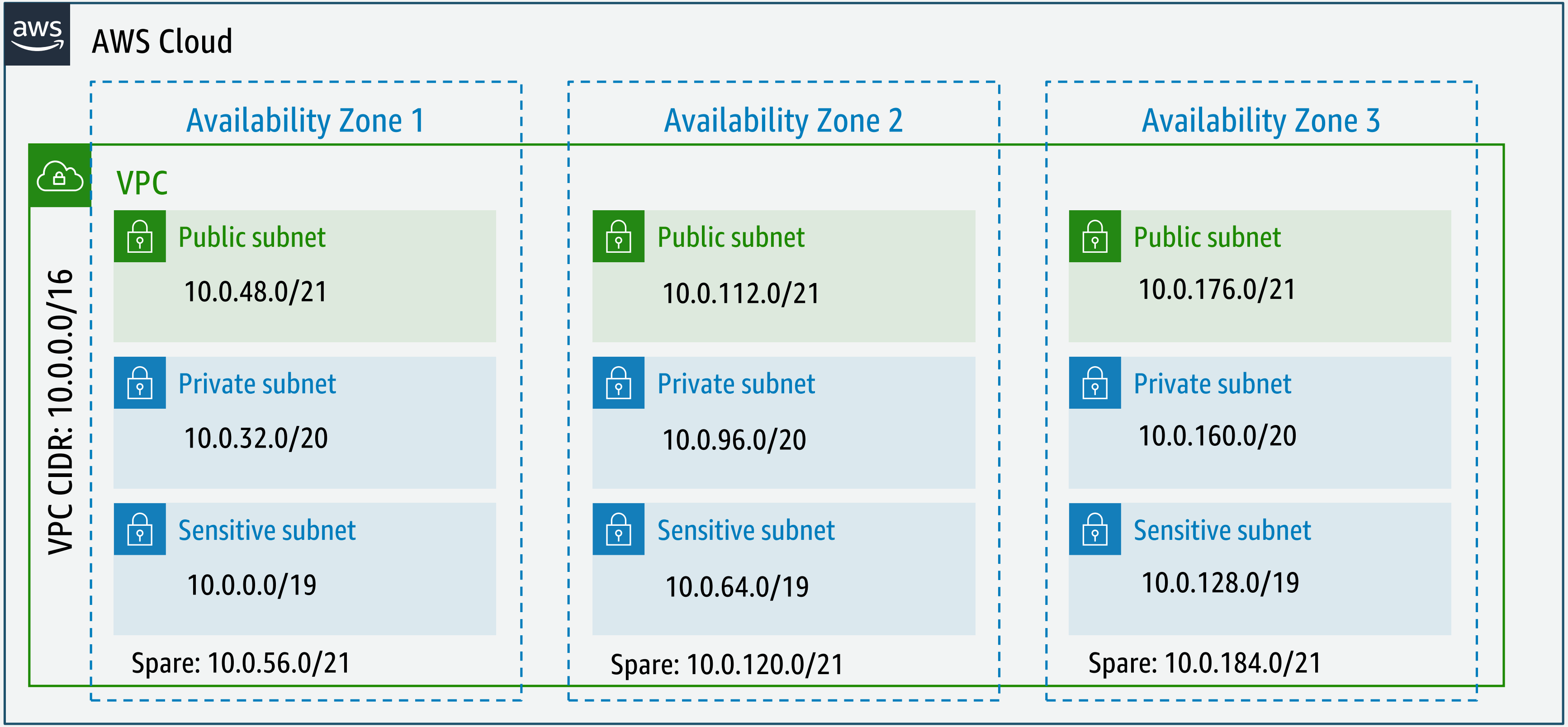
Each AWS Region has multiple Availability Zones



A VPC spans every Availability Zone in a Region



Subnets



AWS Cloud

VPC

VPC CIDR: 10.0.0.0/16

Availability Zone 1

Public subnet

10.0.48.0/21

Private subnet

10.0.32.0/20

Sensitive subnet

10.0.0.0/19

Spare: 10.0.56.0/21

Availability Zone 2

Public subnet

10.0.112.0/21

Private subnet

10.0.96.0/20

Sensitive subnet

10.0.64.0/19

Spare: 10.0.120.0/21

Availability Zone 3

Public subnet

10.0.176.0/21

Private subnet

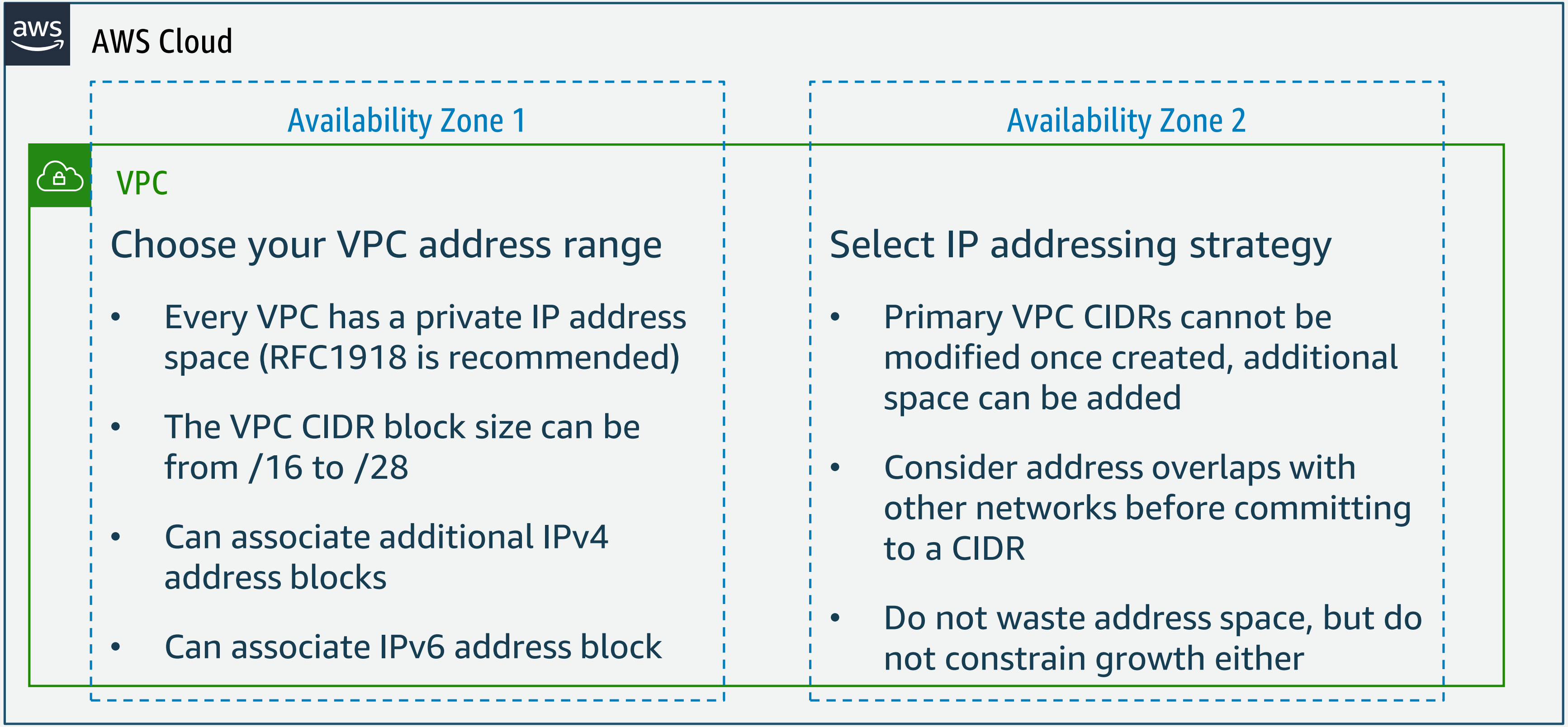
10.0.160.0/20

Sensitive subnet

10.0.128.0/19

Spare: 10.0.184.0/21

Customers have full control over their VPC’s



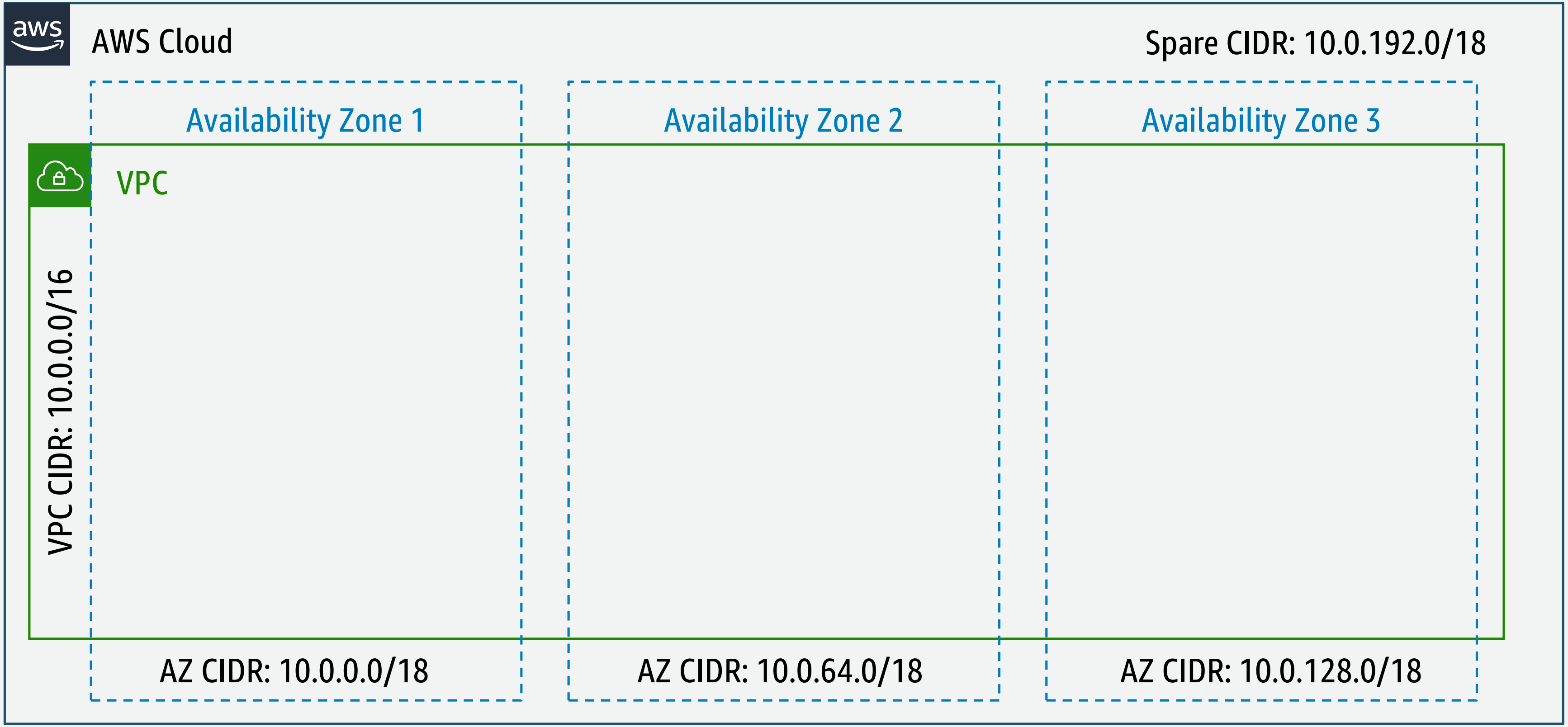
Choose your VPC address range

- Every VPC has a private IP address space (RFC1918 is recommended)
- The VPC CIDR block size can be from /16 to /28
- Can associate additional IPv4 address blocks
- Can associate IPv6 address block

Select IP addressing strategy

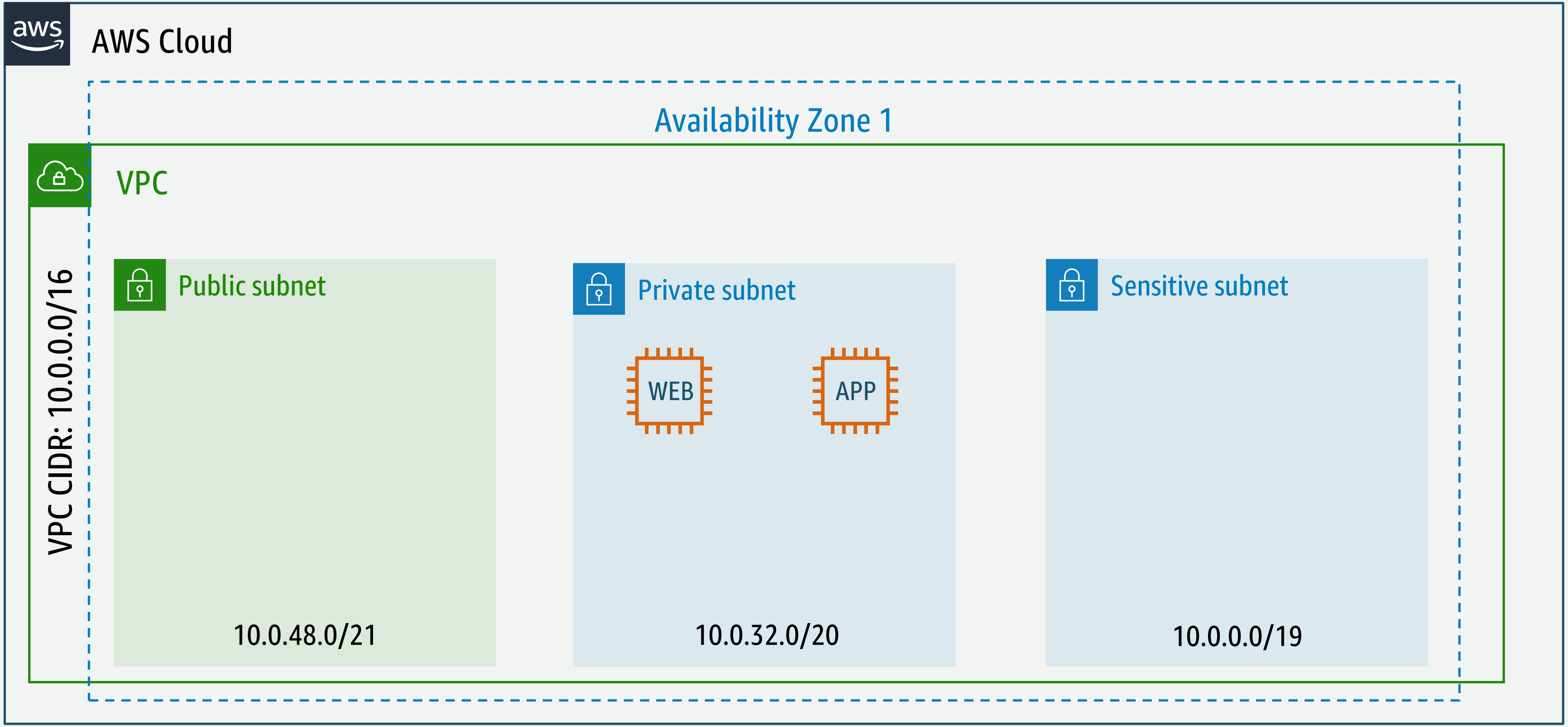
- Primary VPC CIDRs cannot be modified once created, additional space can be added
- Consider address overlaps with other networks before committing to a CIDR
- Do not waste address space, but do not constrain growth either

