AWS Network Overview

양보승

양보승, Boseung Yang

- AWS Professional Services
- Cloud Architect

https://www.linkedin.com/in/bsyang/

Agenda

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

Outcomes

- VPC 설계에 대한 결정
- IP CIDR 범위 결정
- DNS 결정(Amazon DNS vs 자체관리형 AD)
- 연결 결정(Internet Gateway/Direct Connect/VPC)

Virtual Private Cloud (VPC)

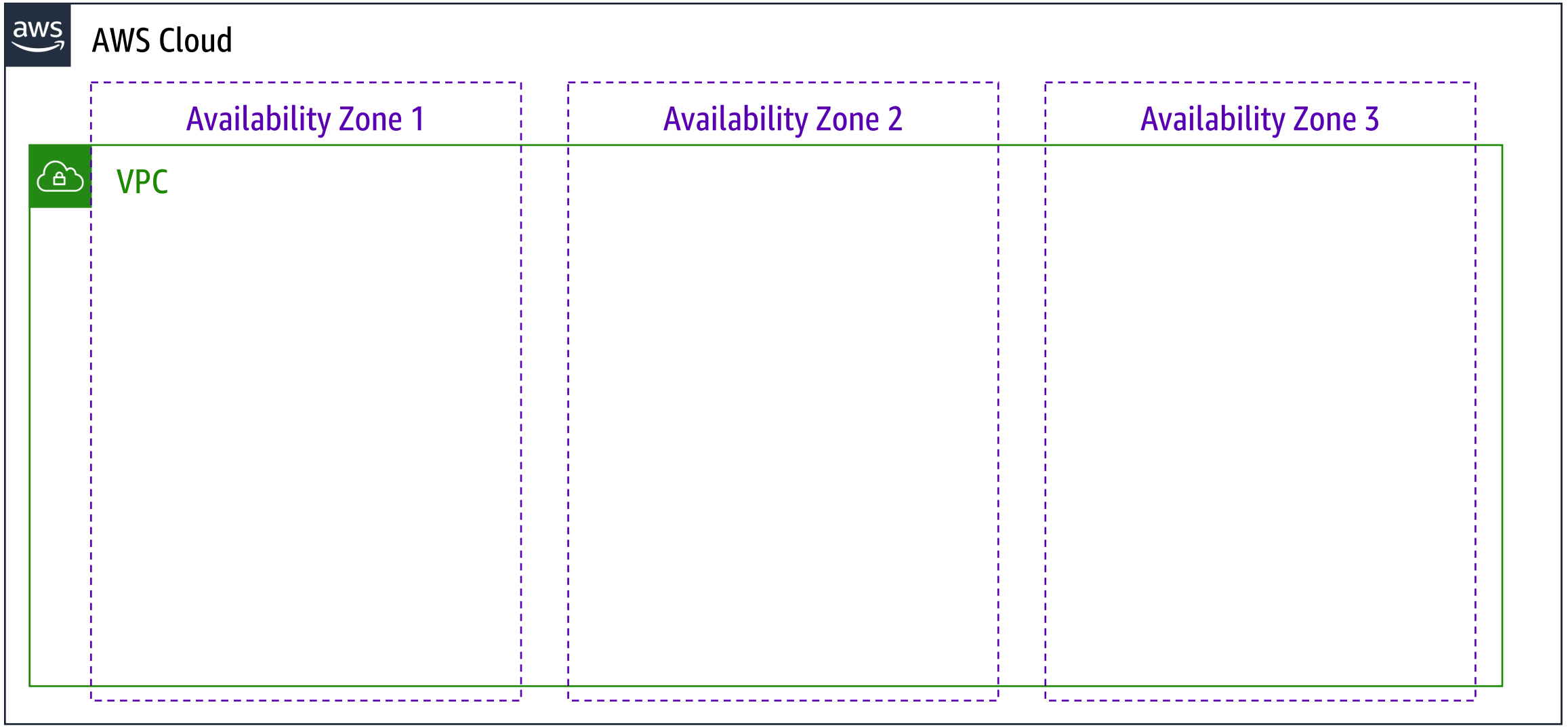
aws professional services

What is a Virtual Private Cloud?

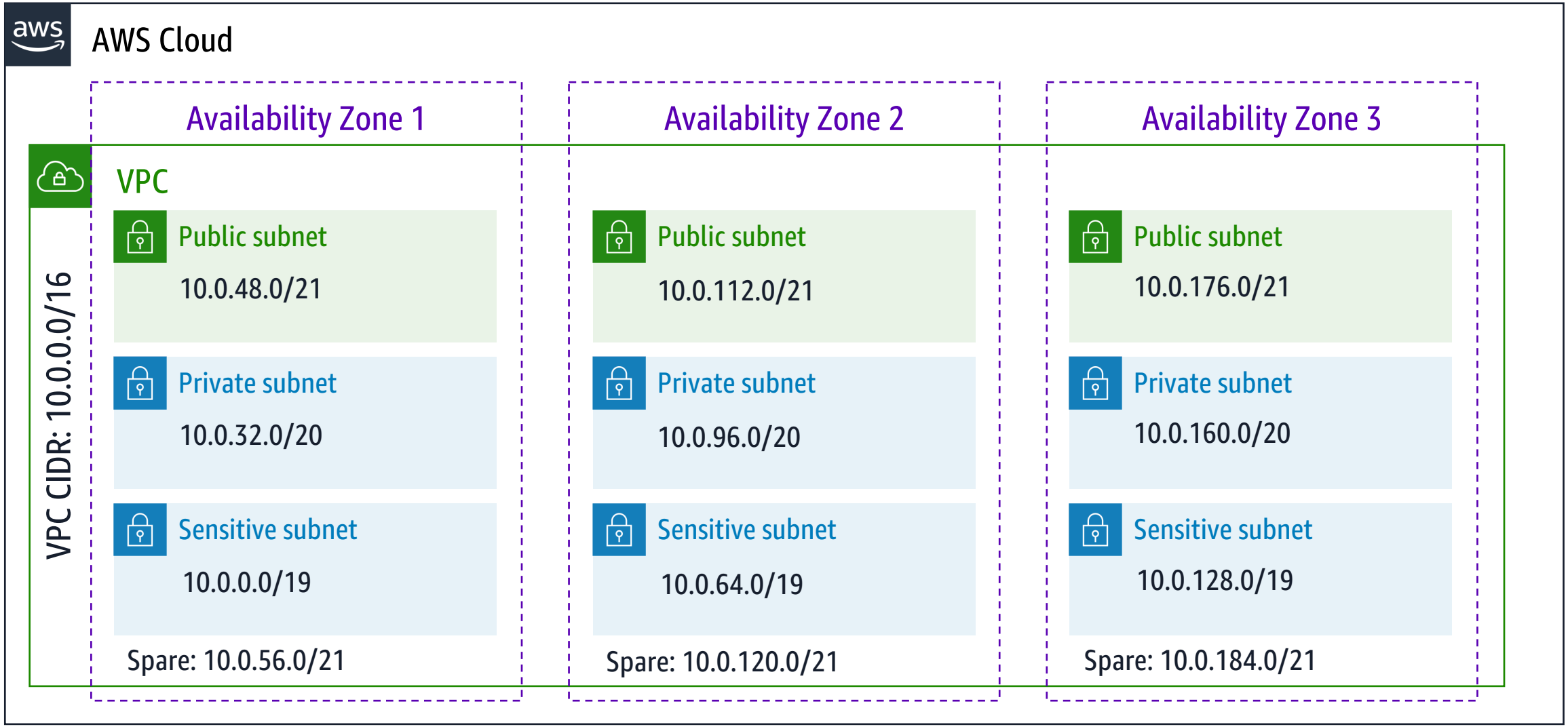
- Software-defined network
- Logically isolated
- Complete control
- Secure
- VPN & Internet connectivity
- Connect your on-premises IT environment

각 AWS 리전에는 여러 가용 영역이 있습니다.

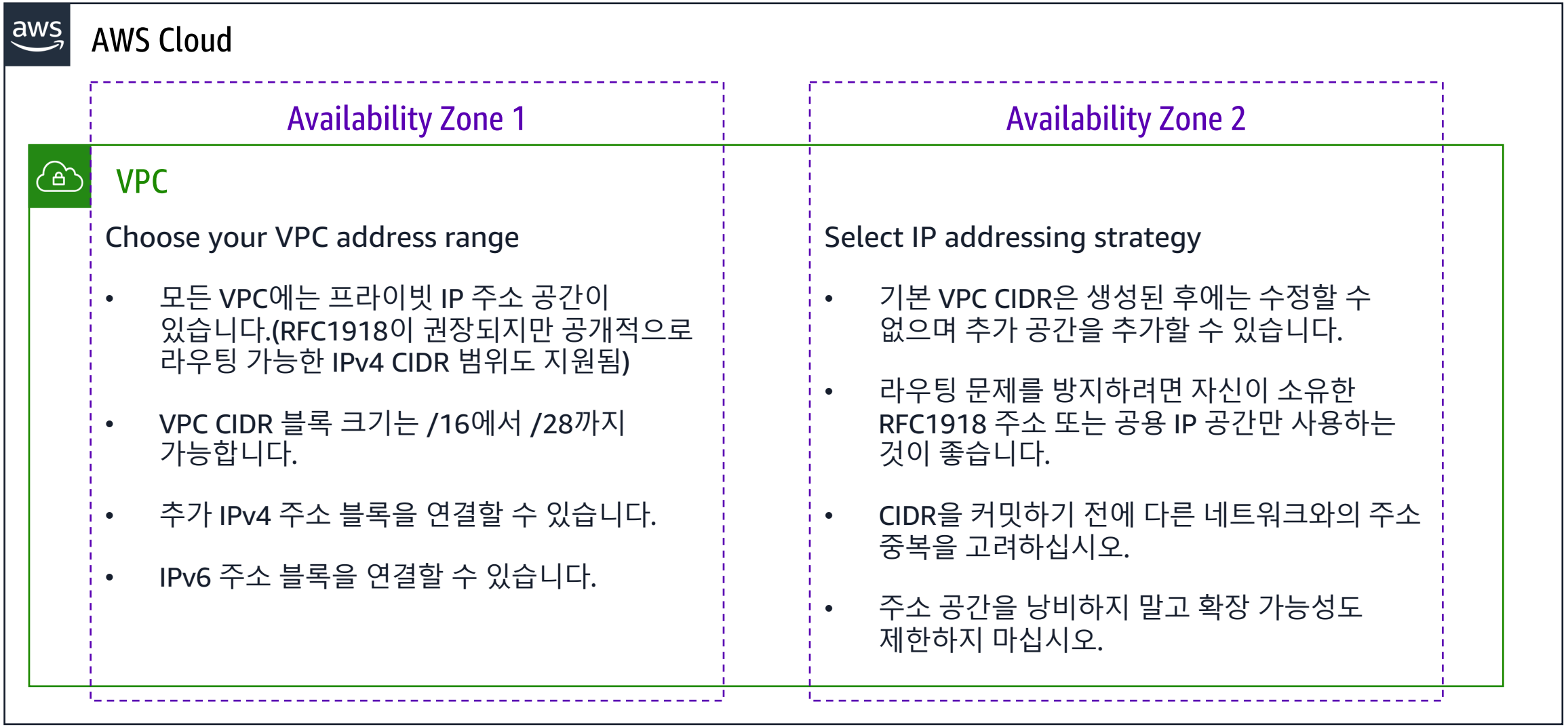
VPC는 리전의 모든 가용 영역에 걸쳐 있습니다.



Subnets


AWS Cloud
Availability Zone 1
Availability Zone 2
Availability Zone 3
VPC
VPC CIDR: 10.0.0.0/16
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
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
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

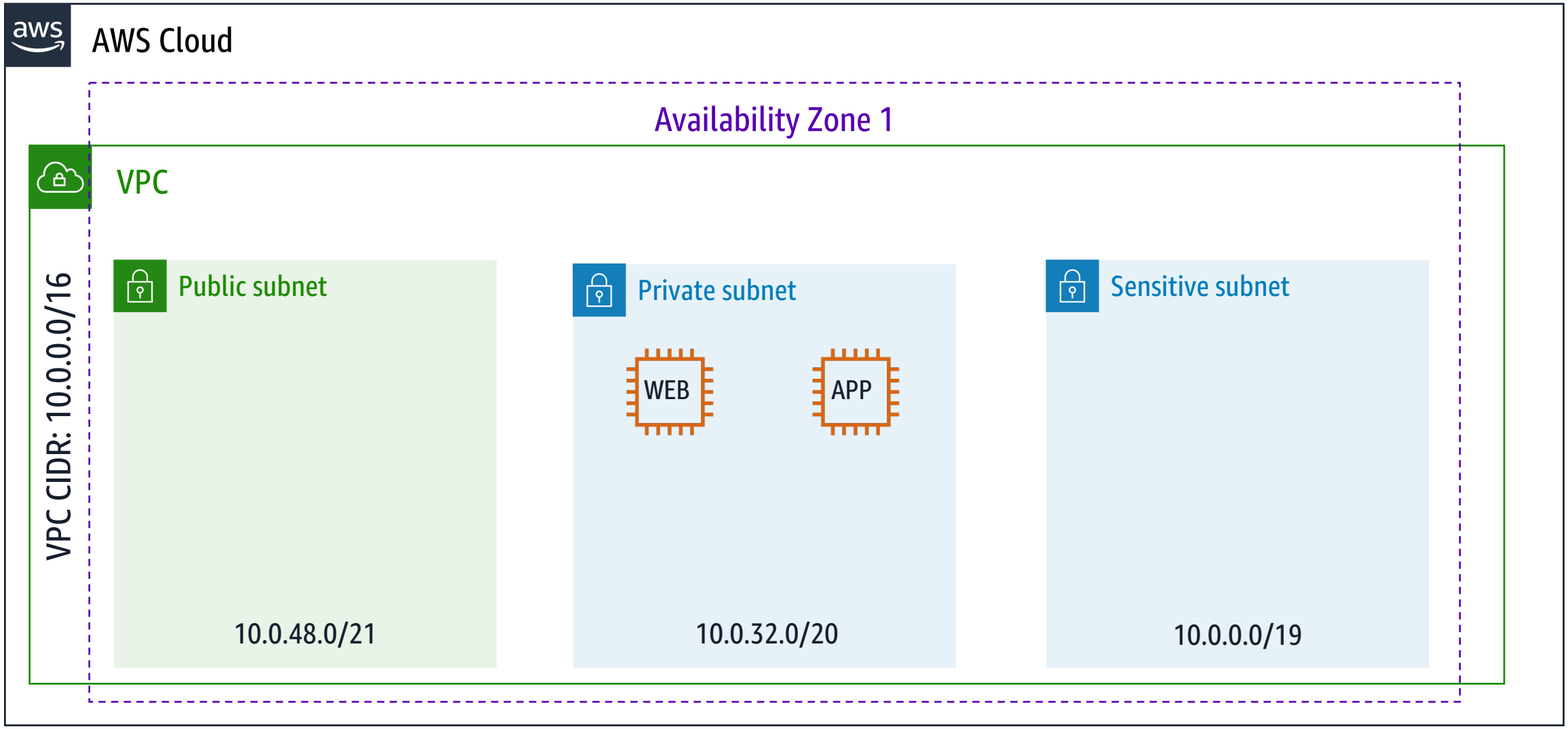
고객은 VPC을 완전하게 제어 할 수 있습니다.



