aws professional services

Overview of Virtual Private Cloud

AWS Security Workshop

Agenda

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

aws professional services

Goals

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

Virtual Private Cloud (VPC)

aws professional services

What is a Virtual Private Cloud?

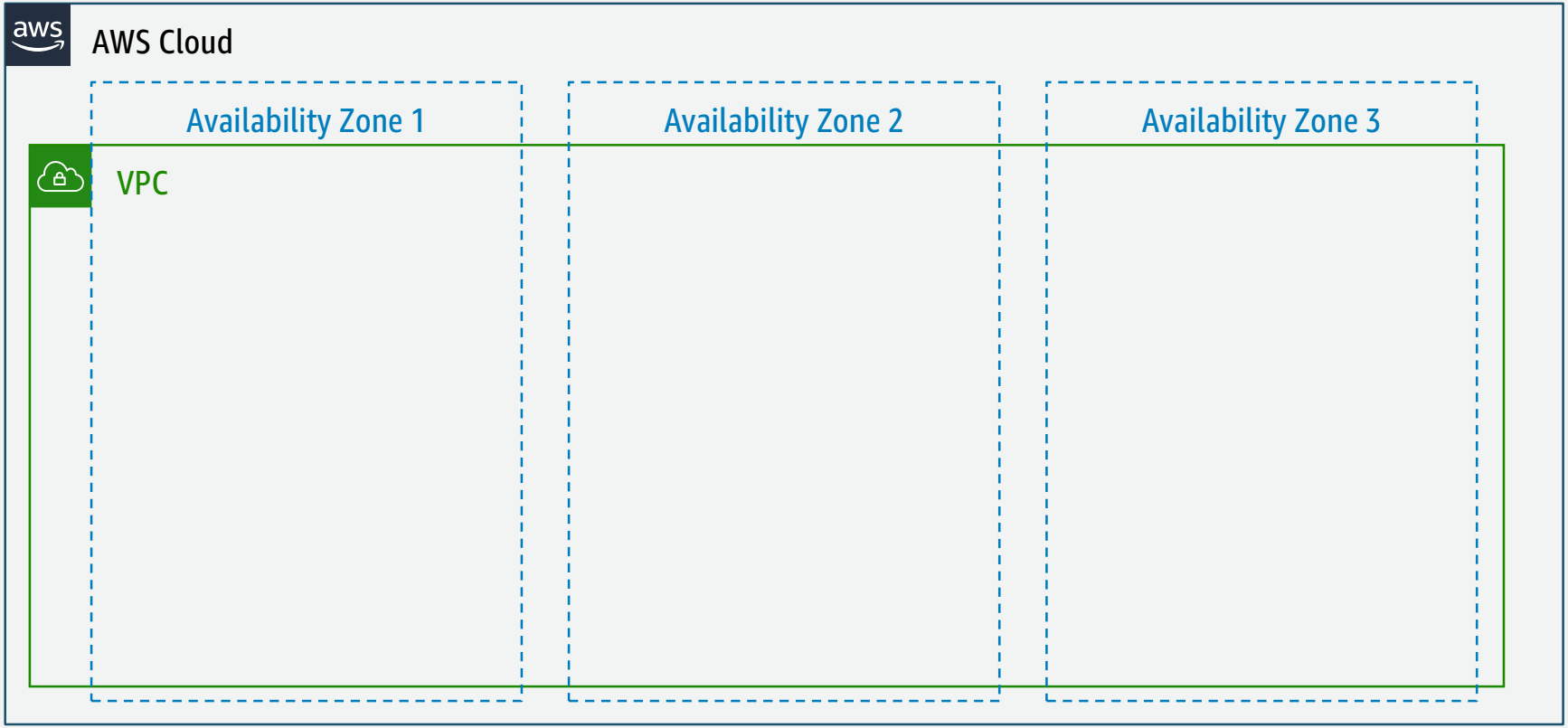
- Software-defined network
- Logically isolated
- Complete control
- Secure
- VPN & Internet connectivity
- Connect your on-premises IT environment

aws professional services

Each AWS Region has multiple Availability Zones

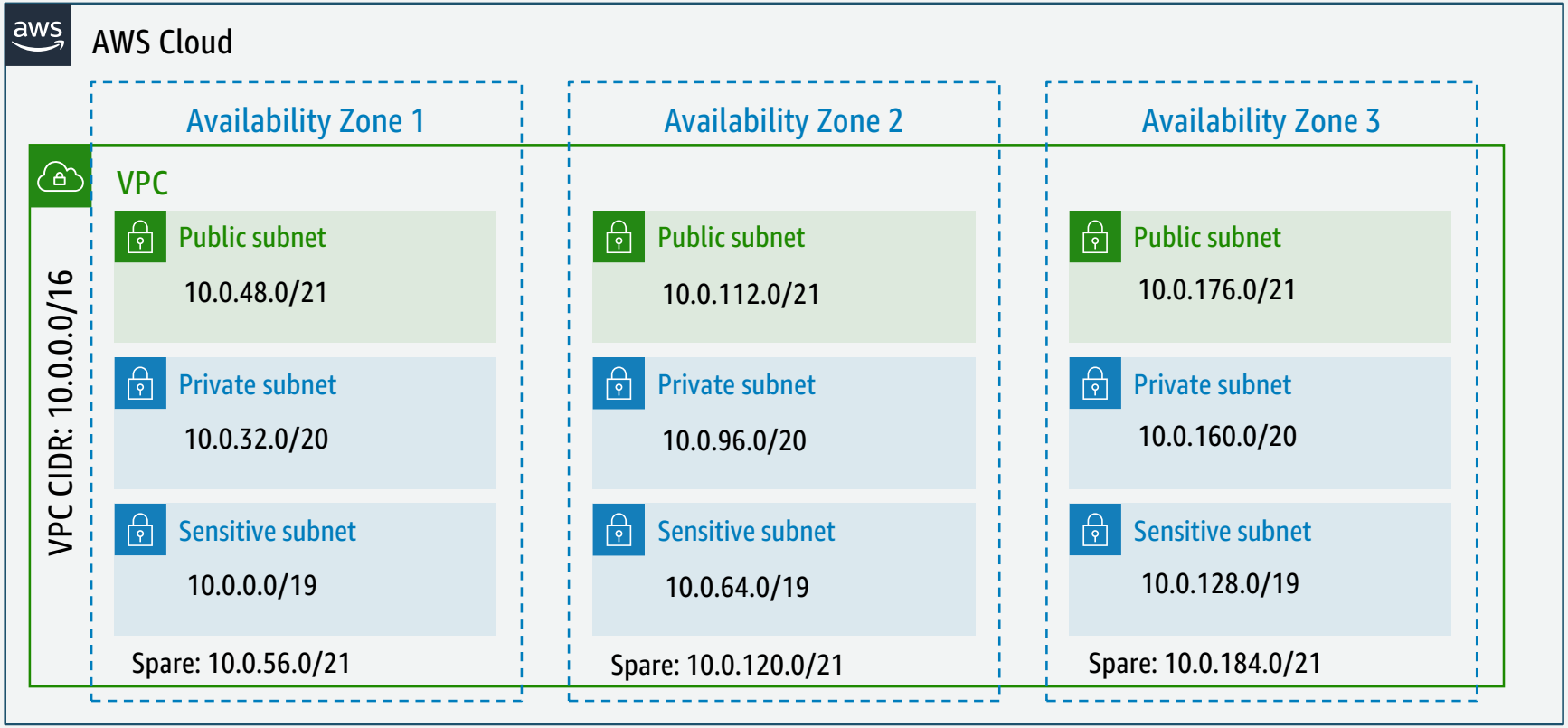
aws professional services

A VPC spans every Availability Zone in a Region



aws professional services

Subnets



aws professional services

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)
- The VPC CIDR block size can be from /16 to /28
- Can associate additional IPv4 address blocks
- Can associate IPv6 address block