Logically allocate CIDR space for each AZ

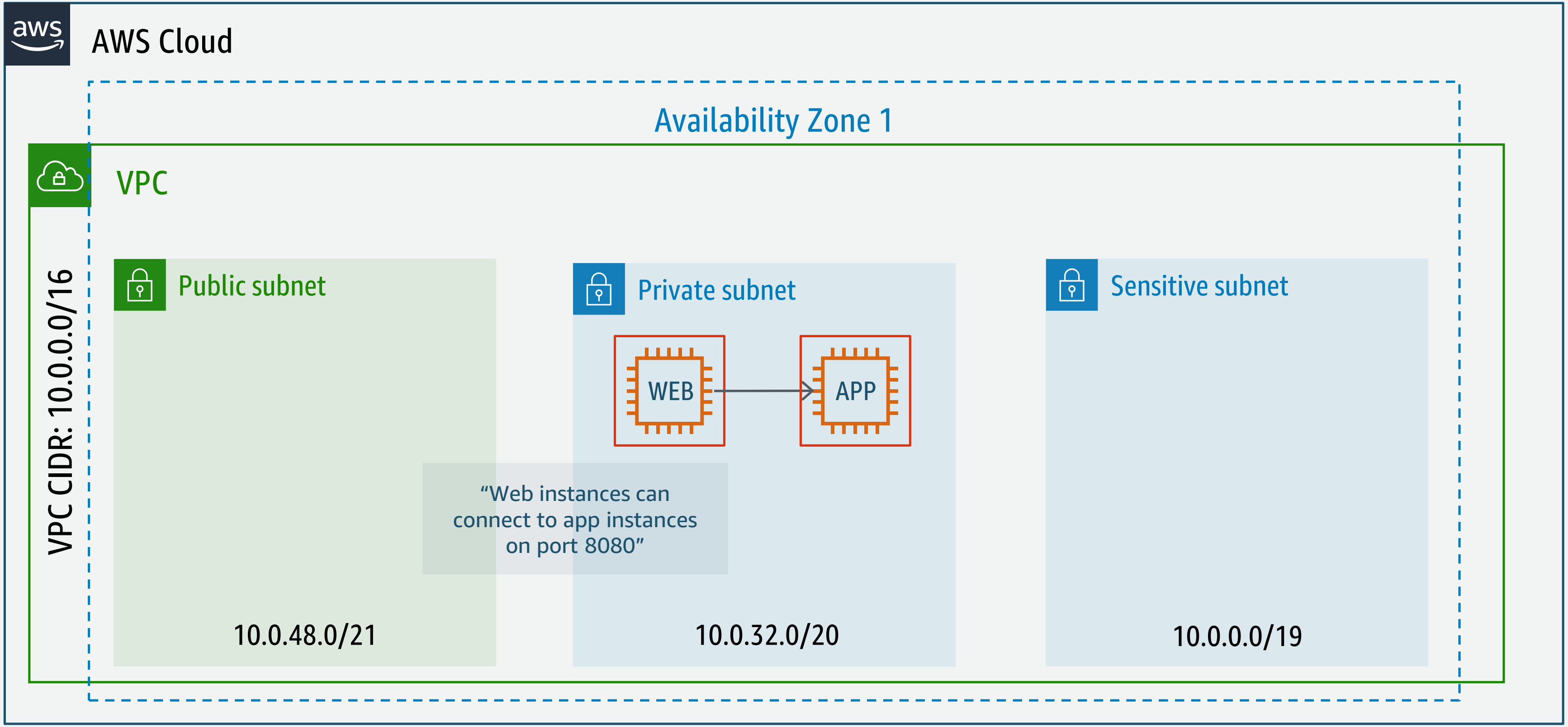


Security Groups

Security Groups – Stateful Firewall



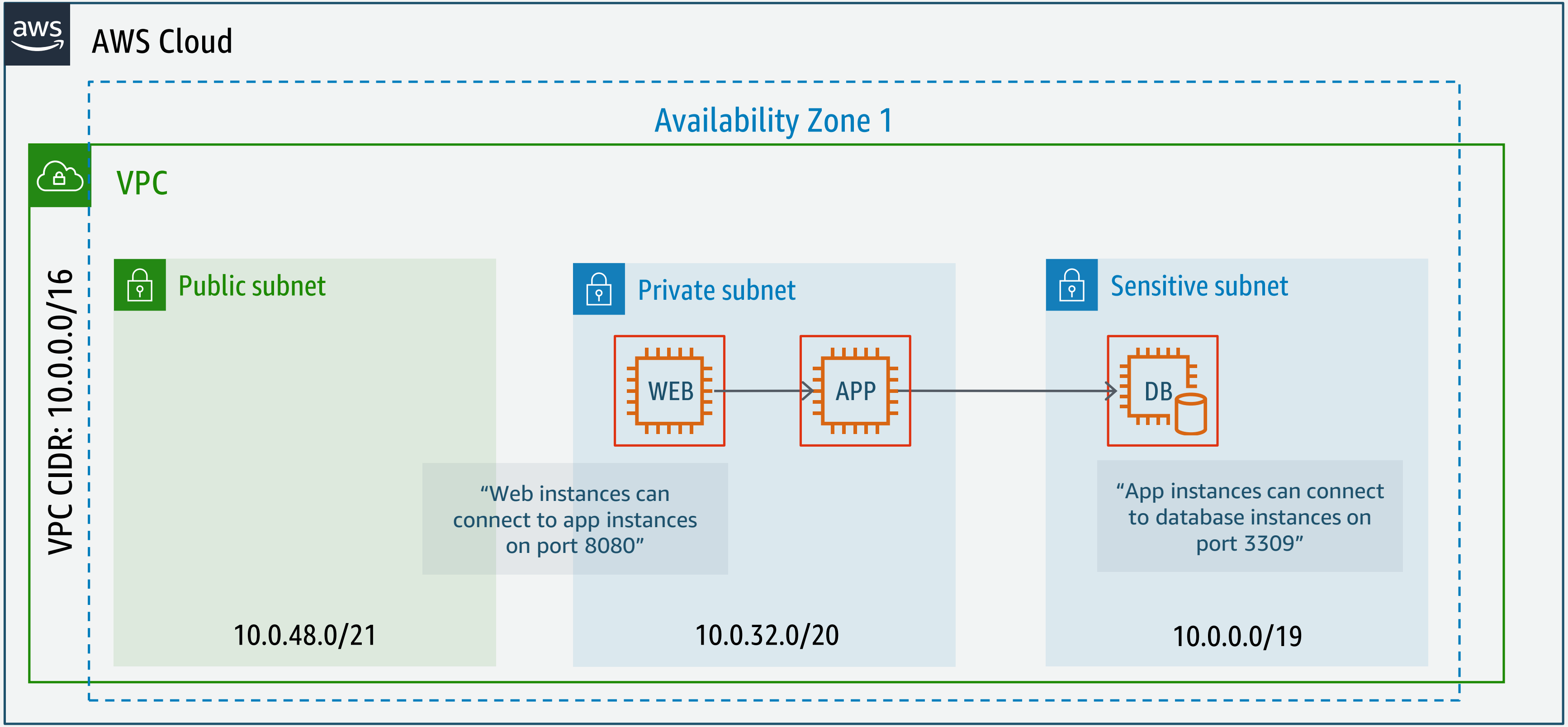
Security Groups – Stateful Firewall



“Web instances can connect to app instances on port 8080”

Amazon Confidential

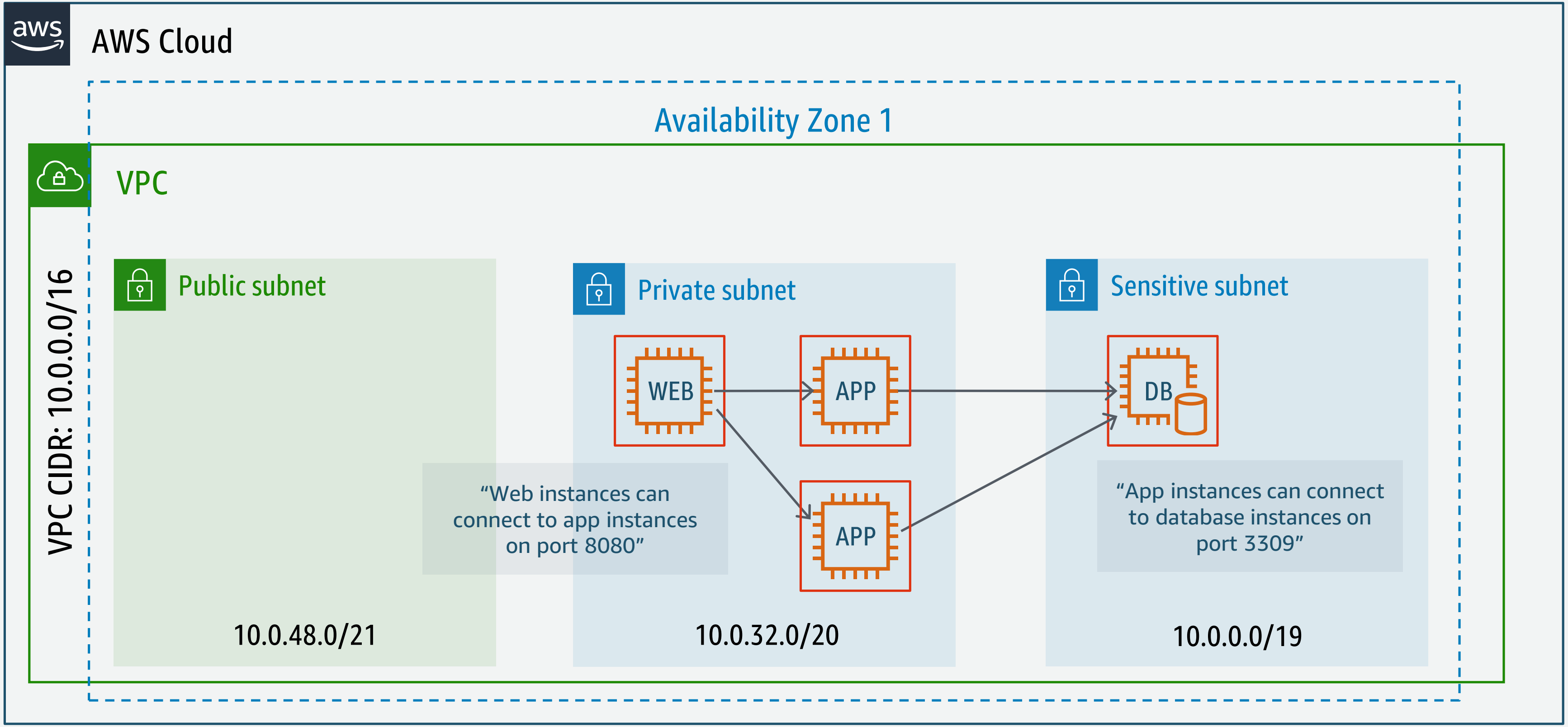
Security Groups – Stateful Firewall



"Web instances can connect to app instances on port 8080"

"App instances can connect to database instances on port 3309"

