



Virtual Private Cloud Basics

Explained by a Triple AWS Certified Cloud Specialist!

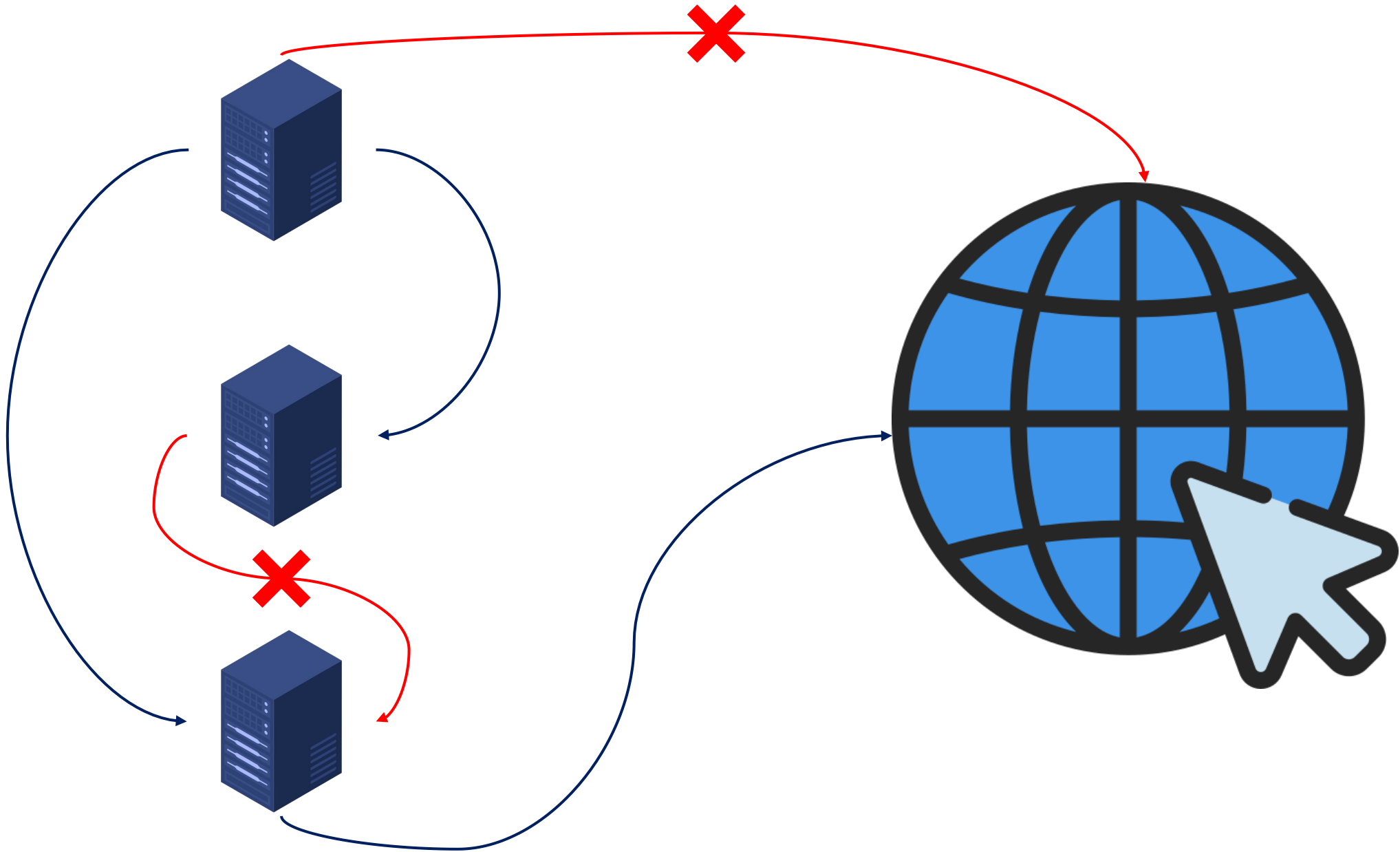






A VPC is a secure, isolated virtual network in the cloud where you can control how resources connect to each other and to the internet.