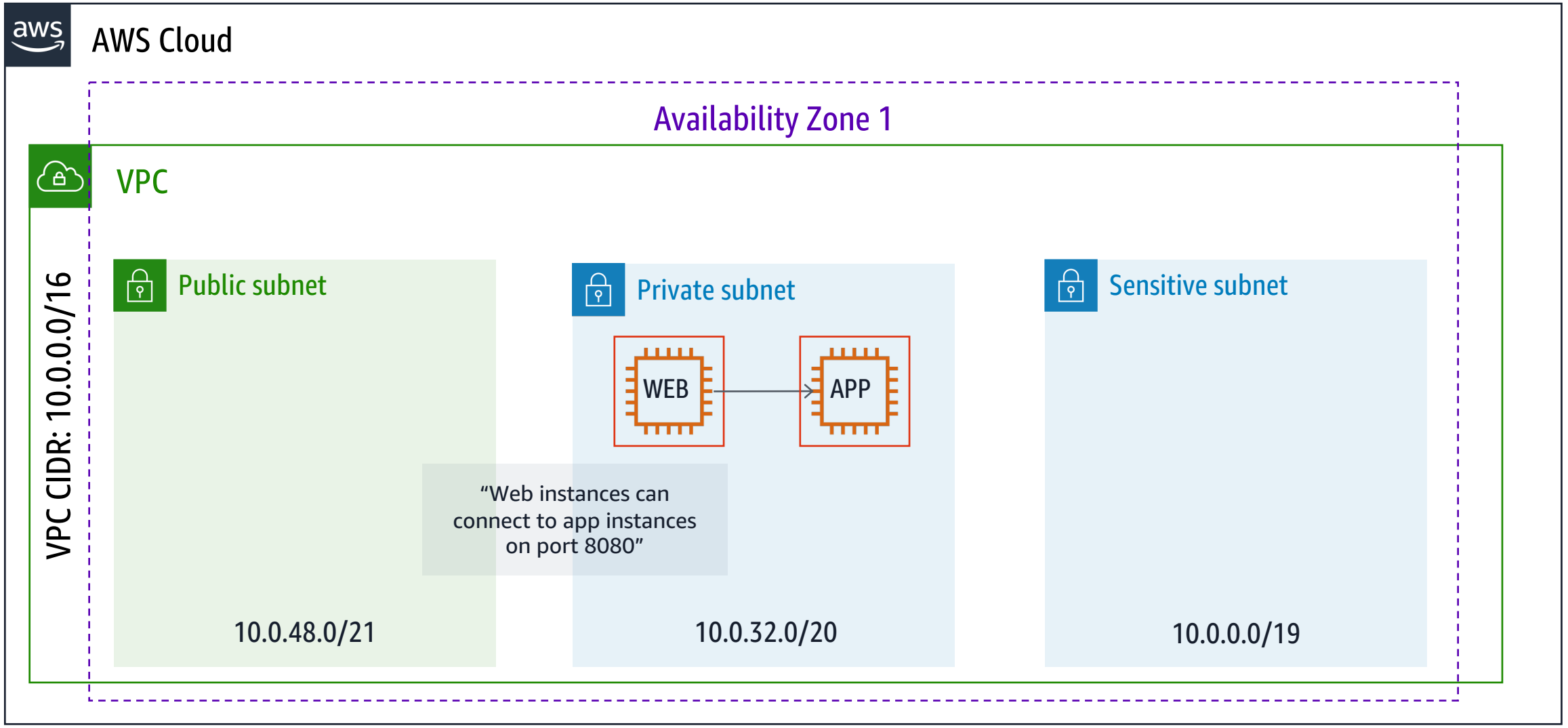
Security Groups

aws professional services

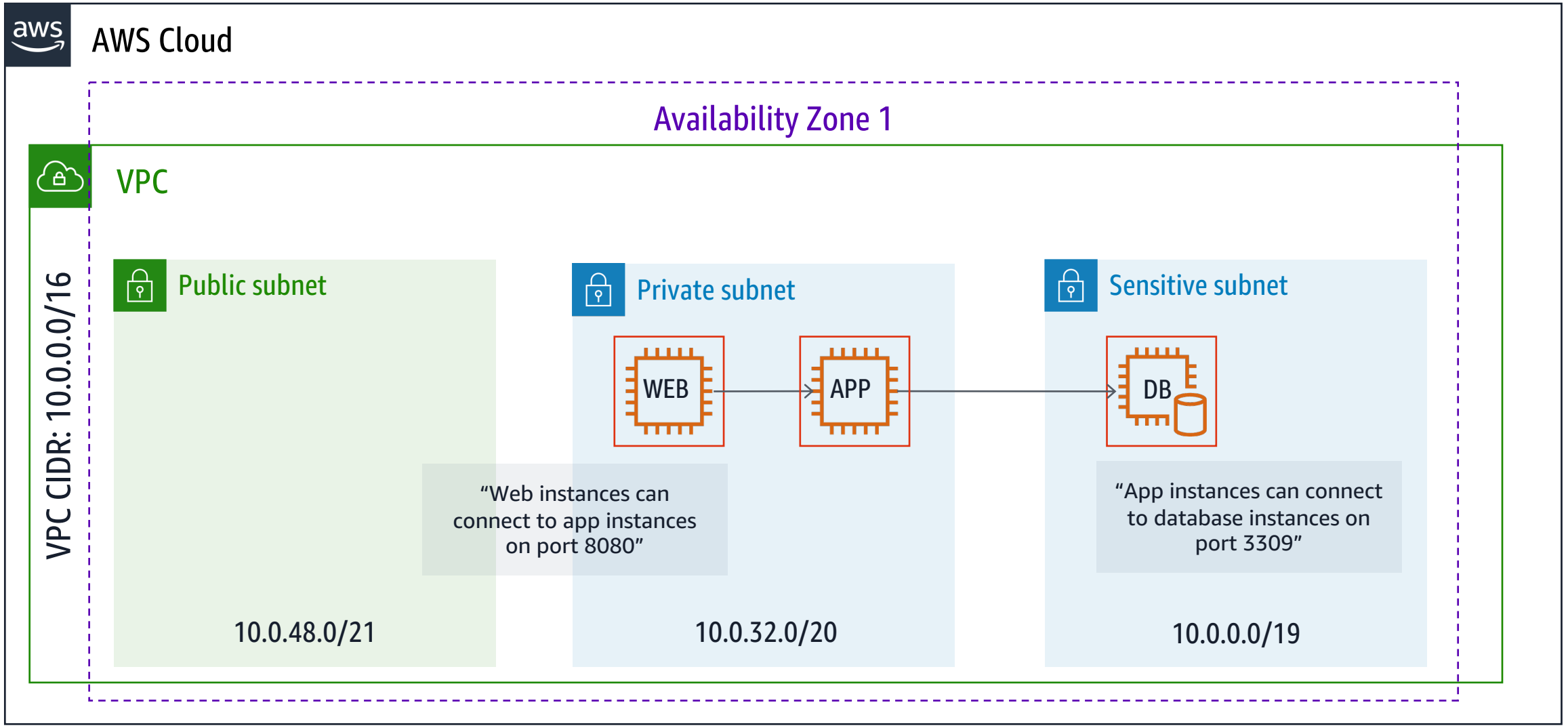
Security Groups – Stateful Firewall



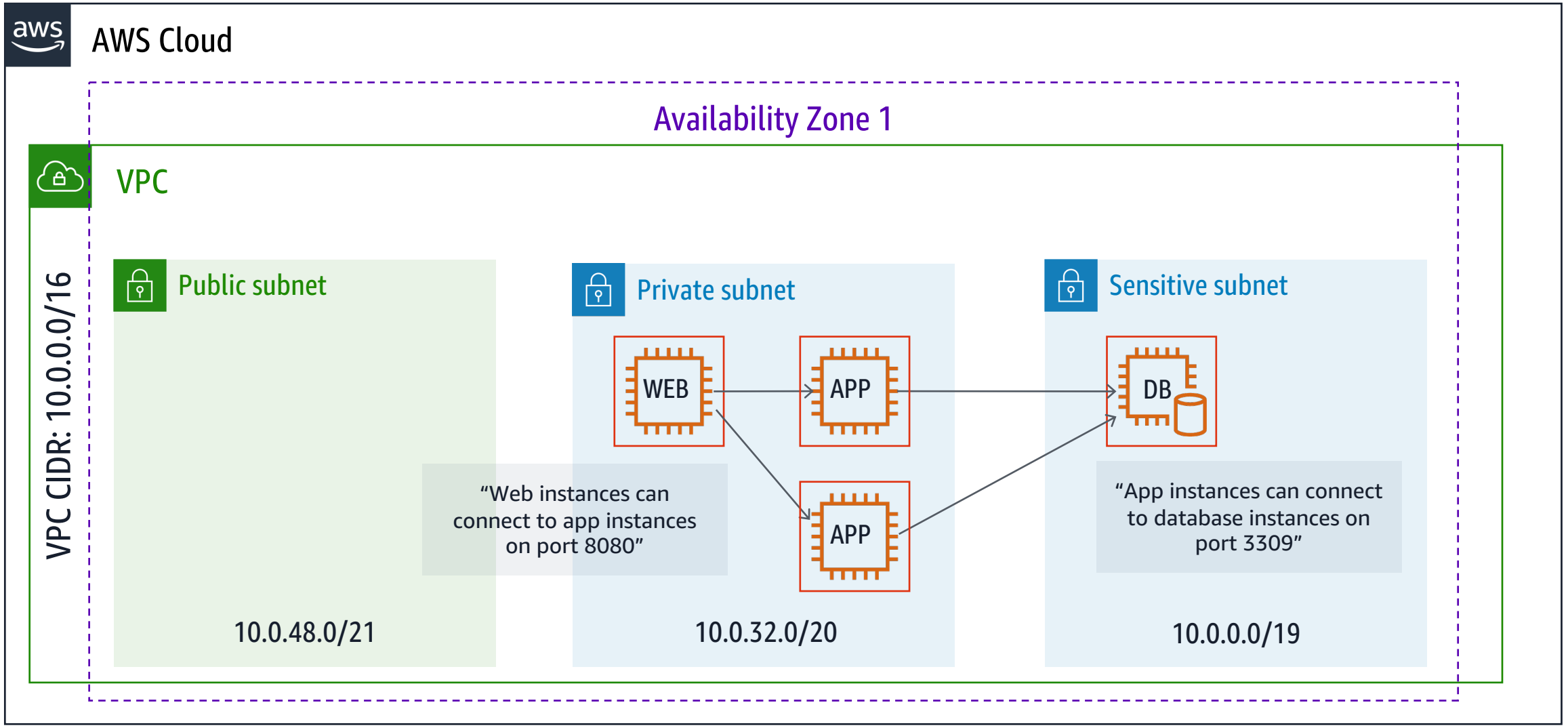
Security Groups – Stateful Firewall



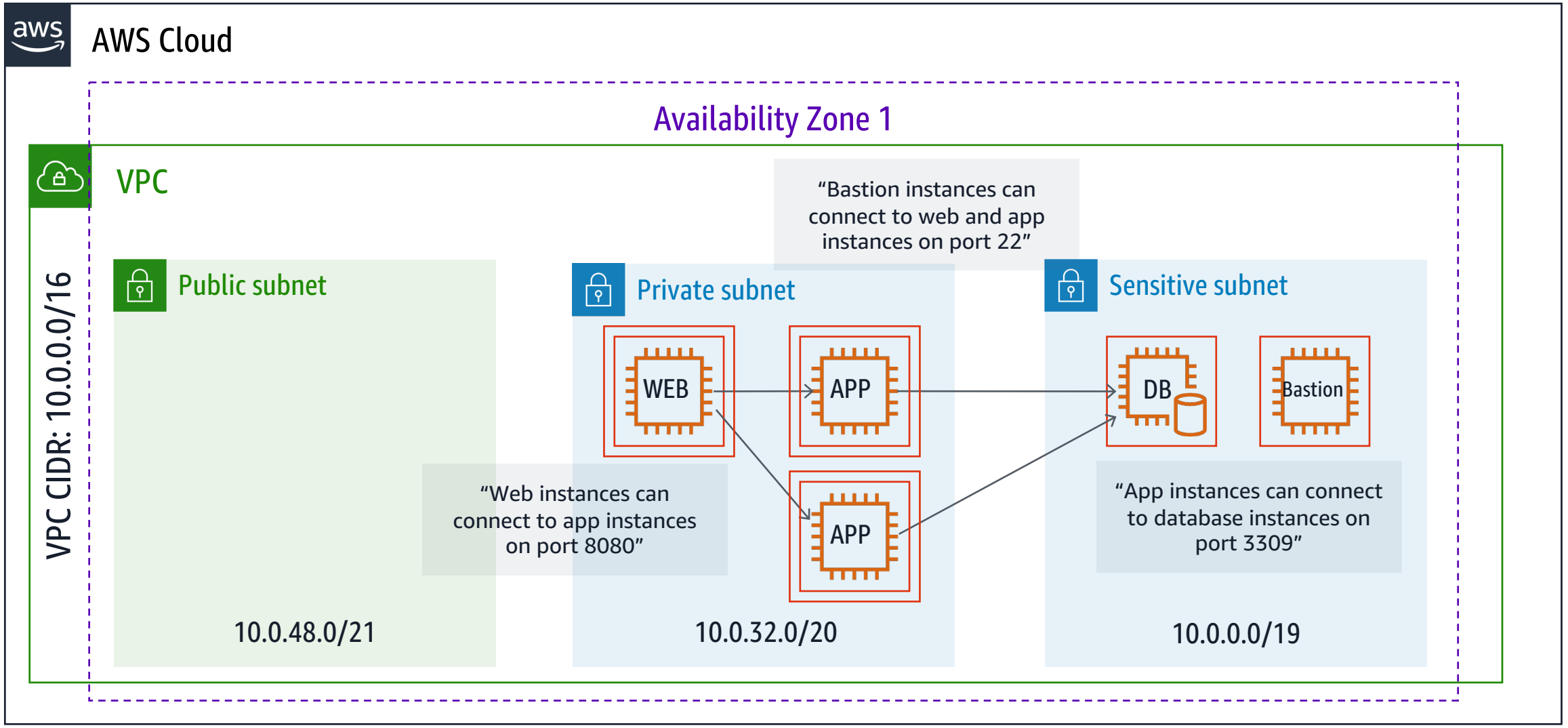
Security Groups – Stateful Firewall



Security Groups – Stateful Firewall



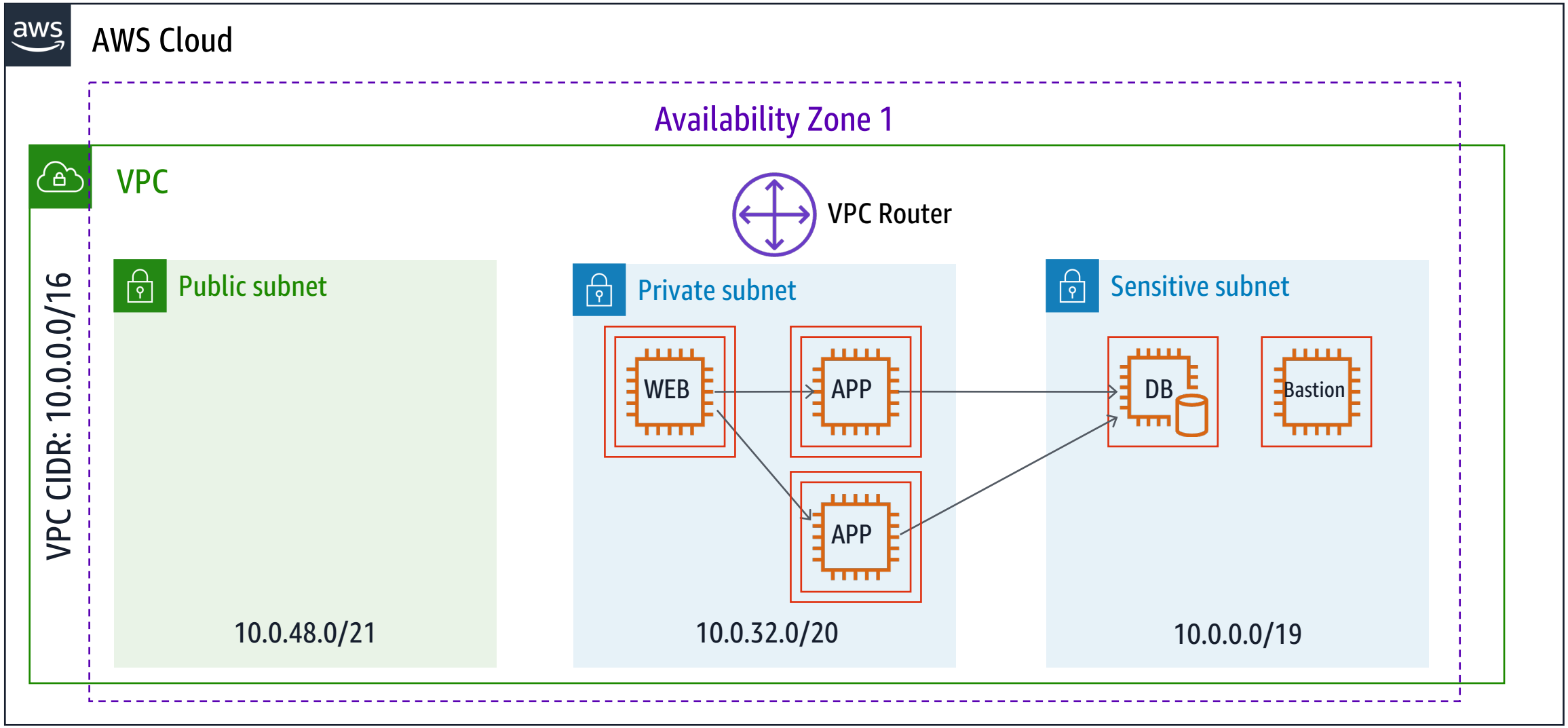
Security Groups – Stateful Firewall



