

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)

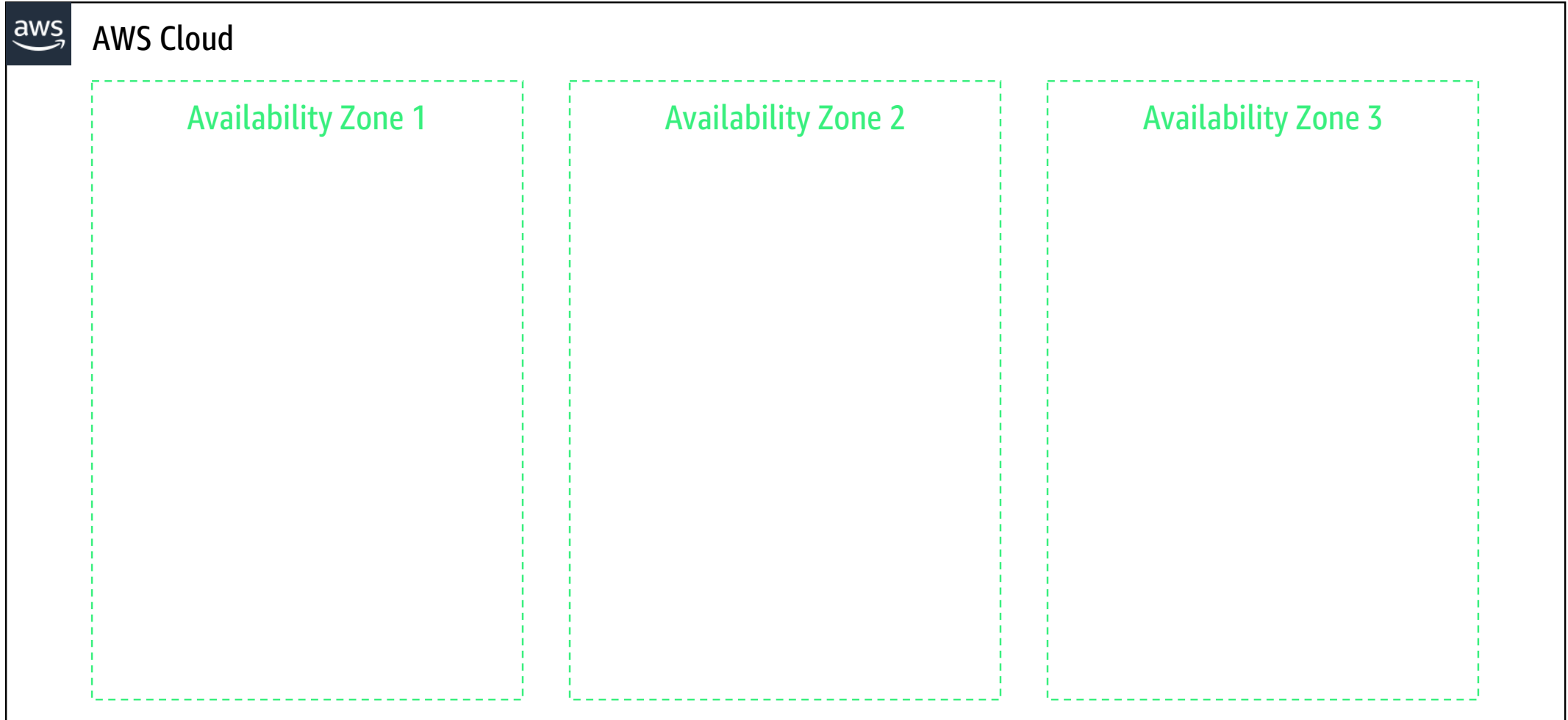
Virtual Private Cloud (VPC)

What is a Virtual Private Cloud?

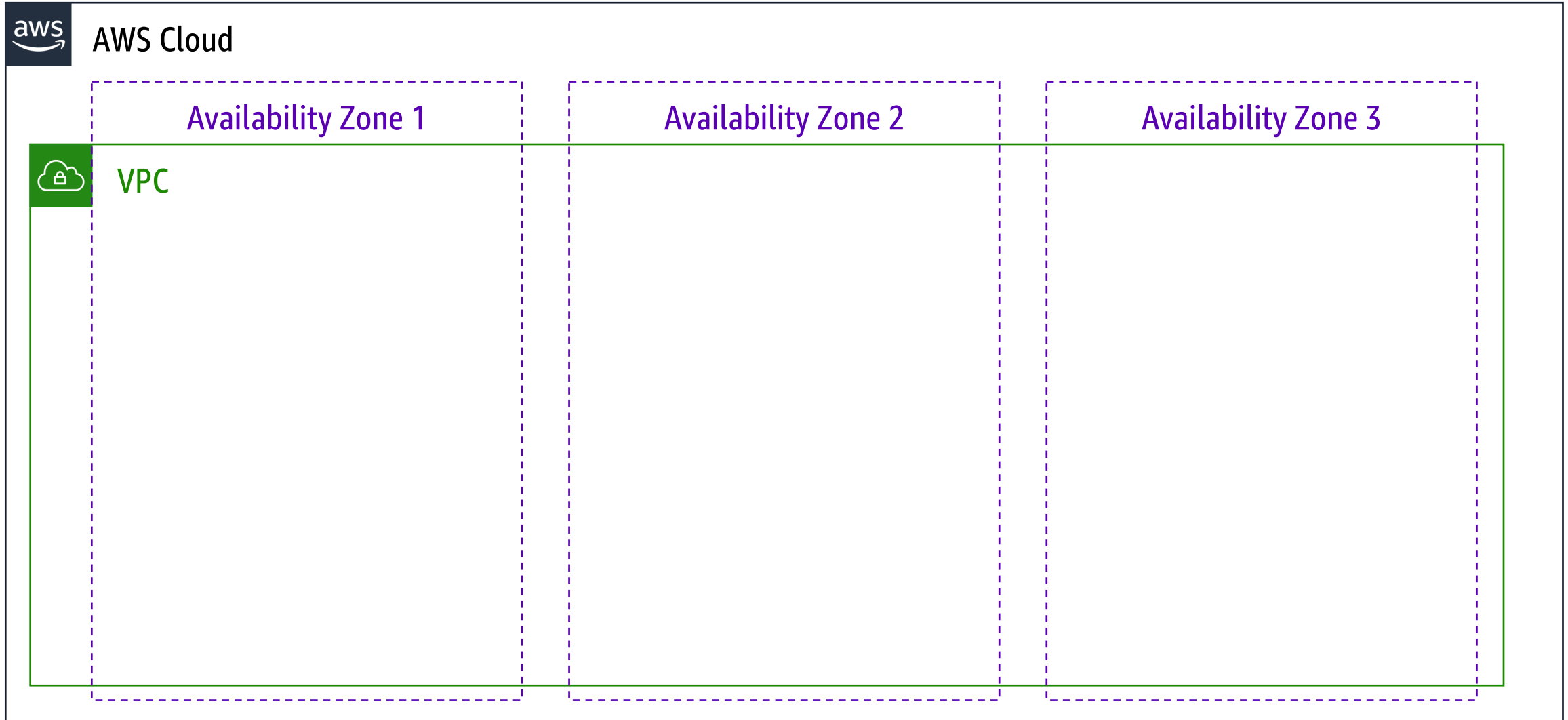
- **Software-defined network**
- **Logically isolated**
- **Complete control**
- **Secure**
- **VPN & Internet connectivity**
- **Connect your on-premises IT environment**



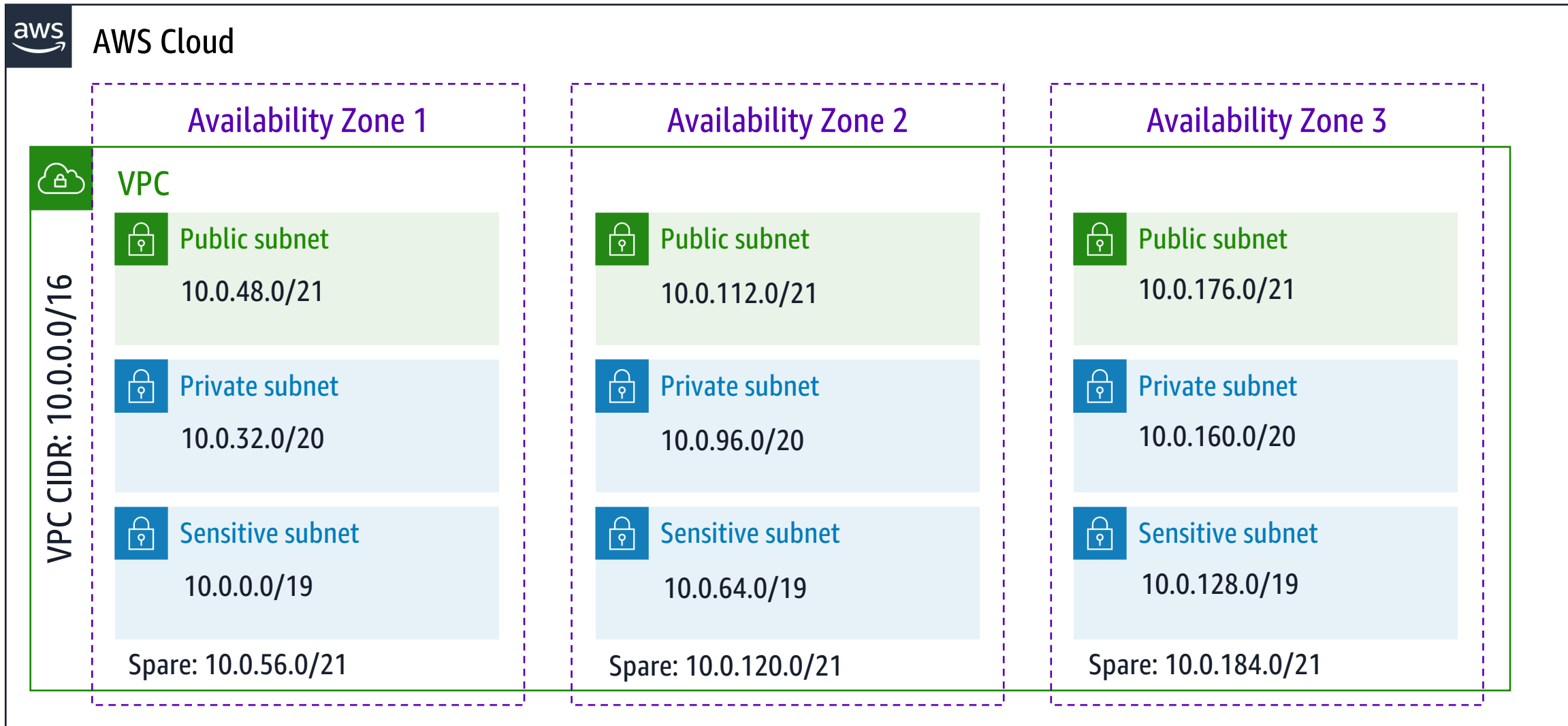
각 AWS 리전에는 여러 가용 영역이 있습니다.



VPC는 리전의 모든 가용 영역에 걸쳐 있습니다.



Subnets



고객은 VPC를 완전하게 제어 할 수 있습니다.