IP Address Range

10.16.0.0

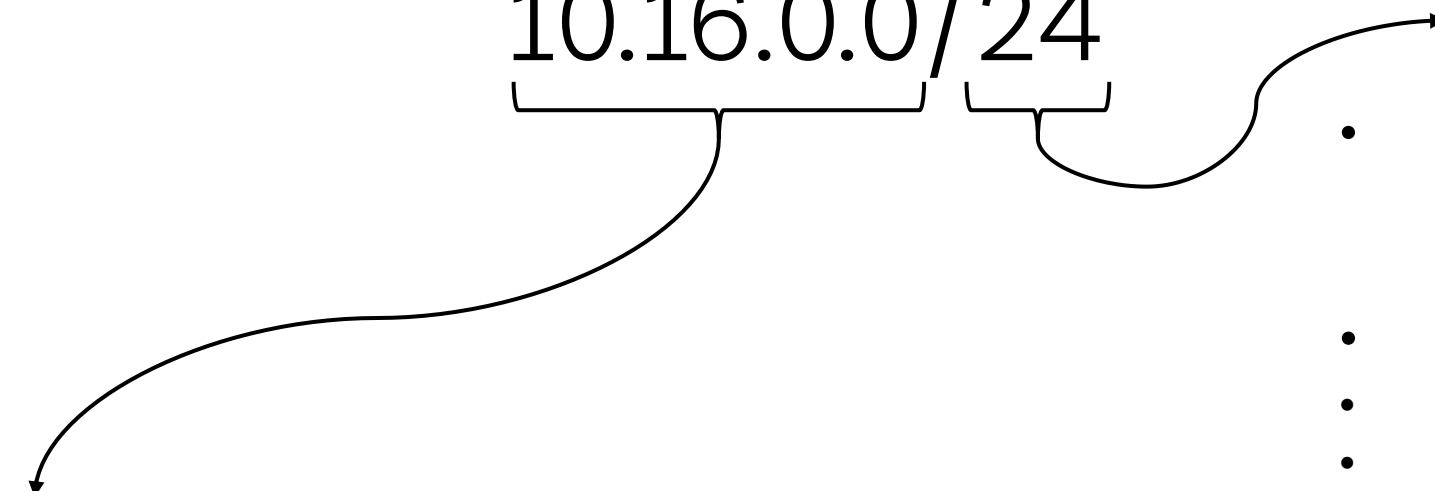


10.16.0.255

IP Address Range

CIDR Block:

10.16.0.0/24



CIDR

- How many IP Addresses in the block?
- $2^{(32-[CIDR])}$
- E.G. $2^{(32-24)} = 2^8 = 256$
- 256 available IPs

Start of Range

VPC
10.16.0.0/20



CIDR Block

- Available IP Addresses = $2^{(32-[CIDR])}$
 - = $2^{(32-20)} = 2^{12} = 4096$

VPC
10.16.0.0/20



10.16.5.171



10.16.11.27

CIDR Block

- Available IP Addresses = $2^{(32-[CIDR])}$
 - = $2^{(32-20)} = 2^{12} = 4096$
- 10.16.0.0 \Rightarrow 10.16.15.255