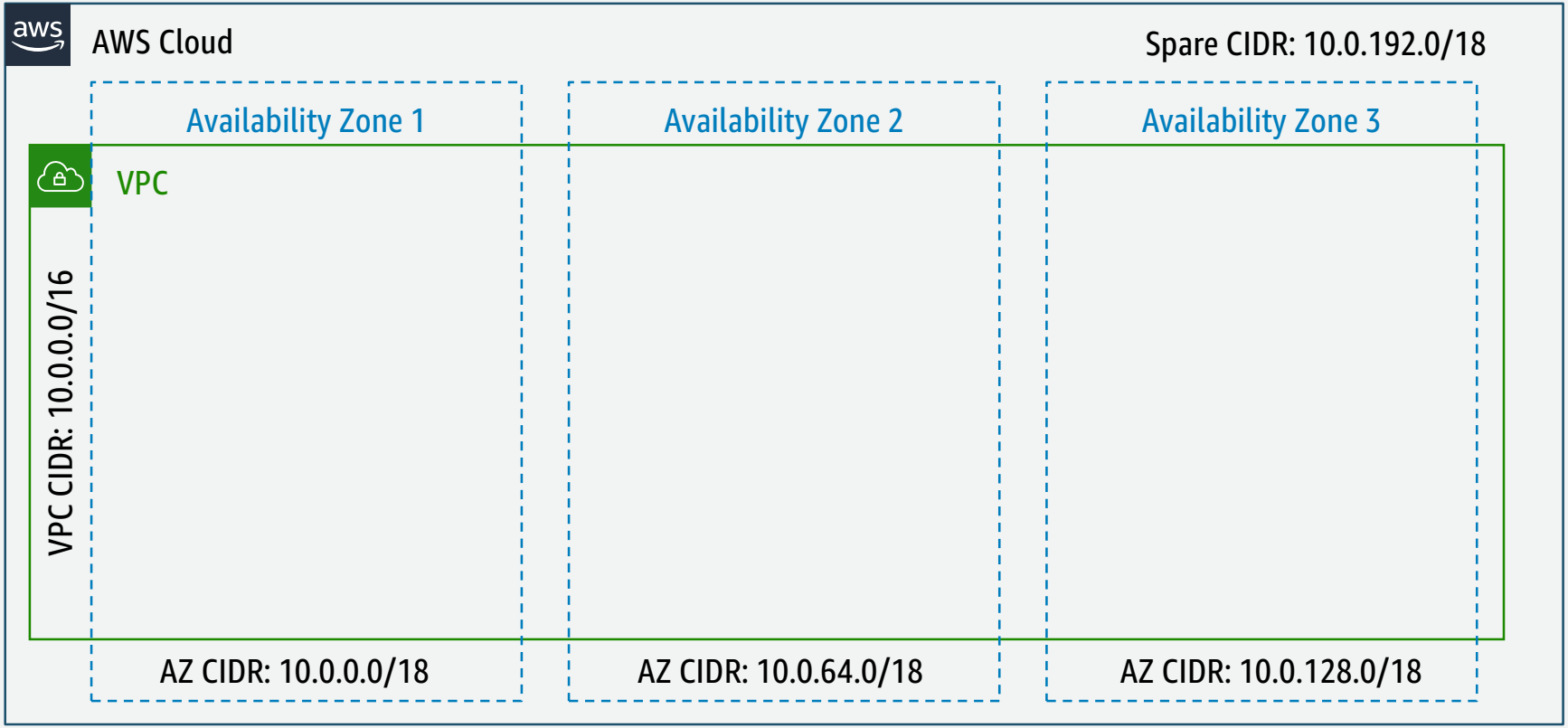
Availability Zone 2

Select IP addressing strategy

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

aws professional services

Logically allocate CIDR space for each AZ

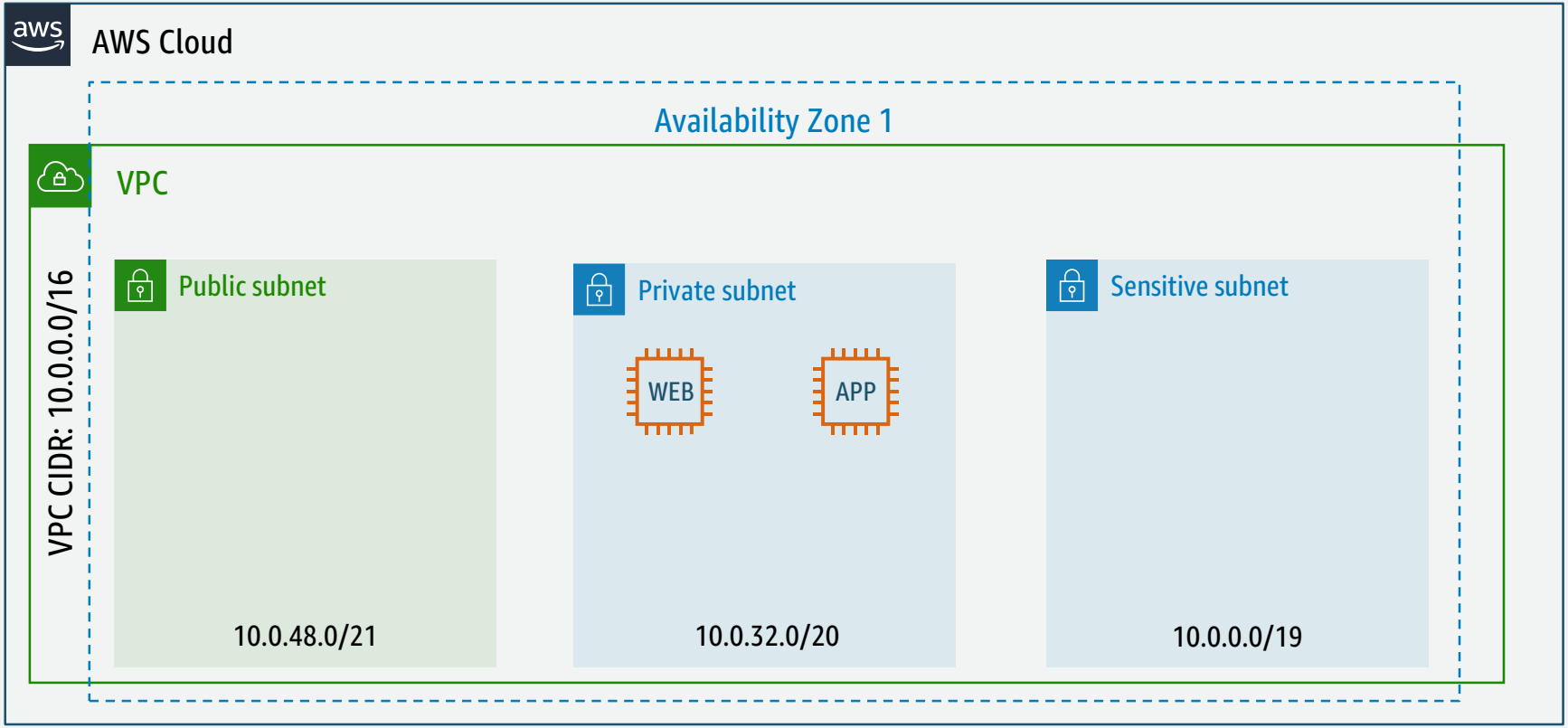


aws professional services

Security Groups

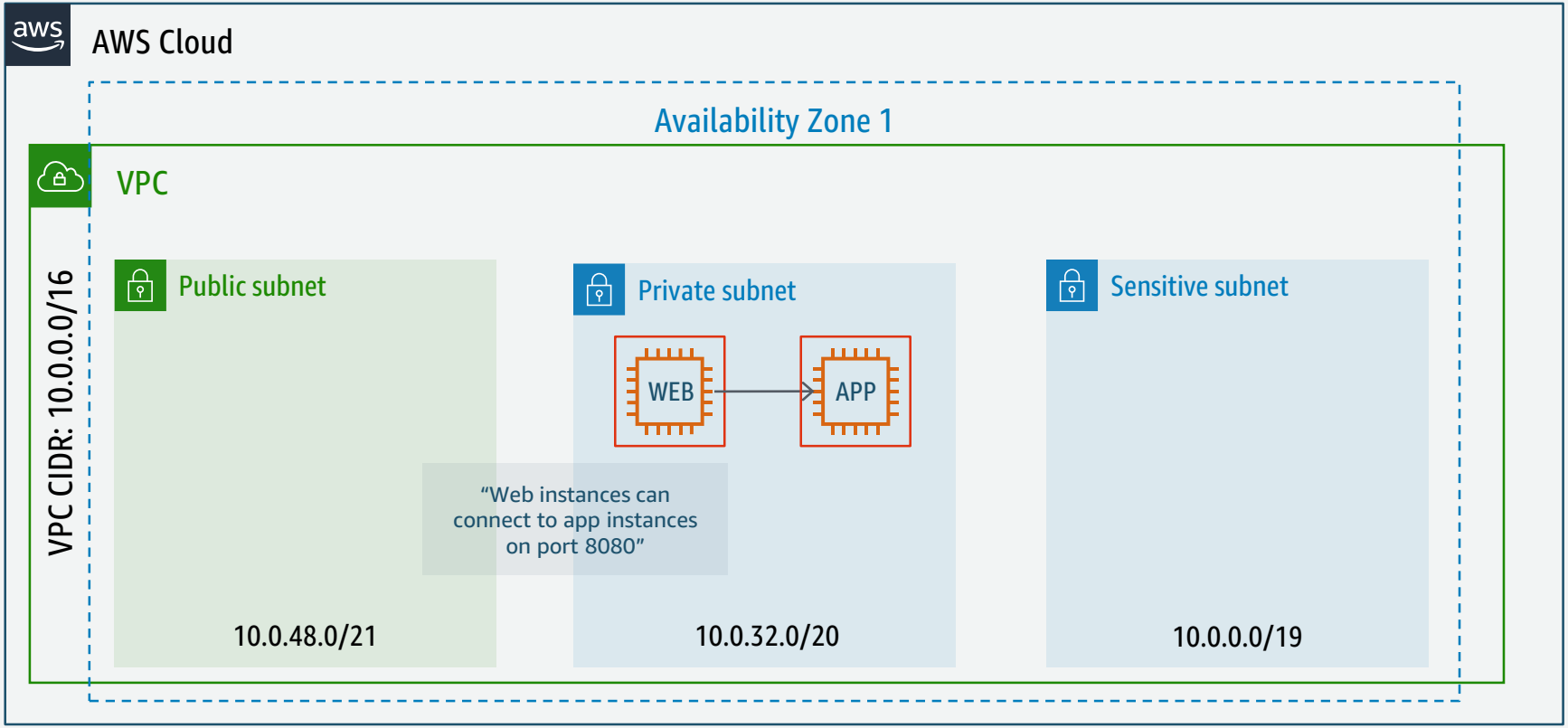
aws professional services

Security Groups – Stateful Firewall



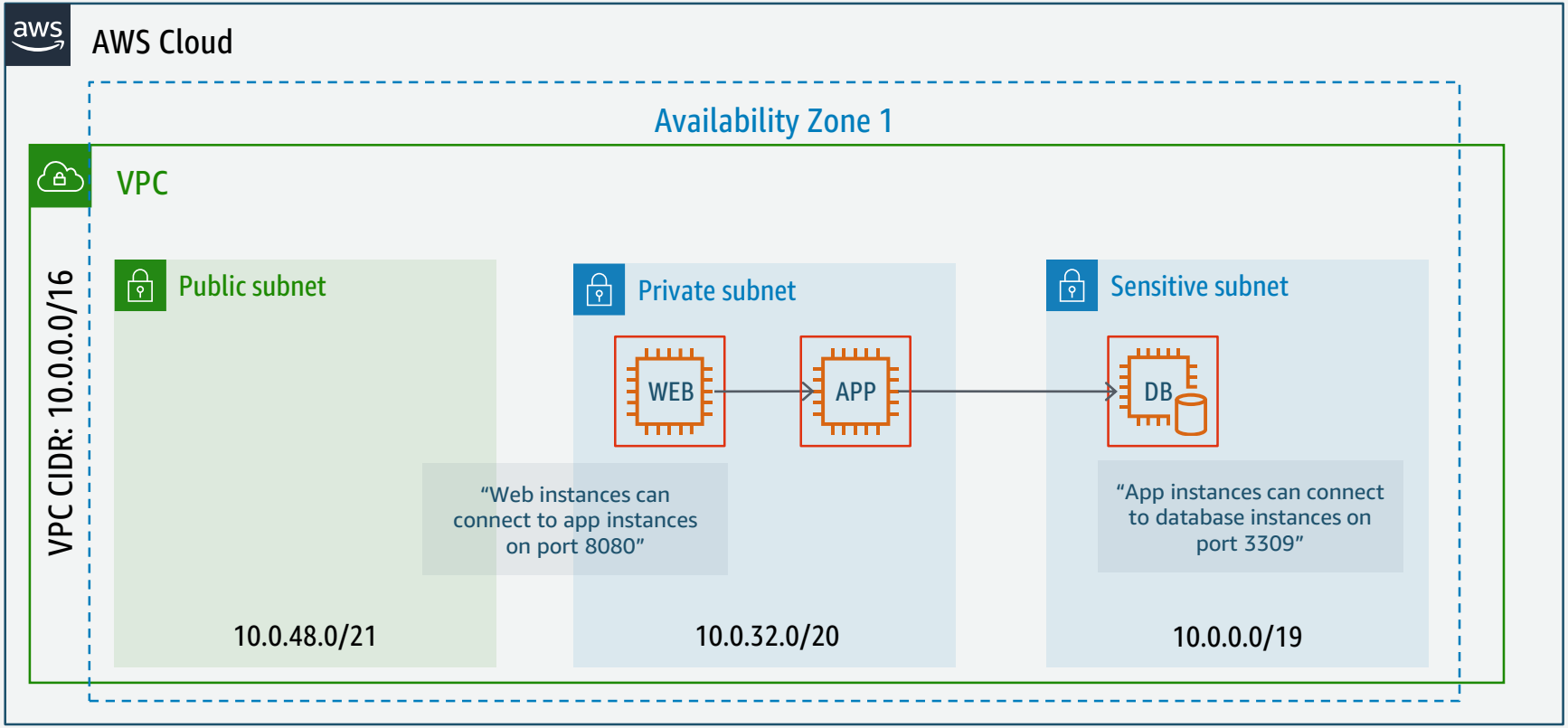
aws professional services

Security Groups – Stateful Firewall



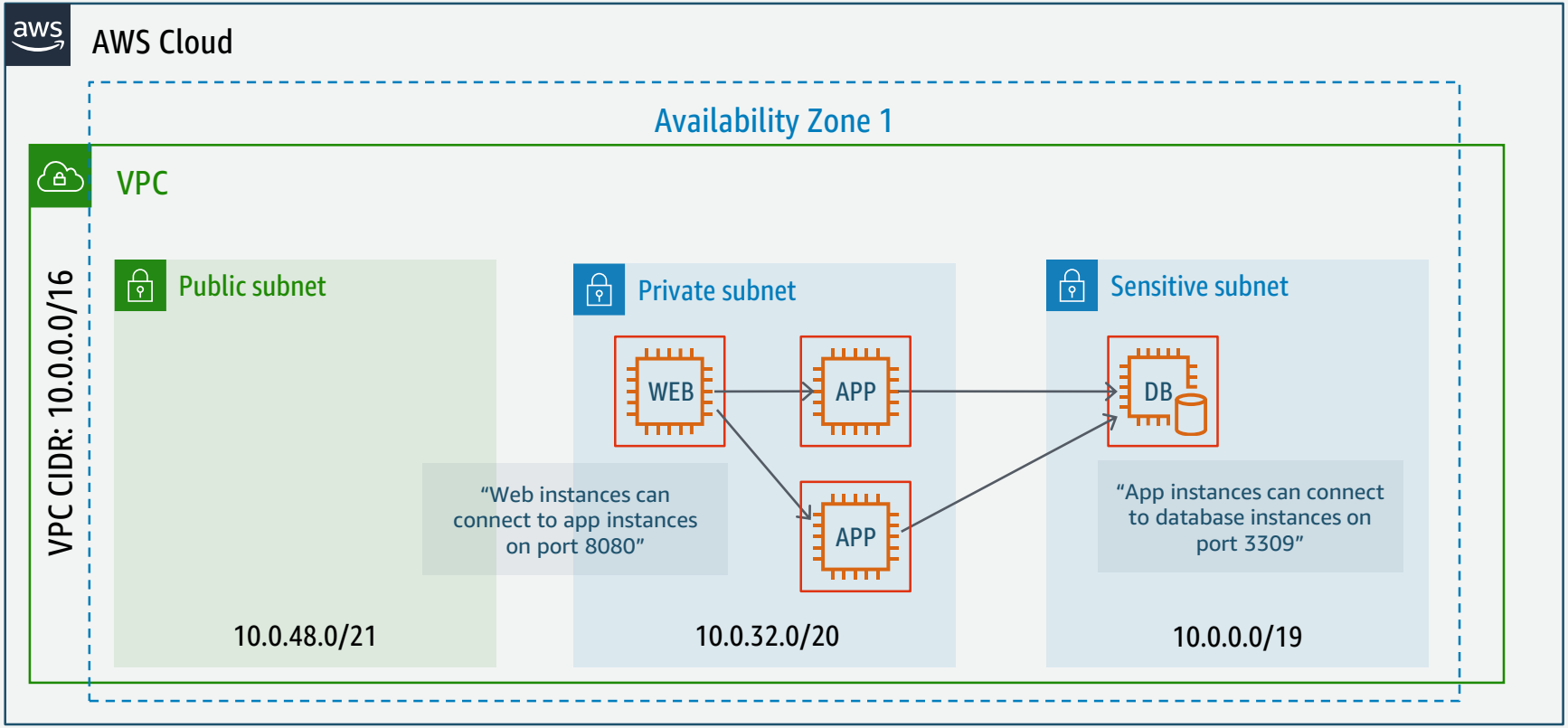