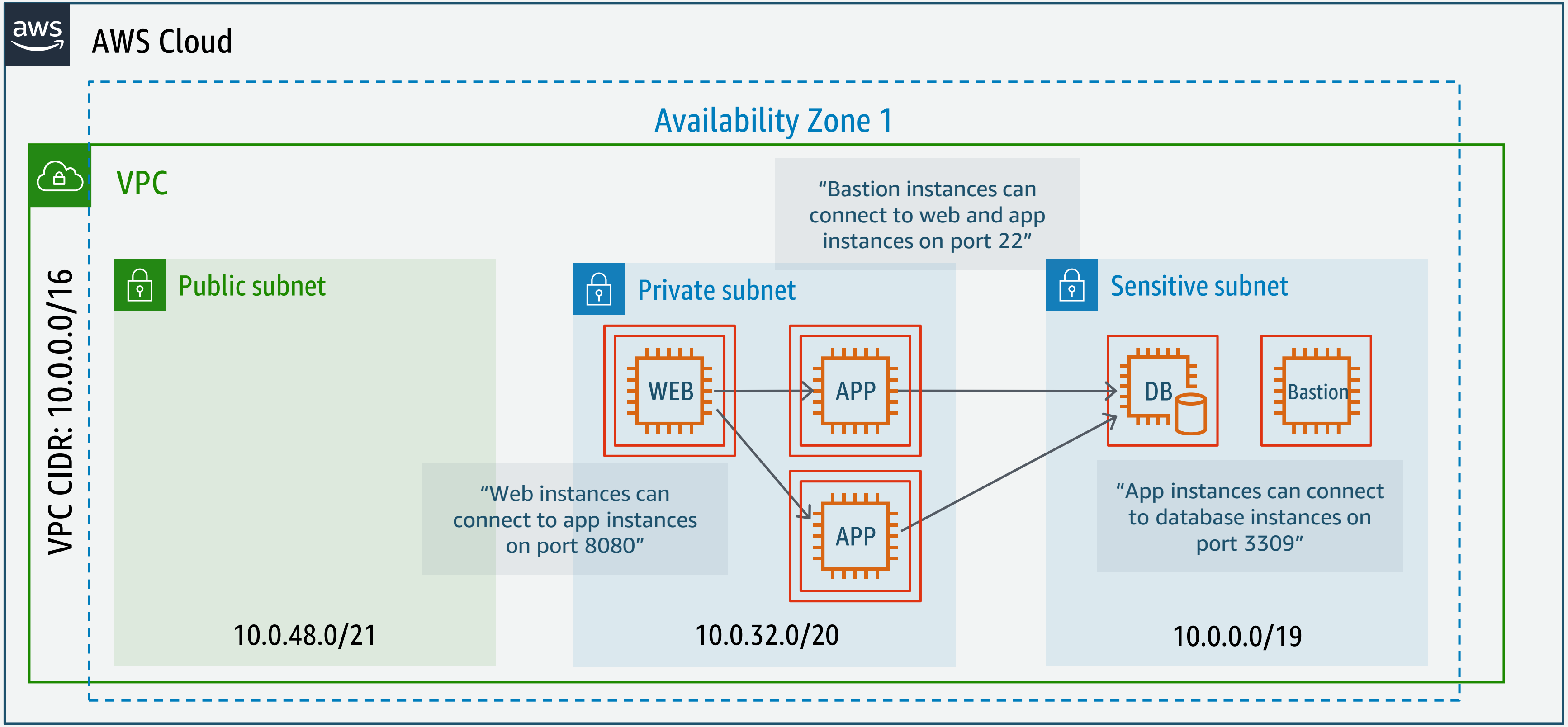
Security Groups – Stateful Firewall



"Web instances can connect to app instances on port 8080"

"App instances can connect to database instances on port 3309"

Security Groups – Stateful Firewall



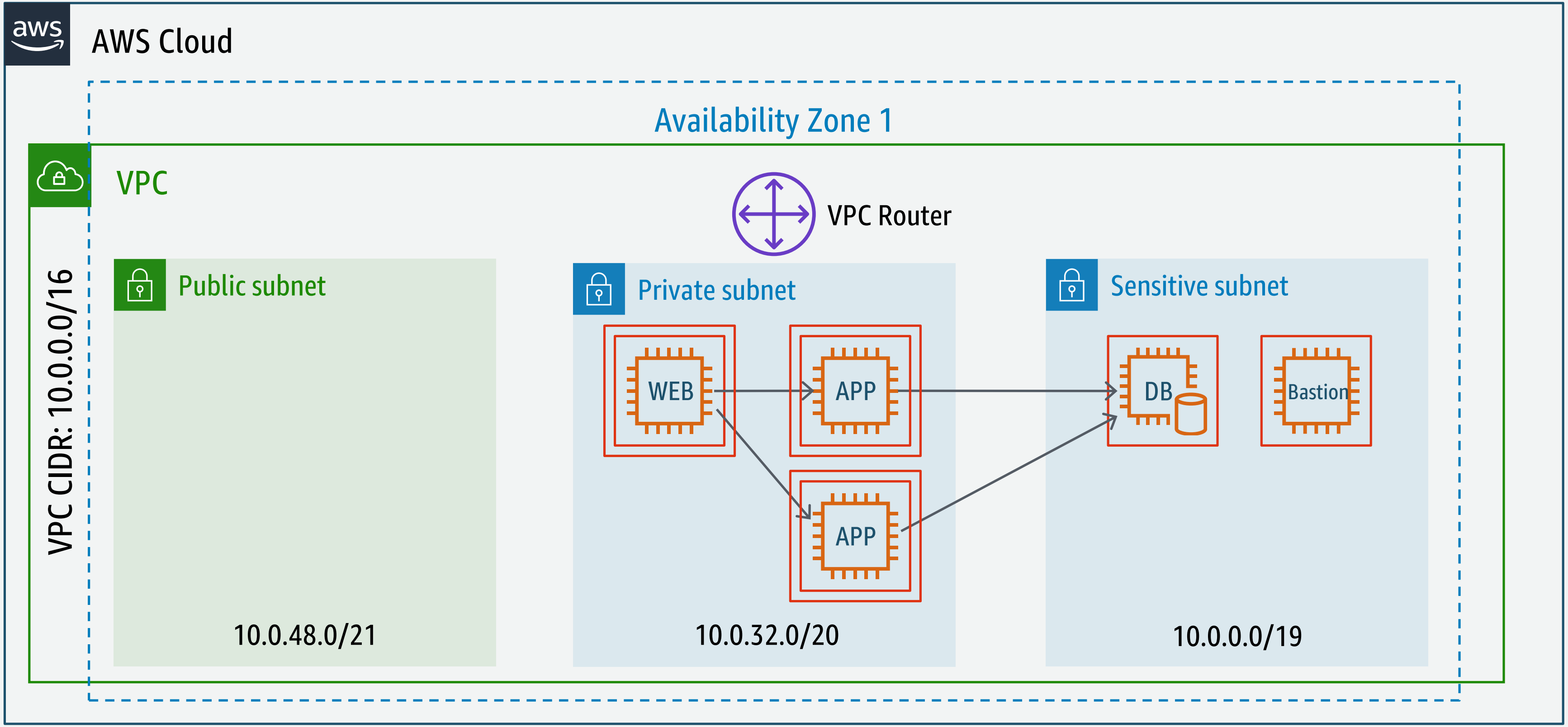
"Bastion instances can connect to web and app instances on port 22"

"Web instances can connect to app instances on port 8080"

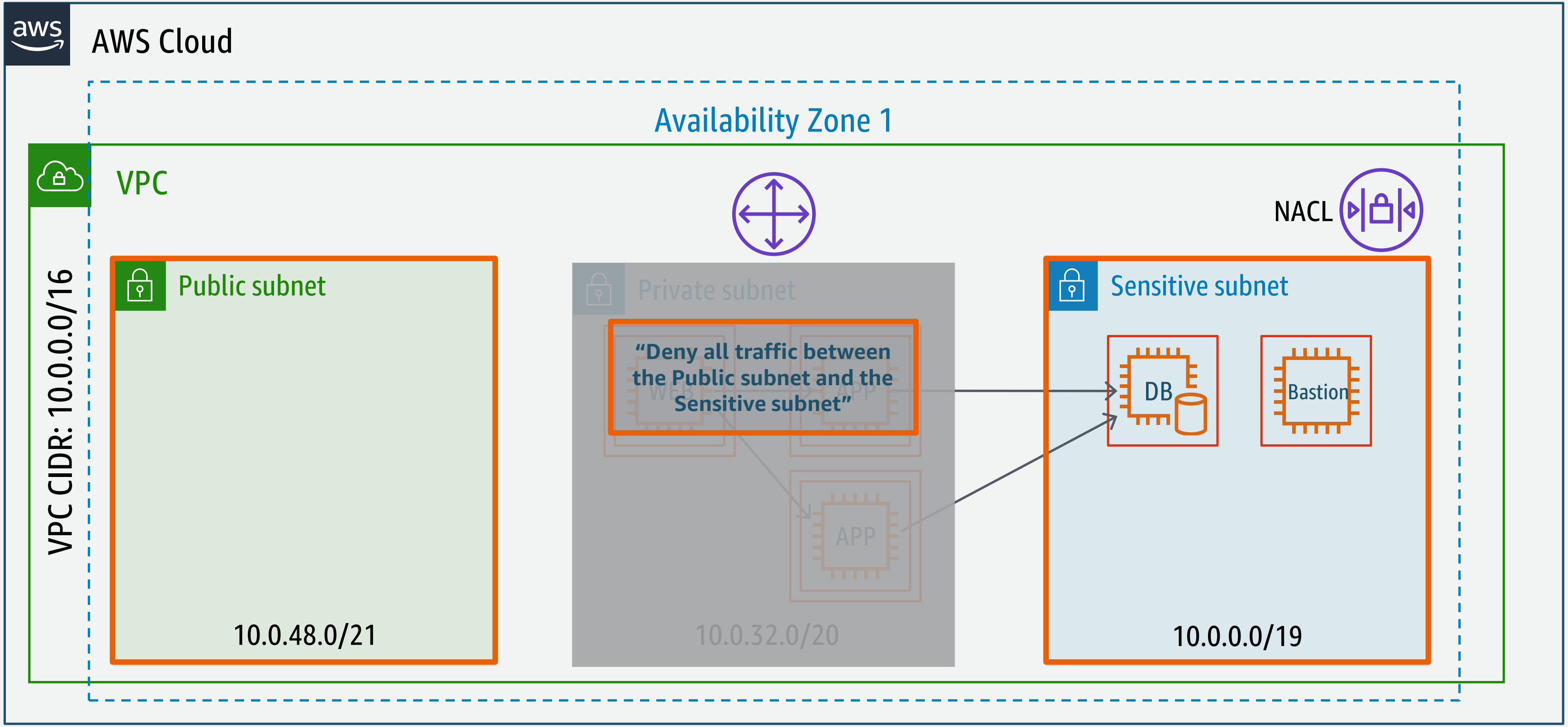
"App instances can connect to database instances on port 3309"

Routing, NACLs, and Load Balancing

Routing

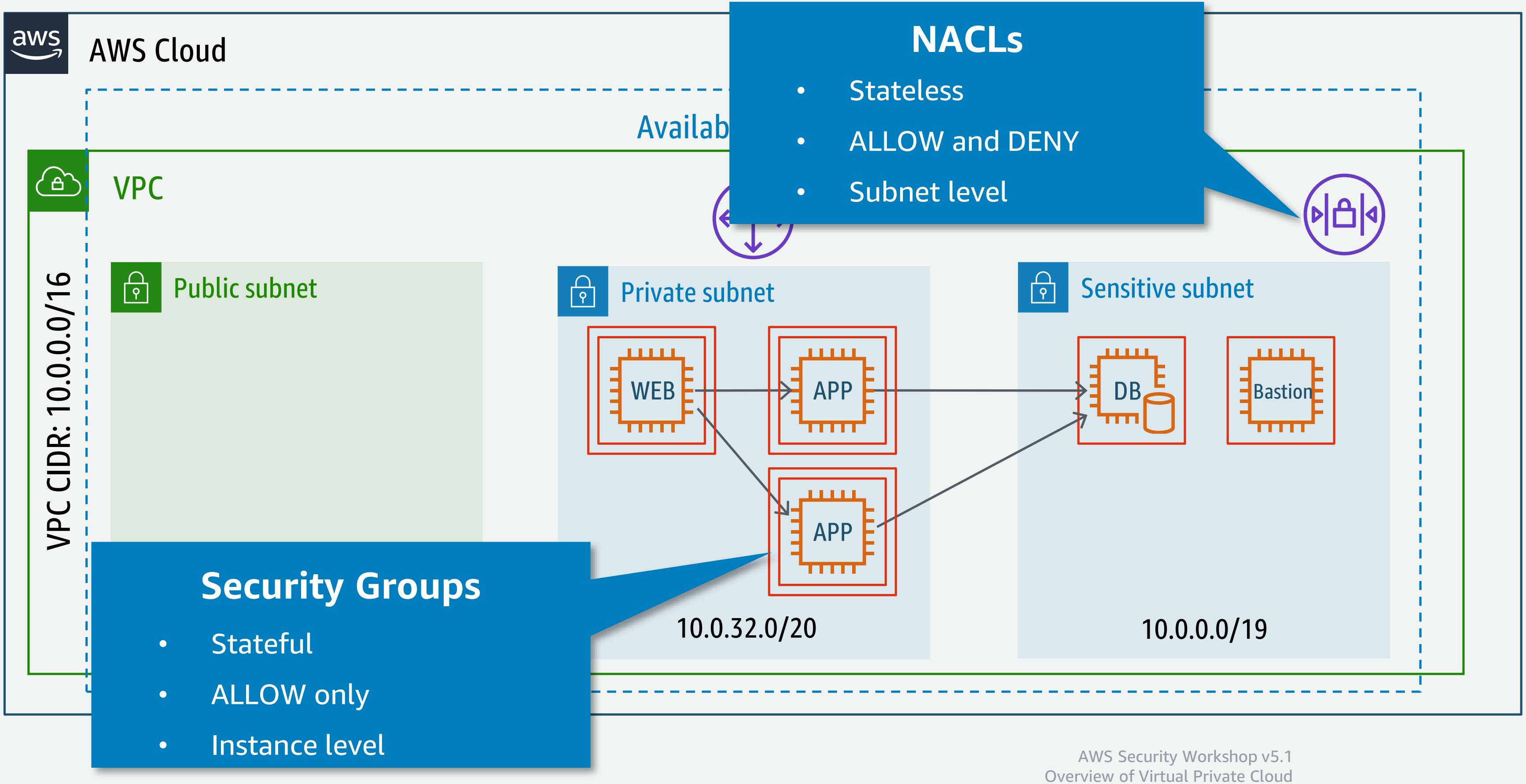

AWS Cloud
Availability Zone 1
VPC
VPC CIDR: 10.0.0.0/16
VPC Router
Public subnet
10.0.48.0/21
Private subnet
WEB
APP
APP
10.0.32.0/20
Sensitive subnet
DB
Bastion
10.0.0.0/19

Network Access Control List (NACL)



"Deny all traffic between the Public subnet and the Sensitive subnet"