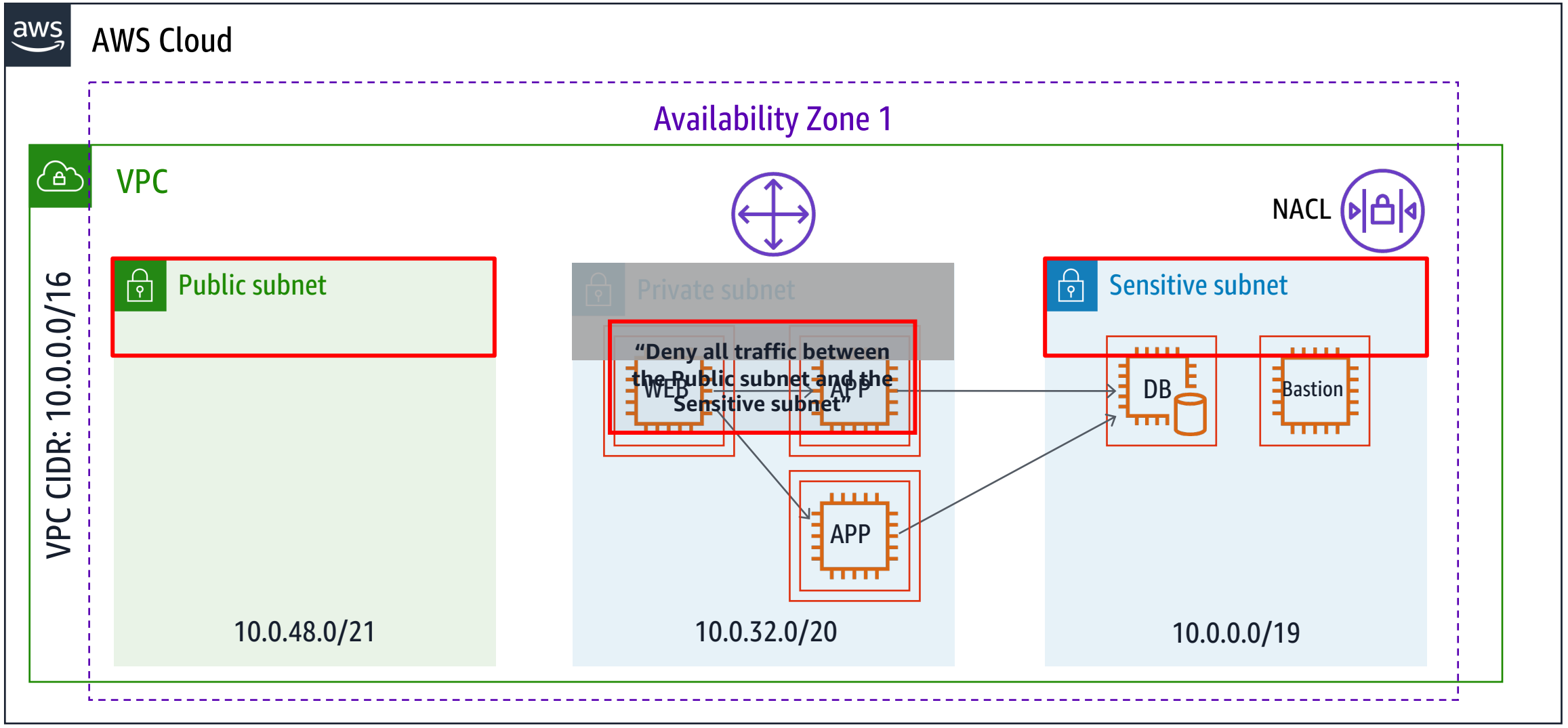
Routing, NACLS's, and Load Balancing

aws professional services

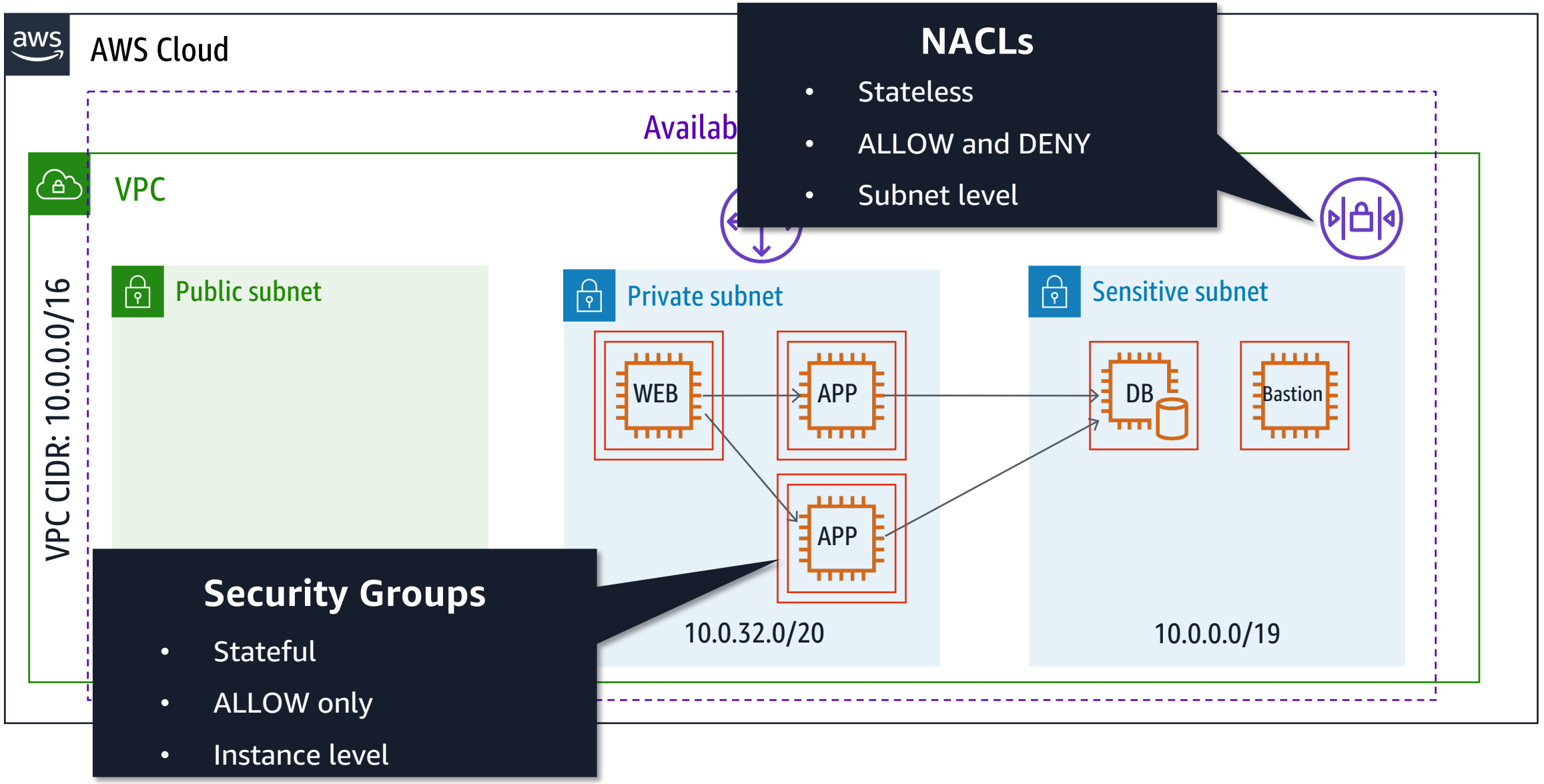
Routing


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

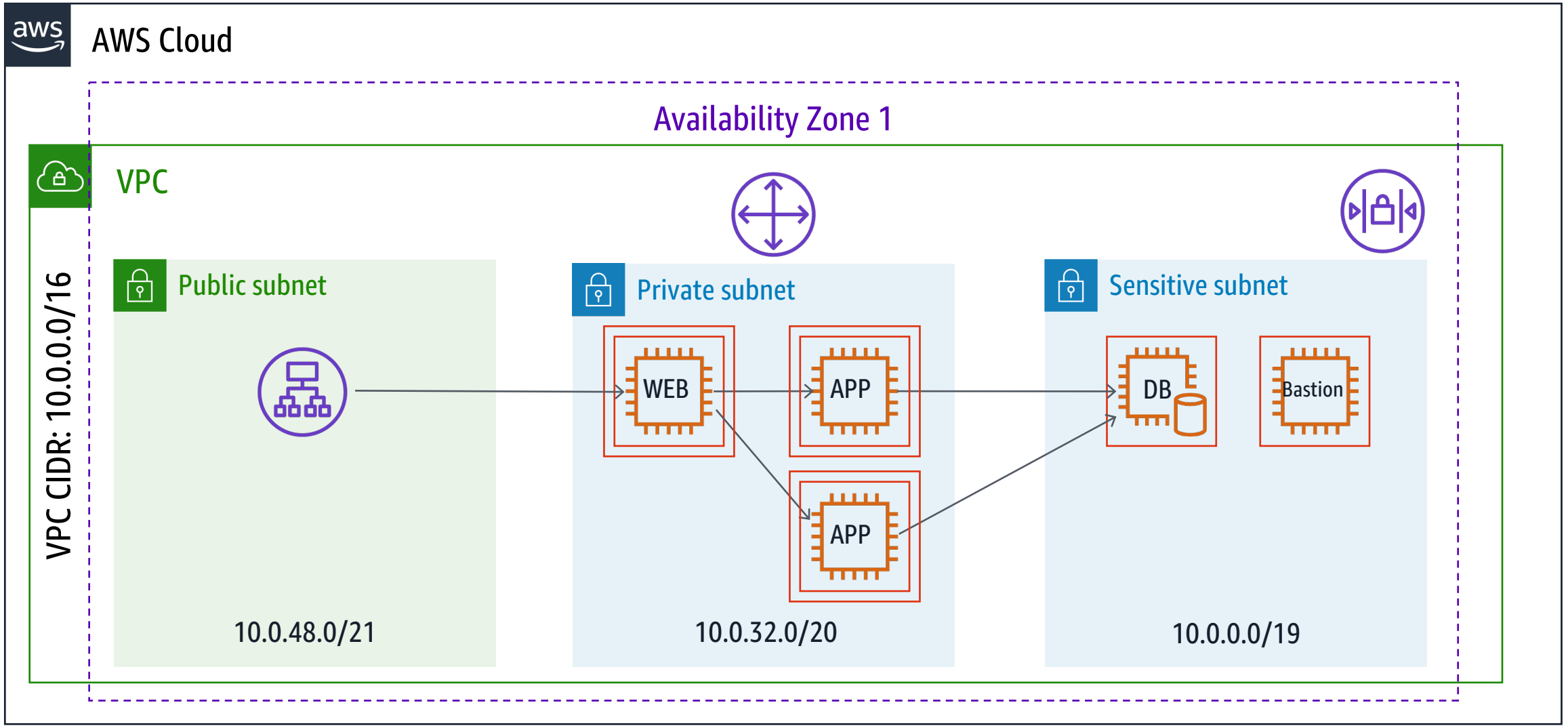
Network Access Control List (NACL)



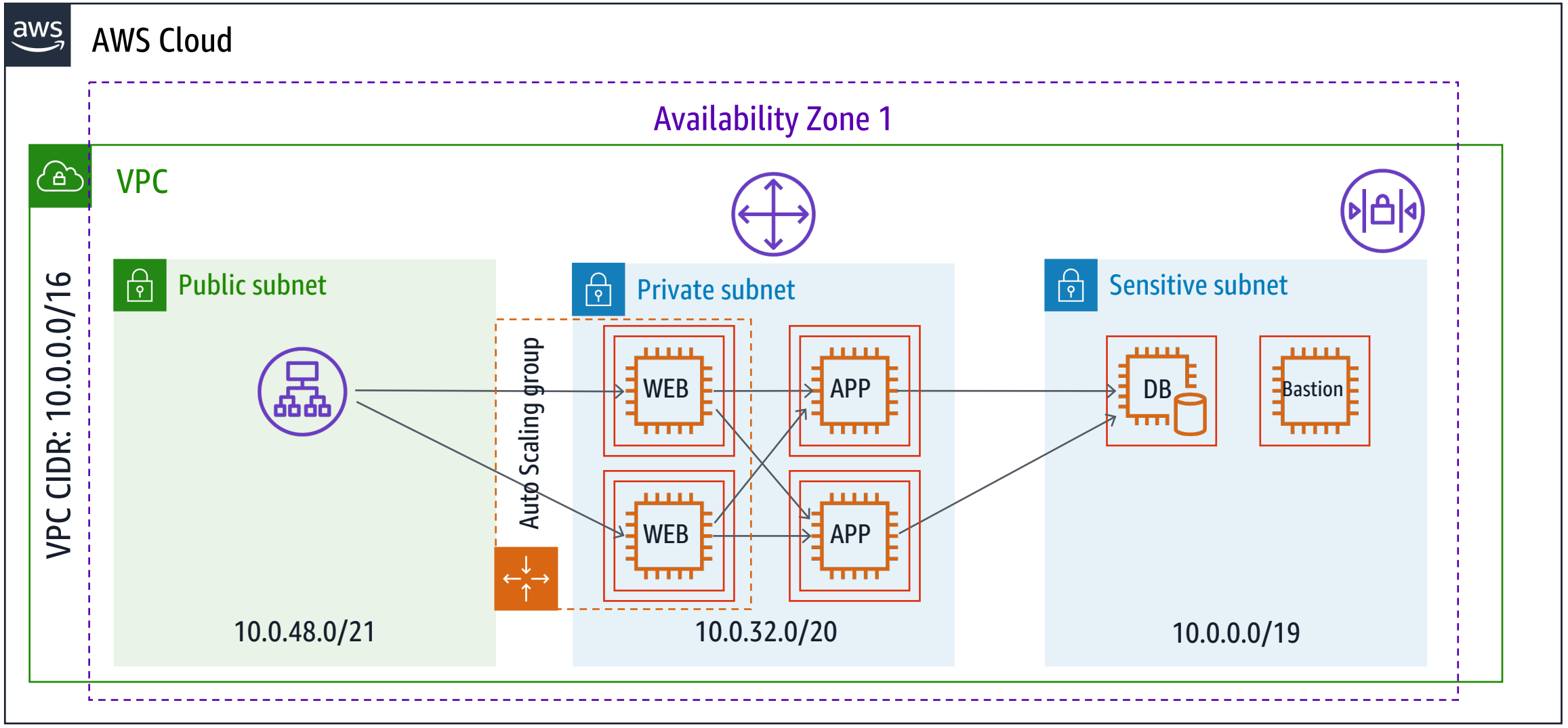
NACLs and Security Groups



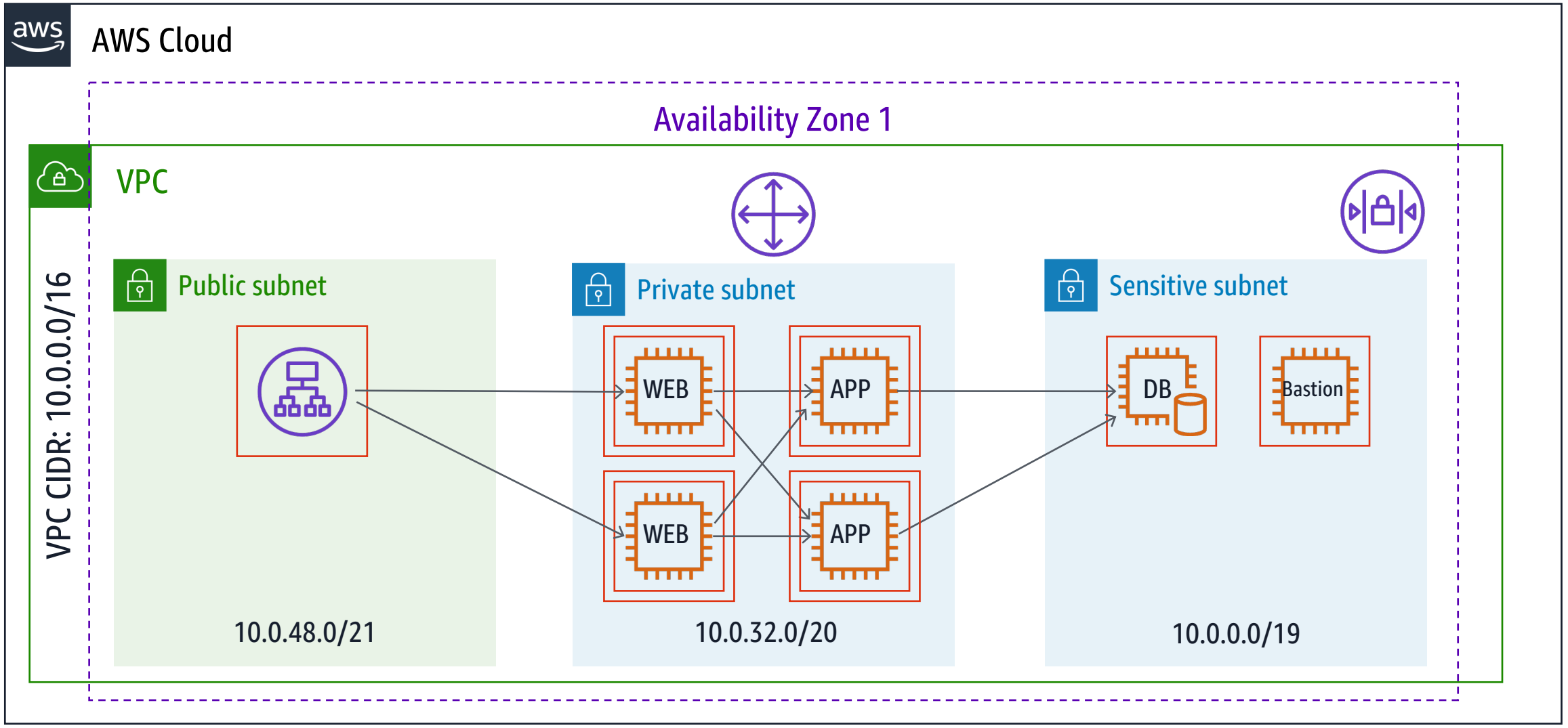
Load Balancing



Load Balancing