aws professional services

Security Groups – Stateful Firewall



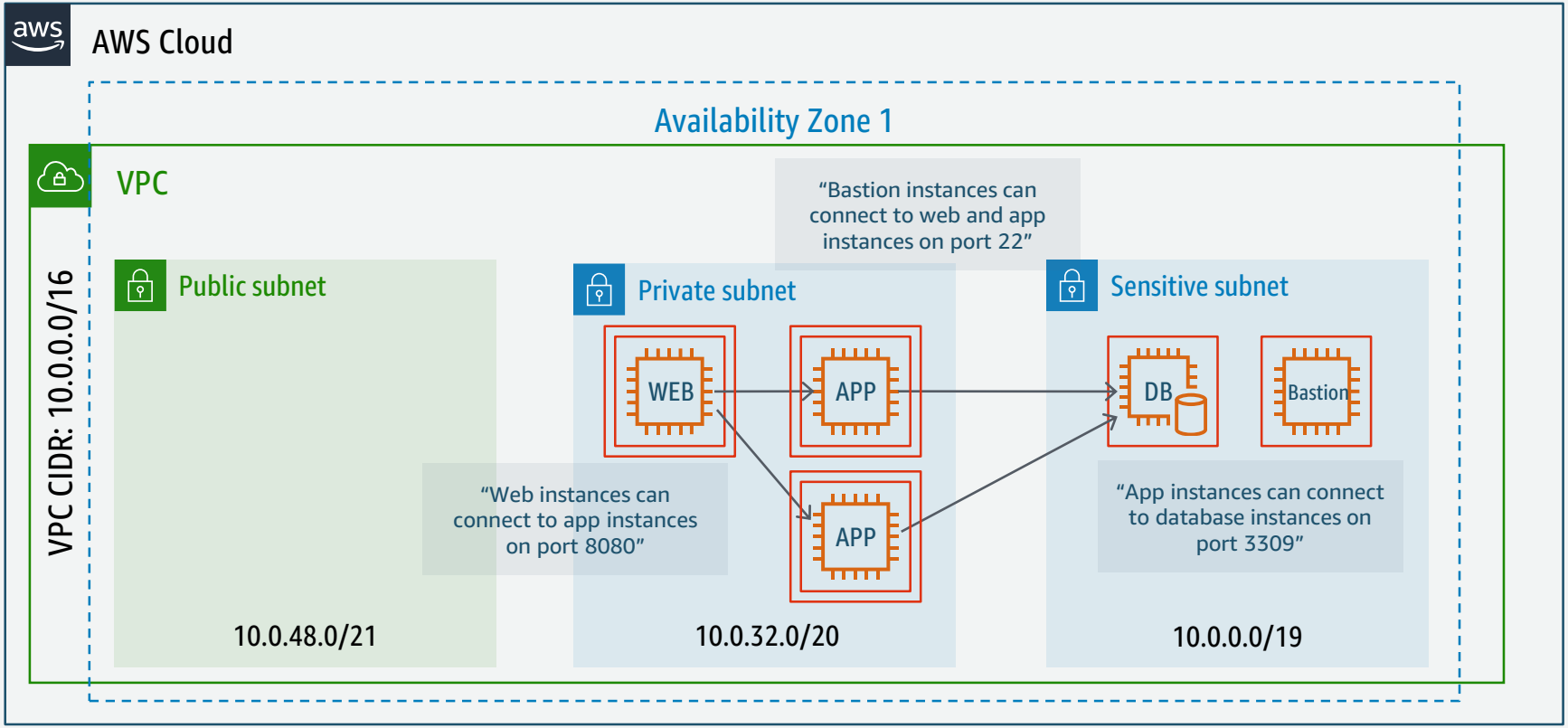
aws professional services

Security Groups – Stateful Firewall



aws professional services

Security Groups – Stateful Firewall

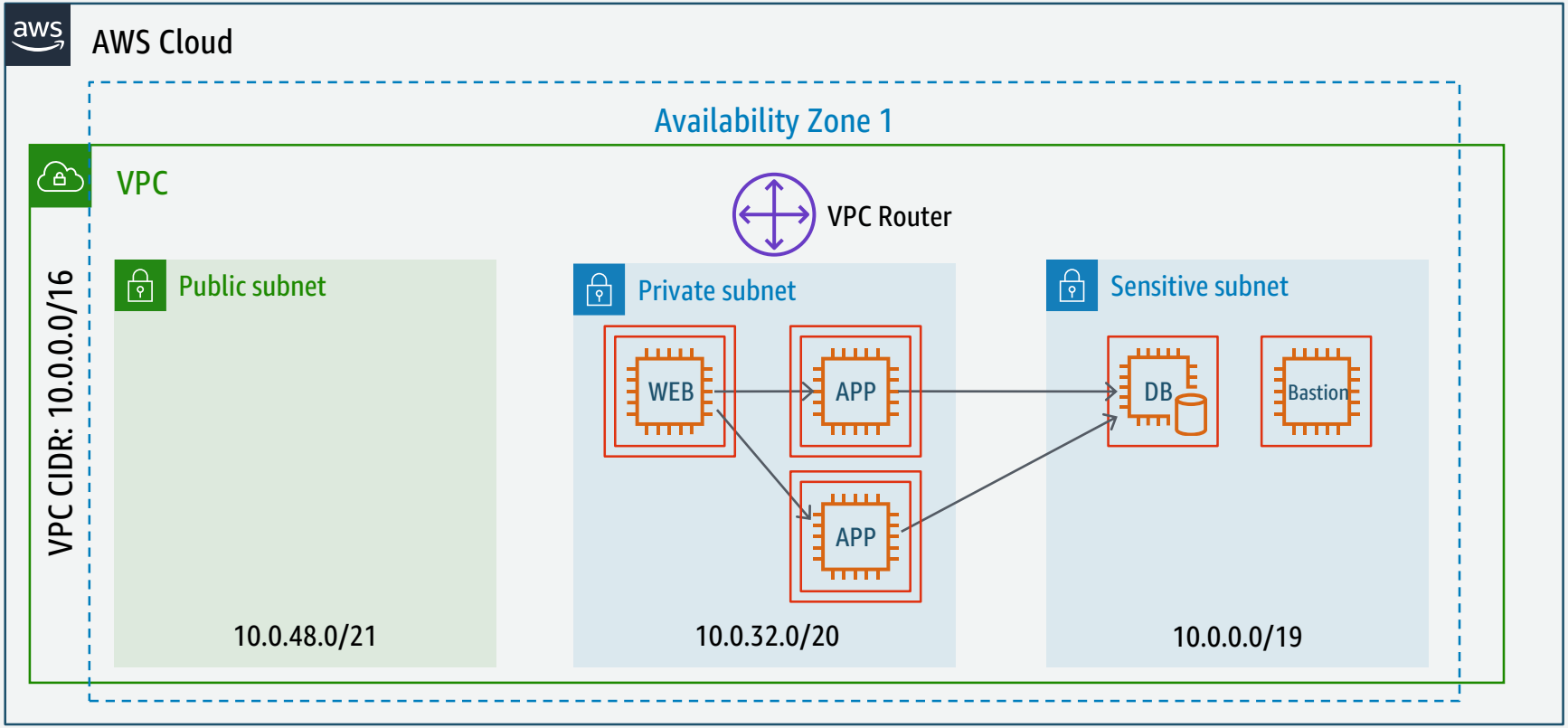


aws professional services

Routing, NACLs, and Load Balancing

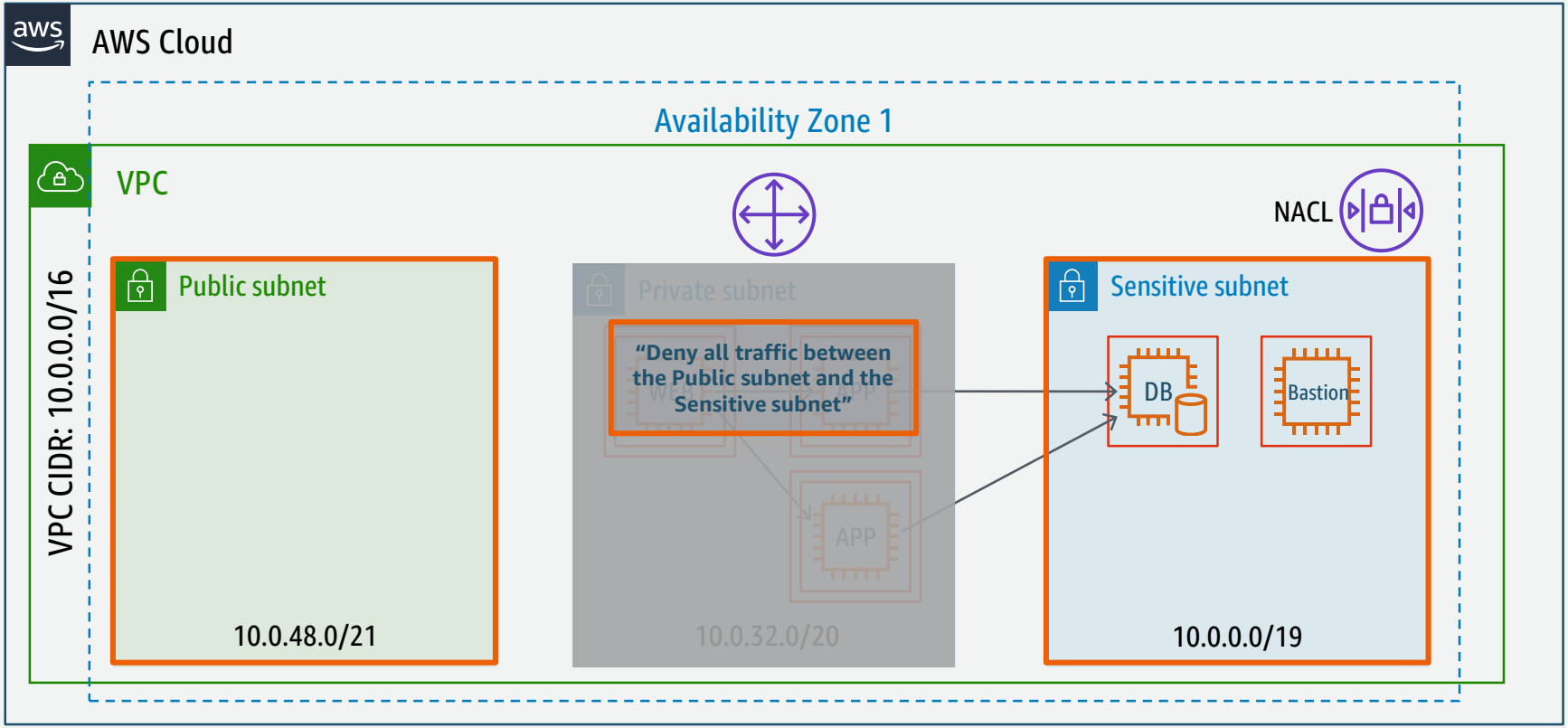
aws professional services

Routing



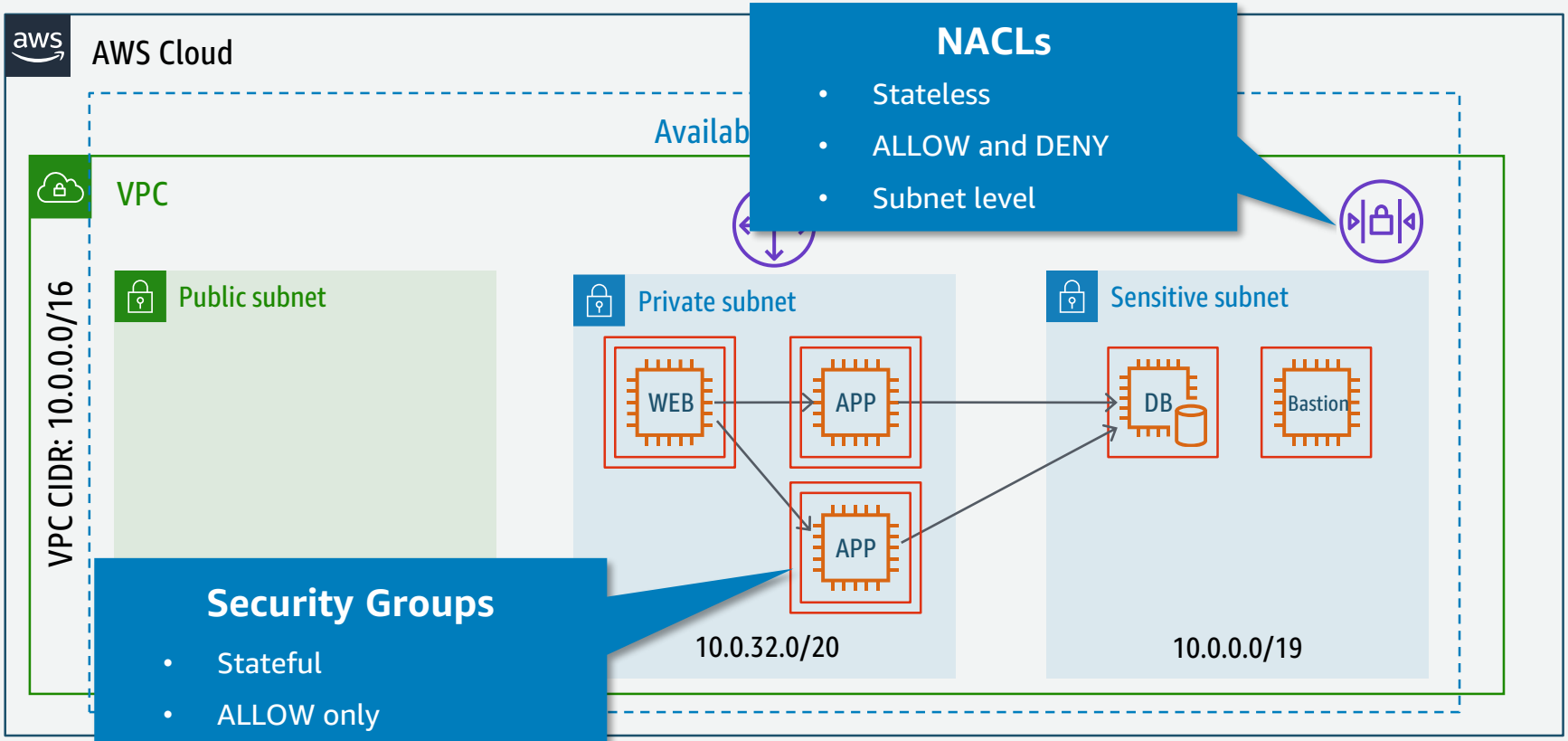
aws professional services

Network Access Control List (NACL)