AWS Cloud

Availability Zone 1

Availability Zone 2



VPC

Choose your VPC address range

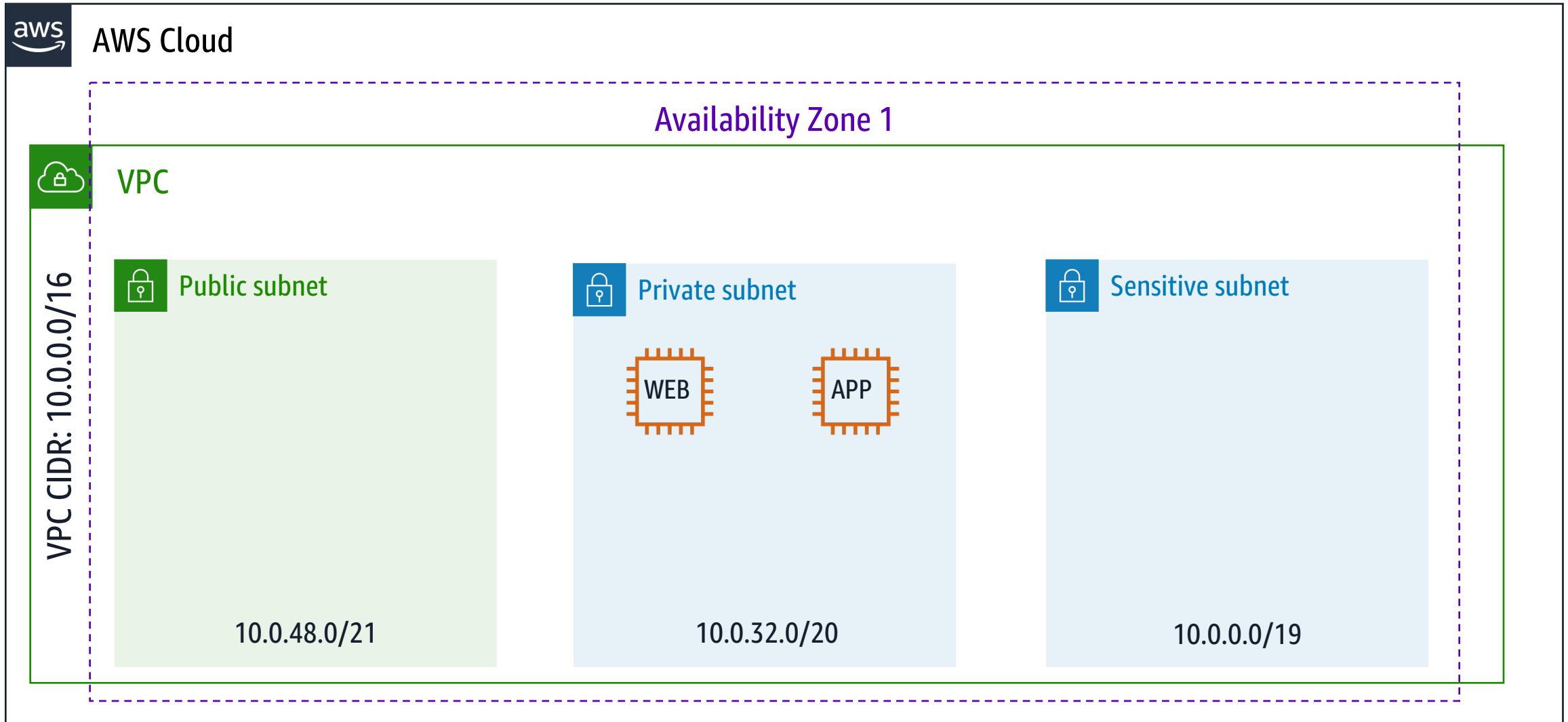
- 모든 VPC에는 프라이빗 IP 주소 공간이 있습니다.(RFC1918이 권장되지만 공개적으로 라우팅 가능한 IPv4 CIDR 범위도 지원됨)
- VPC CIDR 블록 크기는 /16에서 /28까지 가능합니다.
- 추가 IPv4 주소 블록을 연결할 수 있습니다.
- IPv6 주소 블록을 연결할 수 있습니다.

Select IP addressing strategy

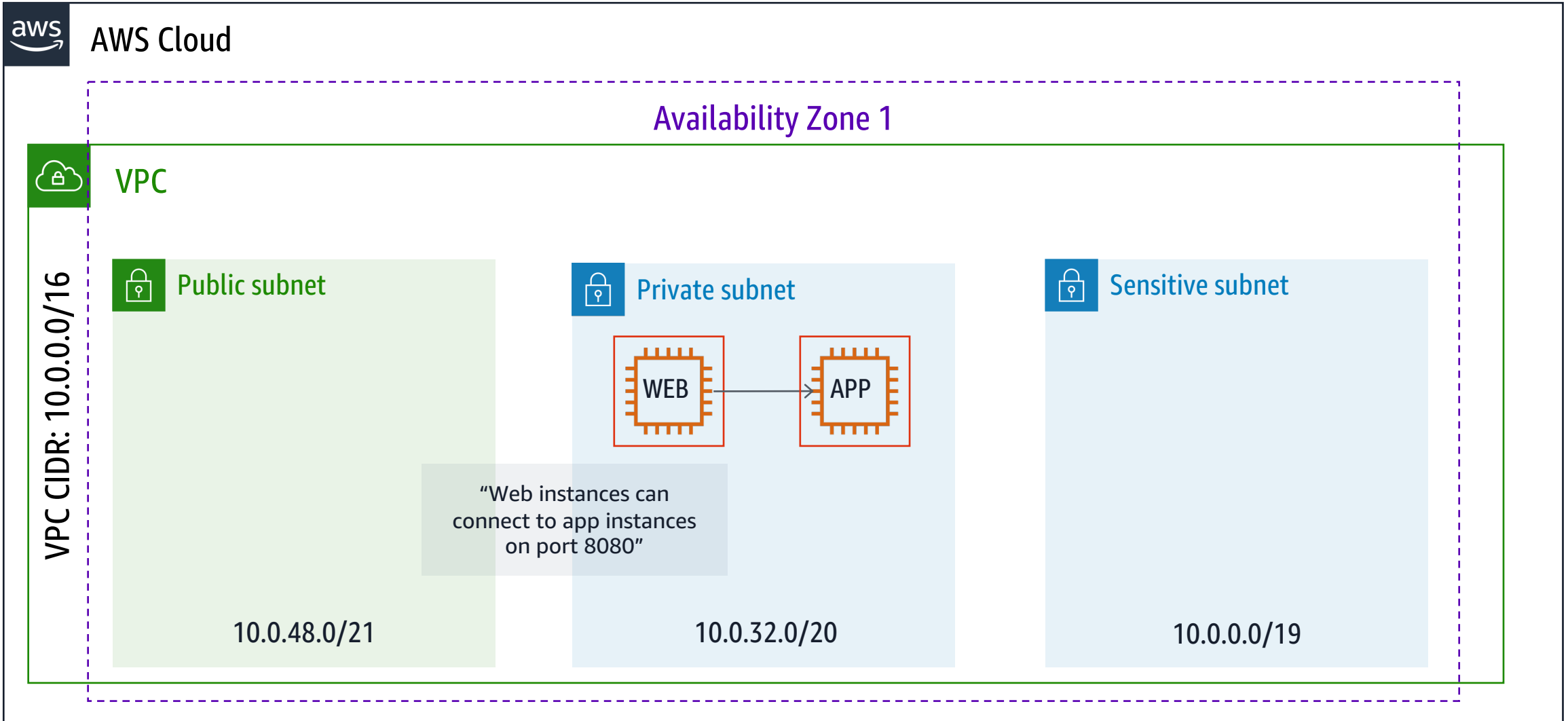
- 기본 VPC CIDR은 생성된 후에는 수정할 수 없으며 추가 공간을 추가할 수 있습니다.
- 라우팅 문제를 방지하려면 자신이 소유한 RFC1918 주소 또는 공용 IP 공간만 사용하는 것이 좋습니다.
- CIDR을 커밋하기 전에 다른 네트워크와의 주소 중복을 고려하십시오.
- 주소 공간을 낭비하지 말고 확장 가능성도 제한하지 마십시오.