Load Balancing



Load Balancing – ELB Types

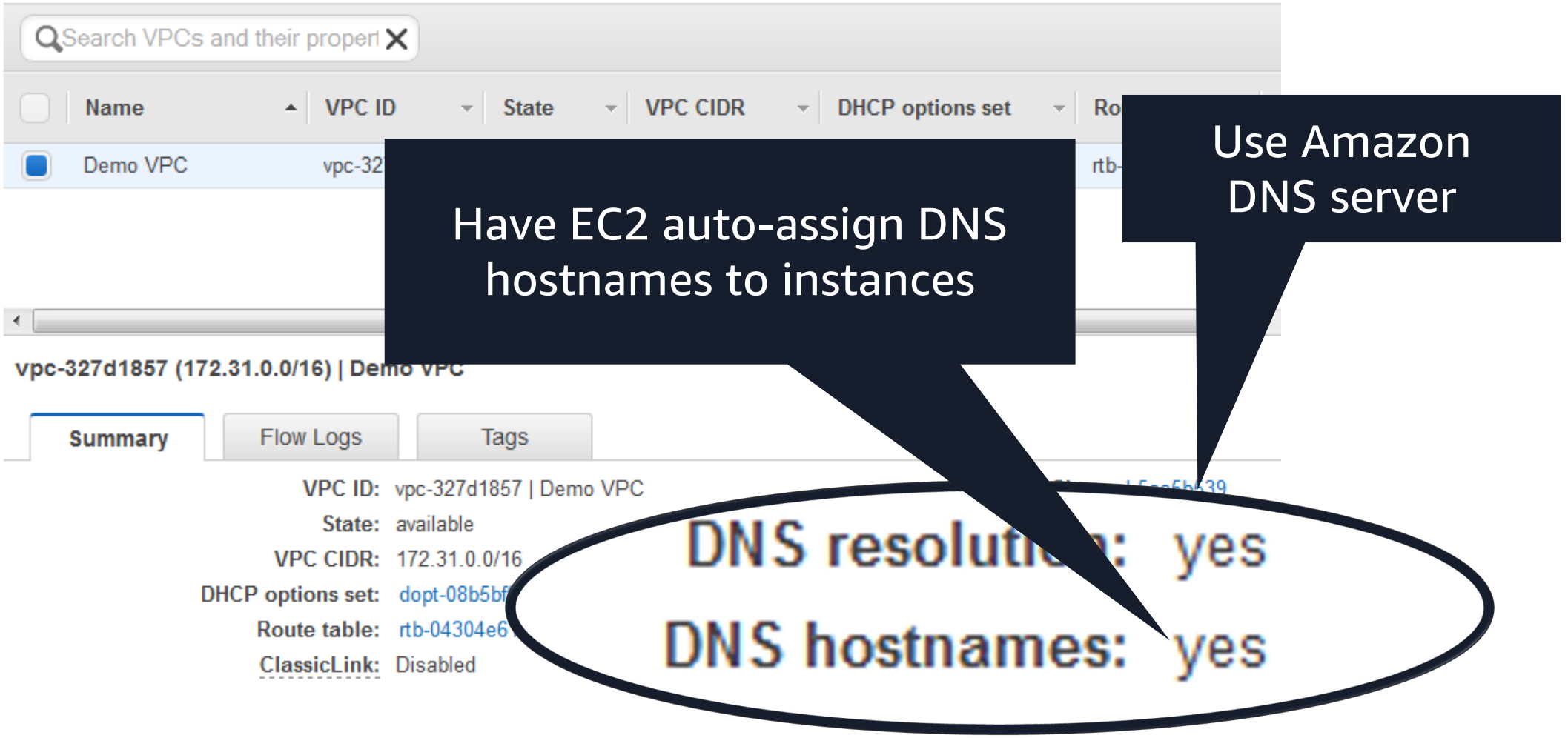
	Classic Load Balancer	Application Load Balancer	Network Load Balancer	Gateway Load Balancer
Protocols	TCP, SSL/TLS, HTTP, HTTPS	HTTP, HTTPS, gRPC	TCP, UDP, TLS	GENEVE
Network Layer	L4 – L7	L7	L4	L3 – L4
IP address as a target	✗	✓	✓	✓
Lambda function as a target	✗	✓	✗	✗
Server Name Indication (SNI)	✗	✓	✗	✗
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