aws professional services

NACLs and Security Groups



NACLs

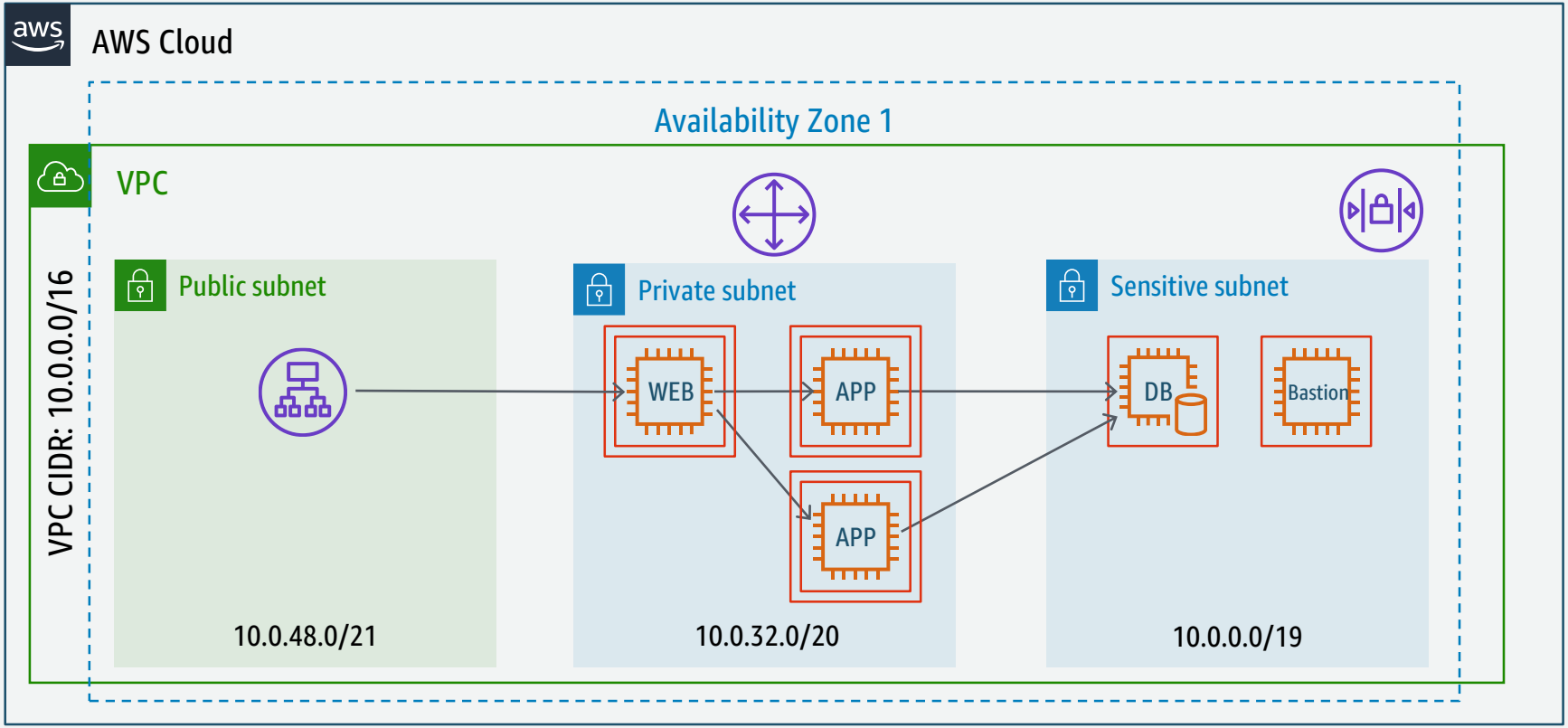
- Stateless
- ALLOW and DENY
- Subnet level