Security Groups

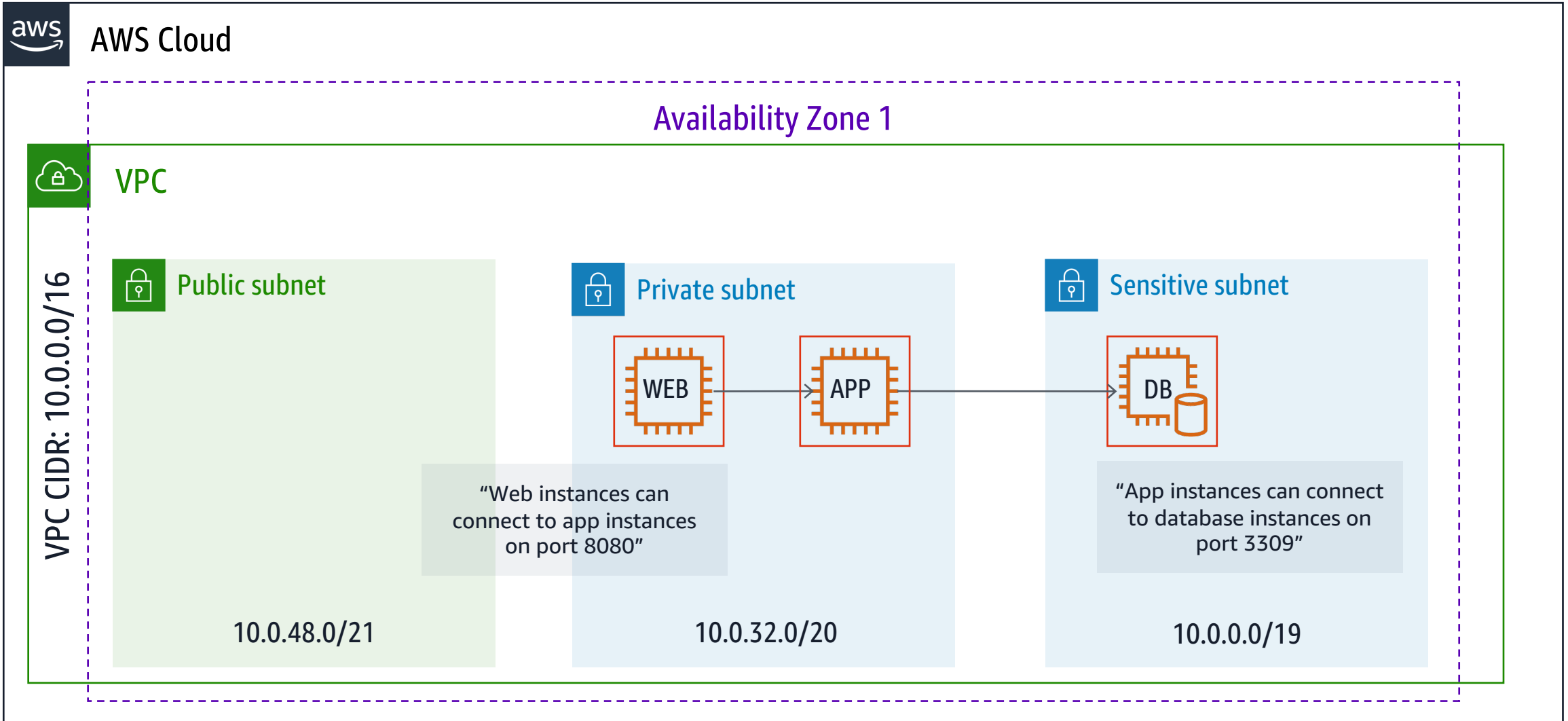
Security Groups – Stateful Firewall



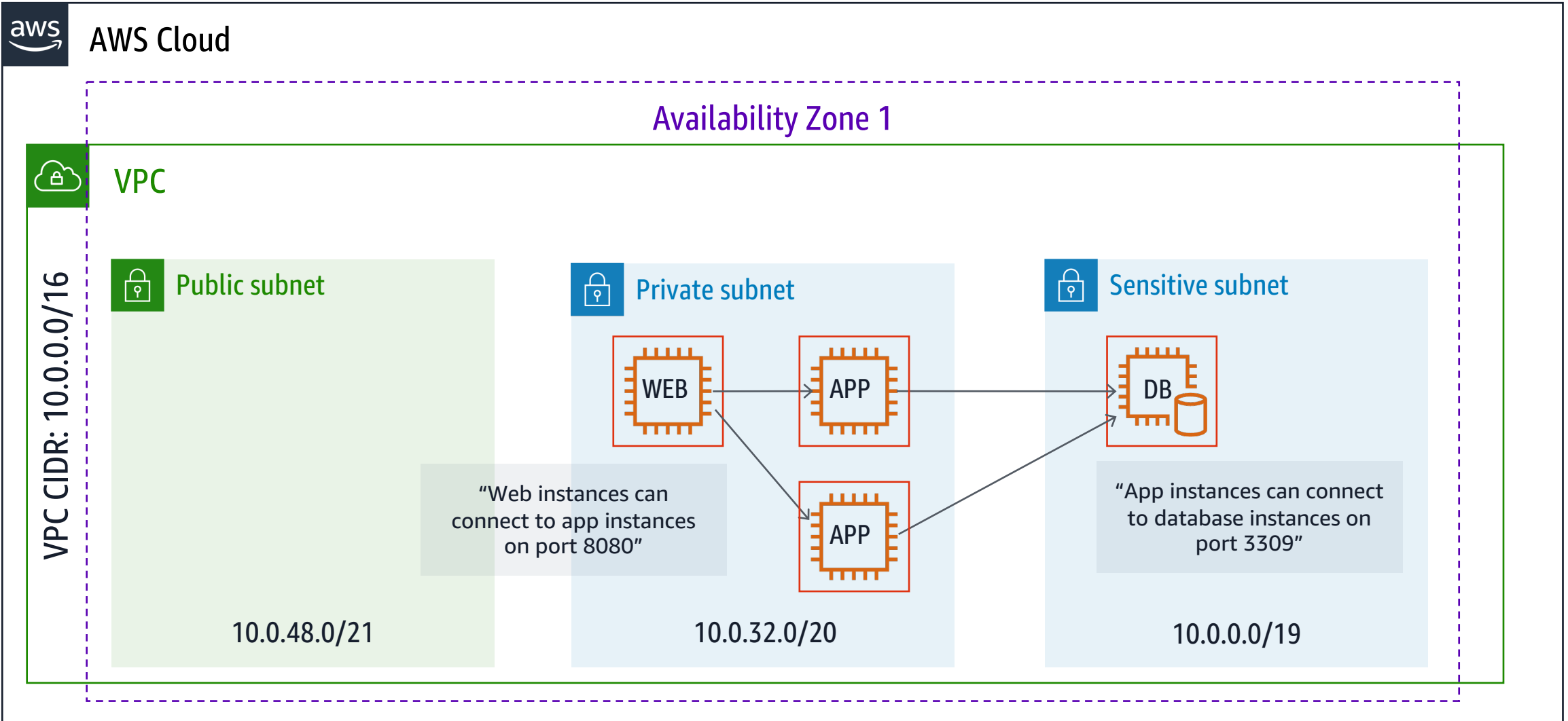
Security Groups – Stateful Firewall



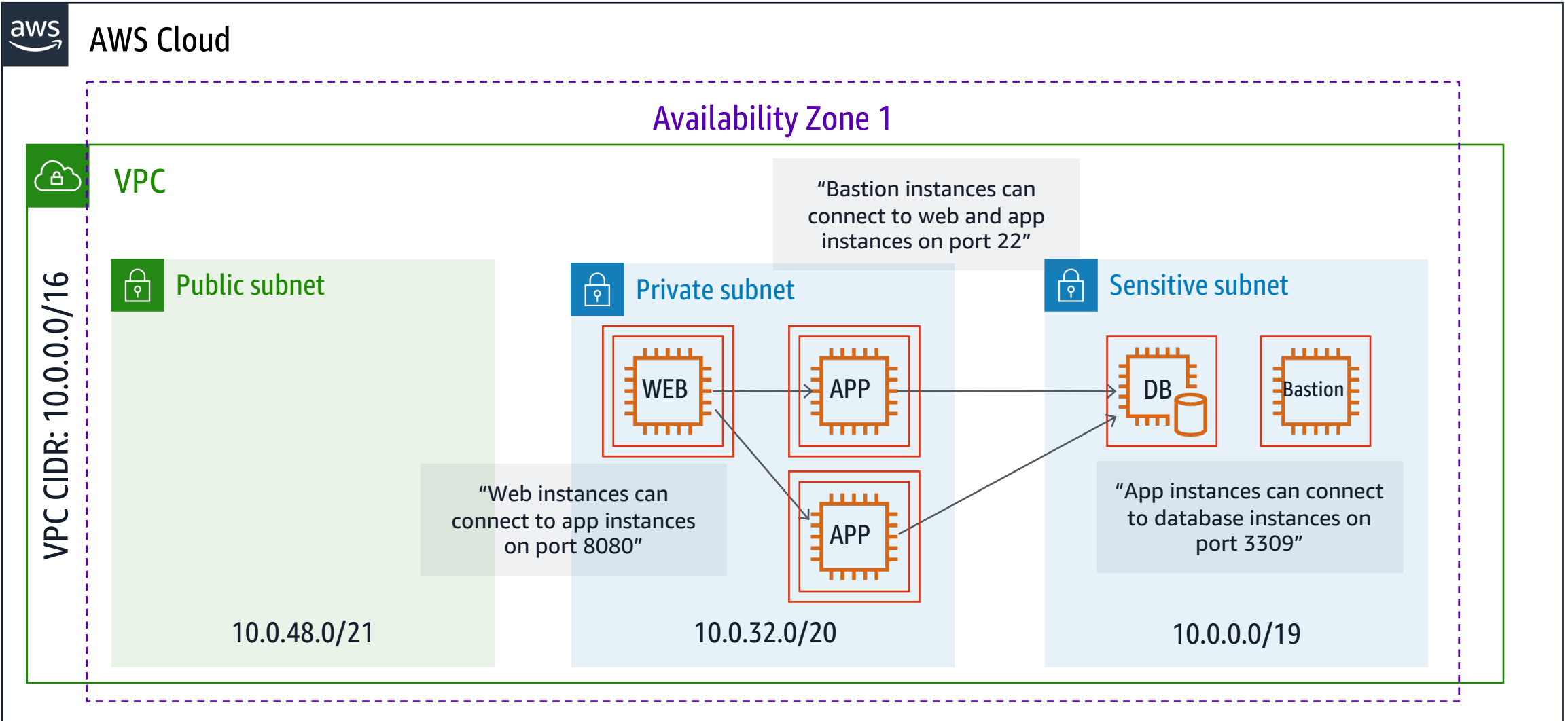
Security Groups – Stateful Firewall



Security Groups – Stateful Firewall



Security Groups – Stateful Firewall



Routing, NACLs's, and Load Balancing

Routing



AWS Cloud

Availability Zone 1



VPC

VPC CIDR: 10.0.0.0/16



Public subnet

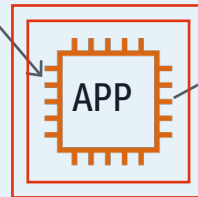
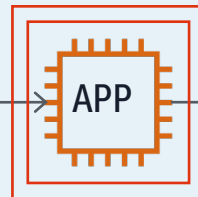
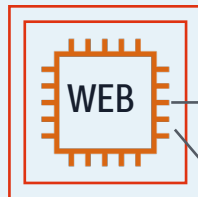
10.0.48.0/21