aws professional services

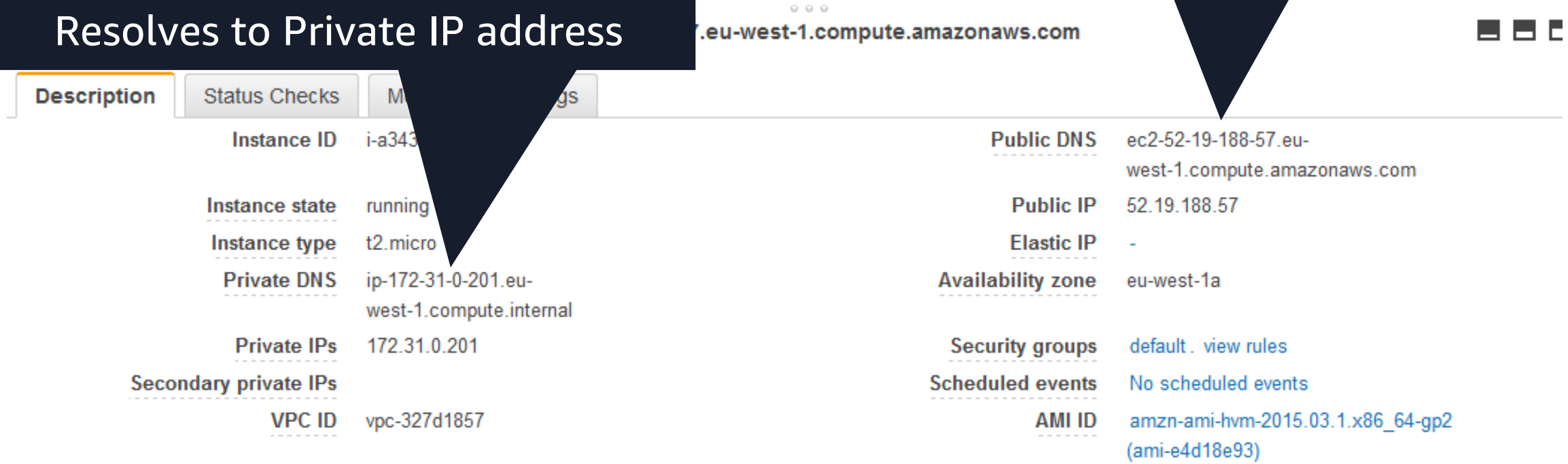
VPC DNS Options



EC2 DNS Hostnames

External DNS name:
Resolves to…

Internal DNS hostname:
Resolves to Private IP address



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

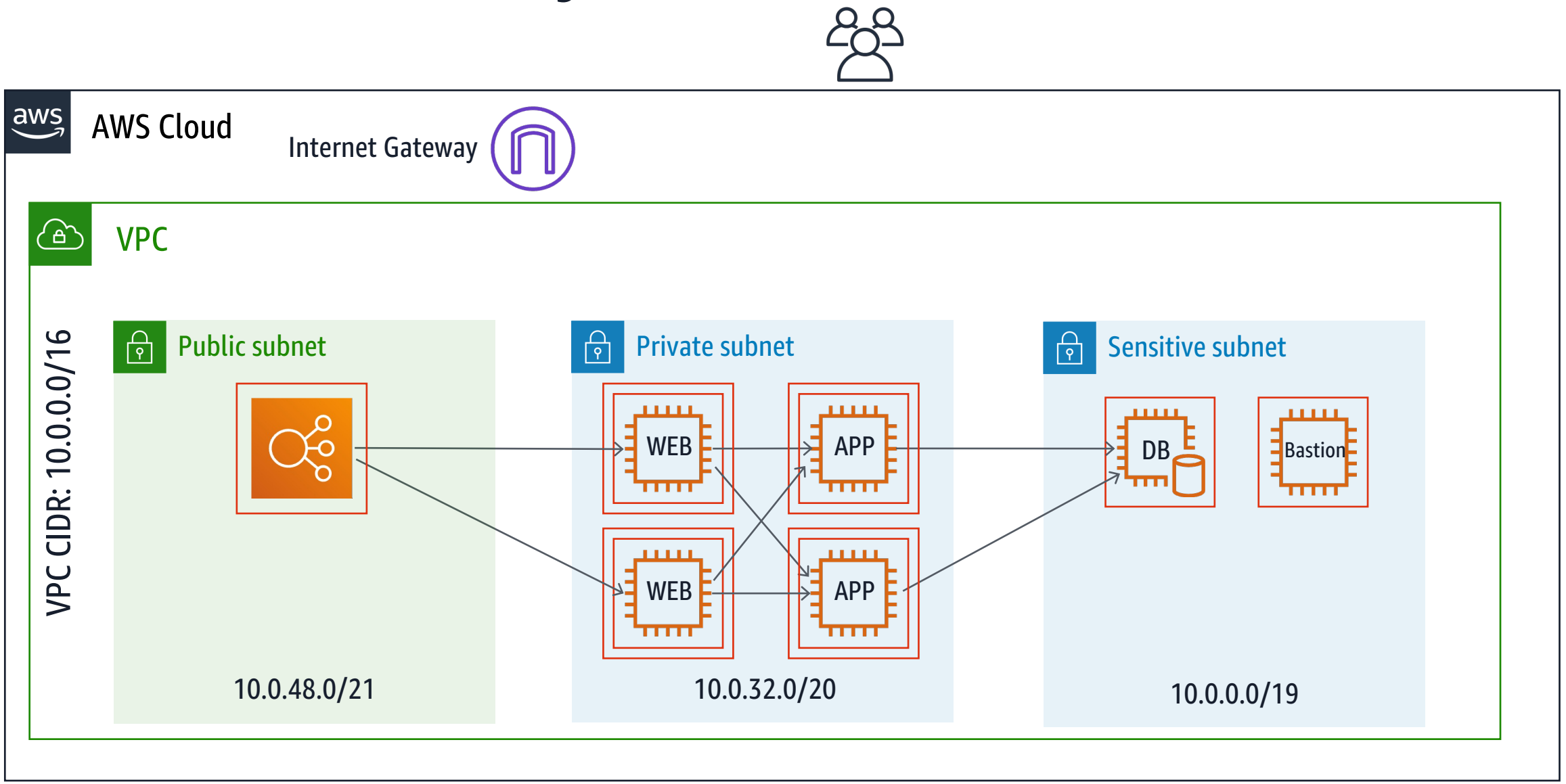
```
[ec2-user@ip-172-31-0-201 ~]$ dig ec2-52-18-10-57.eu-west-1.compute.amazonaws.com