Security Groups

- Stateful
- ALLOW only
- Instance level

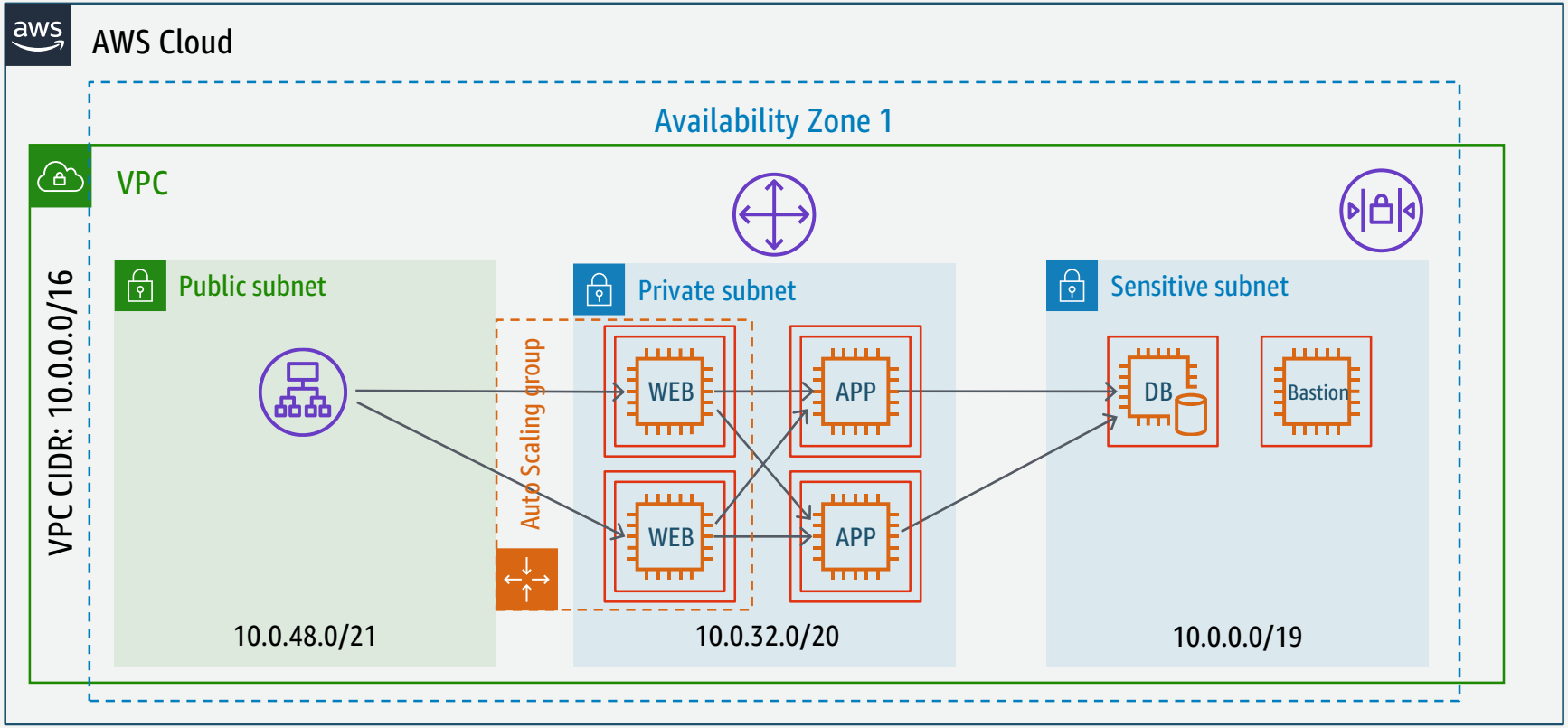
aws professional services

Load Balancing



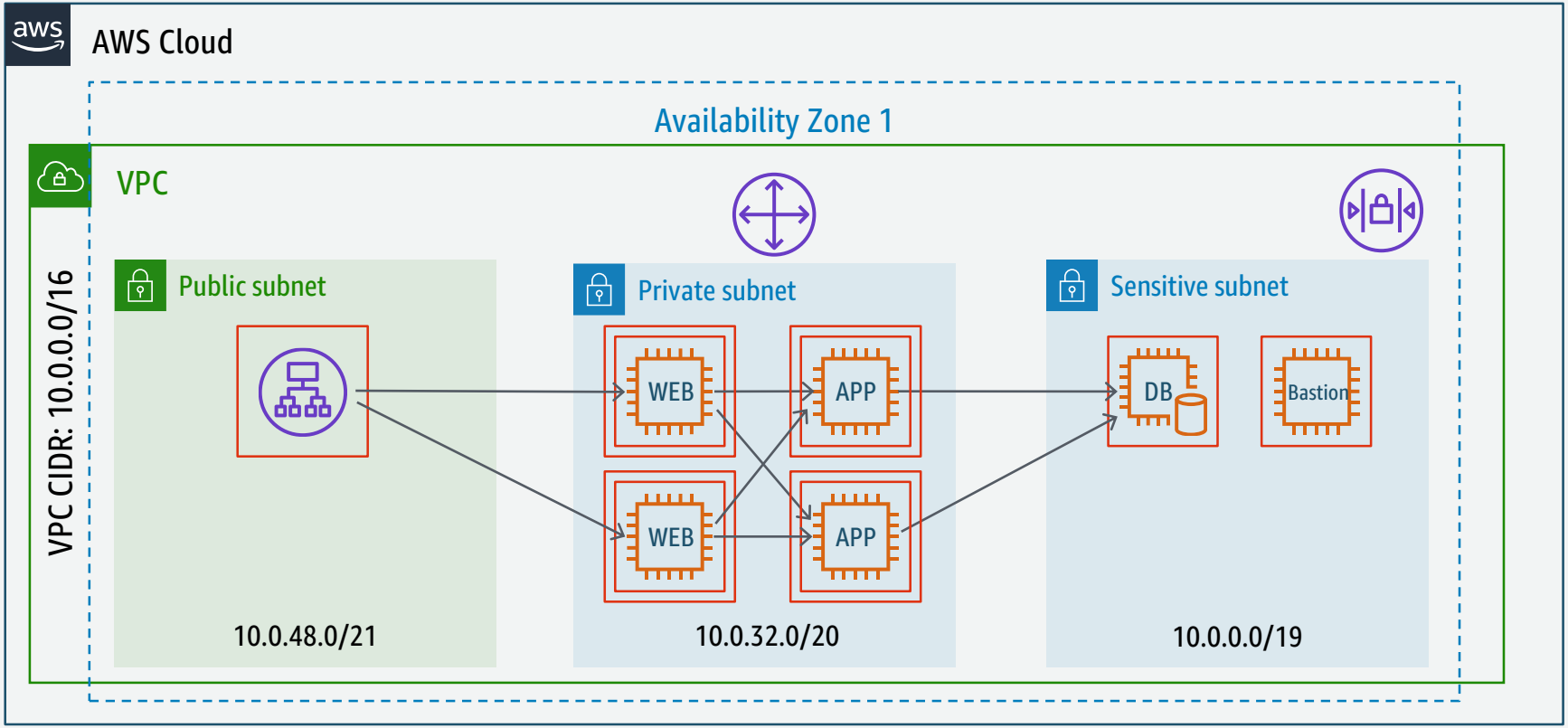
aws professional services

Load Balancing



aws professional services

Load Balancing



aws professional services

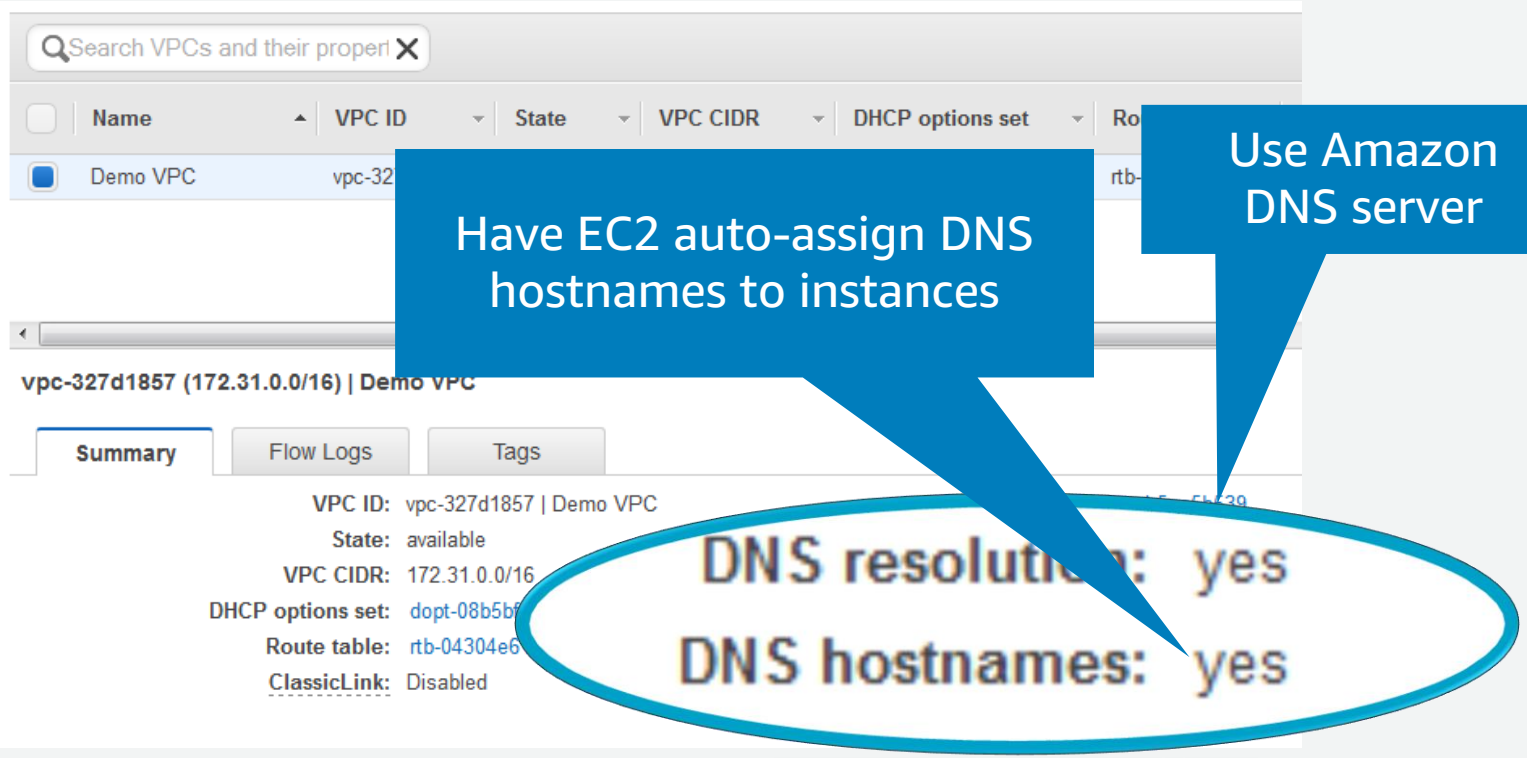
Load Balancing – ELB Types

	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

aws professional services

VPC DNS Options



aws professional services

EC2 DNS Hostnames

External DNS name:
Resolves to…

Internal DNS hostname:
Resolves to Private IP address

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

Description | Status Checks | M… gs

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)