VPC Router



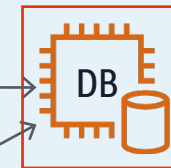
Private subnet



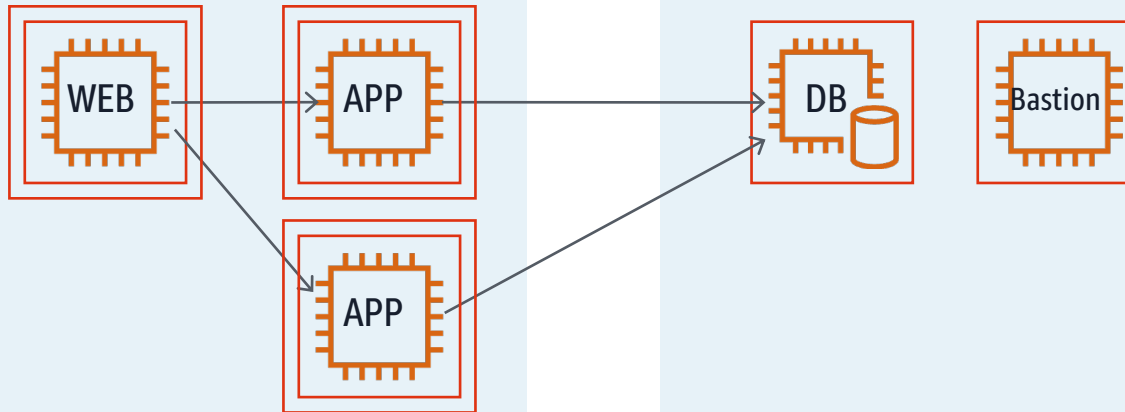
10.0.32.0/20



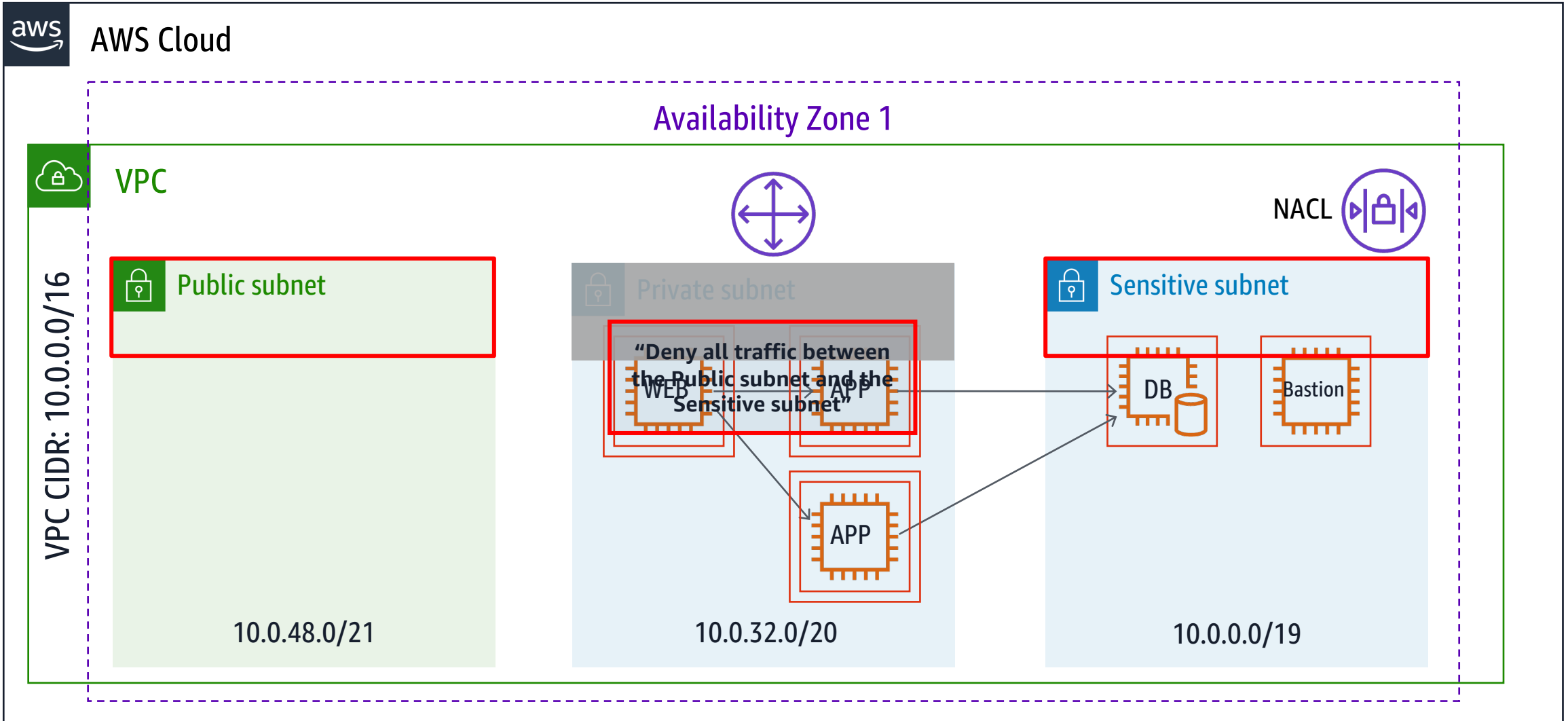
Sensitive subnet



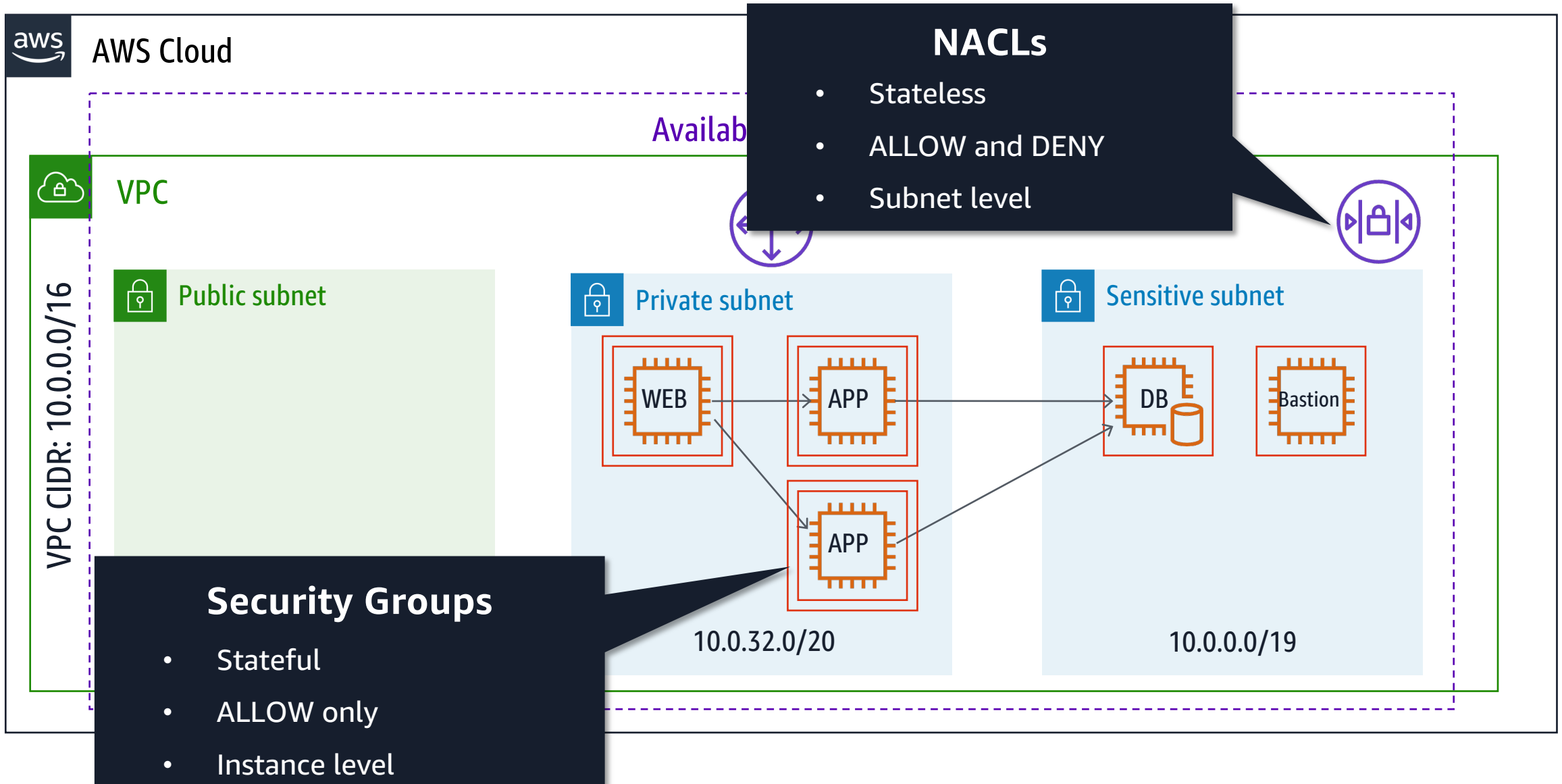
10.0.0.0/19



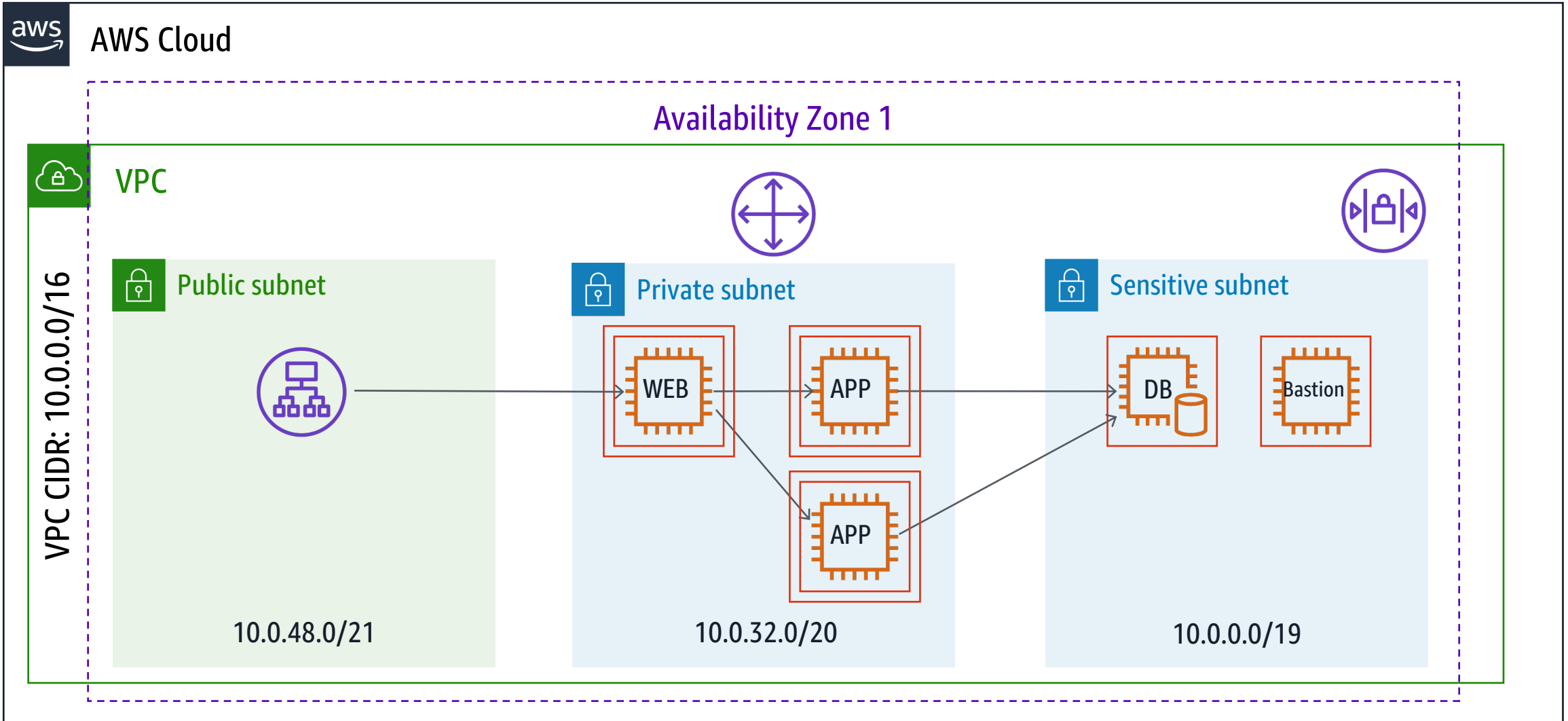
Network Access Control List (NACL)