VPC

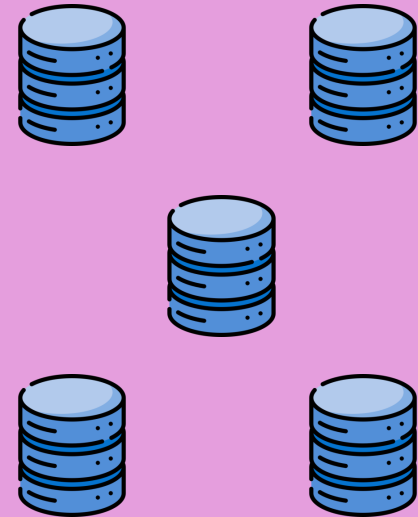
10.16.0.0/20



WEB Subnet
10.16.0.0/21



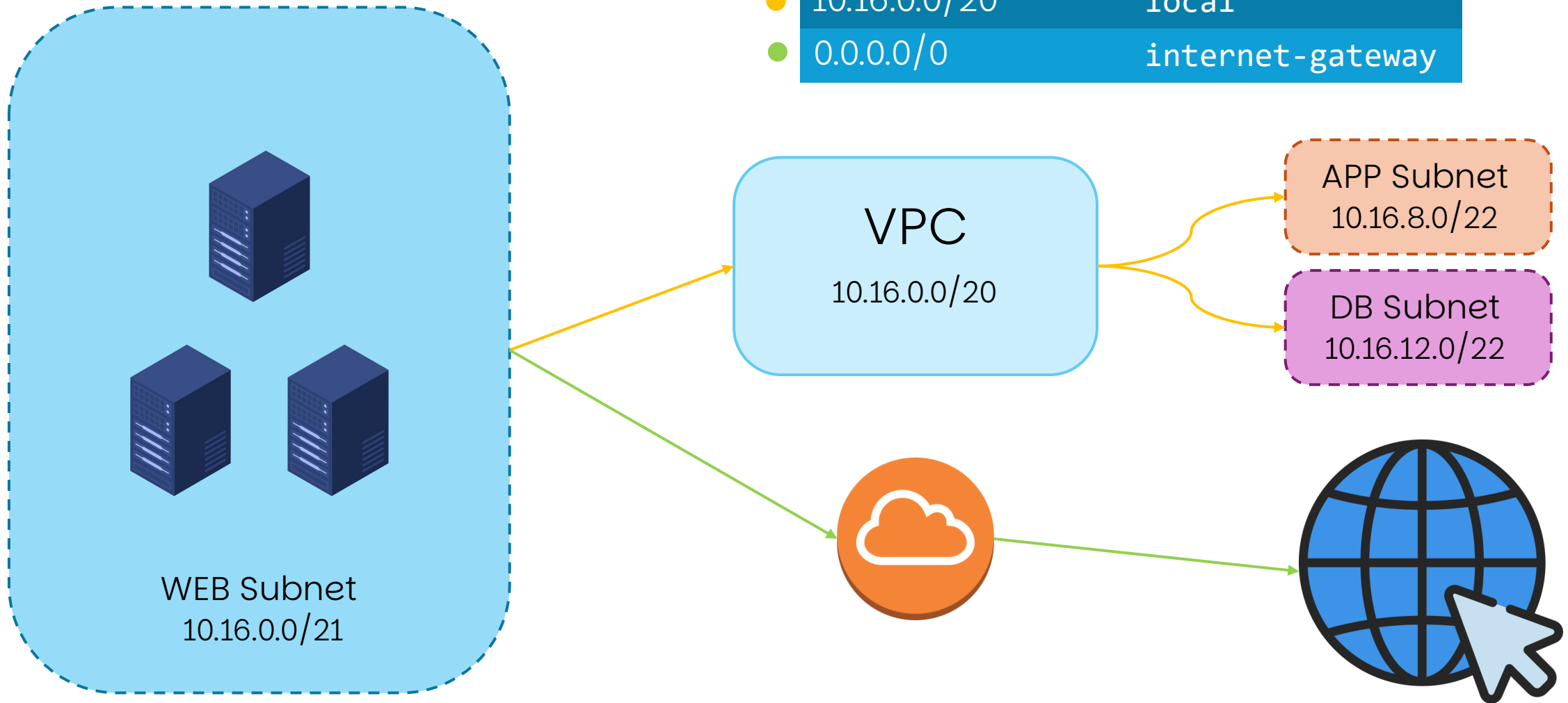
APP Subnet
10.16.8.0/22