NACLs and Security Groups



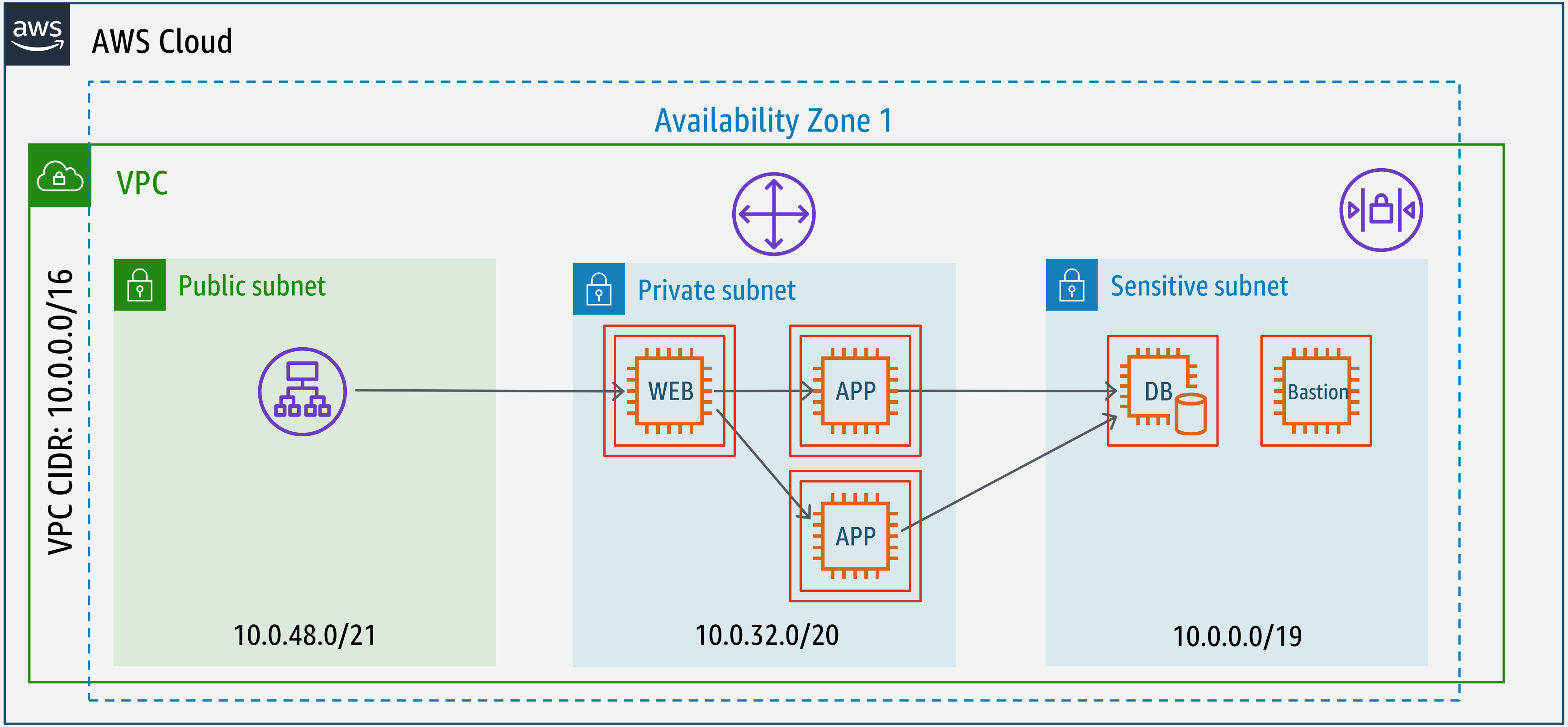
NACLs

- Stateless
- ALLOW and DENY
- Subnet level

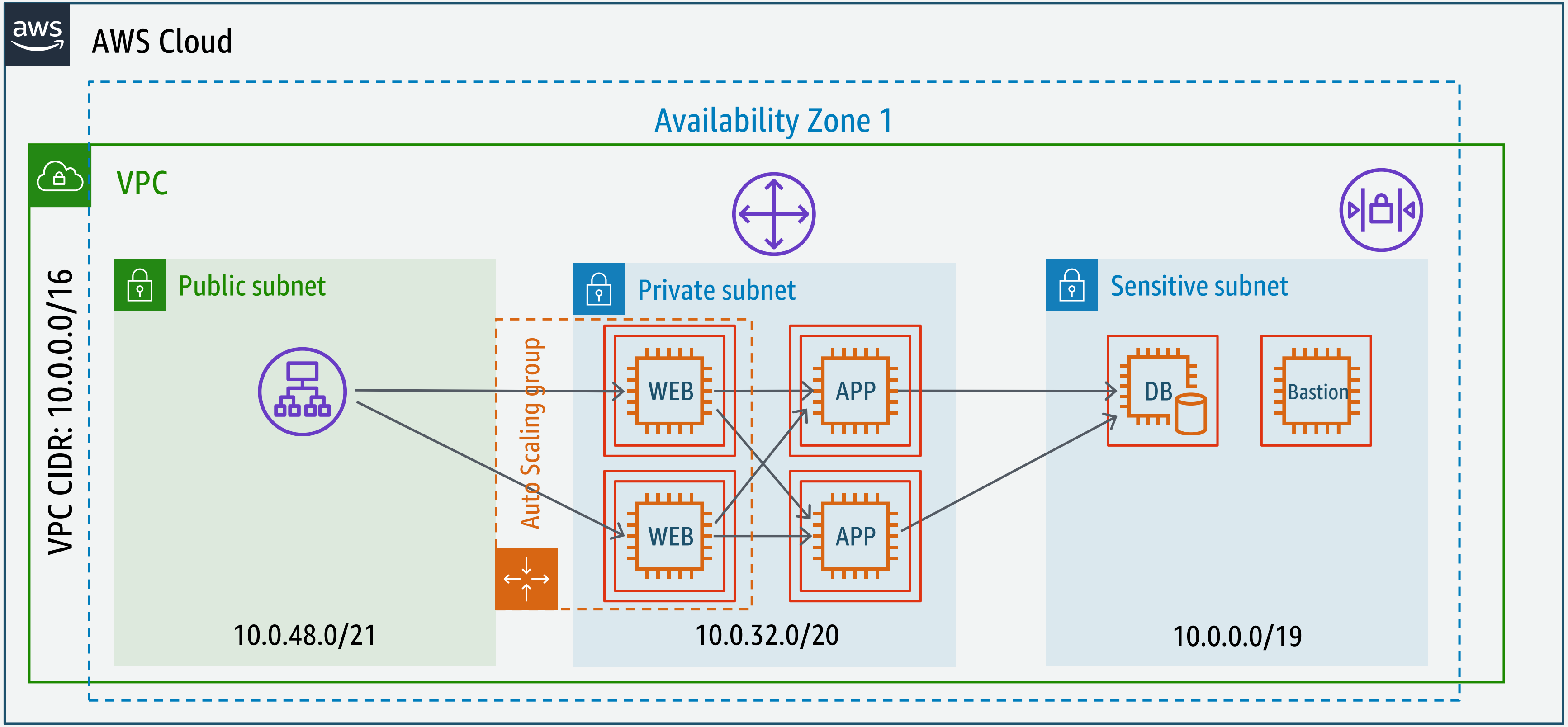
Security Groups

- Stateful
- ALLOW only
- Instance level

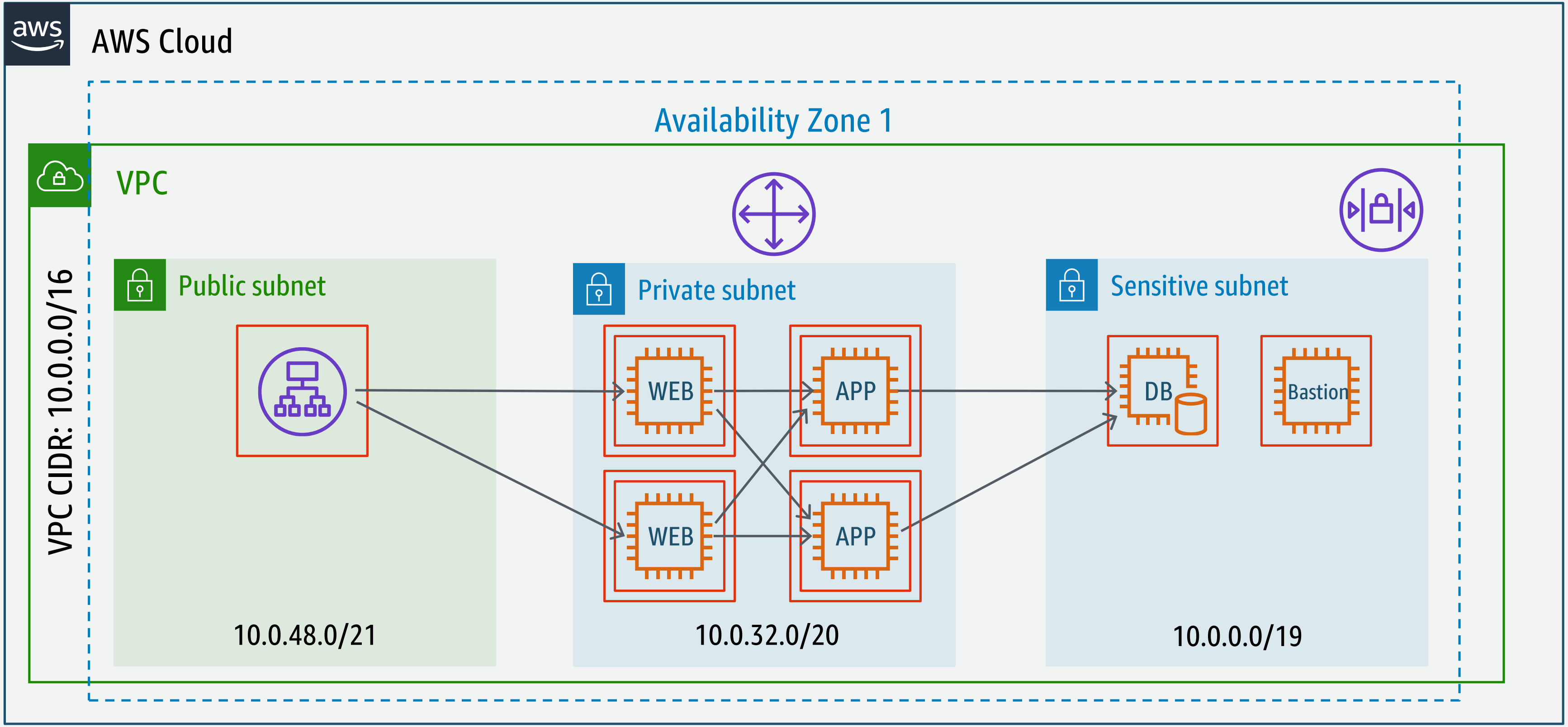
Load Balancing



Load Balancing



Load Balancing

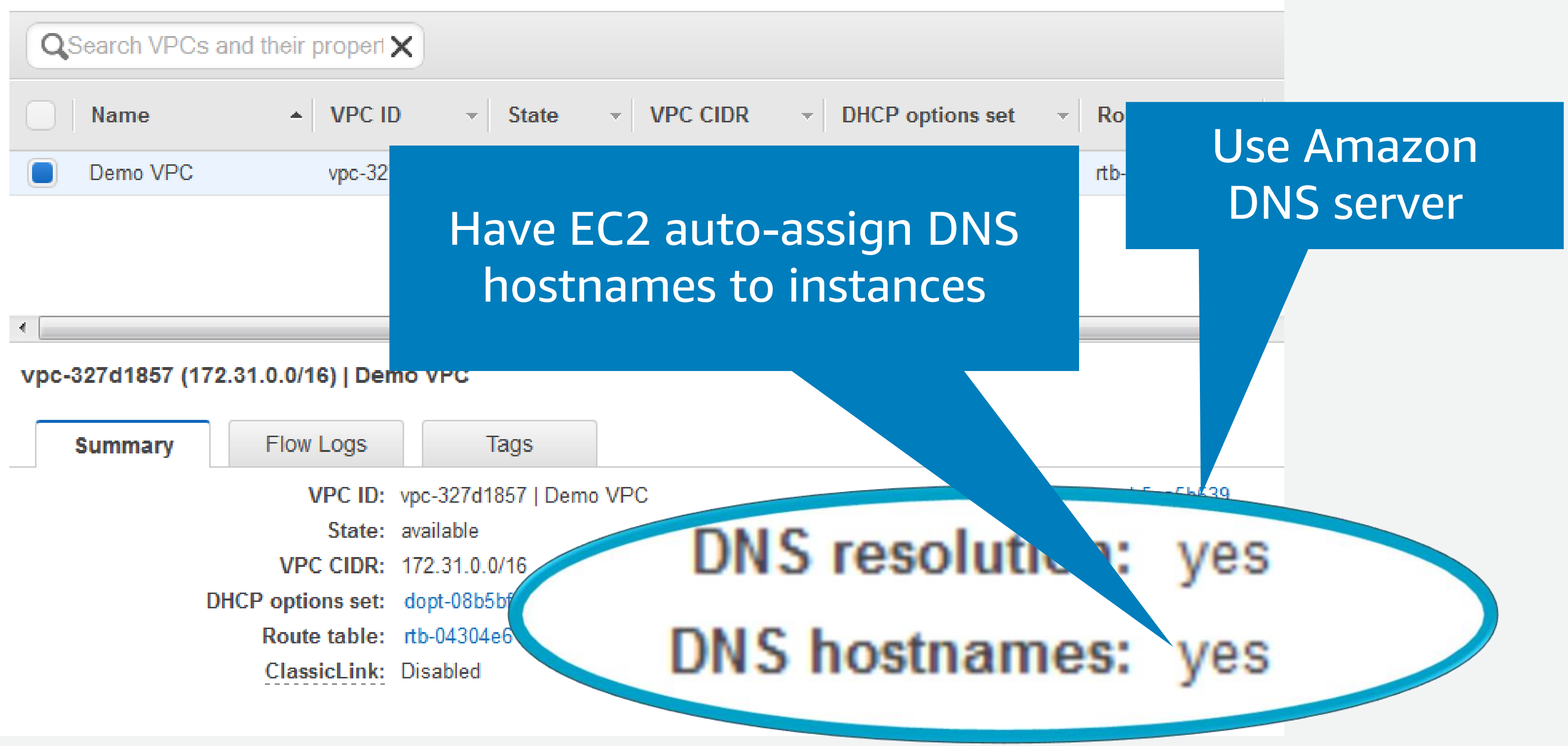


Load Balancing – ELB Types

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

DNS

VPC DNS Options



Name	VPC ID	State	VPC CIDR	DHCP options set	Ro
Demo VPC	vpc-32				rtb-

vpc-327d1857 (172.31.0.0/16) | Demo VPC

VPC ID: vpc-327d1857 | Demo VPC
State: available
VPC CIDR: 172.31.0.0/16
DHCP options set: dopt-08b5bf
Route table: rtb-04304e6
ClassicLink: Disabled