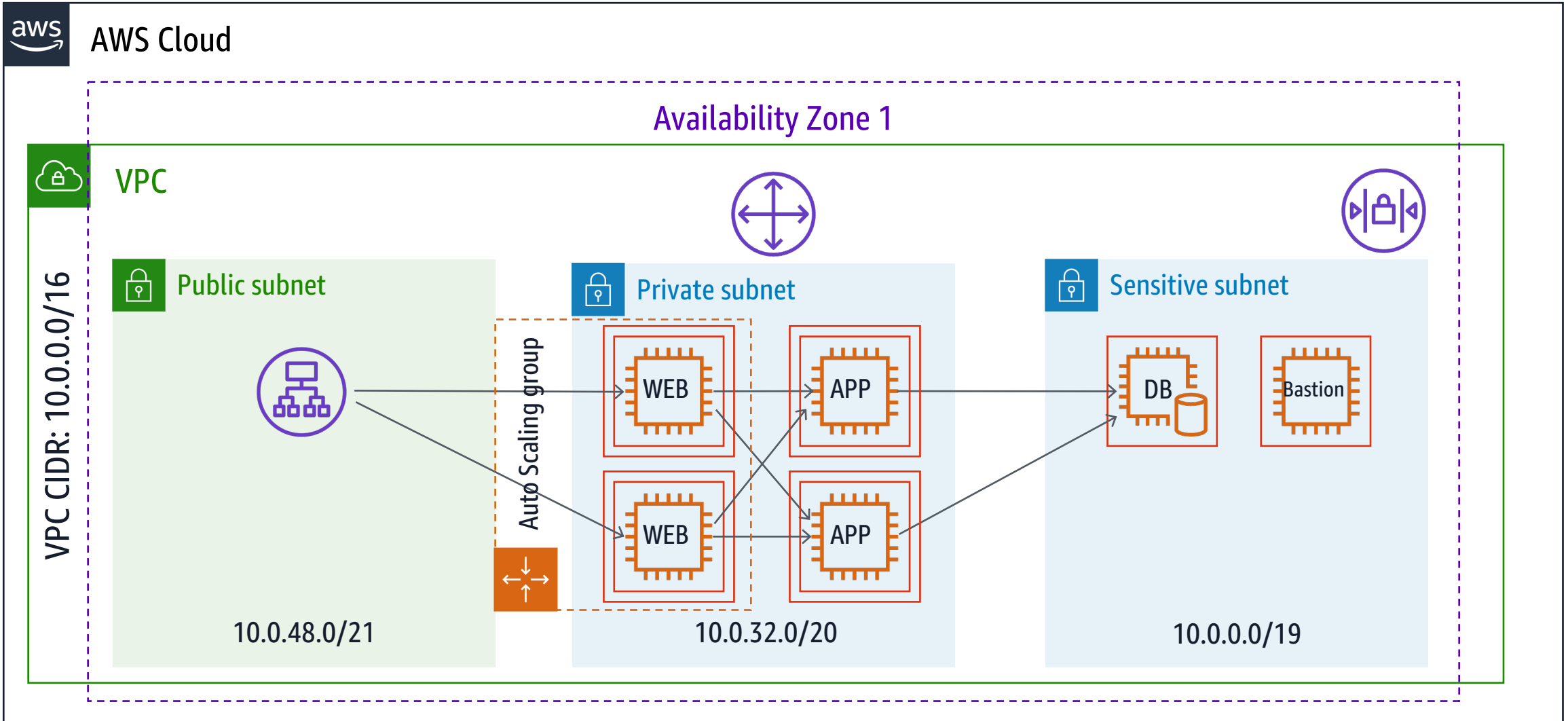
NACLs and Security Groups



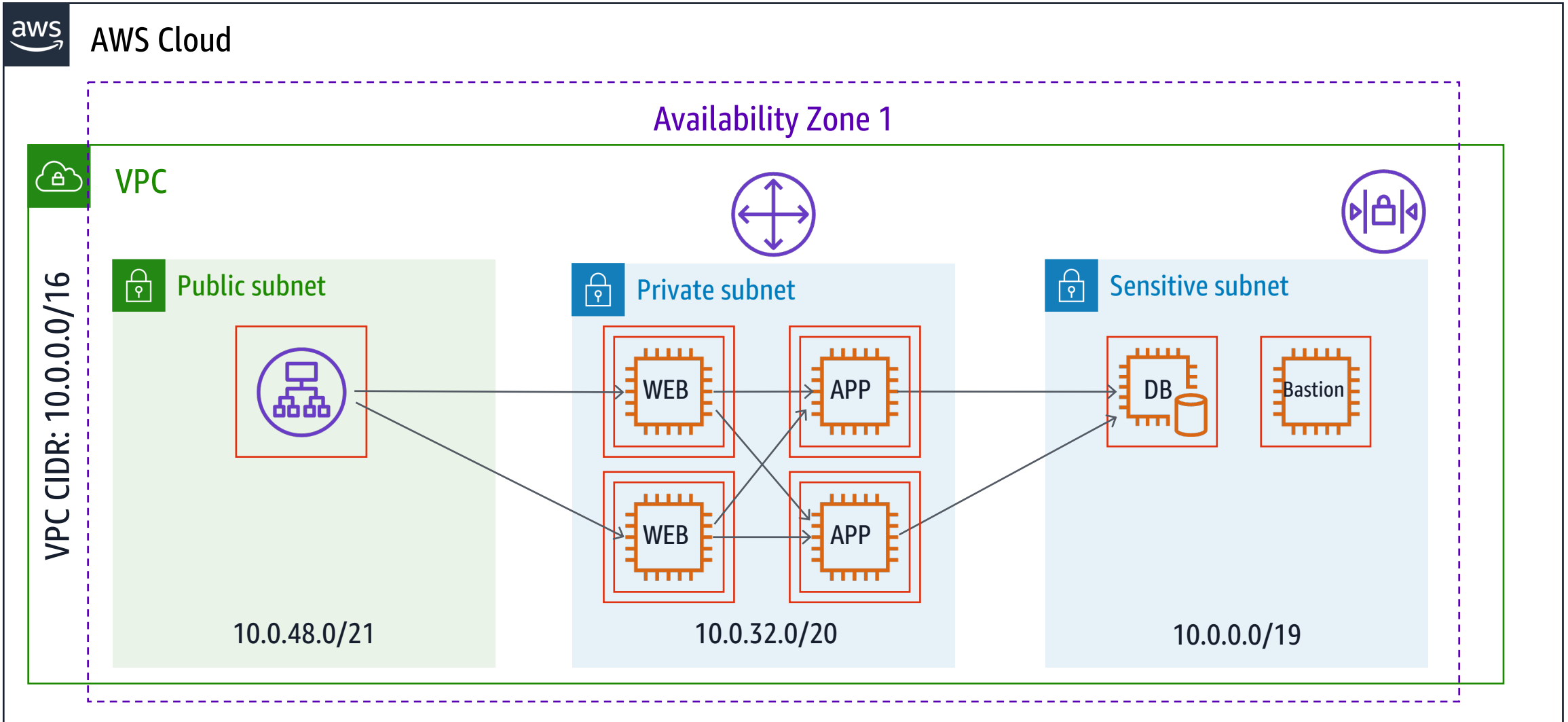
Load Balancing







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

VPC DNS Options

The screenshot shows the AWS Management Console interface for a VPC named 'Demo VPC' (ID: vpc-327d1857). The 'Summary' tab is selected, displaying the following details:

- 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

Two callouts highlight specific DNS settings:

- A callout pointing to the 'DHCP options set' field states: "Have EC2 auto-assign DNS hostnames to instances".
- A callout pointing to the 'DNS resolution: yes' and 'DNS hostnames: yes' status indicates: "Use Amazon DNS server".

The status 'DNS resolution: yes' and 'DNS hostnames: yes' are circled in the image.

EC2 DNS Hostnames

Internal DNS hostname:
Resolves to Private IP address

External DNS name:
Resolves to...

ec2-52-19-188-57.eu-west-1.compute.amazonaws.com

Description

Status Checks

Monitoring

Logs

Instance ID i-a343
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

Public DNS ec2-52-19-188-57.eu-west-1.compute.amazonaws.com

Public IP 52.19.188.57

Elastic IP -

Availability zone eu-west-1a

Security groups [default](#) [view rules](#)

Scheduled events [No scheduled events](#)

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



AWS Cloud

Internet Gateway

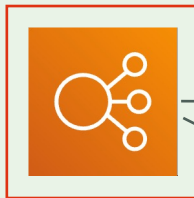


VPC

VPC CIDR: 10.0.0.0/16



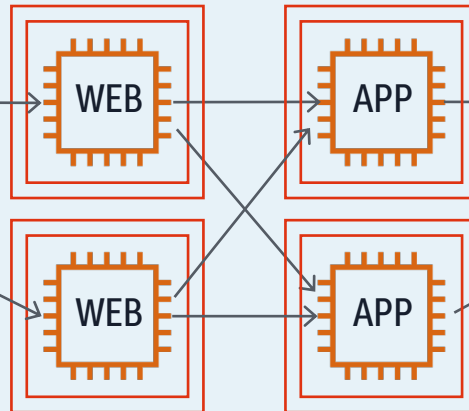
Public subnet



10.0.48.0/21



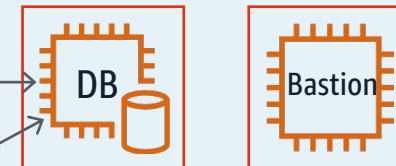
Private subnet



10.0.32.0/20

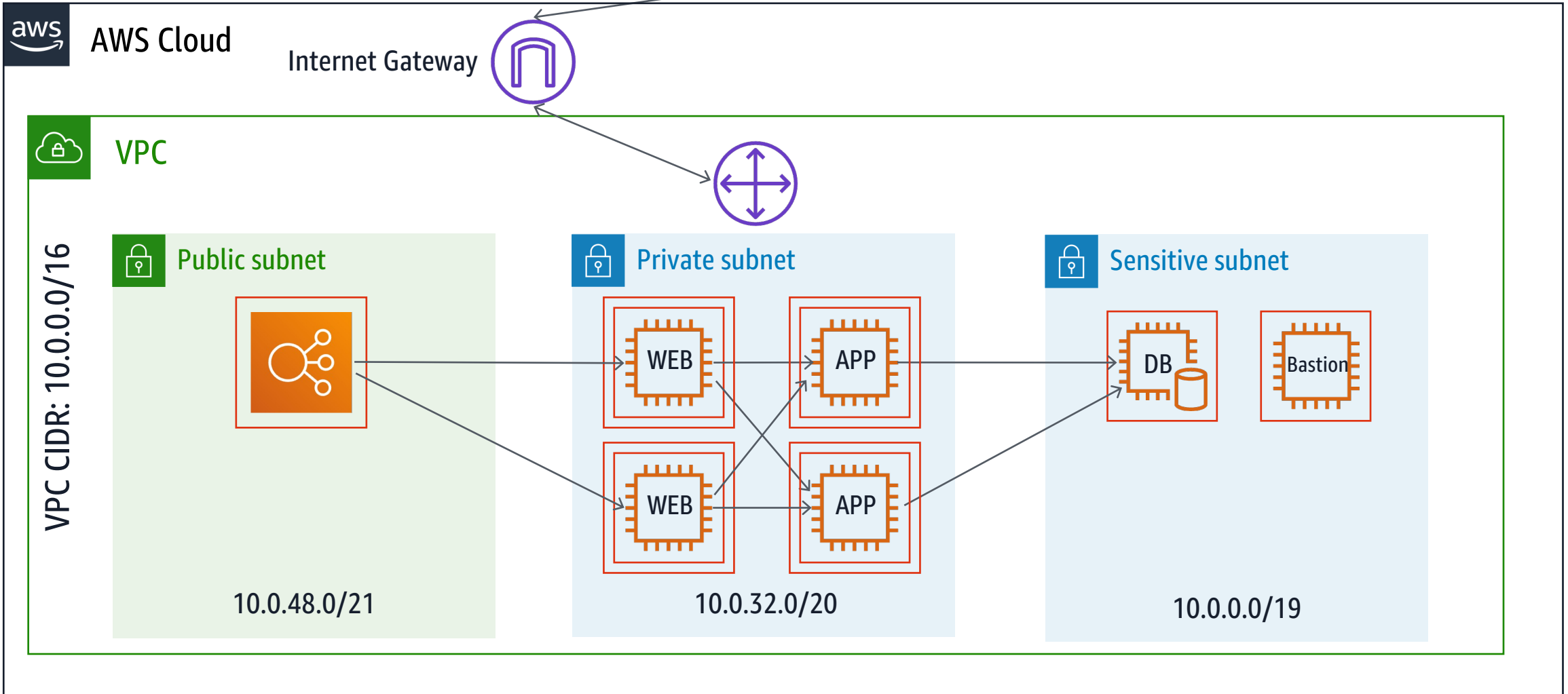
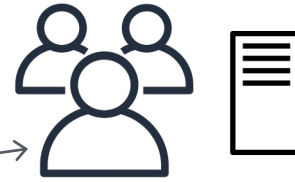


Sensitive subnet

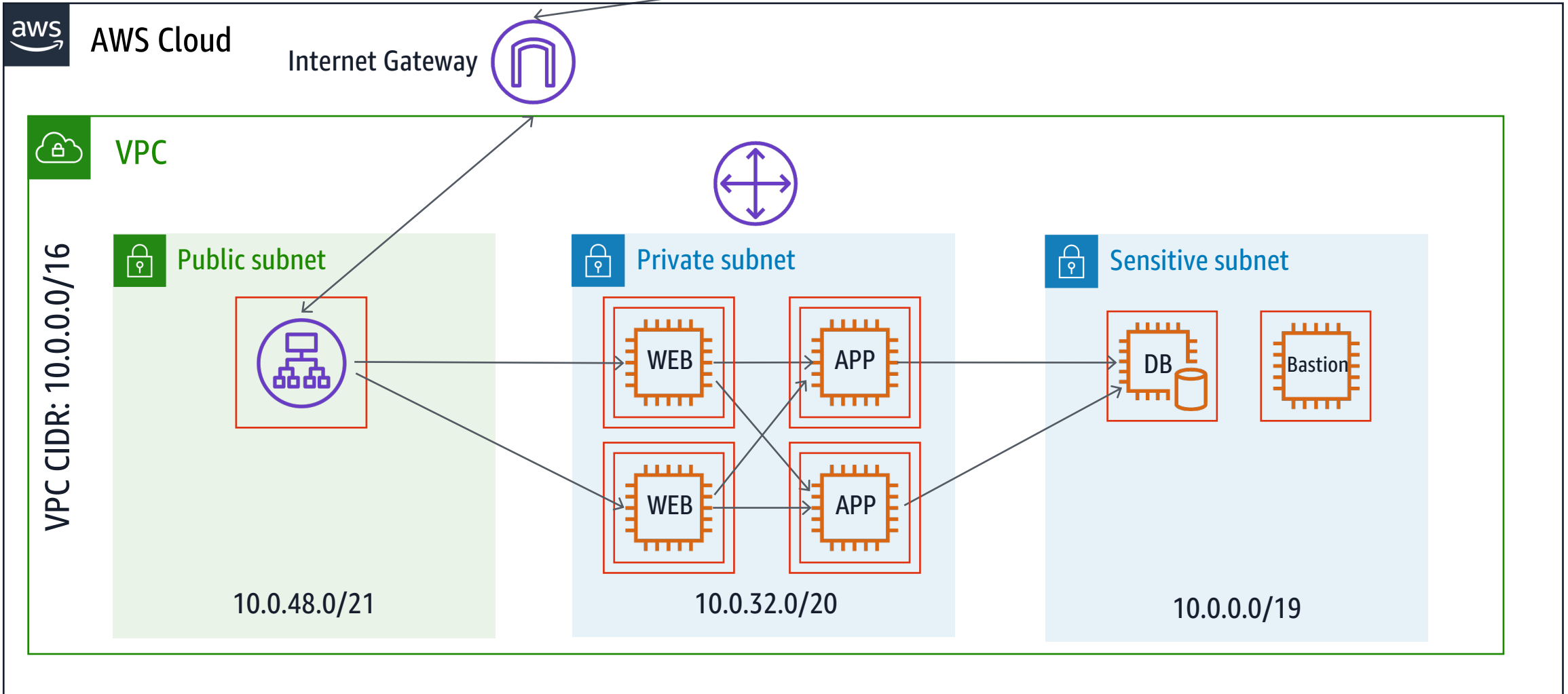
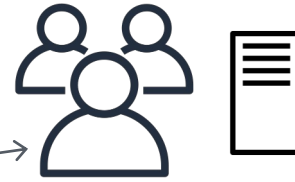