aws professional services

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

aws professional services

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
```

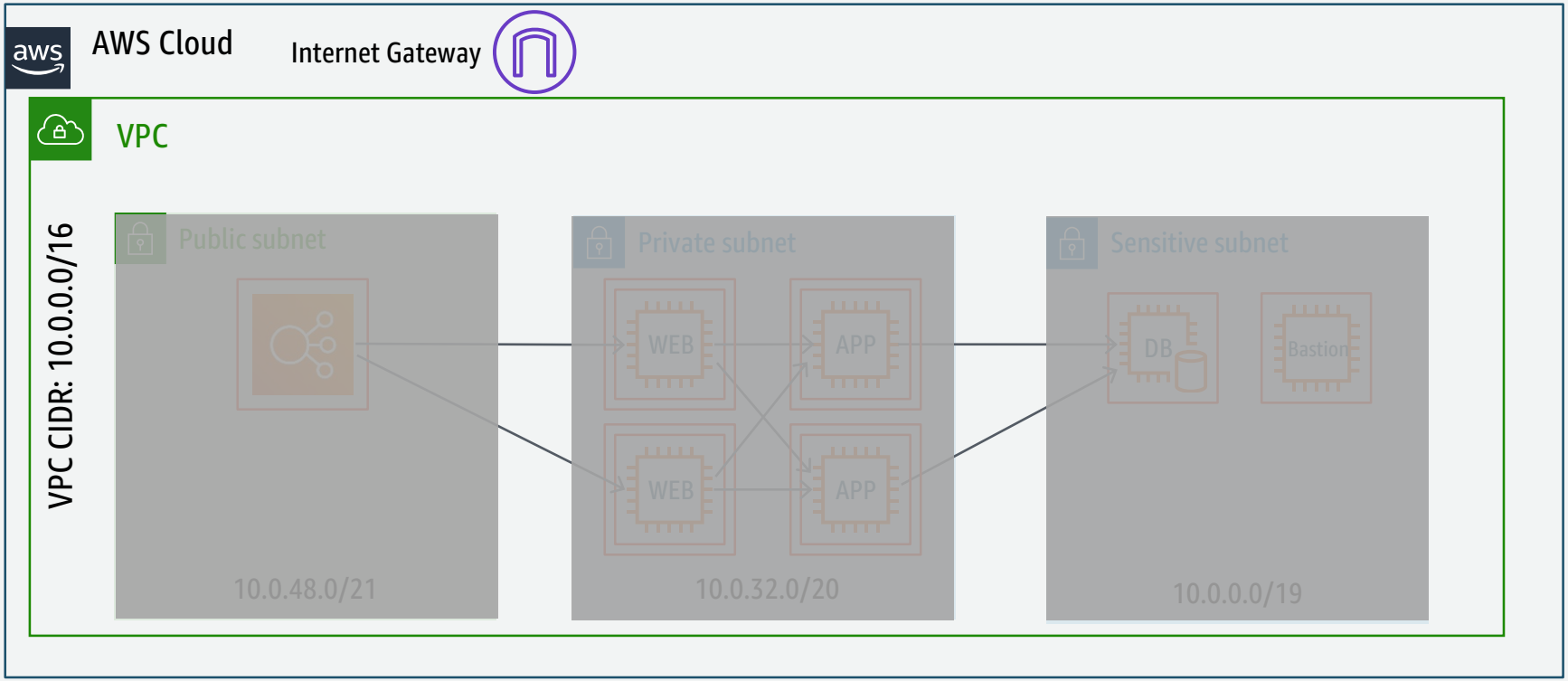
Inside your VPC:
Private IP address

aws professional services

Connectivity

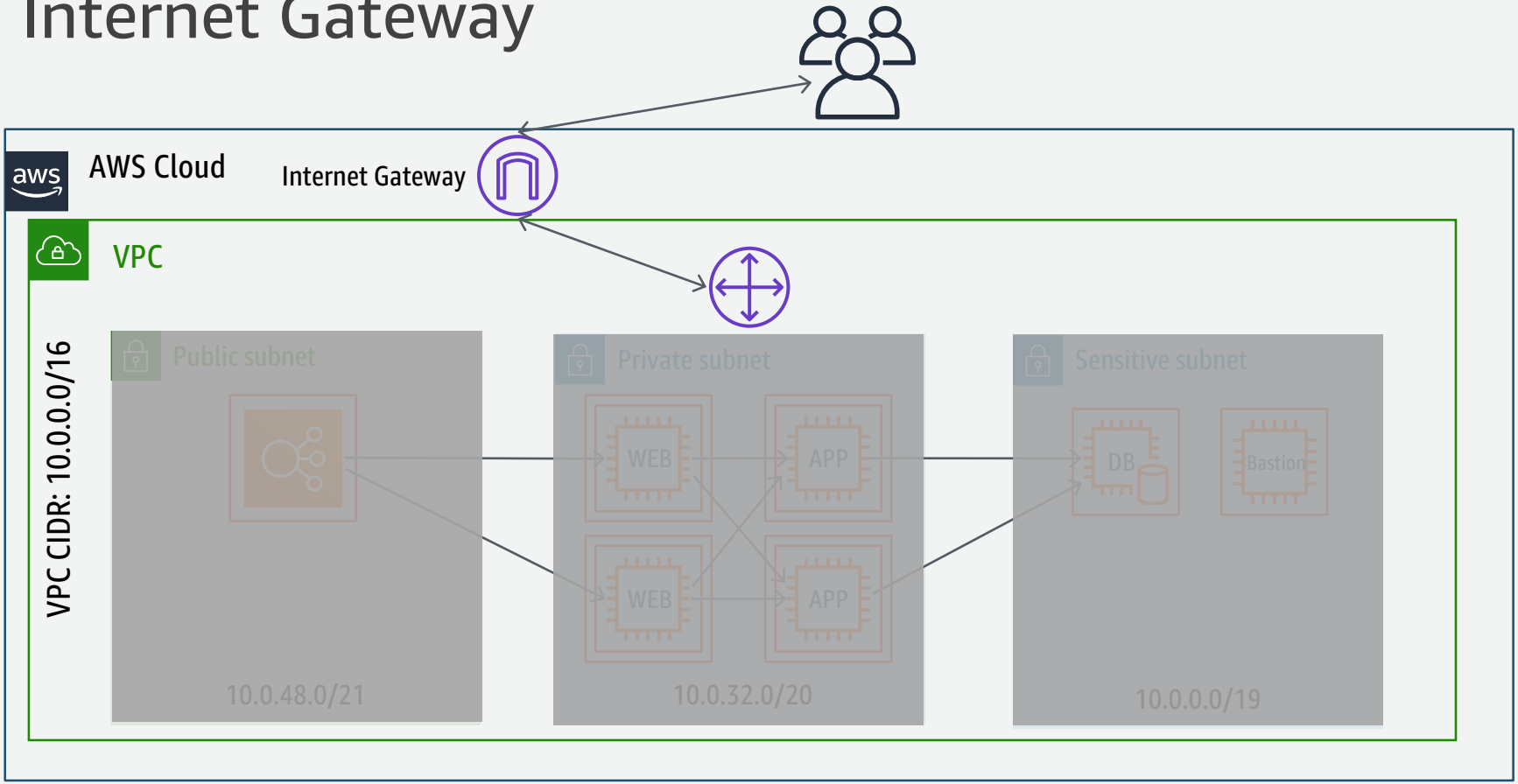
aws professional services

Internet Gateway



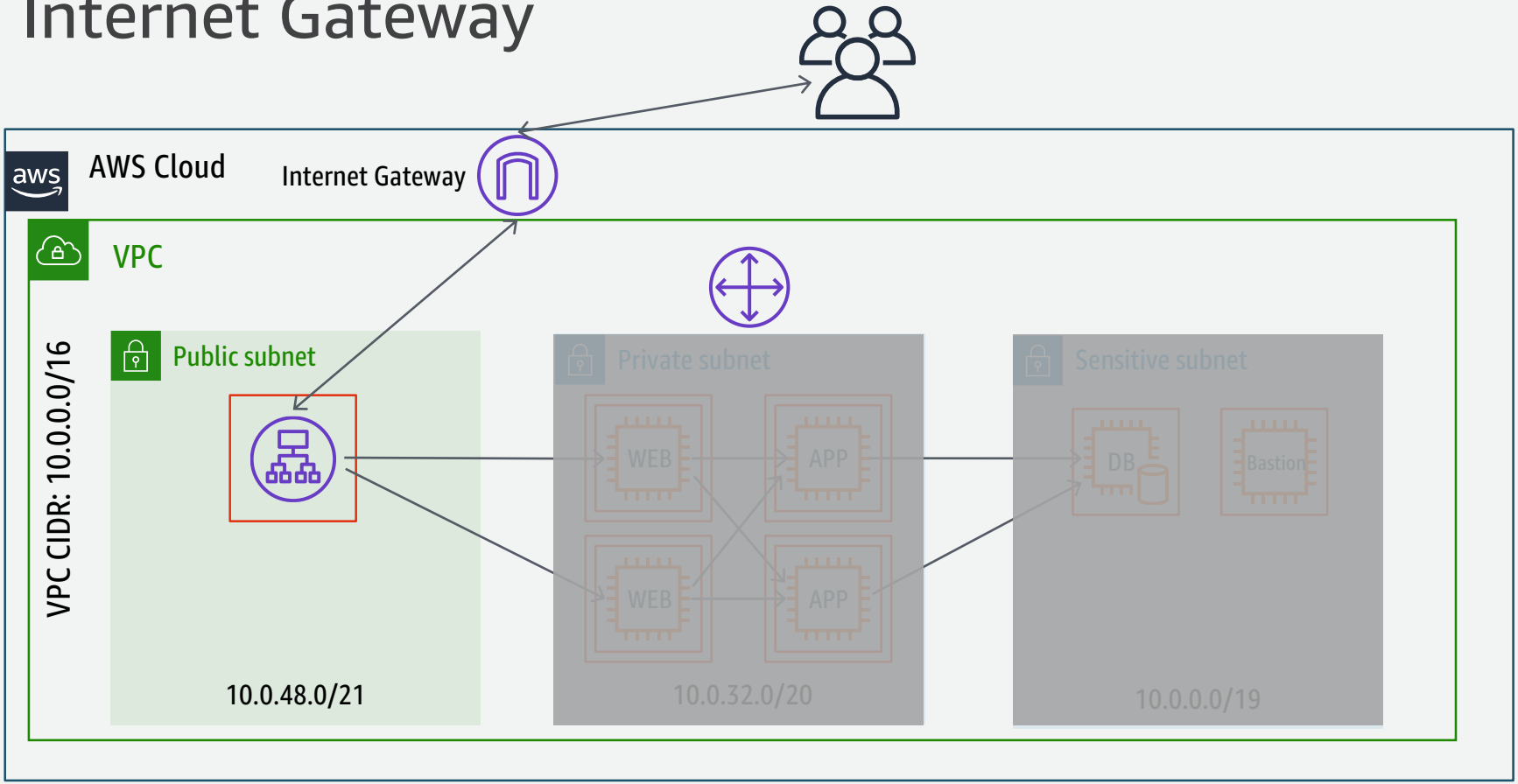
aws professional services

Internet Gateway



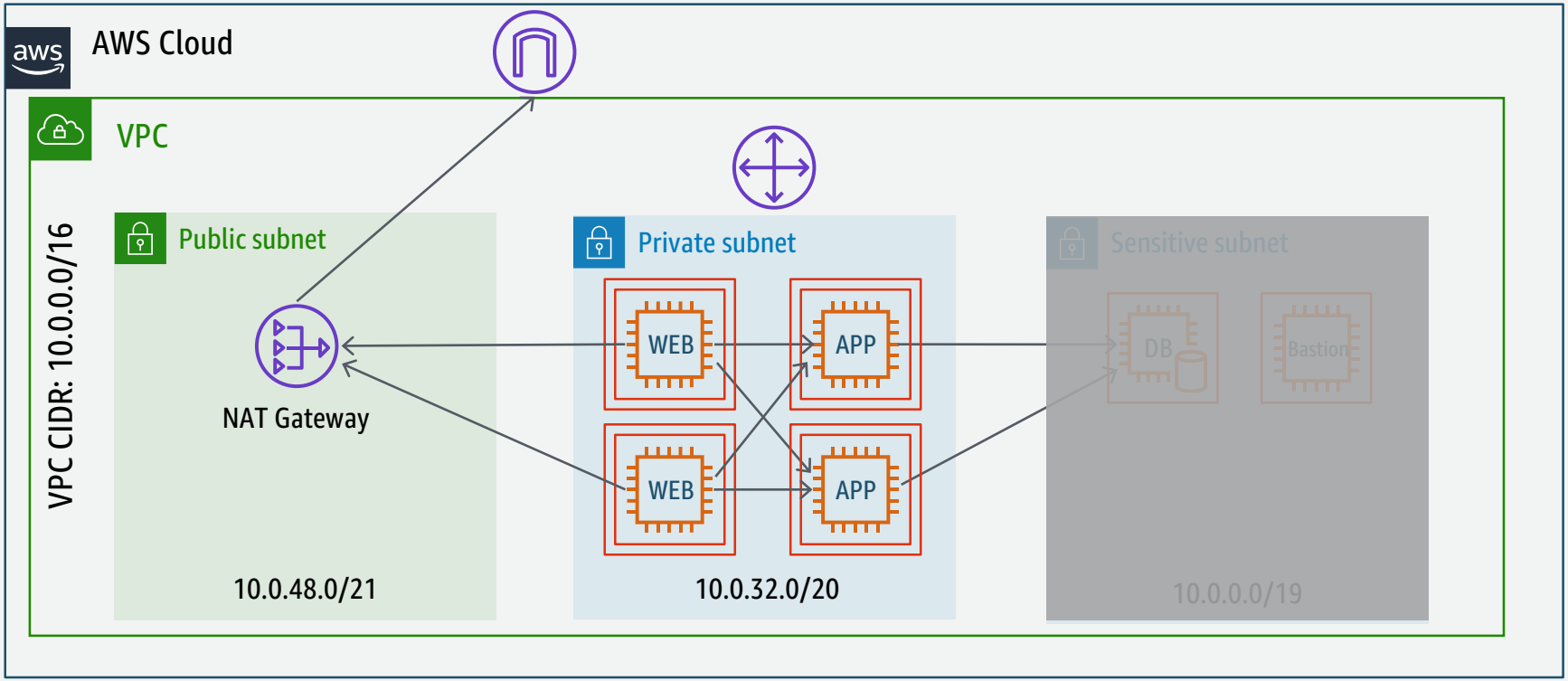