DNS resolution: yes
DNS hostnames: yes

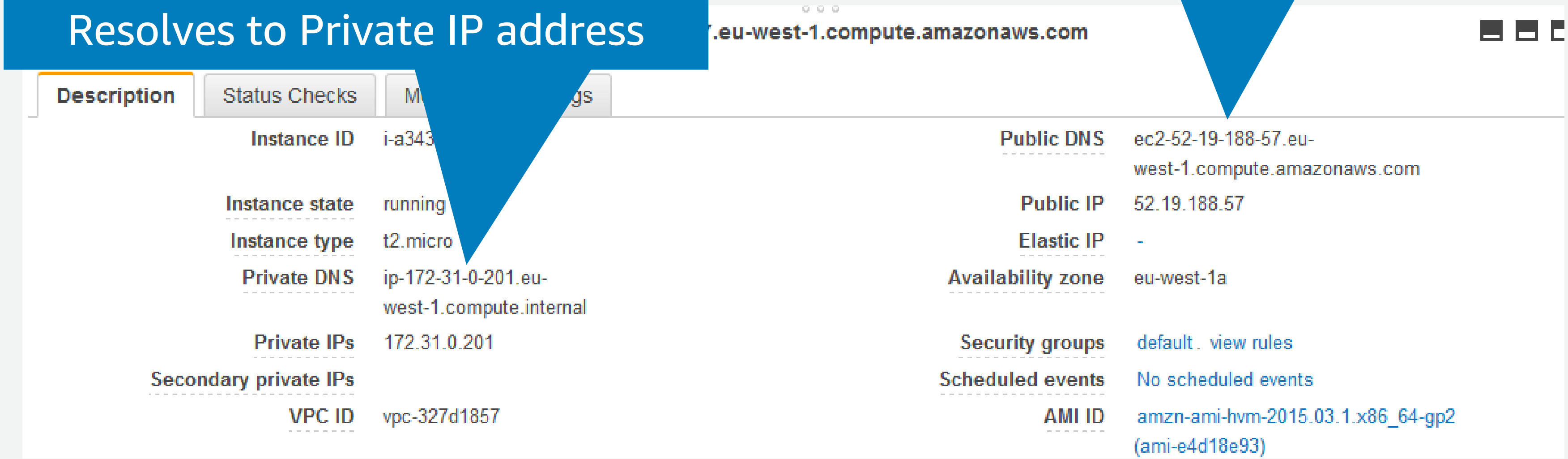
Have EC2 auto-assign DNS hostnames to instances

Use Amazon DNS server

EC2 DNS Hostnames

External DNS name:
Resolves to…

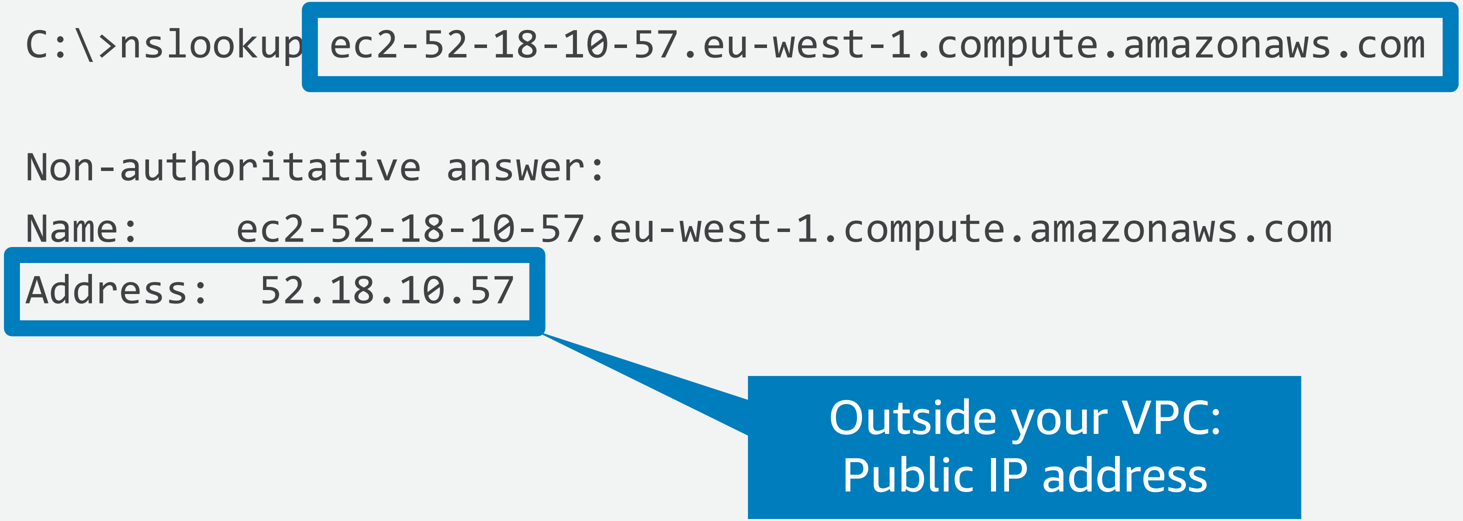
Internal DNS hostname:
Resolves to Private IP address



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

Instance ID	i-a343	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

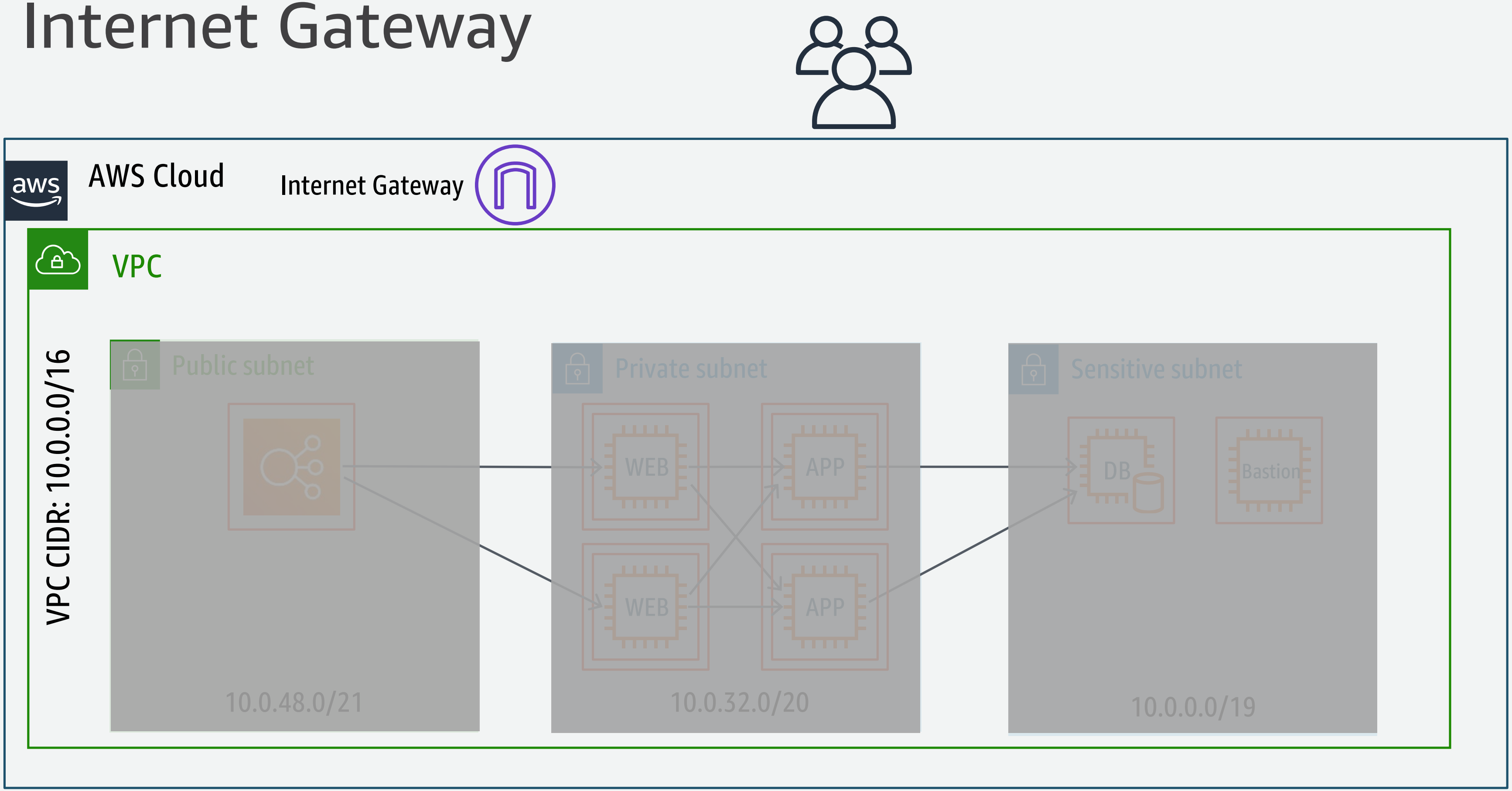
EC2 DNS Hostnames from inside the VPC

```
[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 <<>> ec2-52-18-10-57.eu-west-1.compute.amazonaws.com
;; 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
```