; <<>> 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

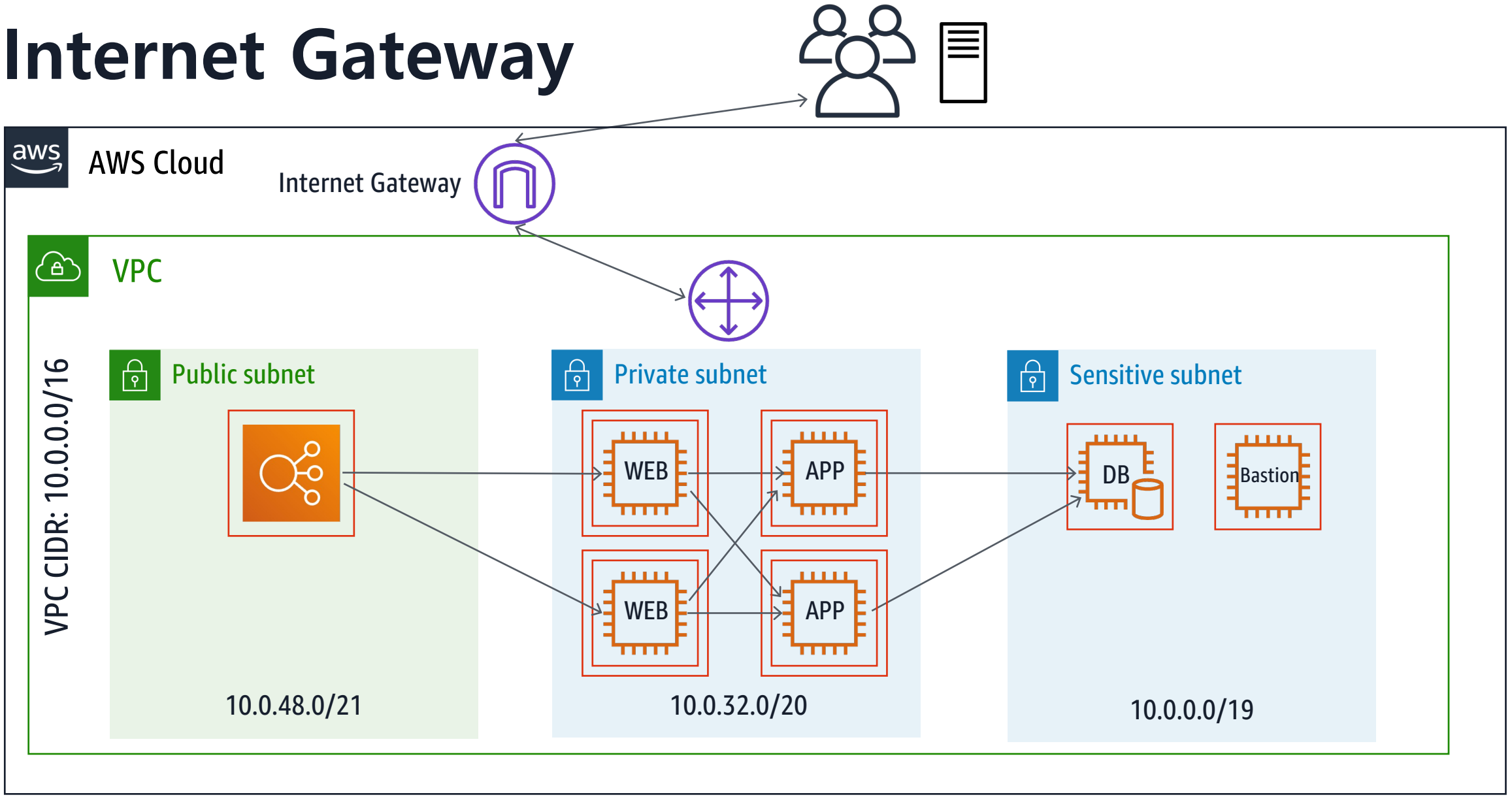
Coneectivity

aws professional services

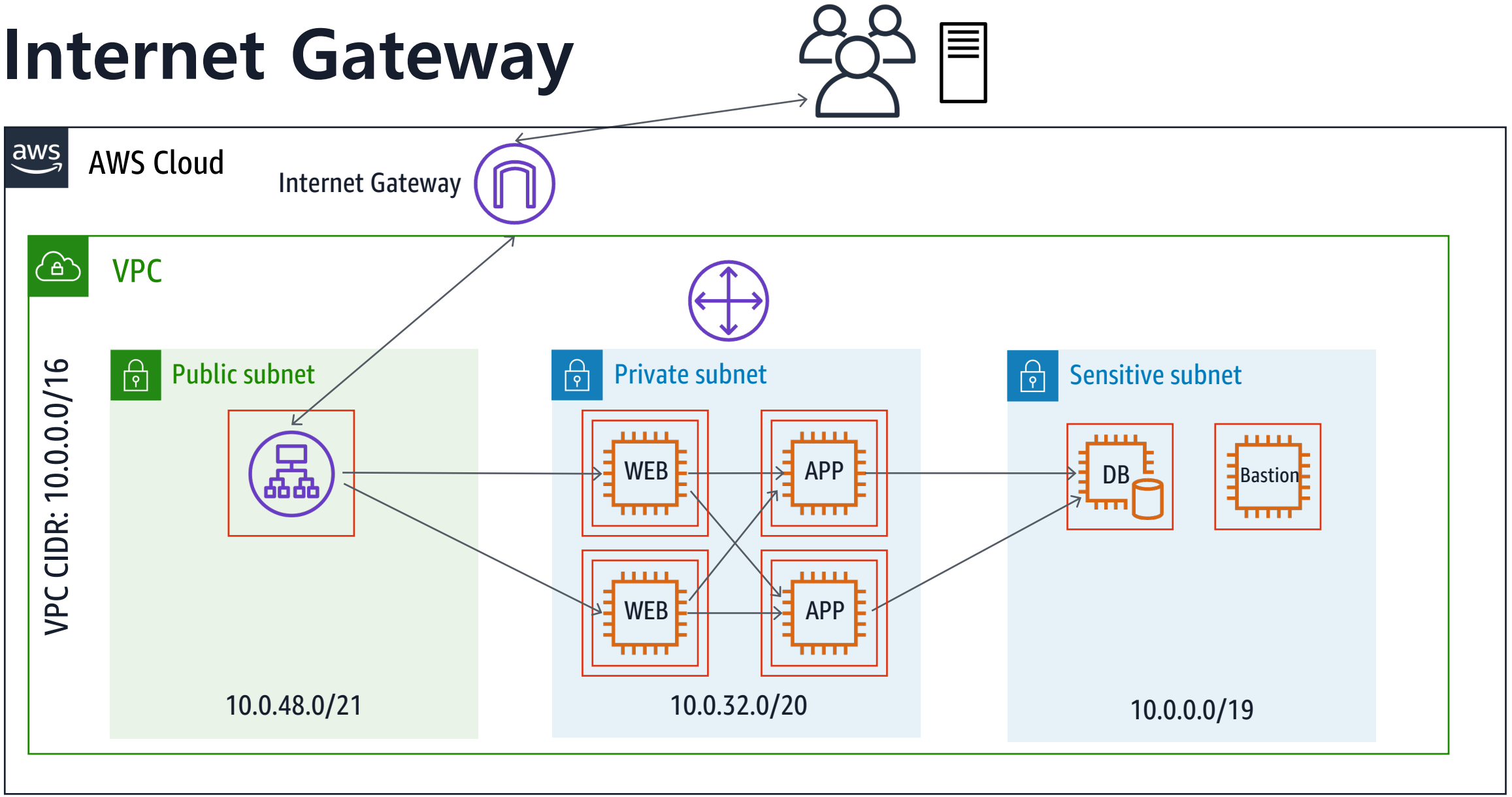
Internet Gateway



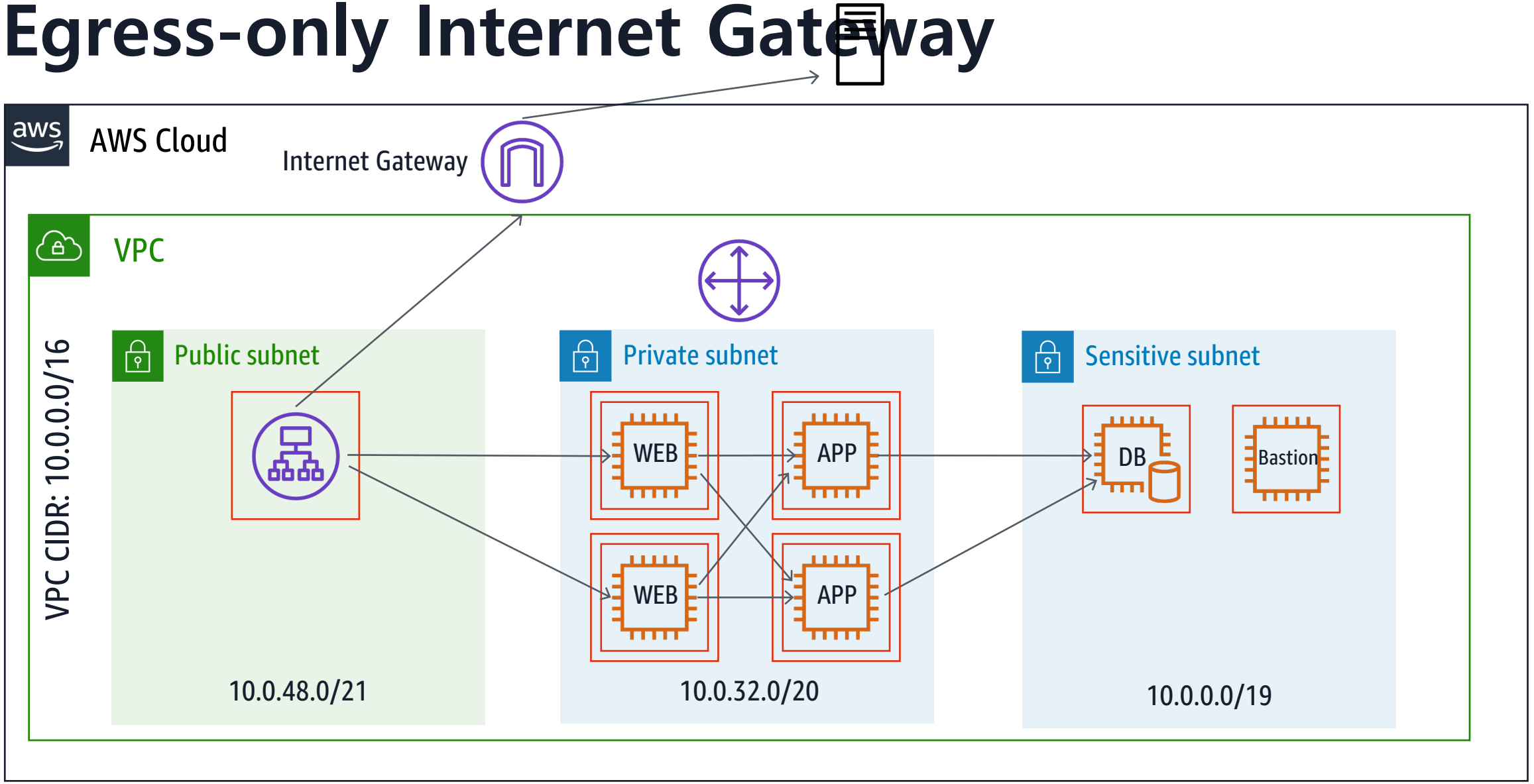
Internet Gateway



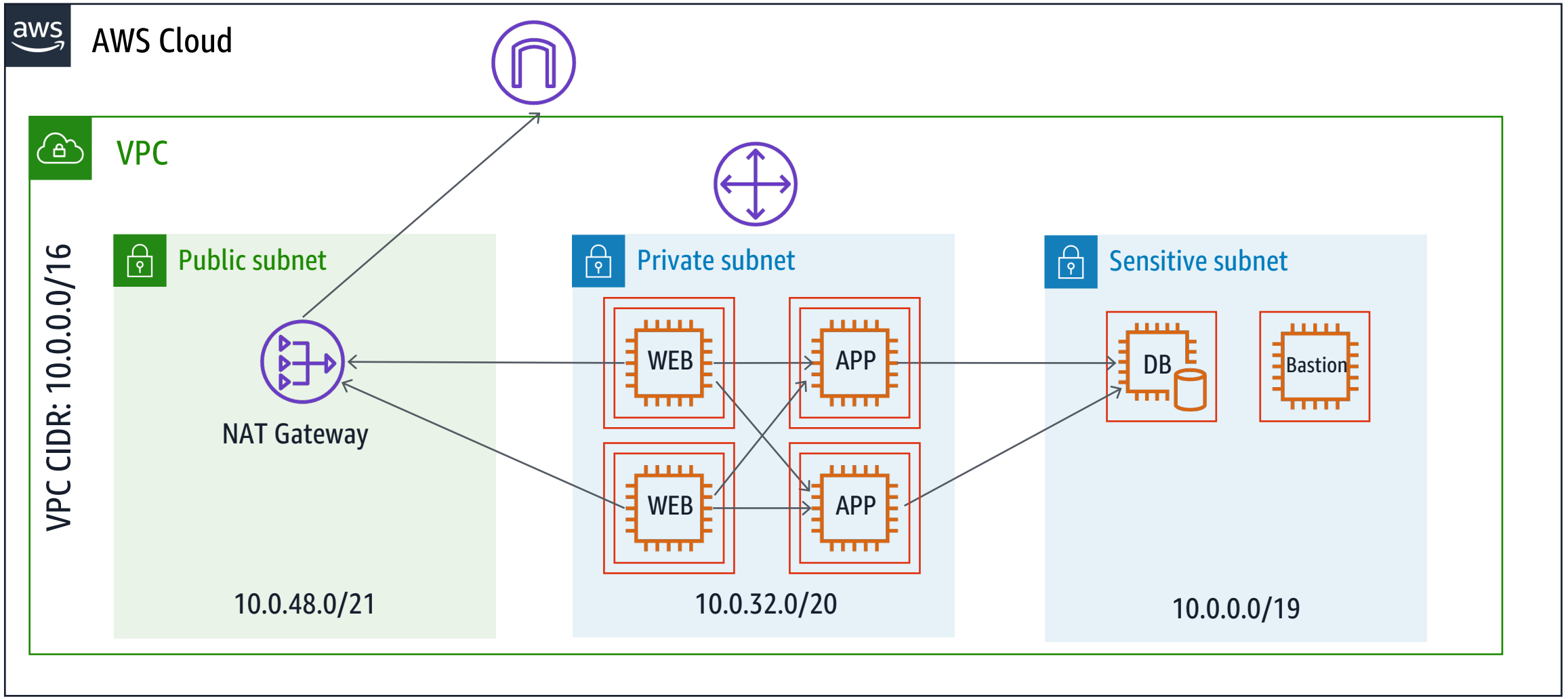
Internet Gateway



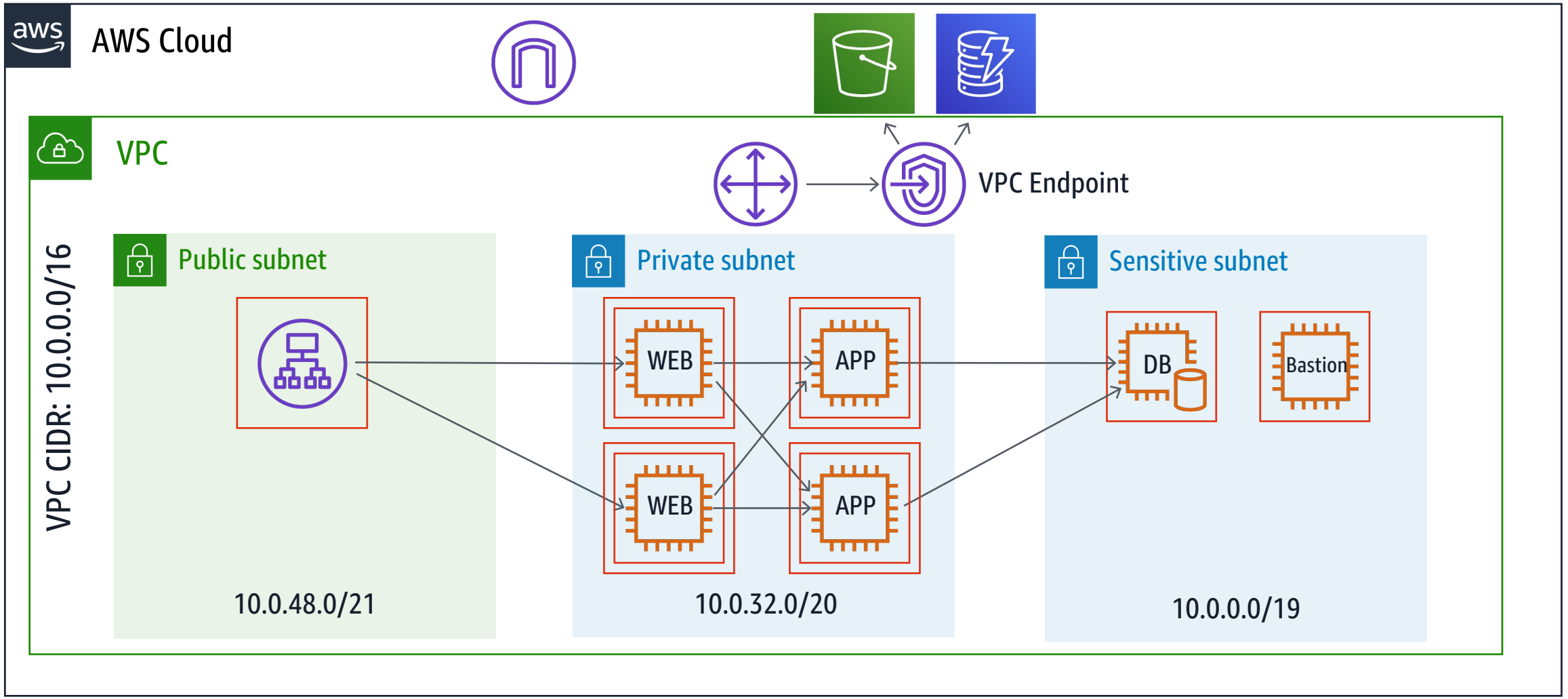
Egress-only Internet Gateway