10.0.0.0/19

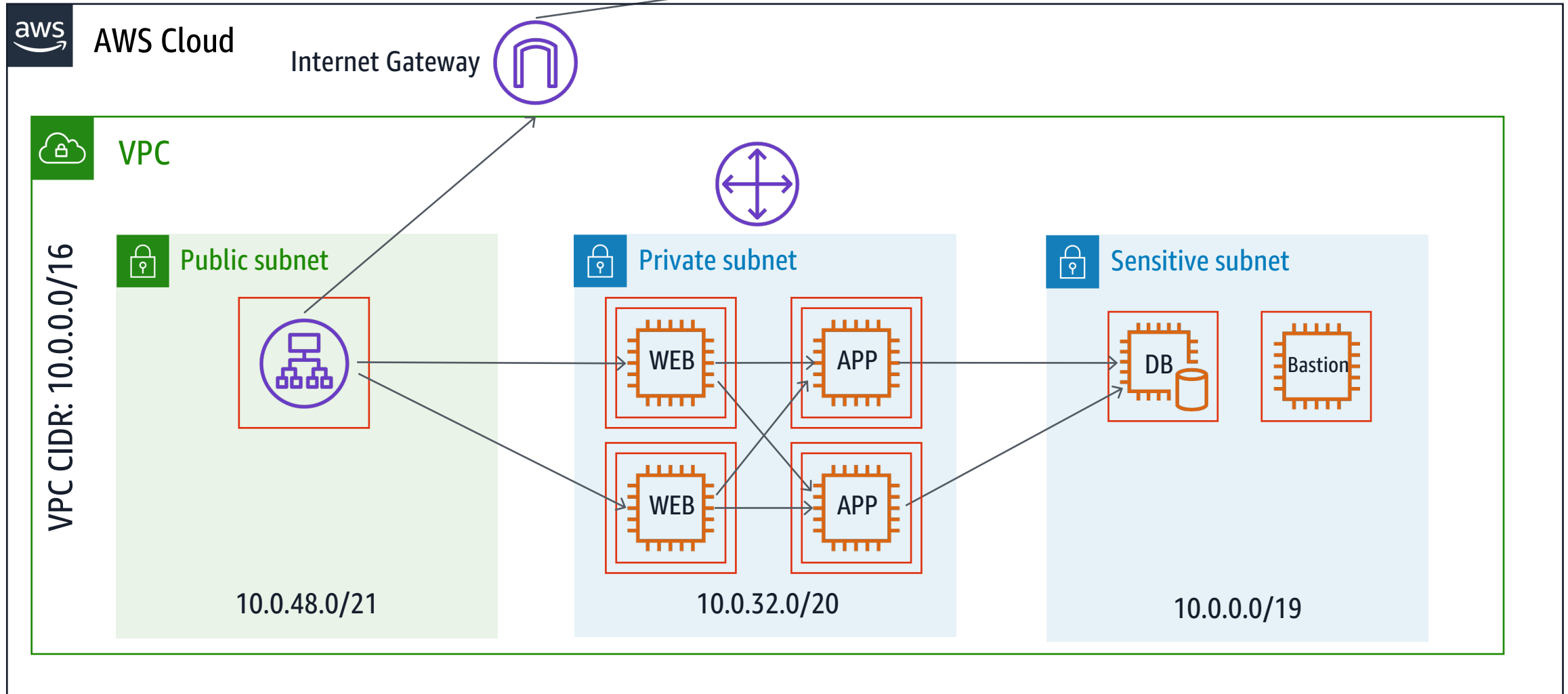
Internet Gateway



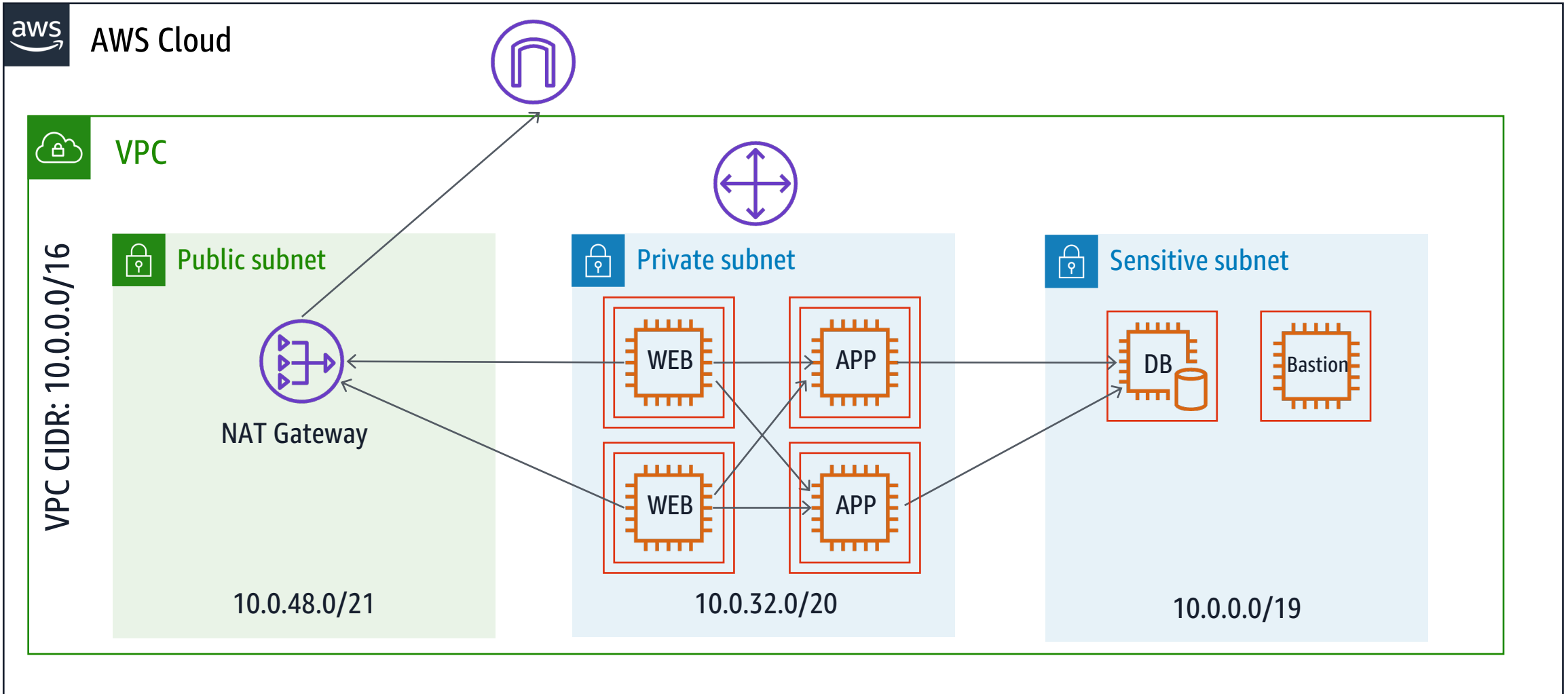
Internet Gateway



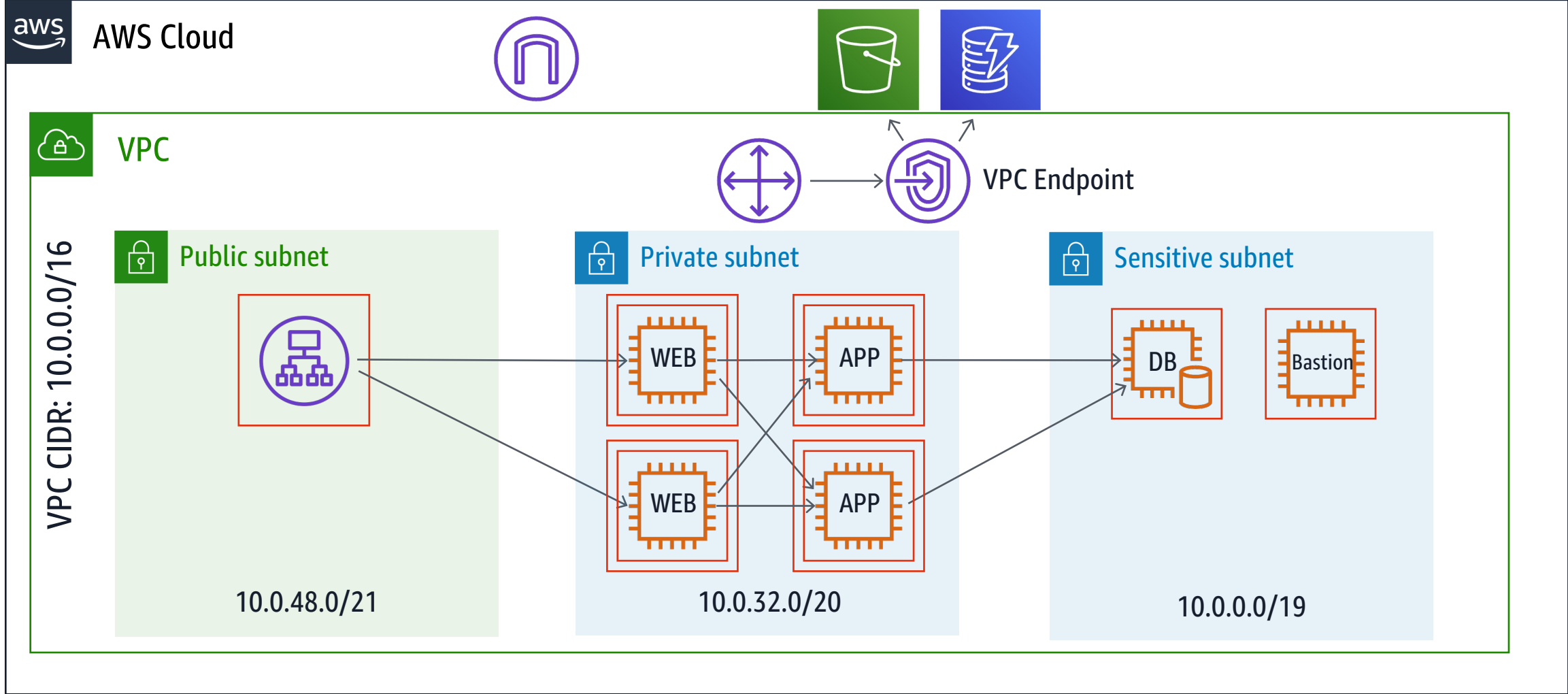
Egress-only Internet Gateway



NAT Gateway



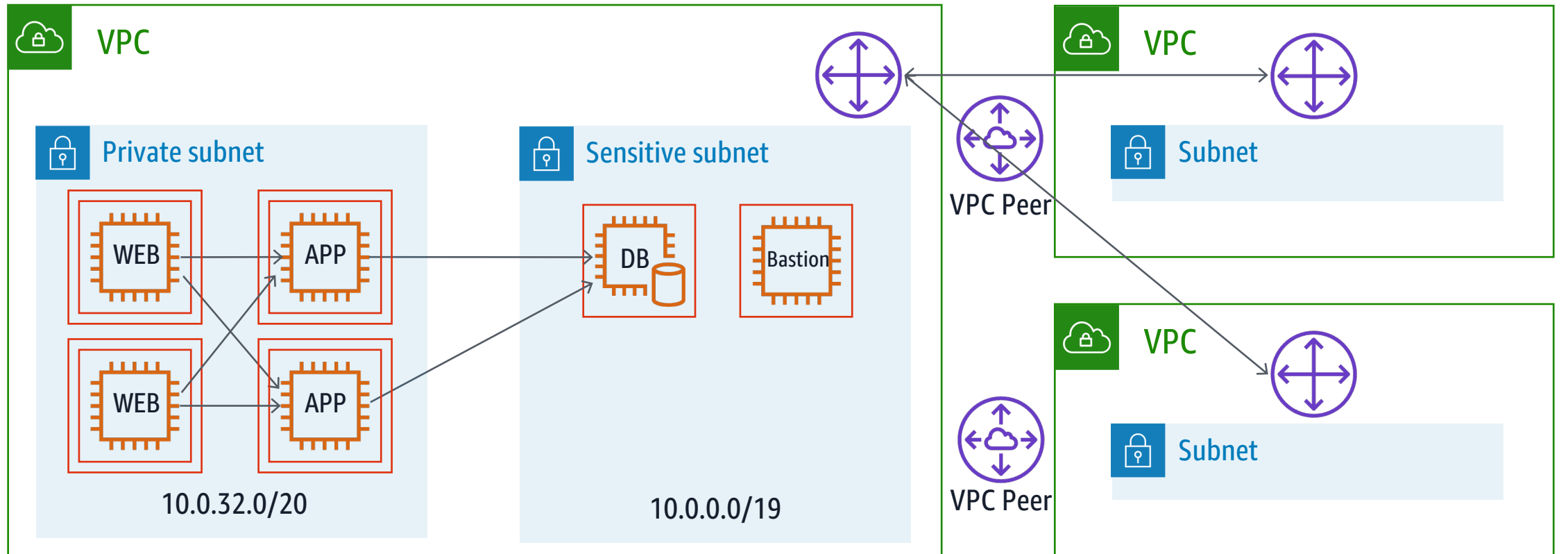