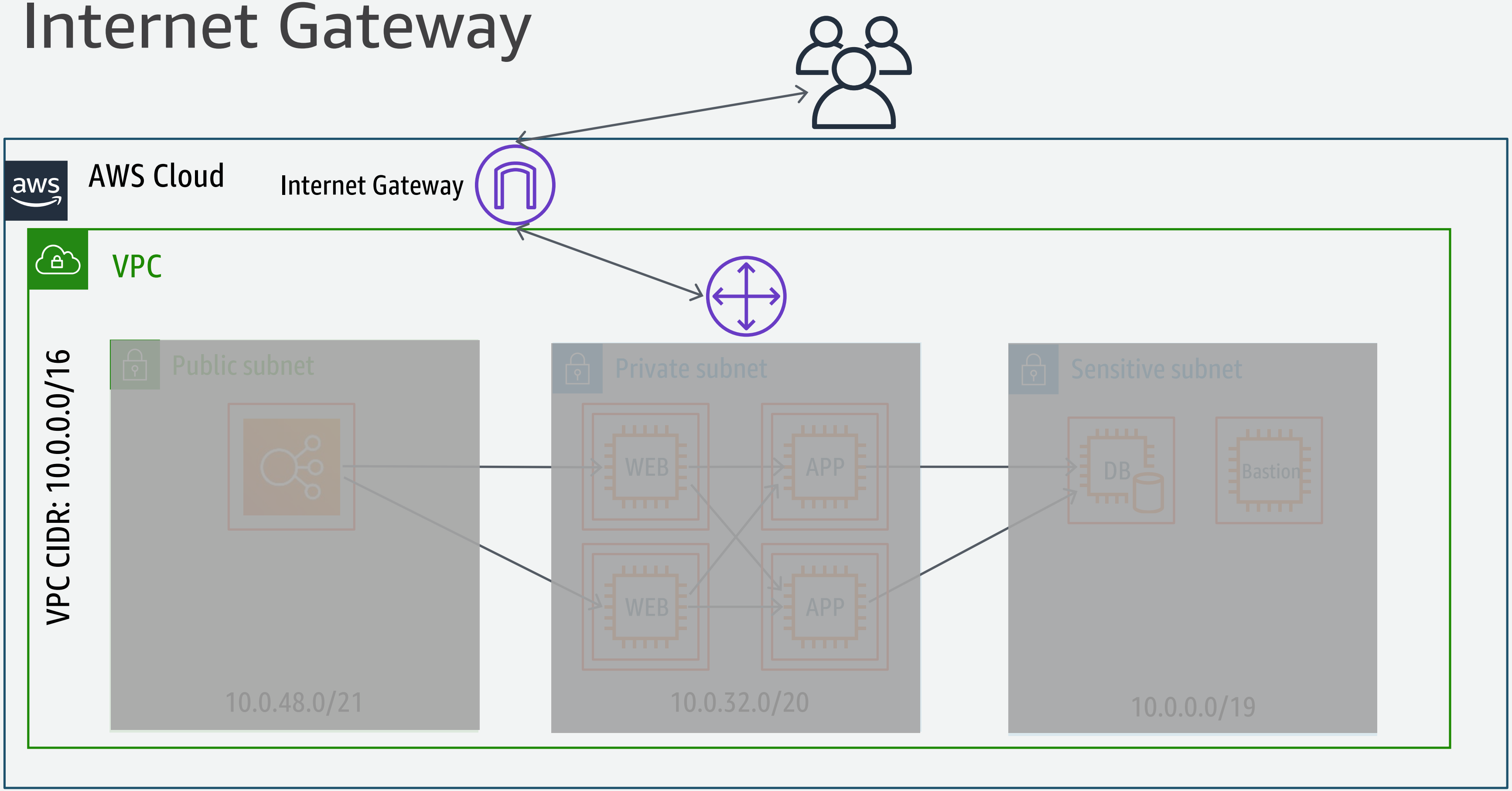
Inside your VPC:
Private IP address

Connectivity

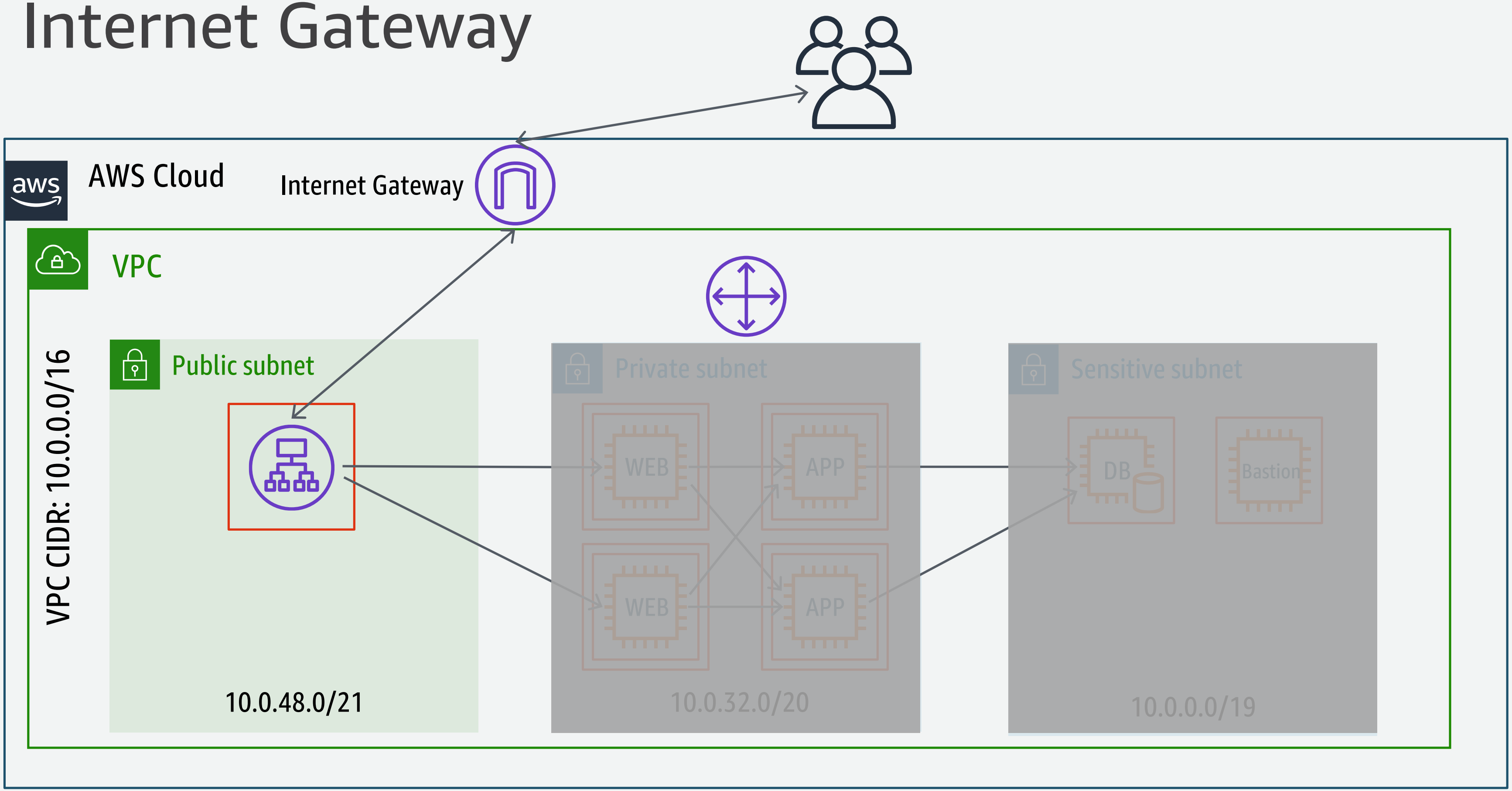
Internet Gateway



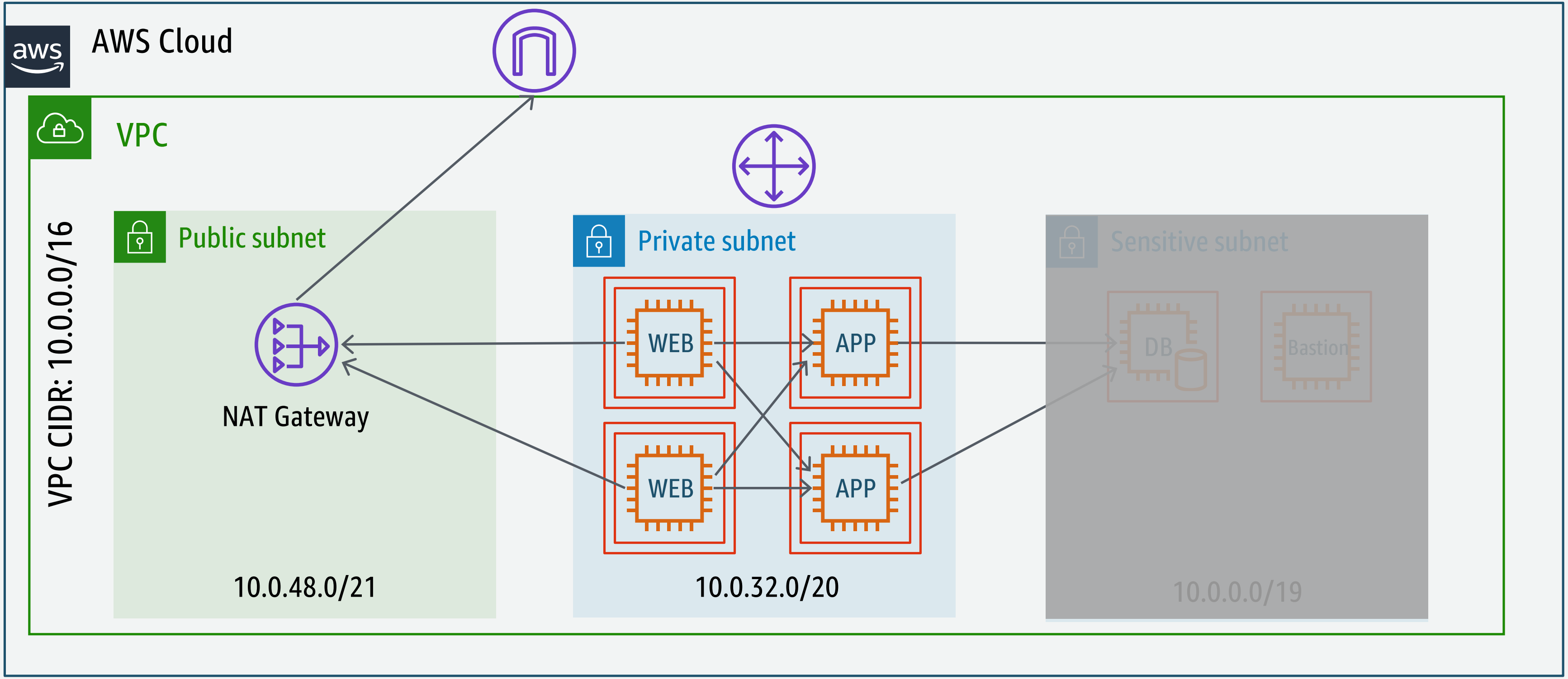
Internet Gateway



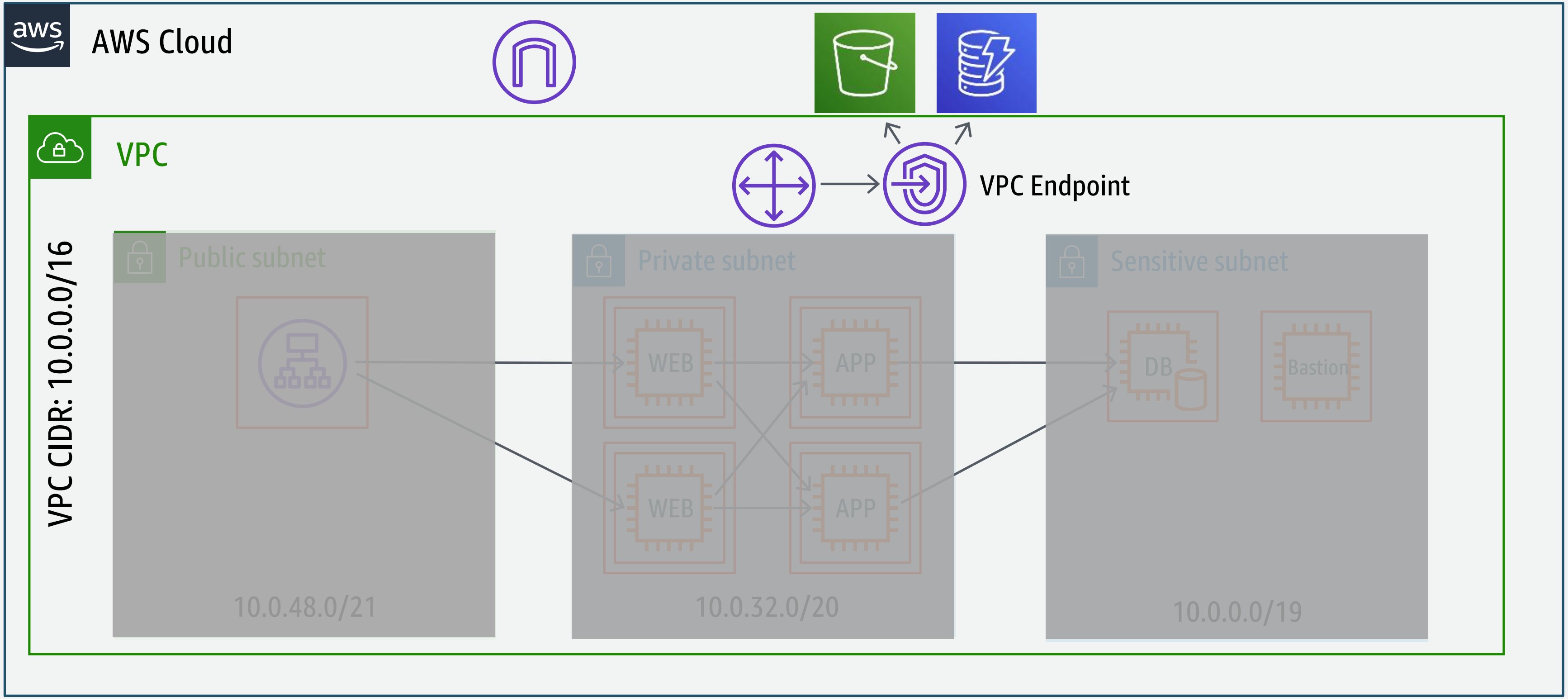
Internet Gateway



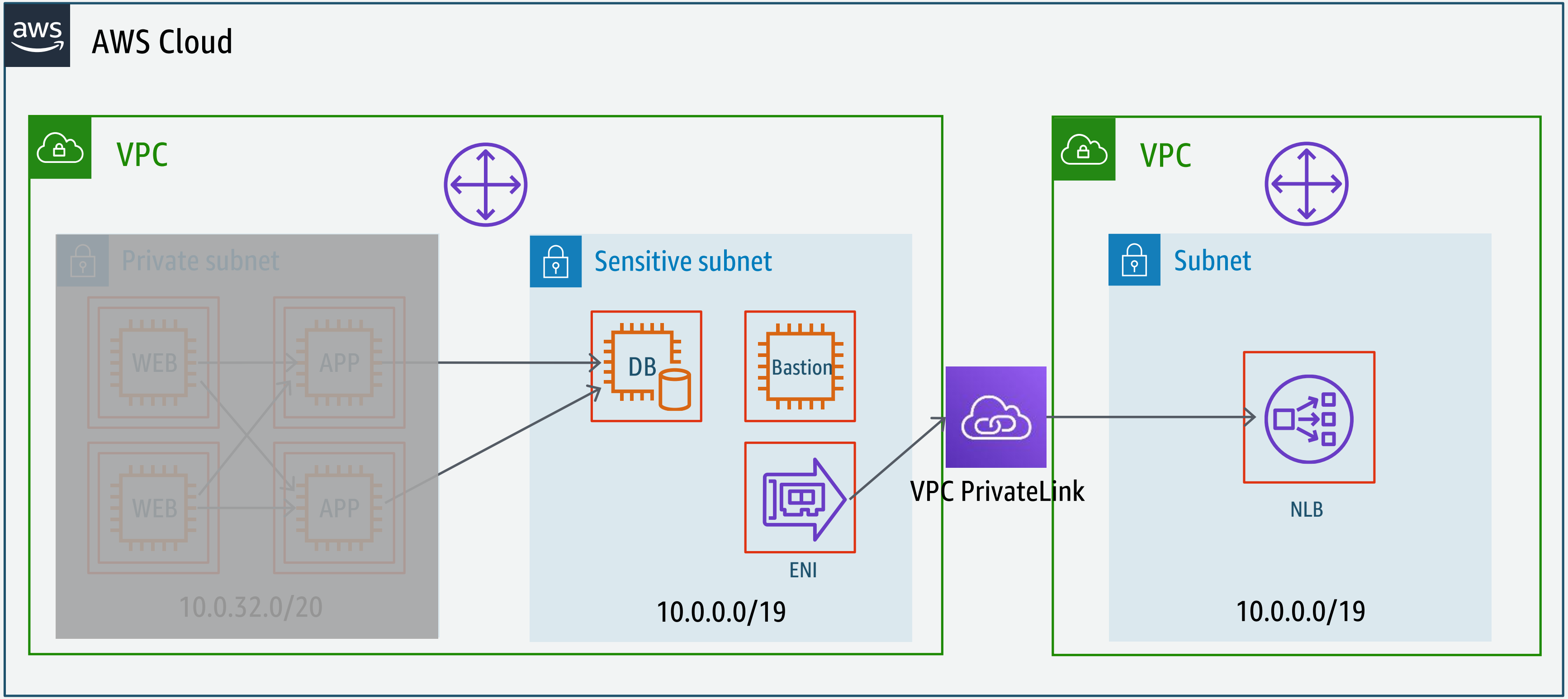
NAT Gateway


AWS Cloud
VPC
VPC CIDR: 10.0.0.0/16
Public subnet
NAT Gateway
10.0.48.0/21
Private subnet
WEB
APP
WEB
APP
10.0.32.0/20
Sensitive subnet
DB
Bastion
10.0.0.0/19