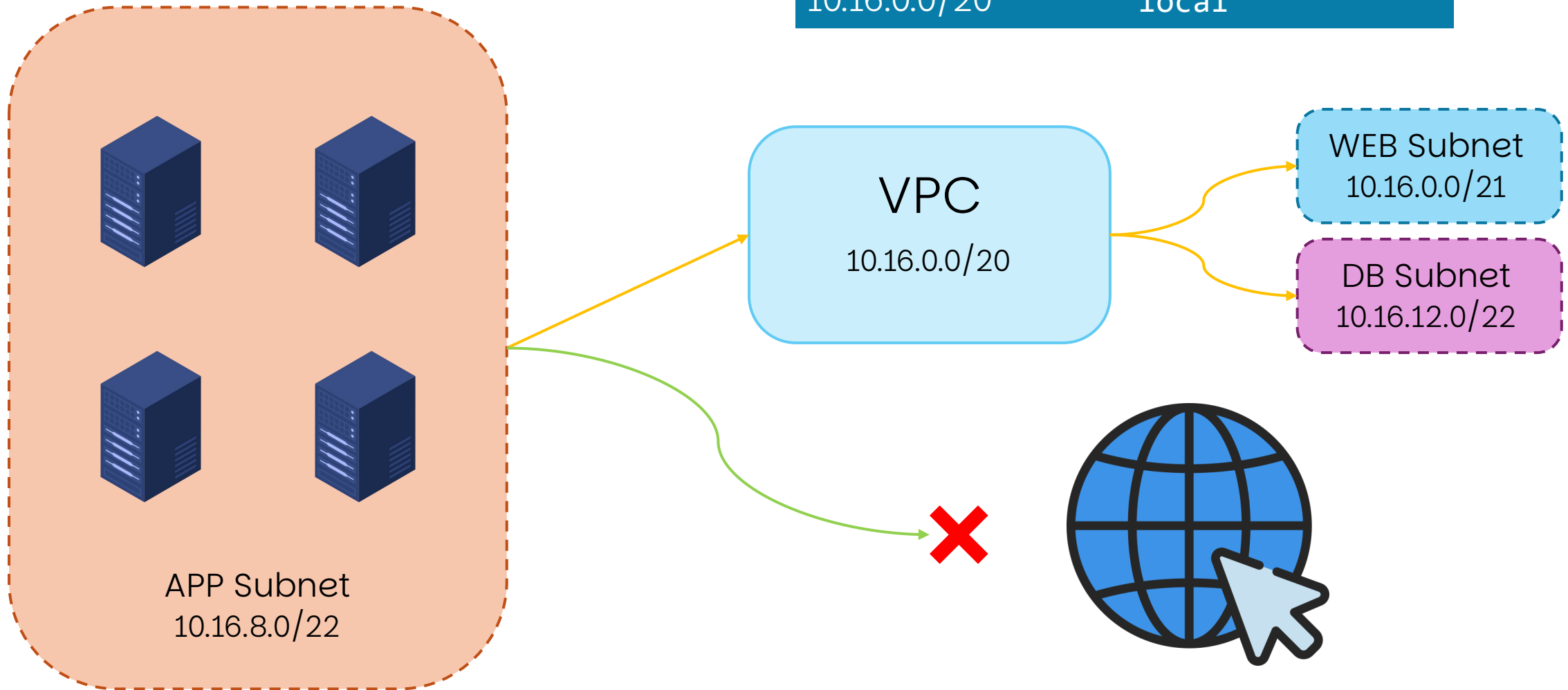
DB Subnet
10.16.12.0/22

Route Tables

Destination	Target
10.16.0.0/20	local
0.0.0.0/0	internet-gateway



Destination	Target