aws professional services

Internet Gateway



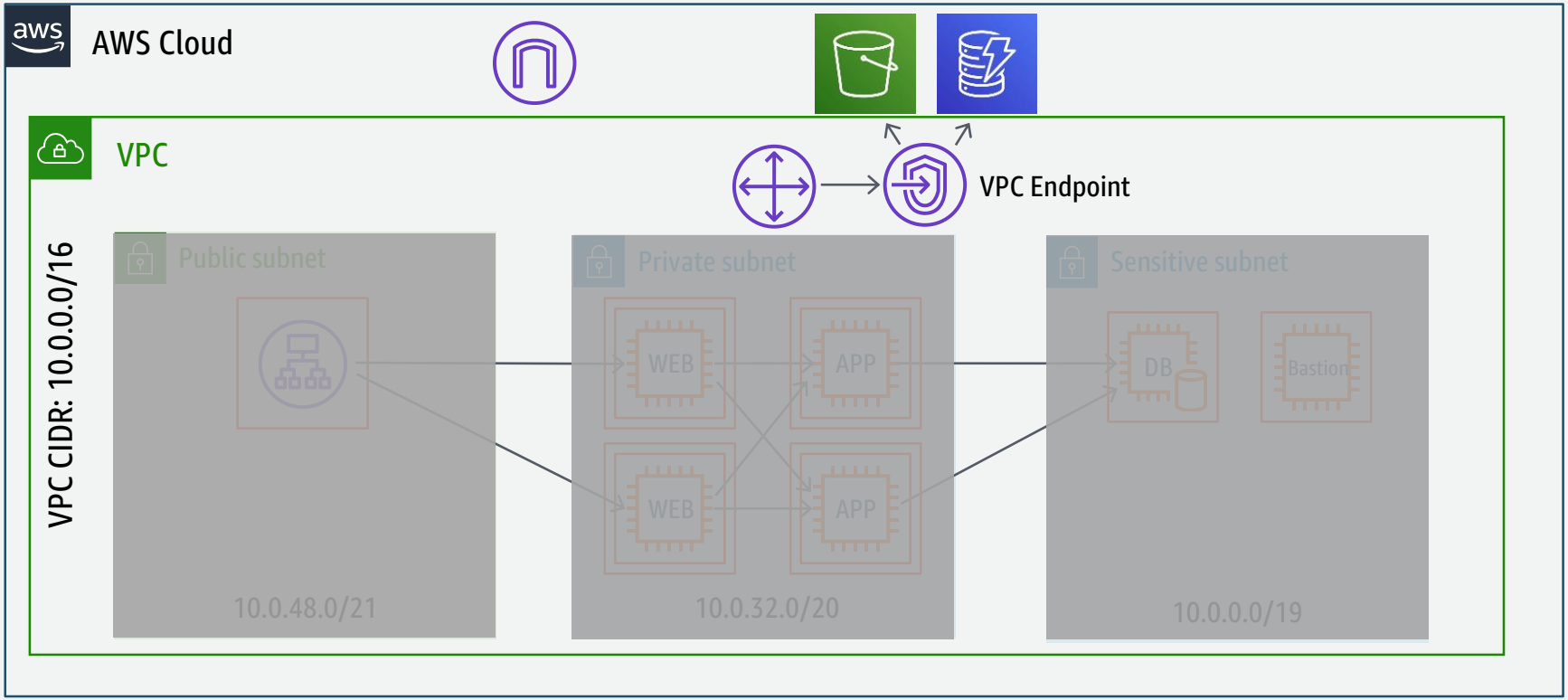
aws professional services

NAT Gateway



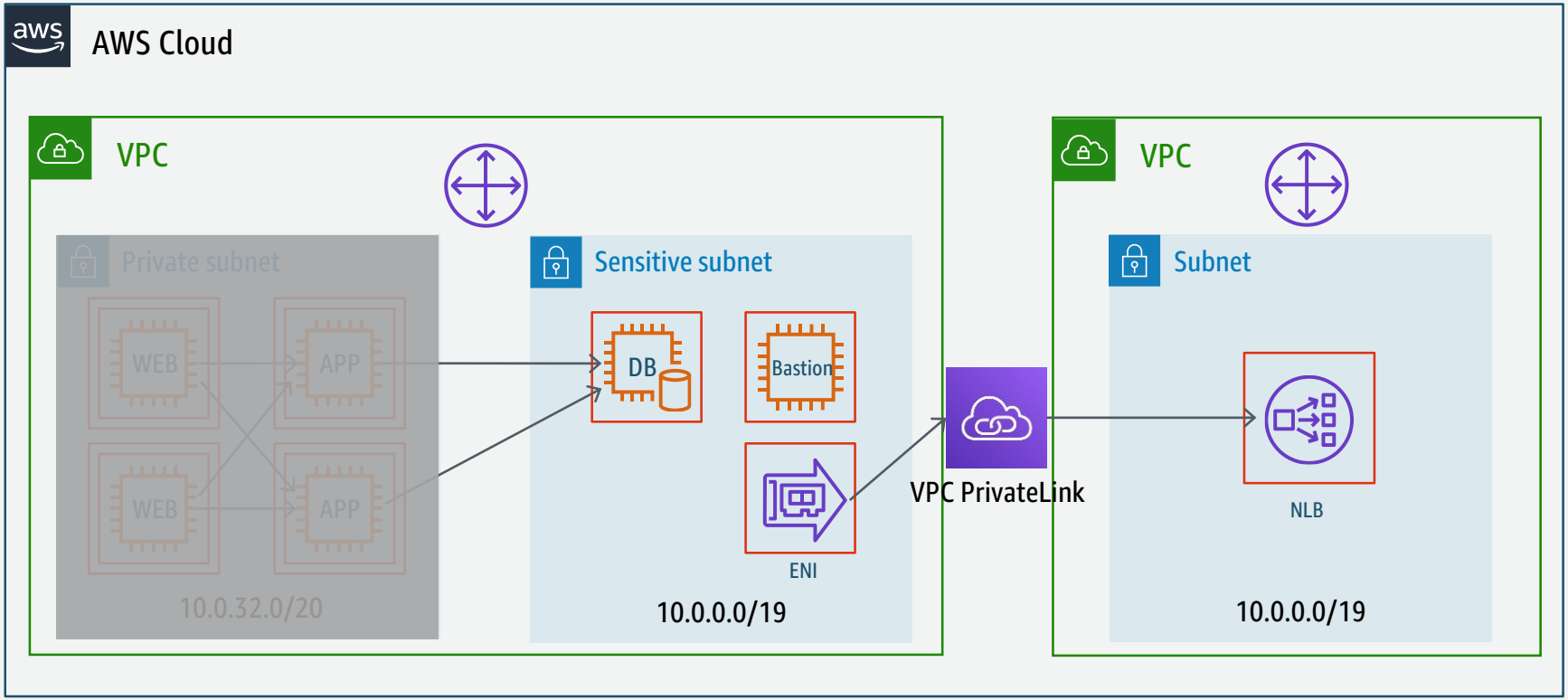
aws professional services

VPC Endpoints



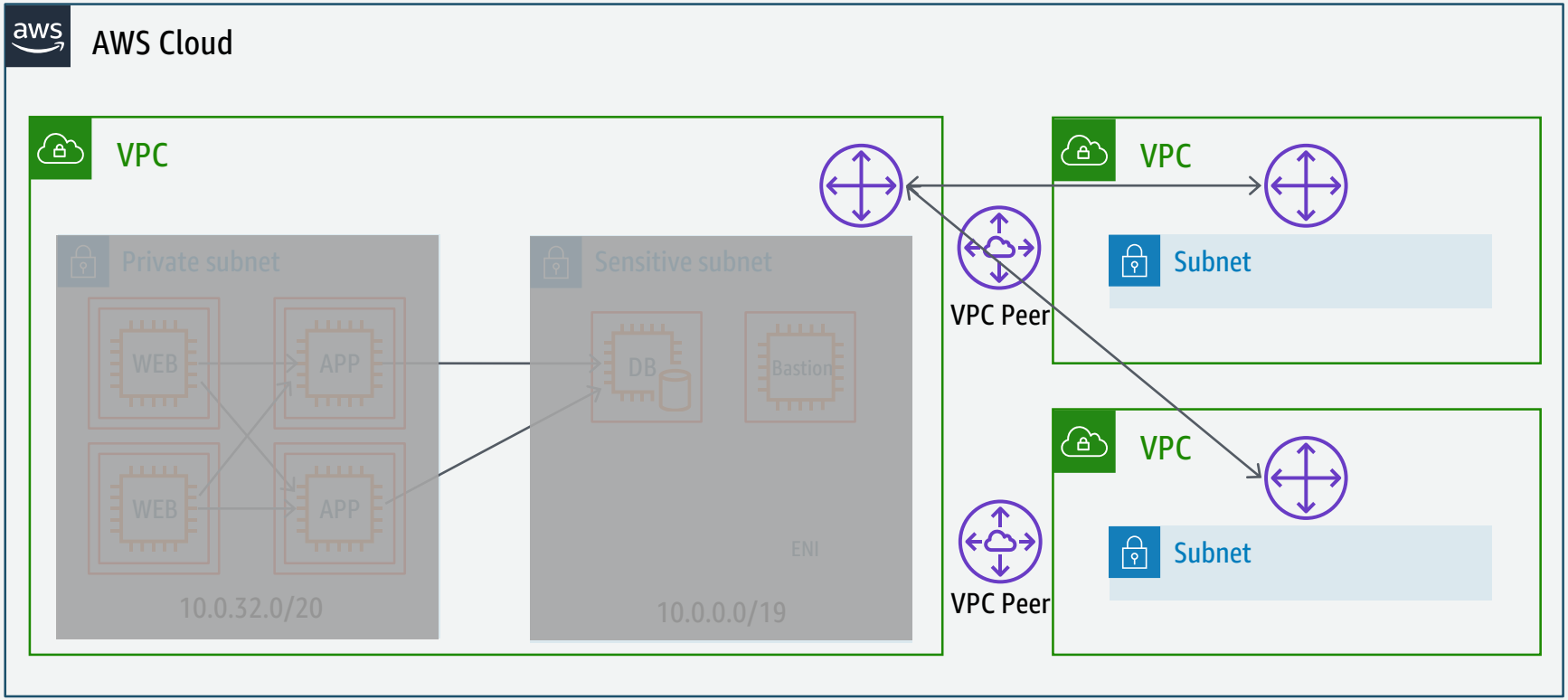
aws professional services

VPC PrivateLink



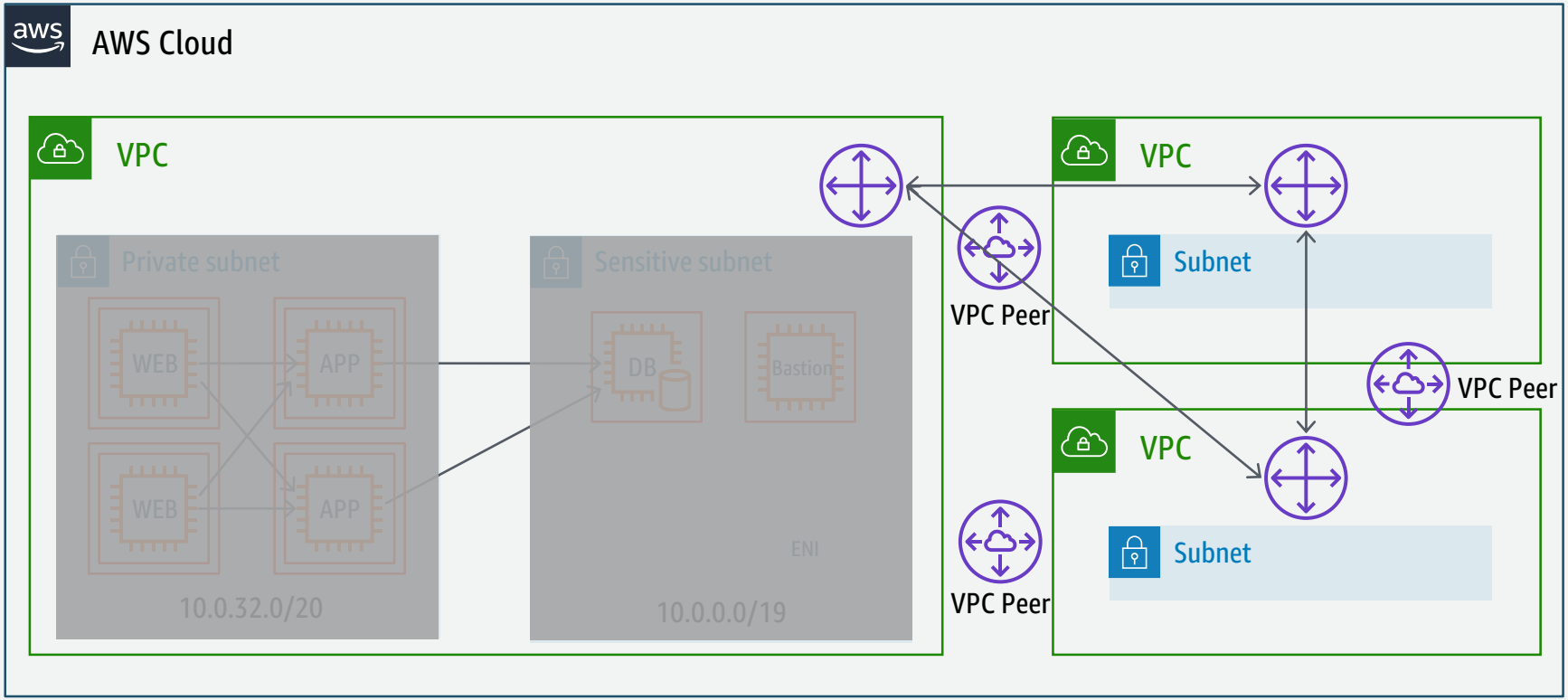
aws professional services

VPC Peering



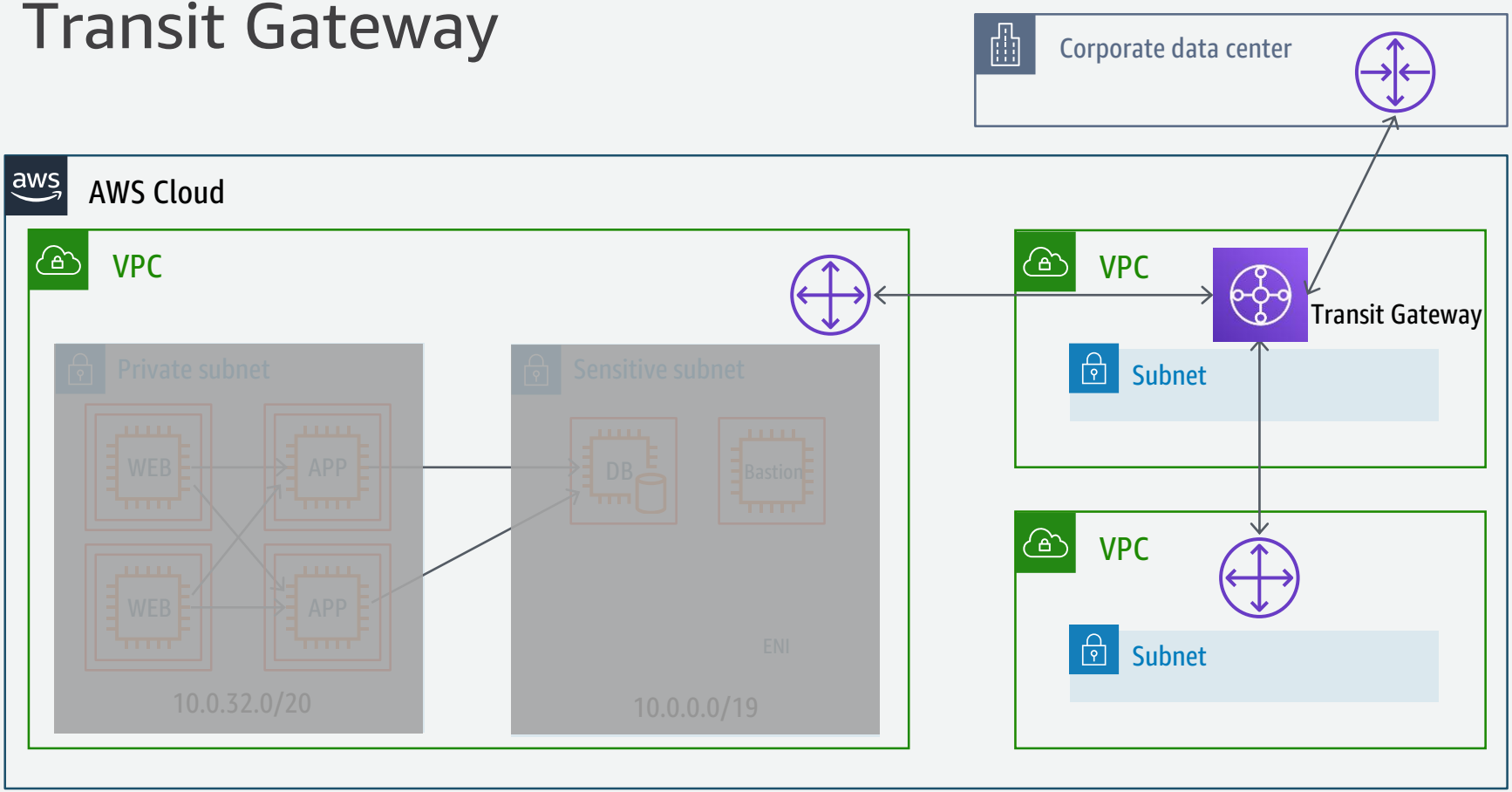
aws professional services

VPC Peering



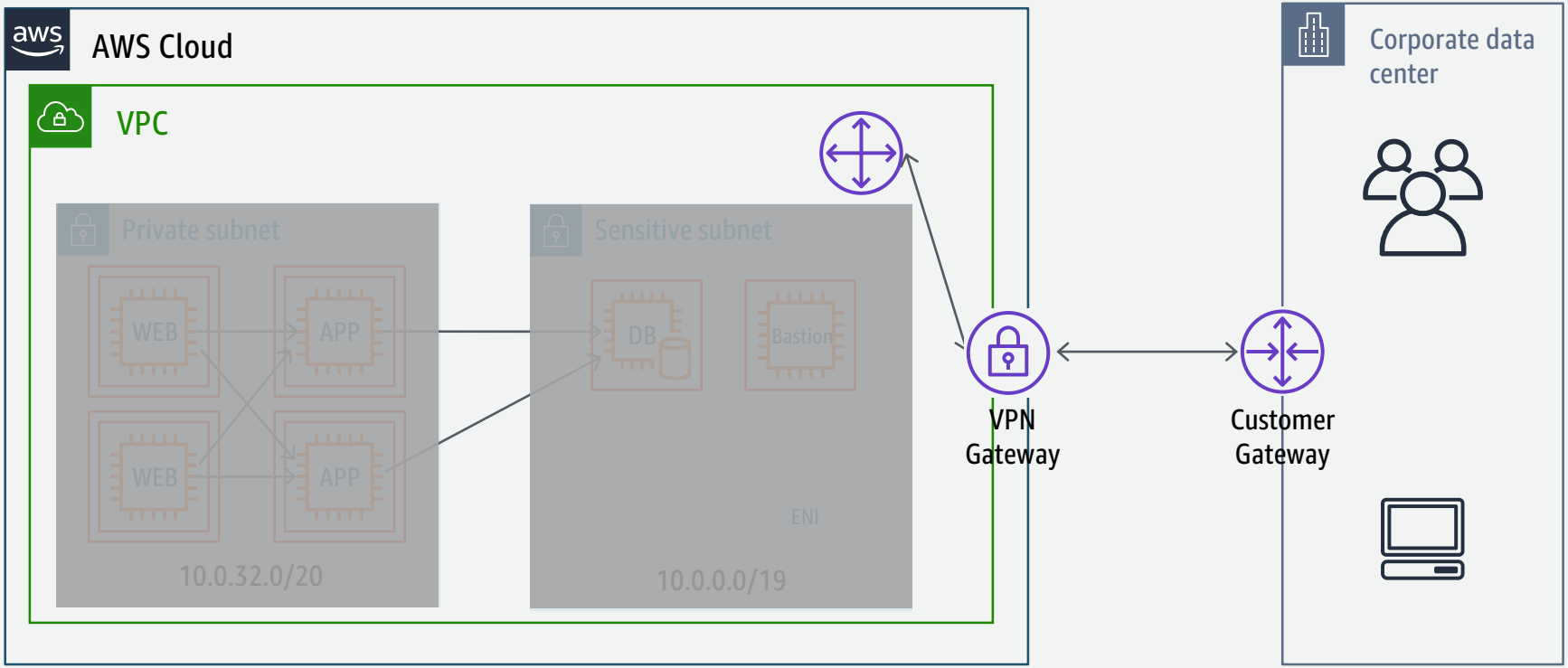