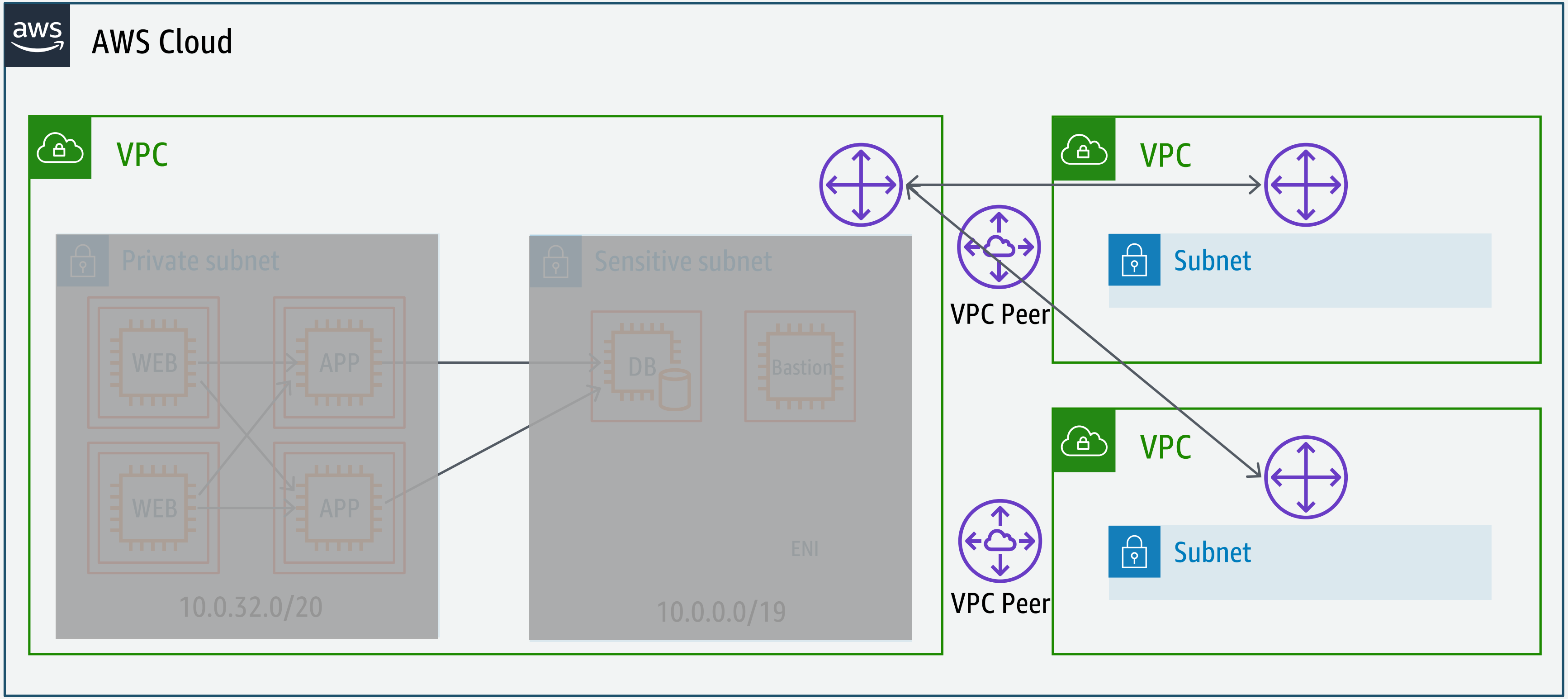
VPC Endpoints



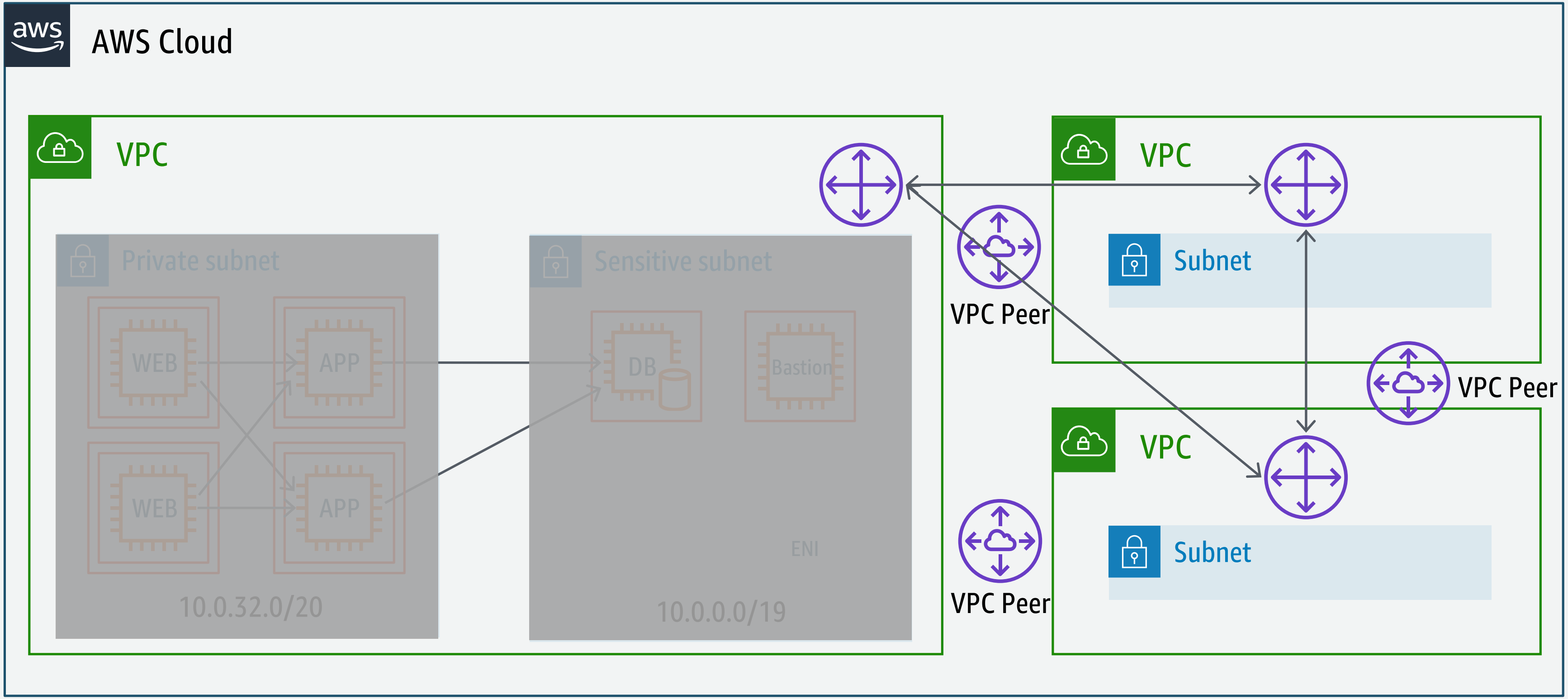
VPC PrivateLink



VPC Peering

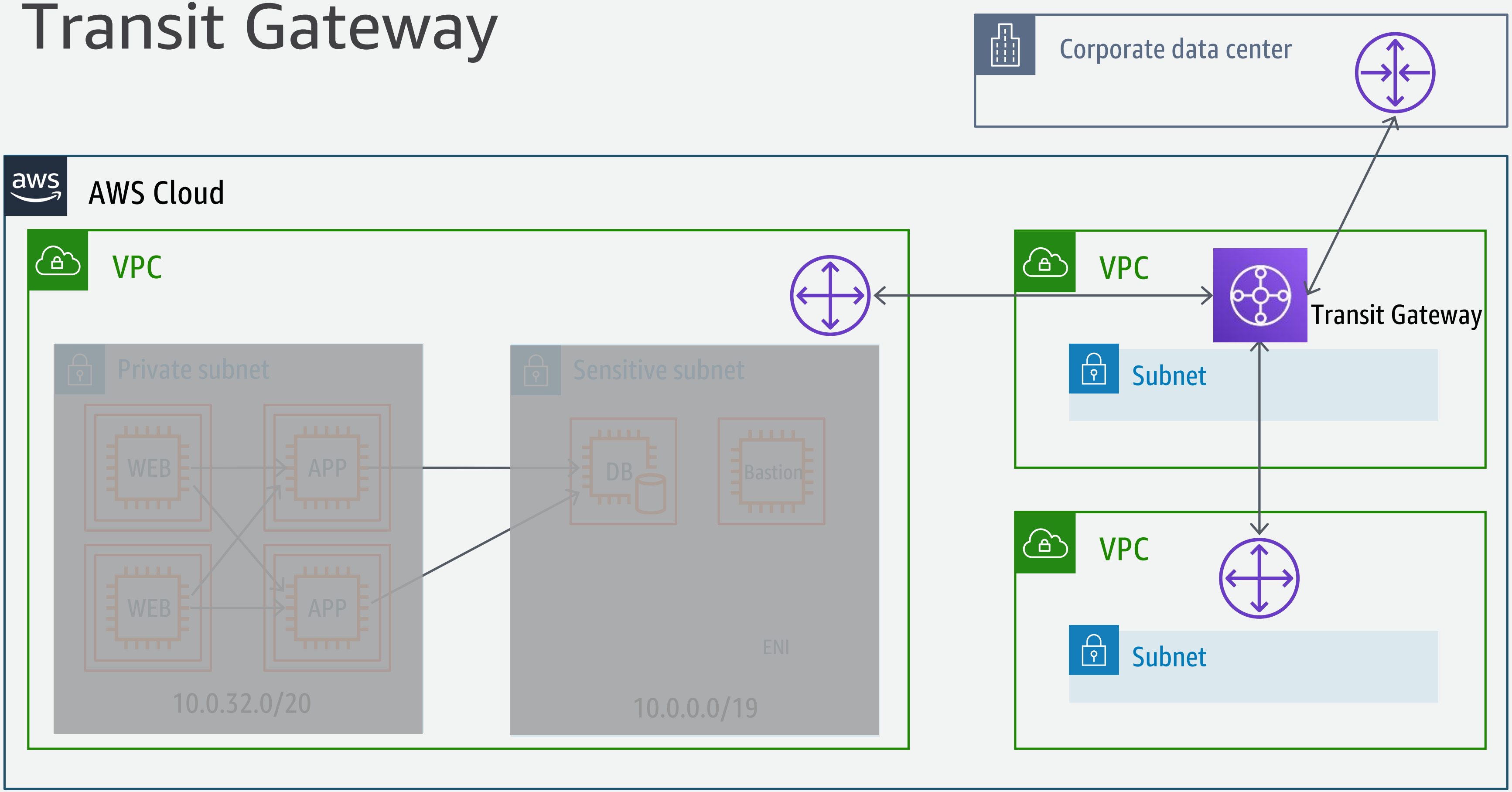

AWS Cloud
VPC
Private subnet
WEB
APP
WEB
APP
10.0.32.0/20
Sensitive subnet
DB
Bastion
ENI
10.0.0.0/19
VPC Peer
VPC Peer
VPC
Subnet
VPC
Subnet

VPC Peering

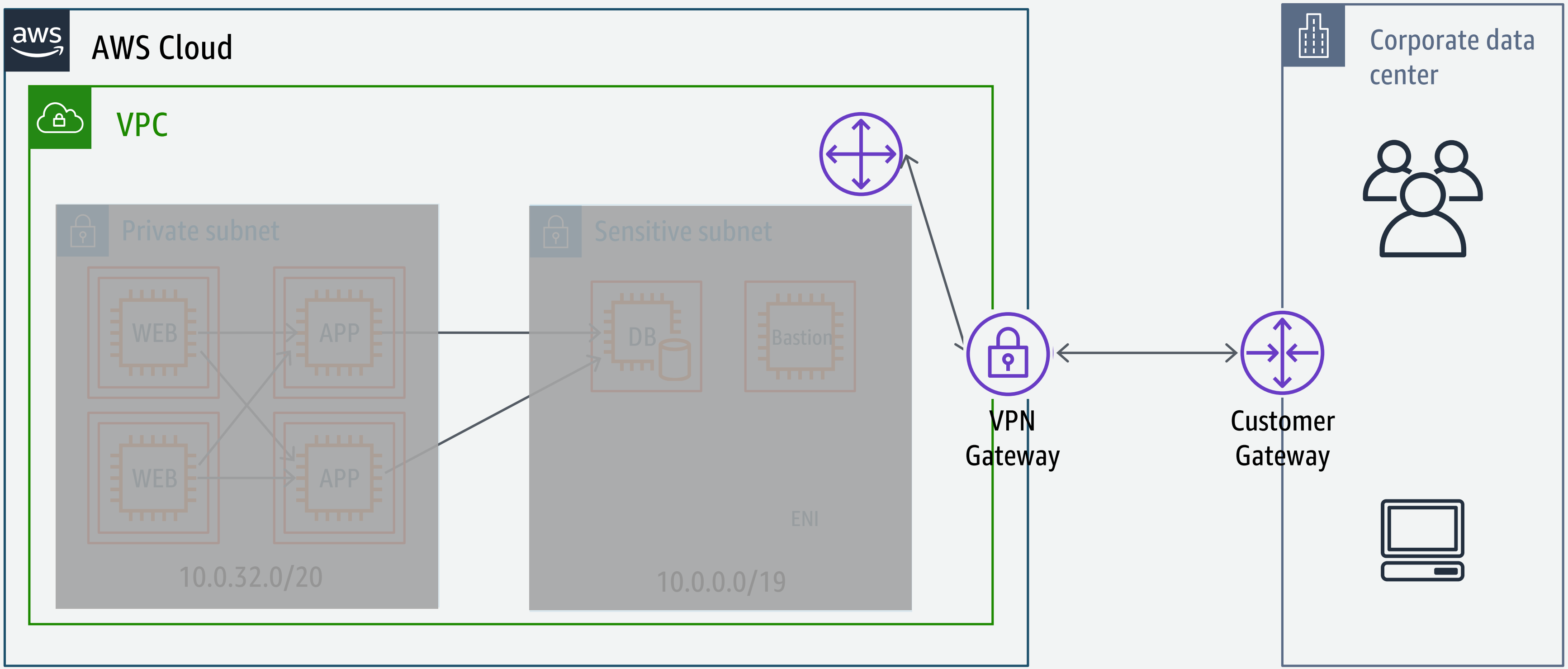


AWS Cloud
VPC
Private subnet
WEB
APP
WEB
APP
10.0.32.0/20
Sensitive subnet
DB
Bastion
ENI
10.0.0.0/19
VPC Peer
VPC Peer
VPC
Subnet
VPC Peer
VPC
Subnet