10.16.0.0/20	local

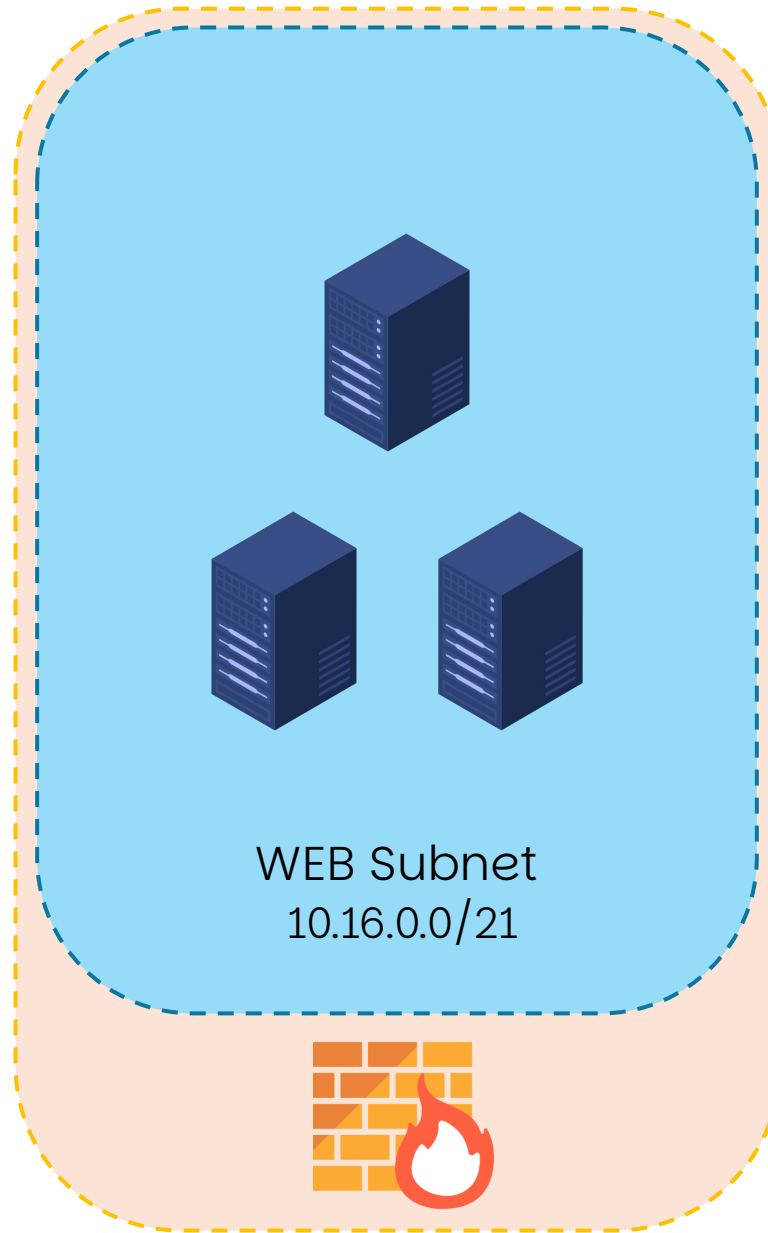


Firewalls

Rule #	Type	Protocol	Port Range	Source	A/D
100	ALL Traffic	ALL	ALL	82.194.5.163/32	DENY