VPC Endpoints



VPC Peering



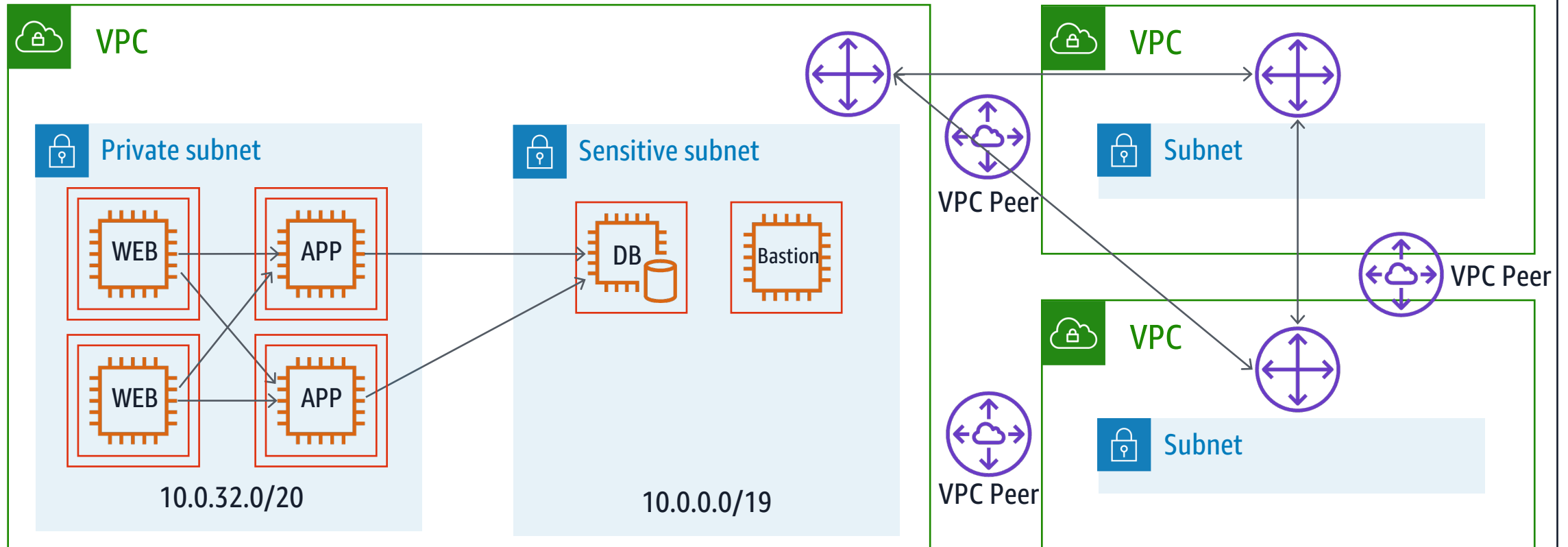
AWS Cloud



VPC Peering

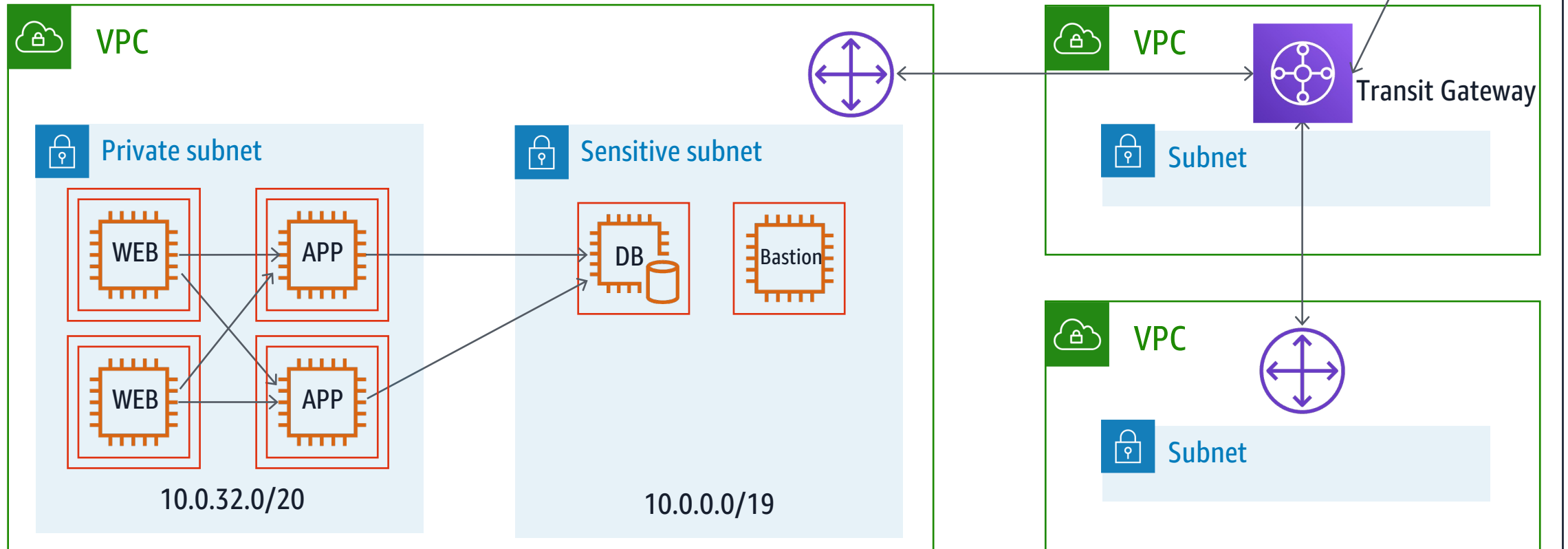


AWS Cloud

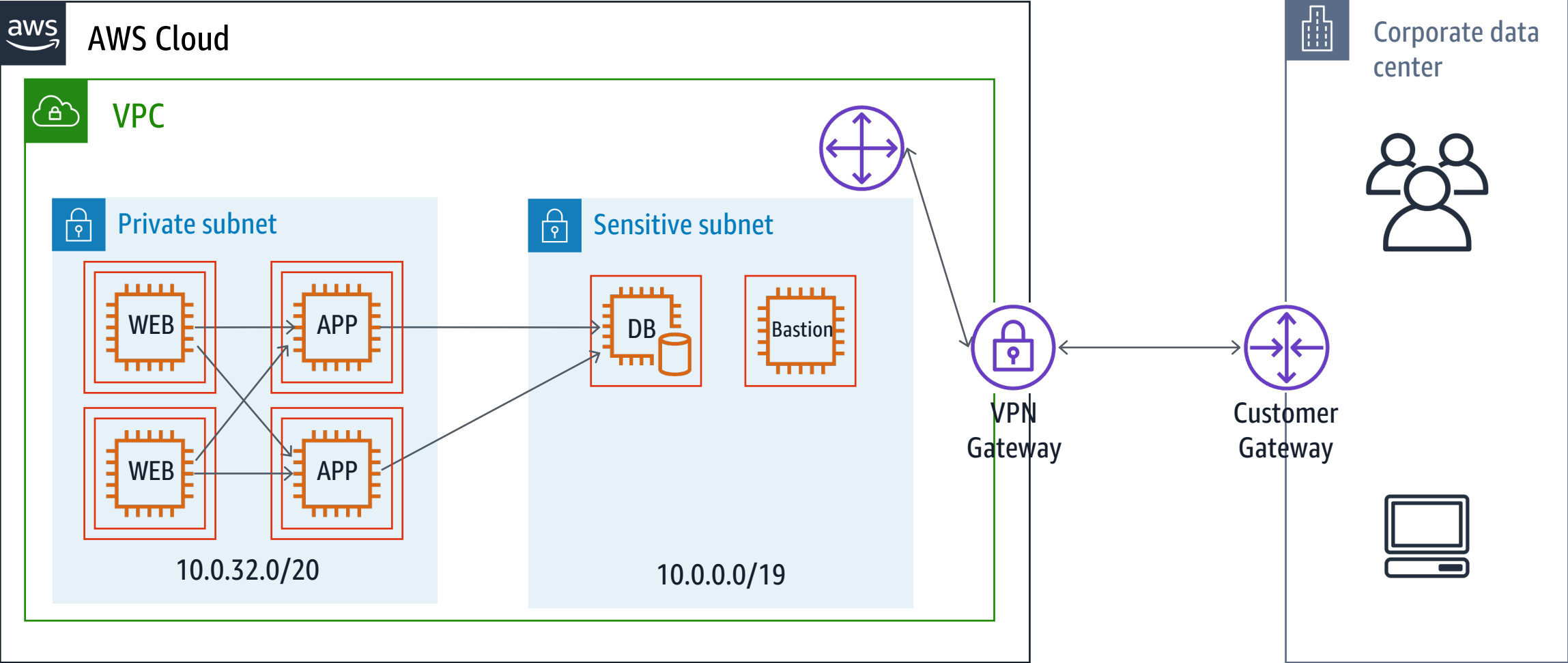


Transit Gateway