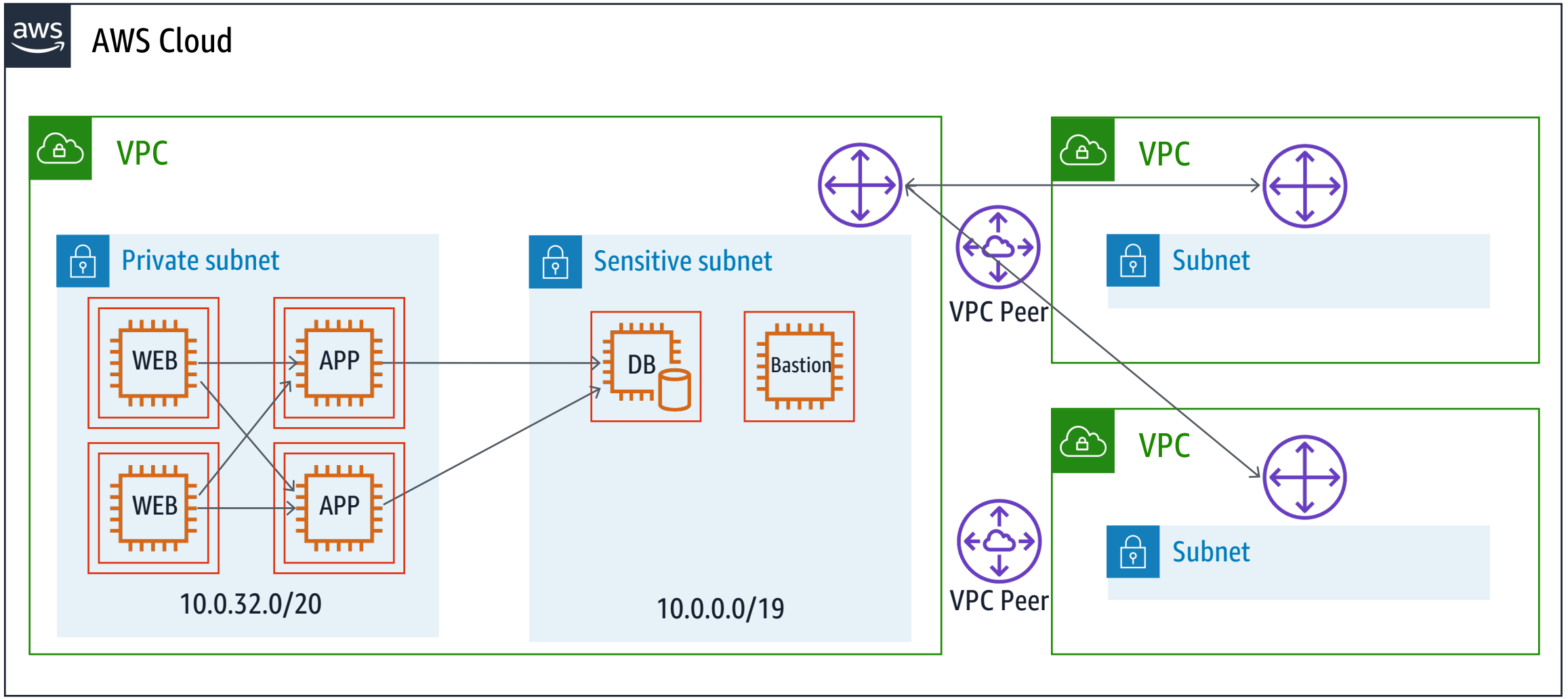
NAT Gateway


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

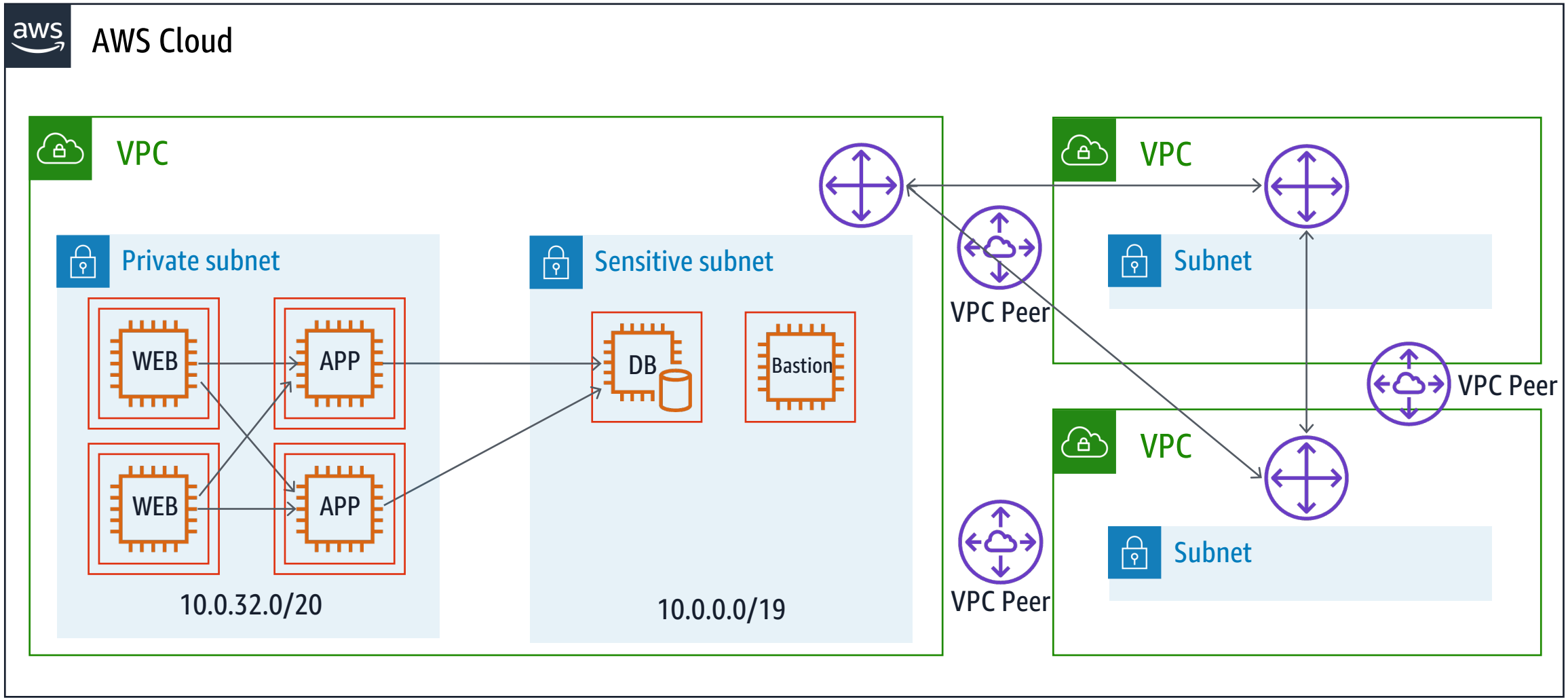
VPC Endpoints



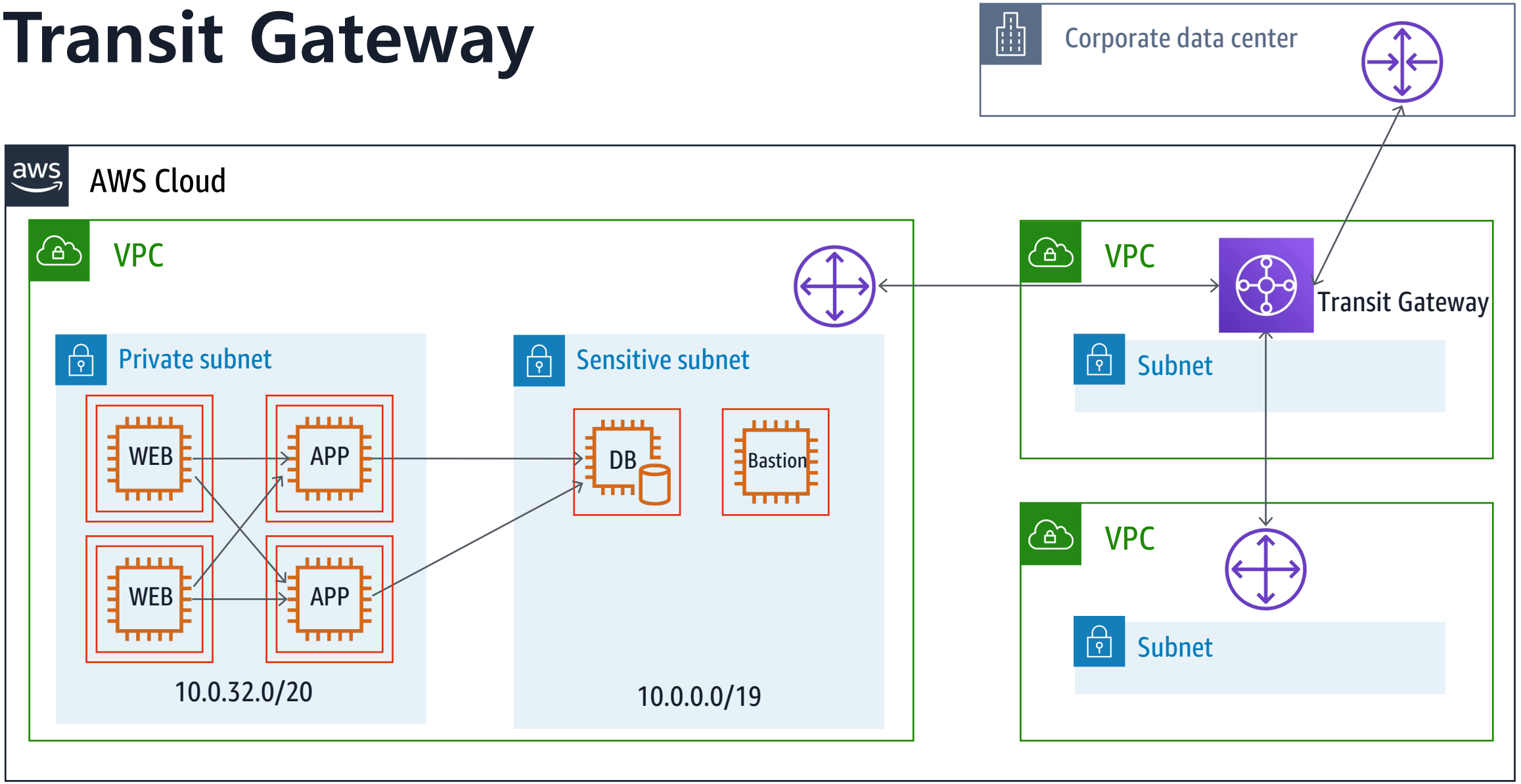
VPC Peering


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

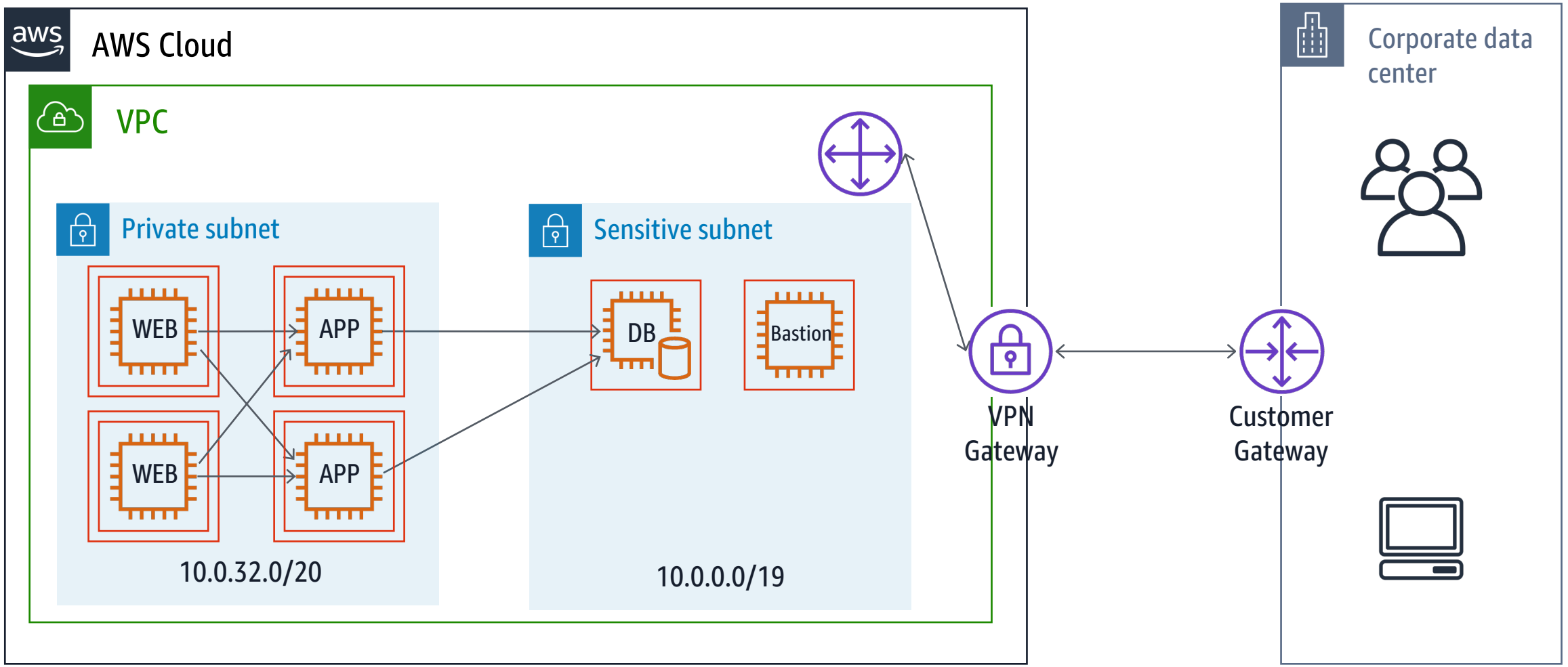
VPC Peering


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