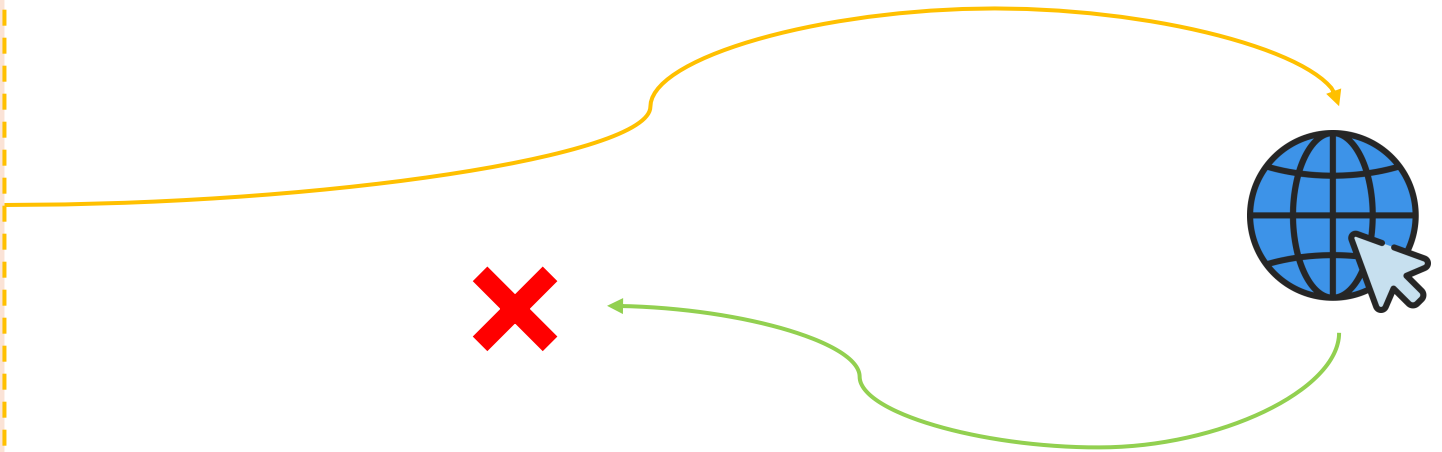
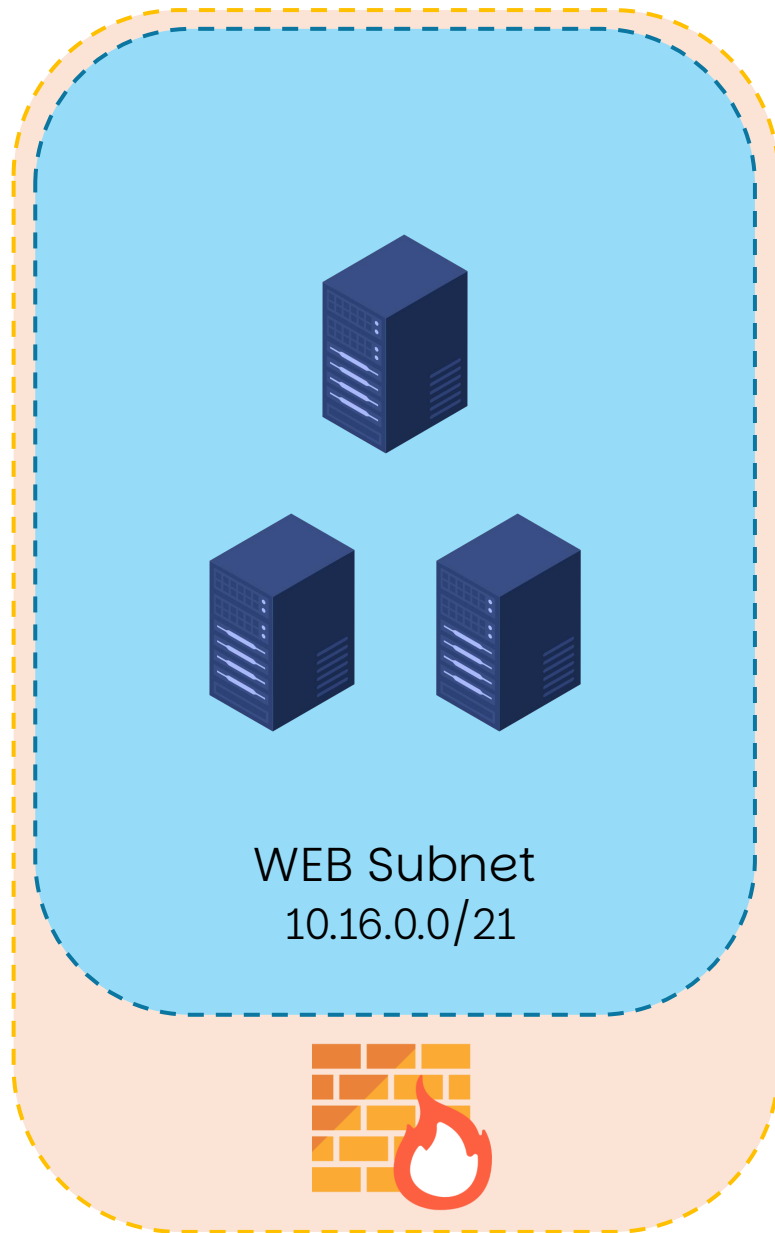