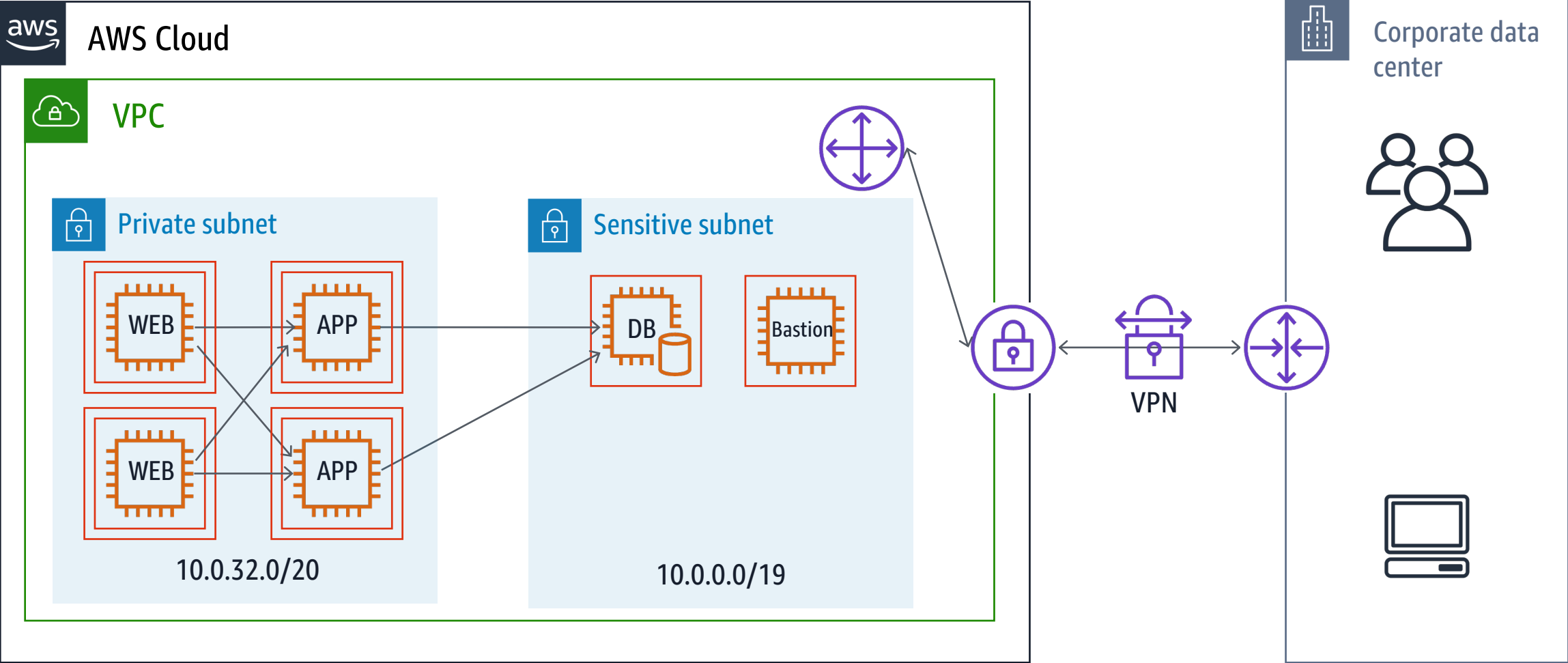
aws AWS Cloud



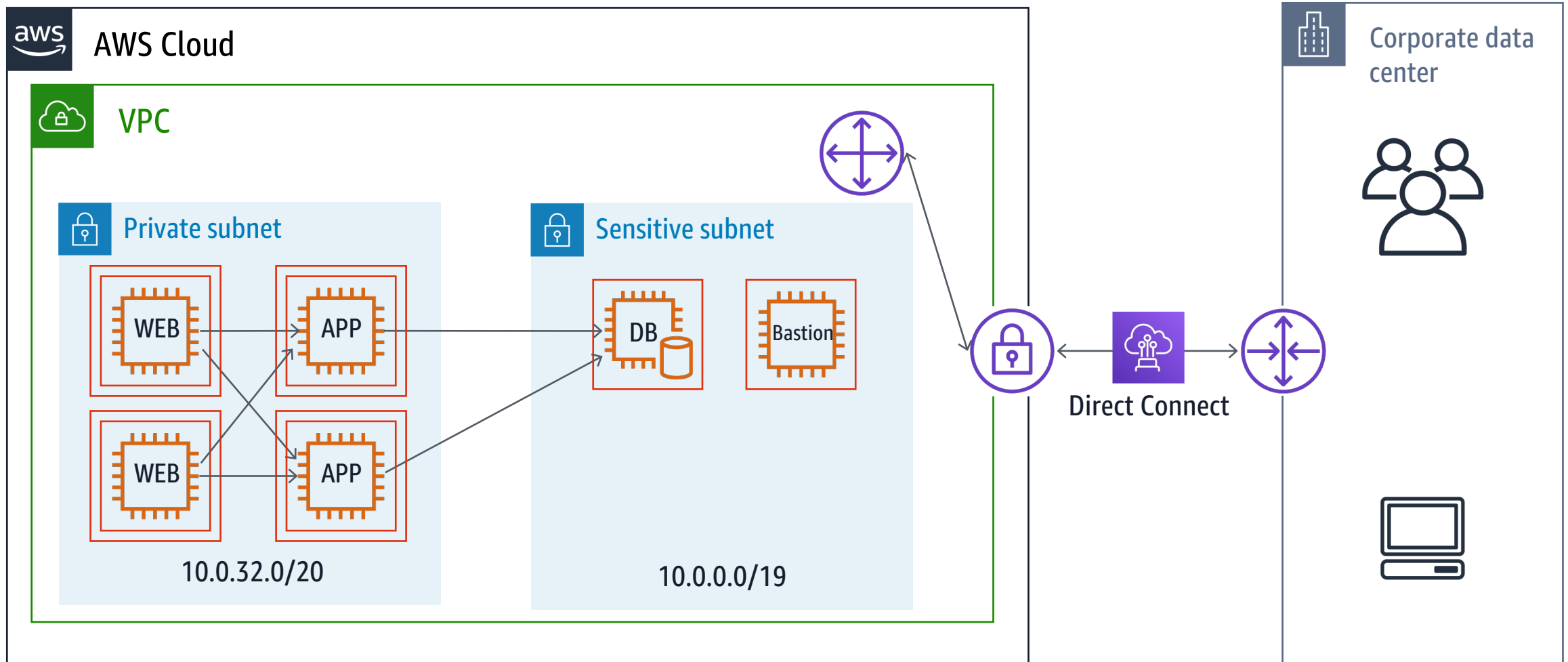
VPN



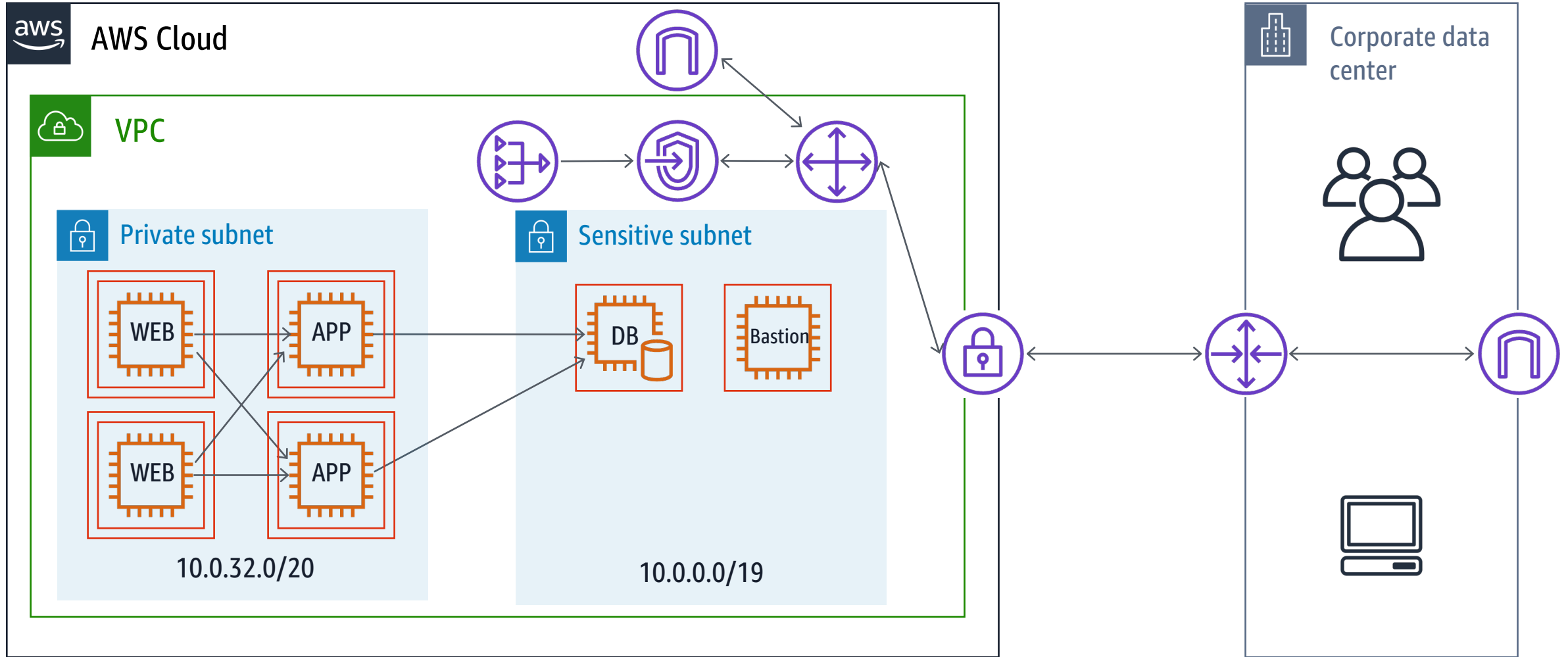
VPN



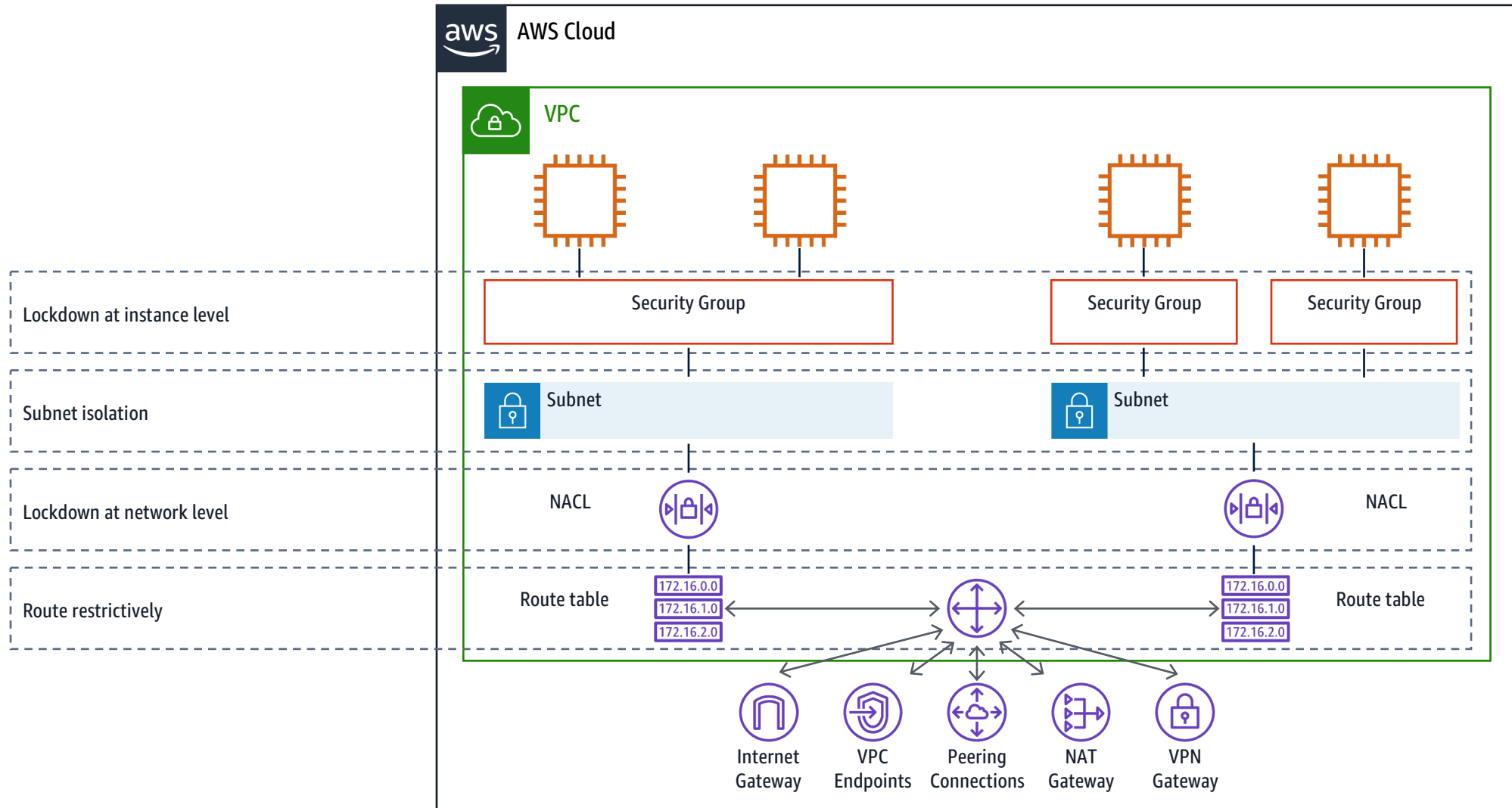
Direct Connect



Multiple Gateways



Network Defense in Depth



감사합니다.