aws professional services

Transit Gateway



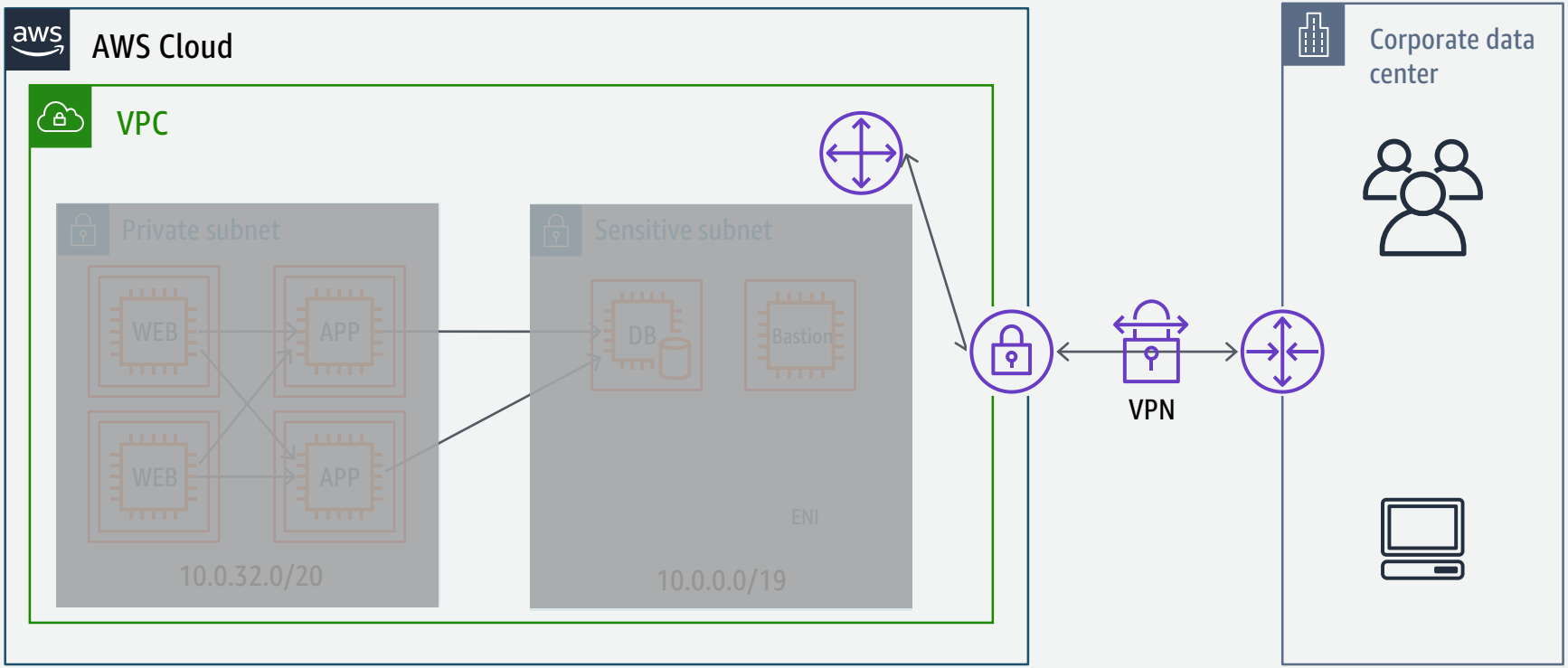
aws professional services

VPN



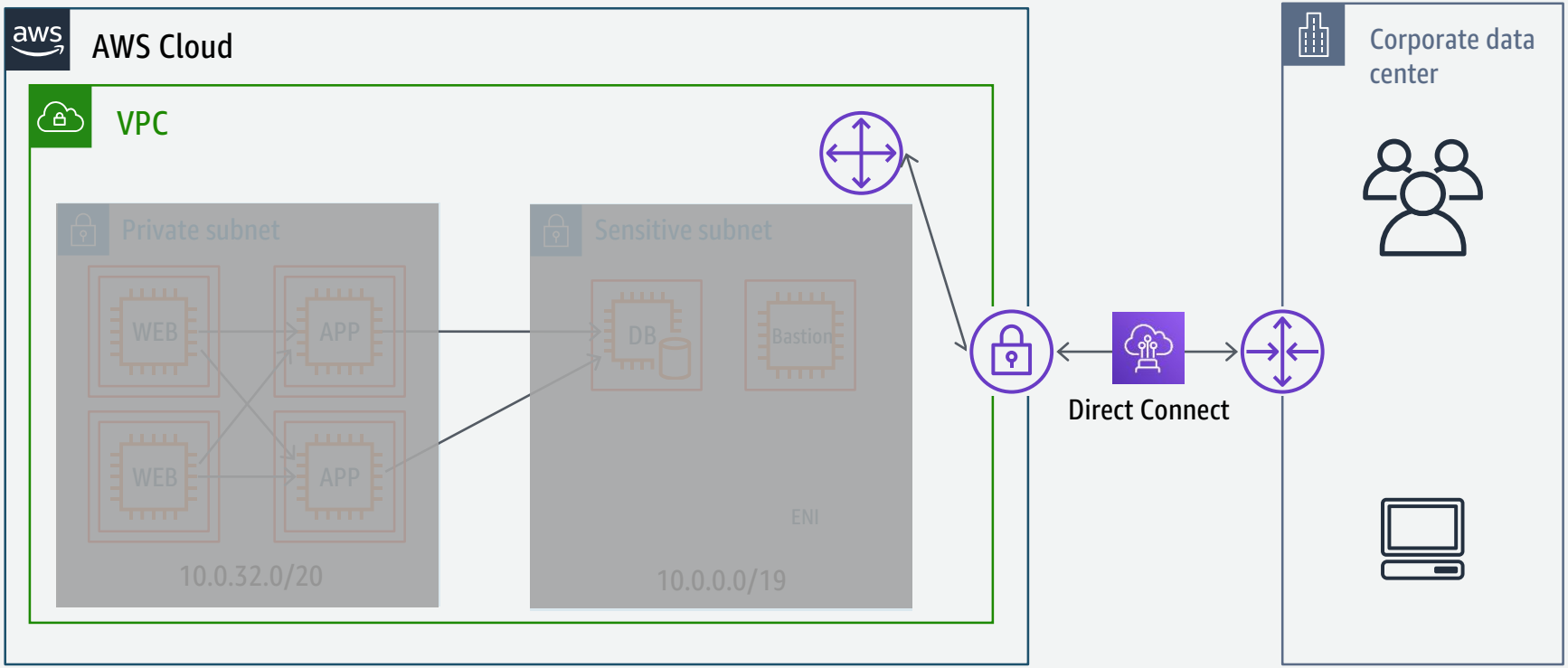
aws professional services

VPN



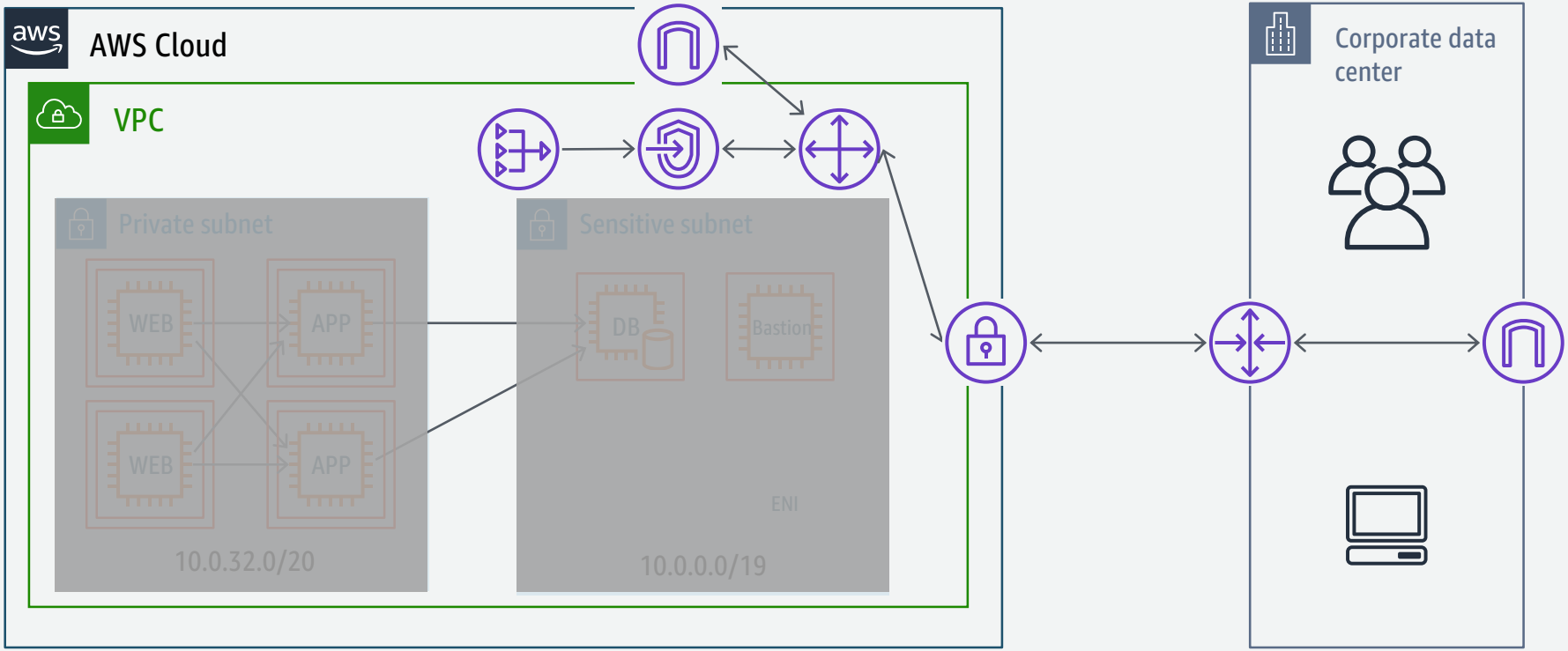
aws professional services

Direct Connect



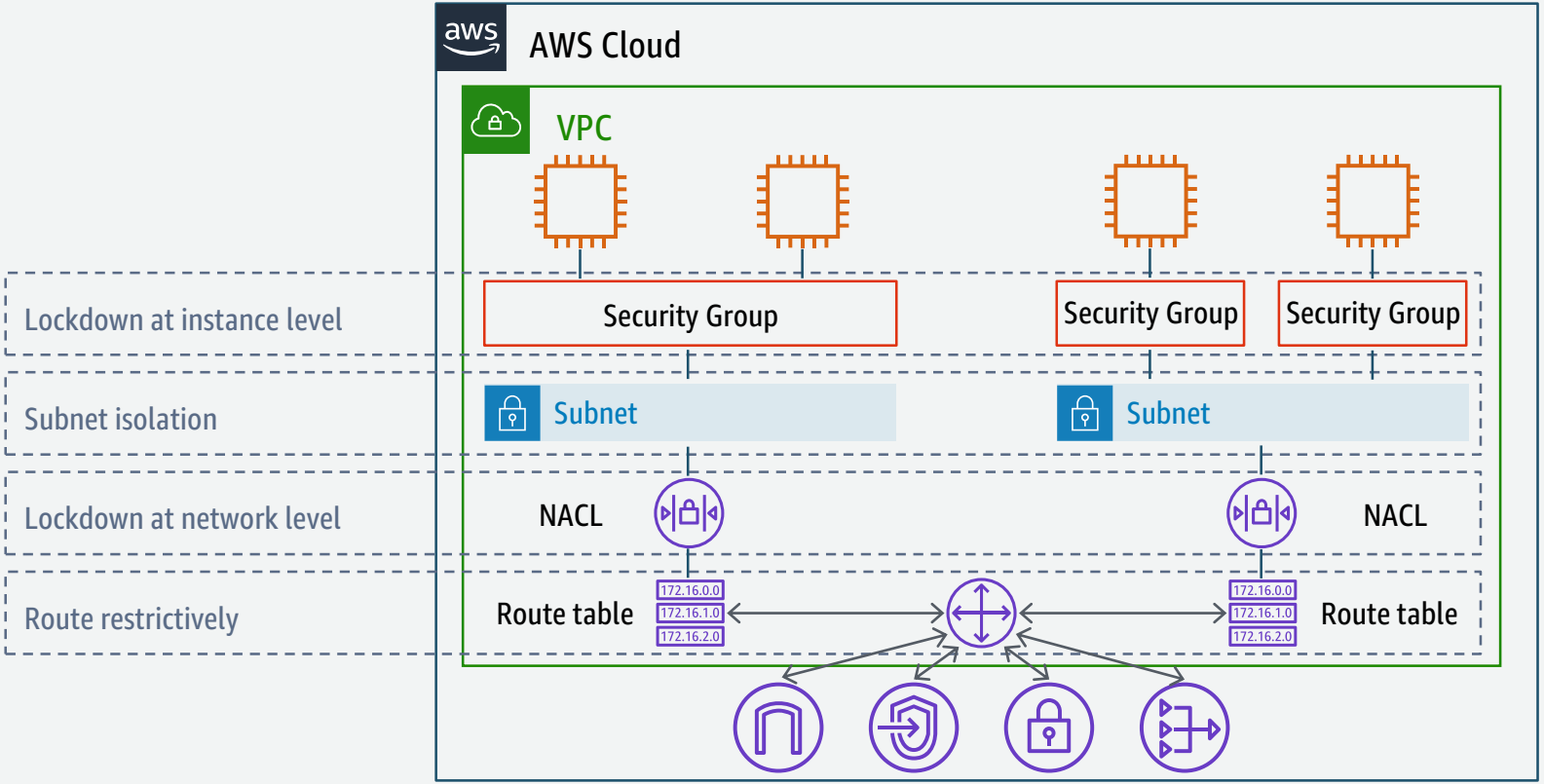
aws professional services

Multiple Gateways



aws professional services

Network Defense in Depth



aws professional services

Questions?

aws professional services