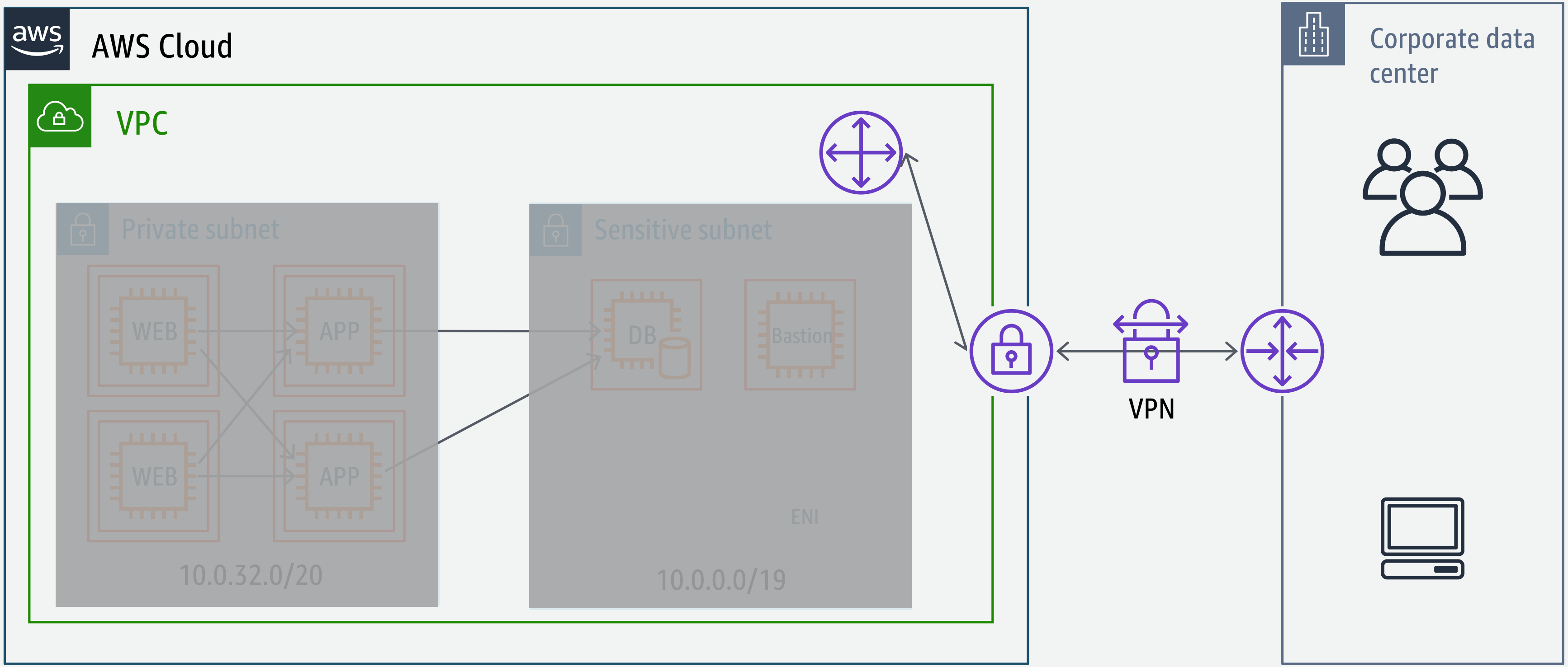
Transit Gateway



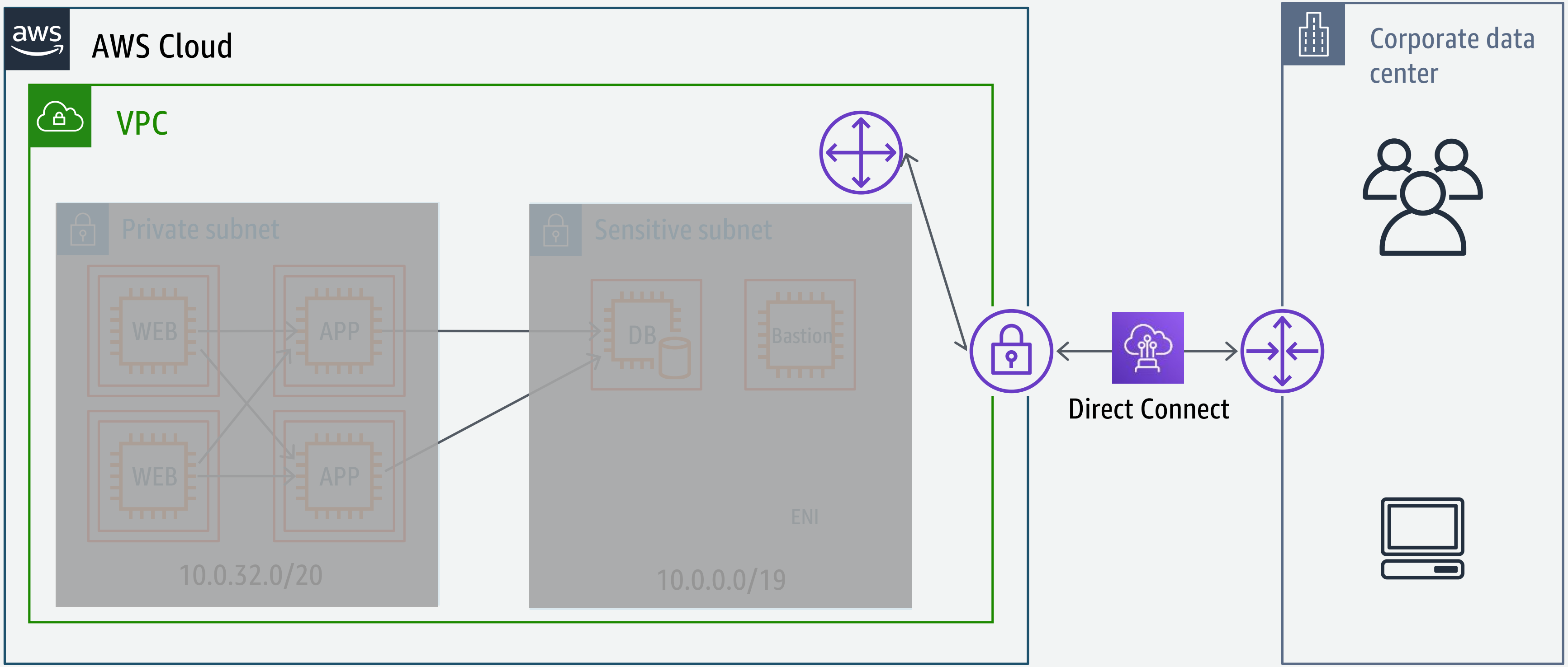
VPN


AWS Cloud
VPC
Private subnet
WEB
APP
WEB
APP
10.0.32.0/20
Sensitive subnet
DB
Bastion
ENI
10.0.0.0/19
VPN Gateway
Customer Gateway
Corporate data center

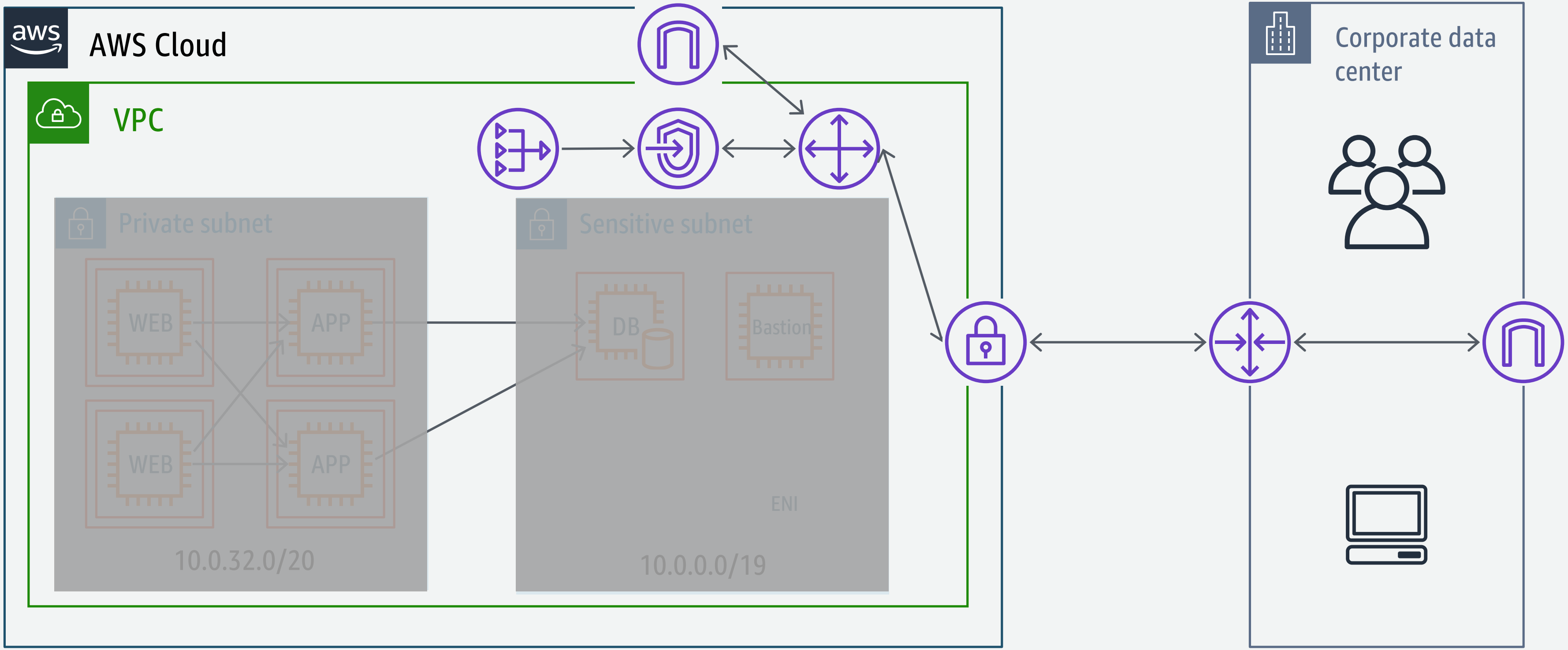
VPN


AWS Cloud
VPC
Private subnet
WEB
APP
WEB
APP
10.0.32.0/20
Sensitive subnet
DB
Bastion
ENI
10.0.0.0/19
VPN
Corporate data center

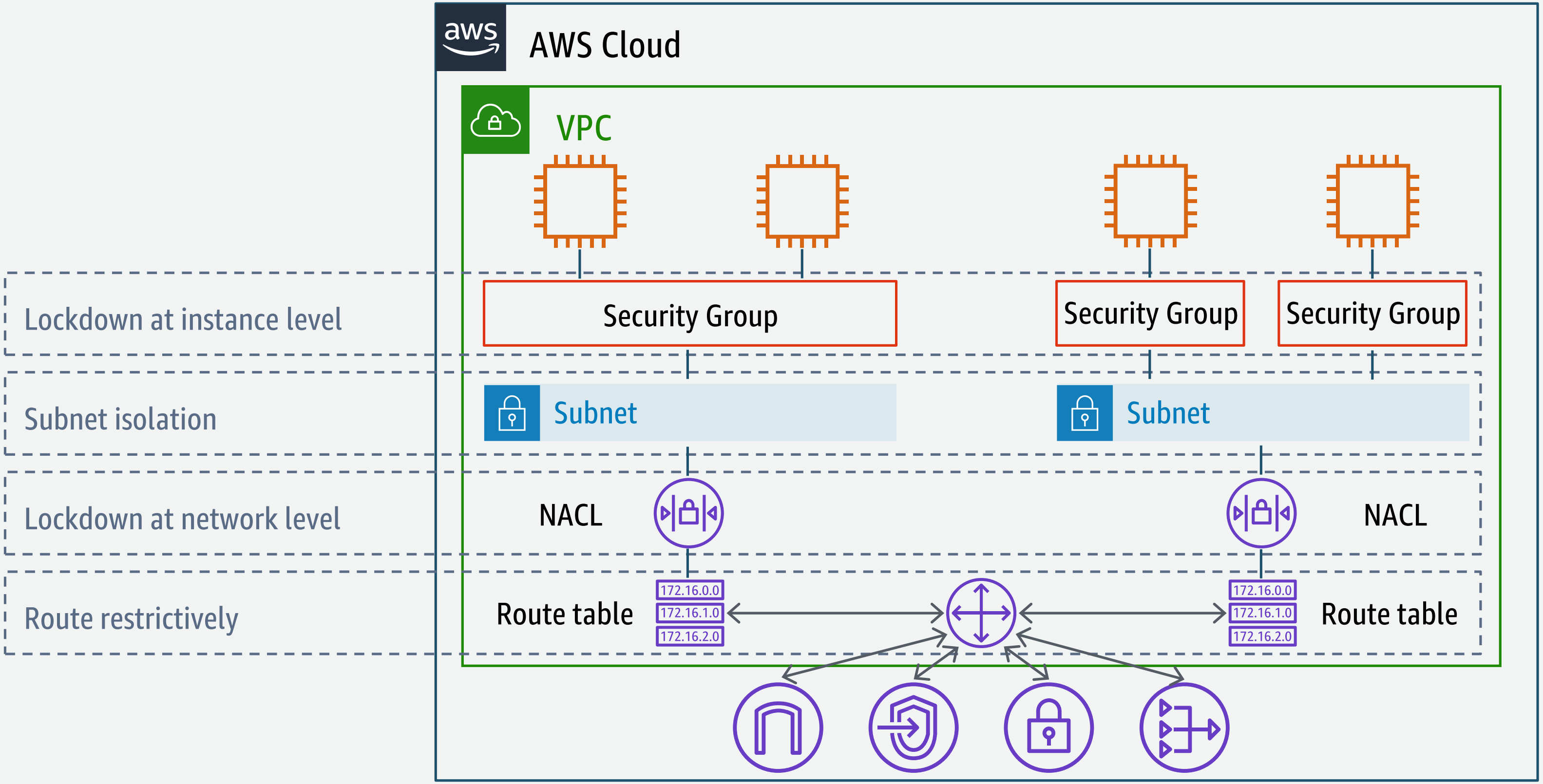
Direct Connect



Multiple Gateways



Network Defense in Depth



Questions?