82.194.5.163



Network ACL

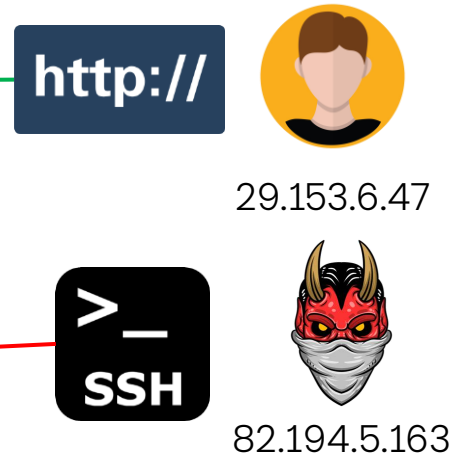
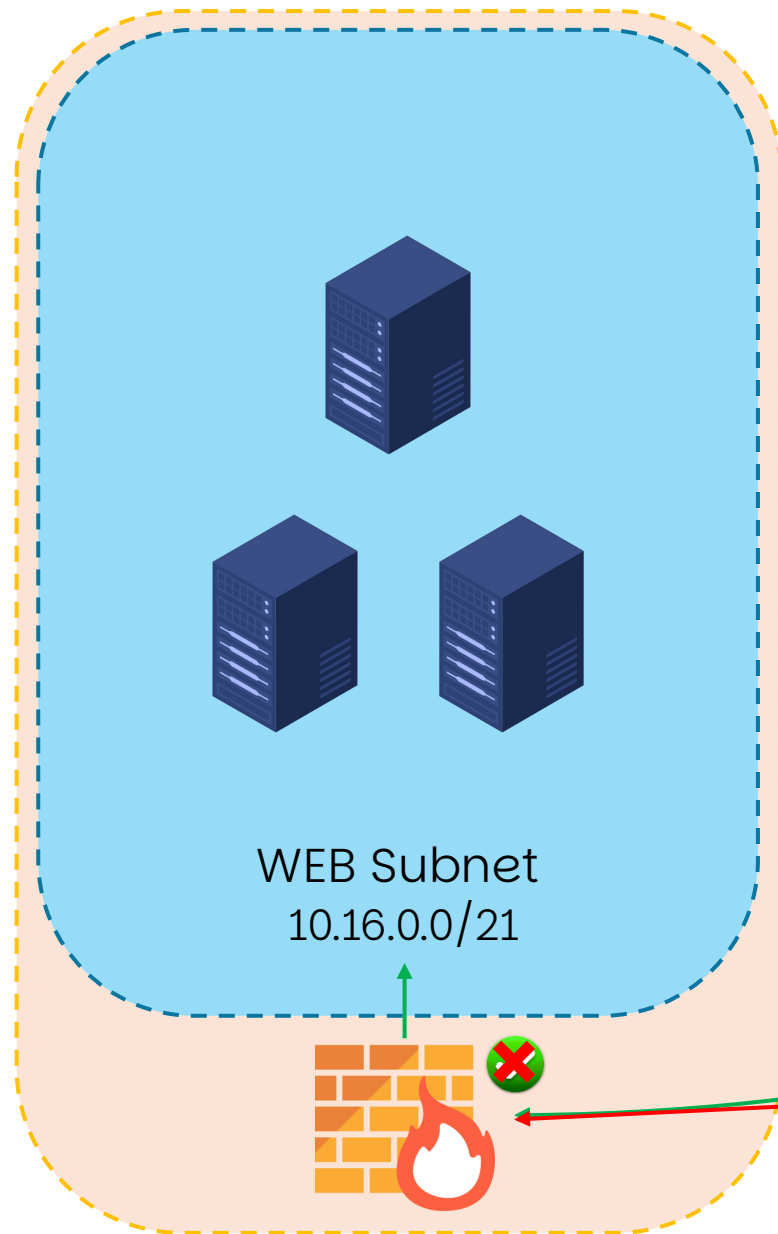
- Operates on subnets
- Stateless
- Have to define both inbound rules and outbound rules