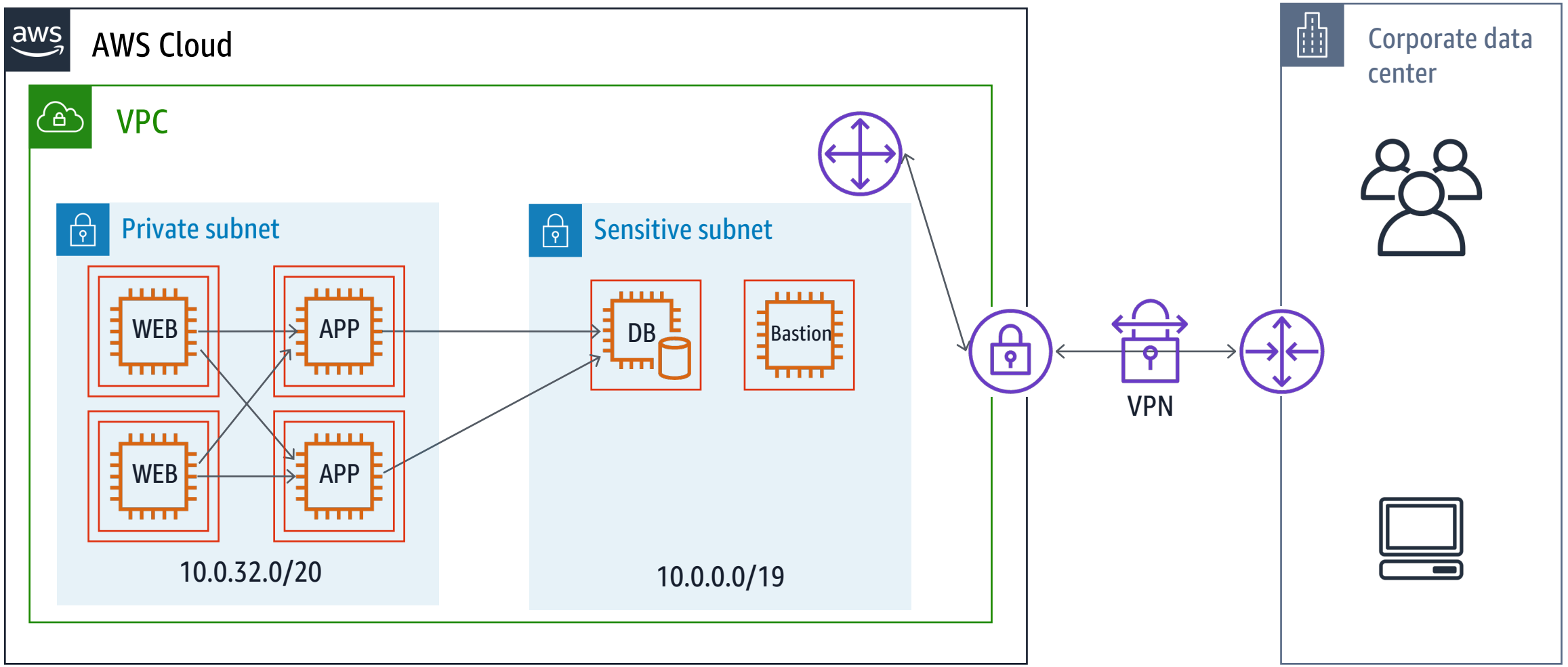
Transit Gateway



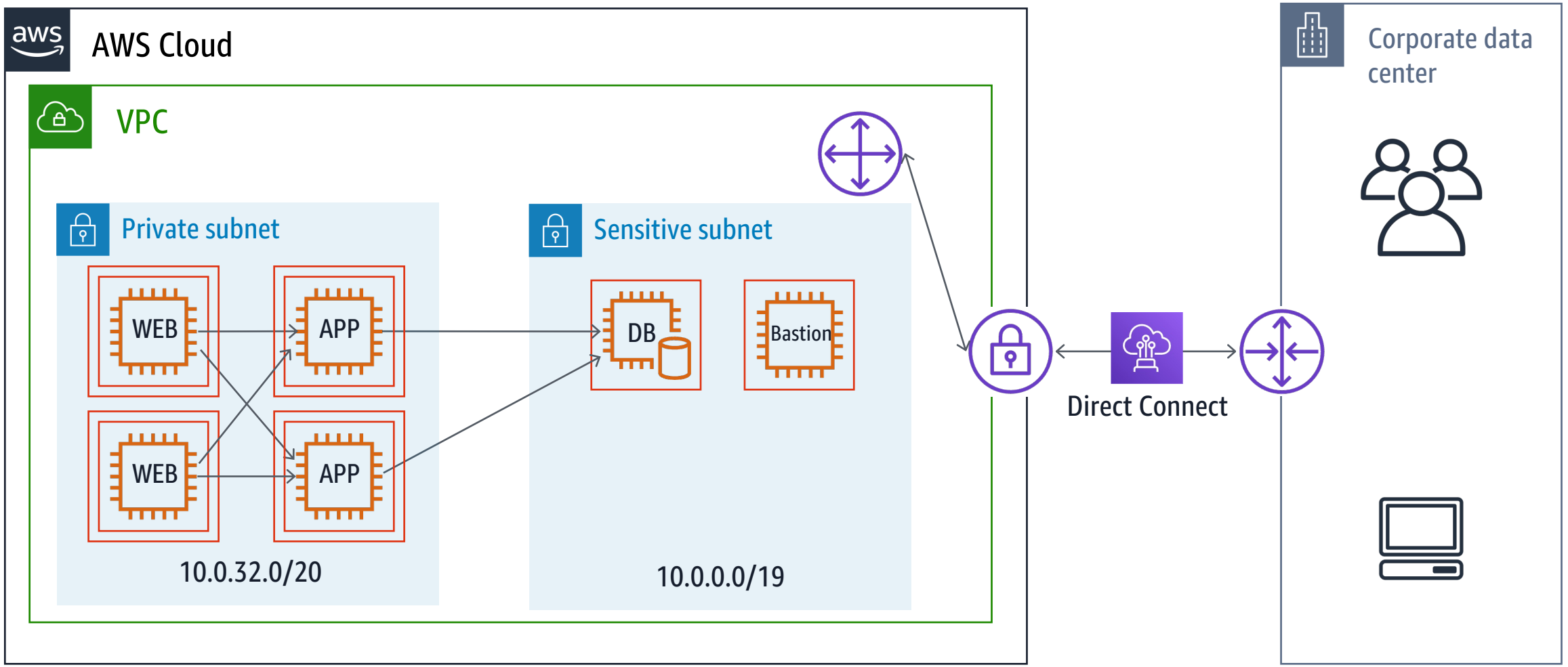
VPN


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

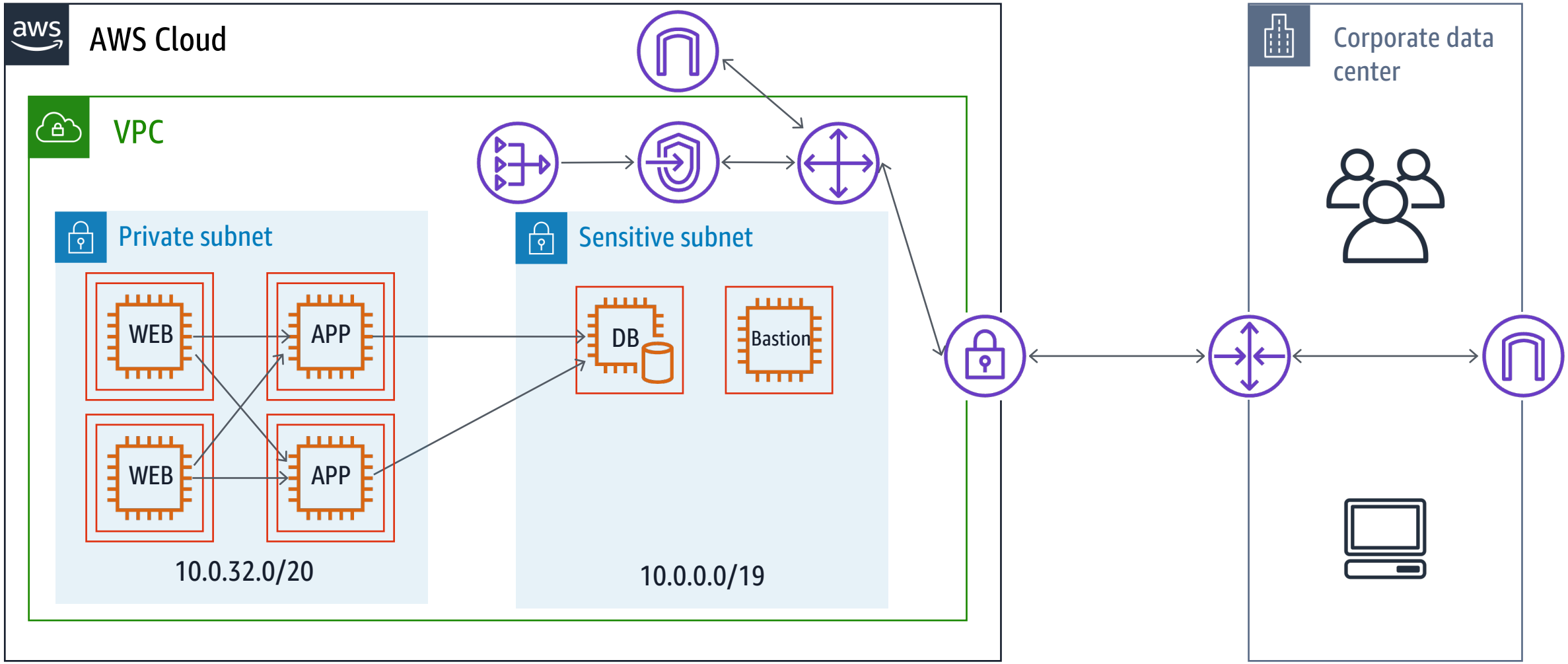
VPN


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

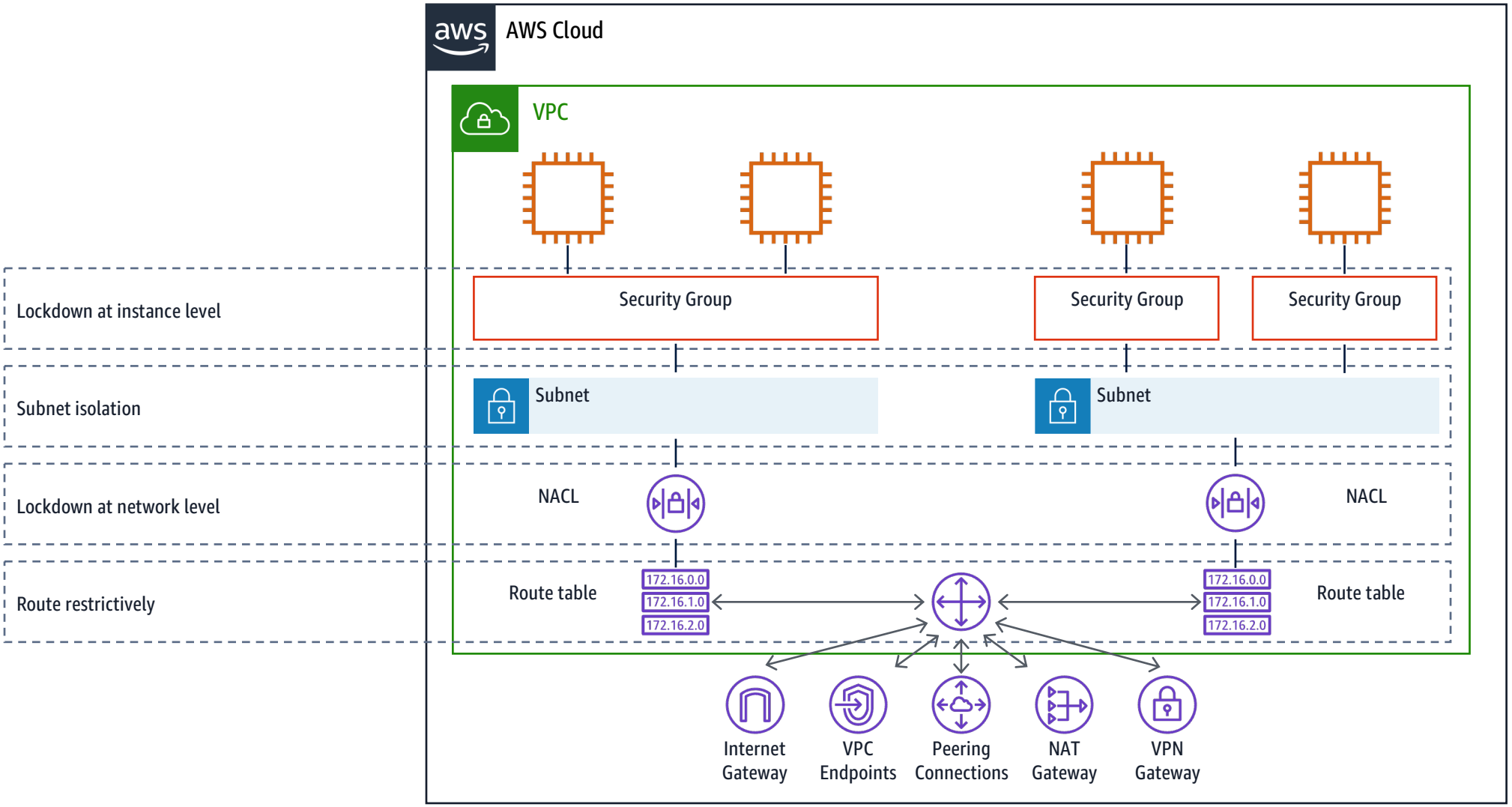
Direct Connect



Multiple Gateways



Network Defense in Depth



감사합니다.