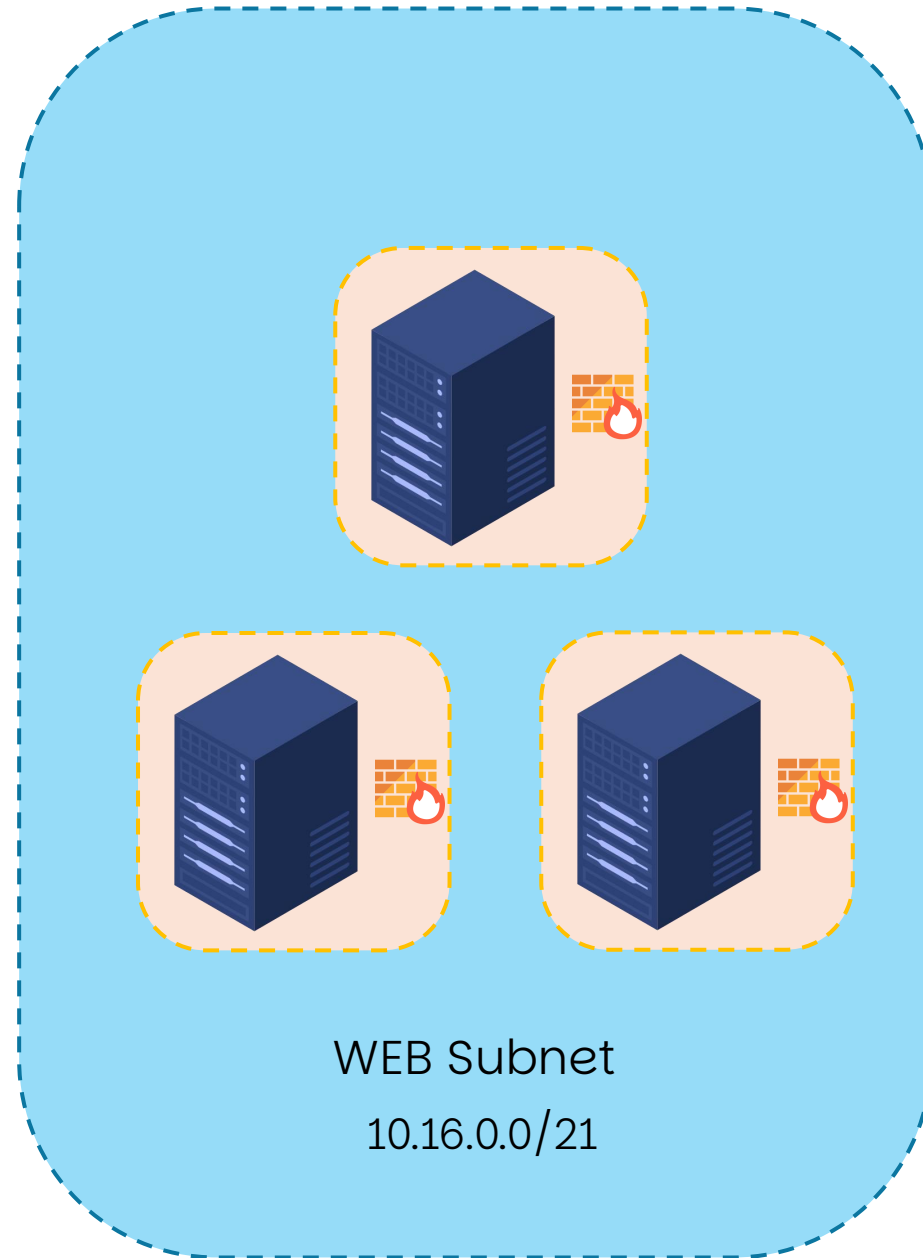


Network ACL

- Operates on subnets
- Stateless
- Have to define both inbound rules and outbound rules
- Rules evaluated in order of Rule #, starting with the lowest

Rule #	Type	Protocol	Port Range	Source	A/D
100	HTTP	TCP	80	0.0.0.0/0	ALLOW
200	ALL	ALL	ALL	0.0.0.0/0	DENY

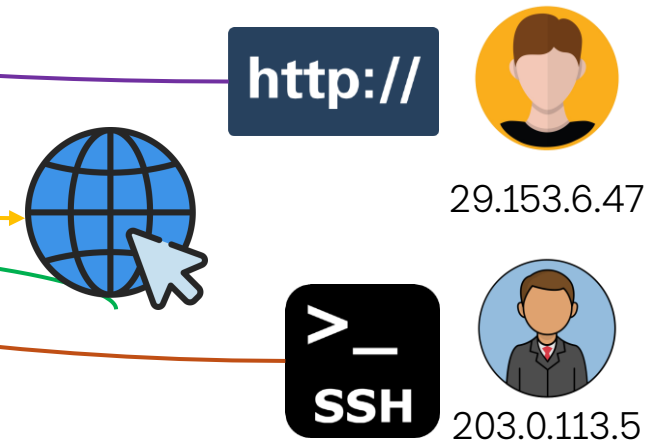
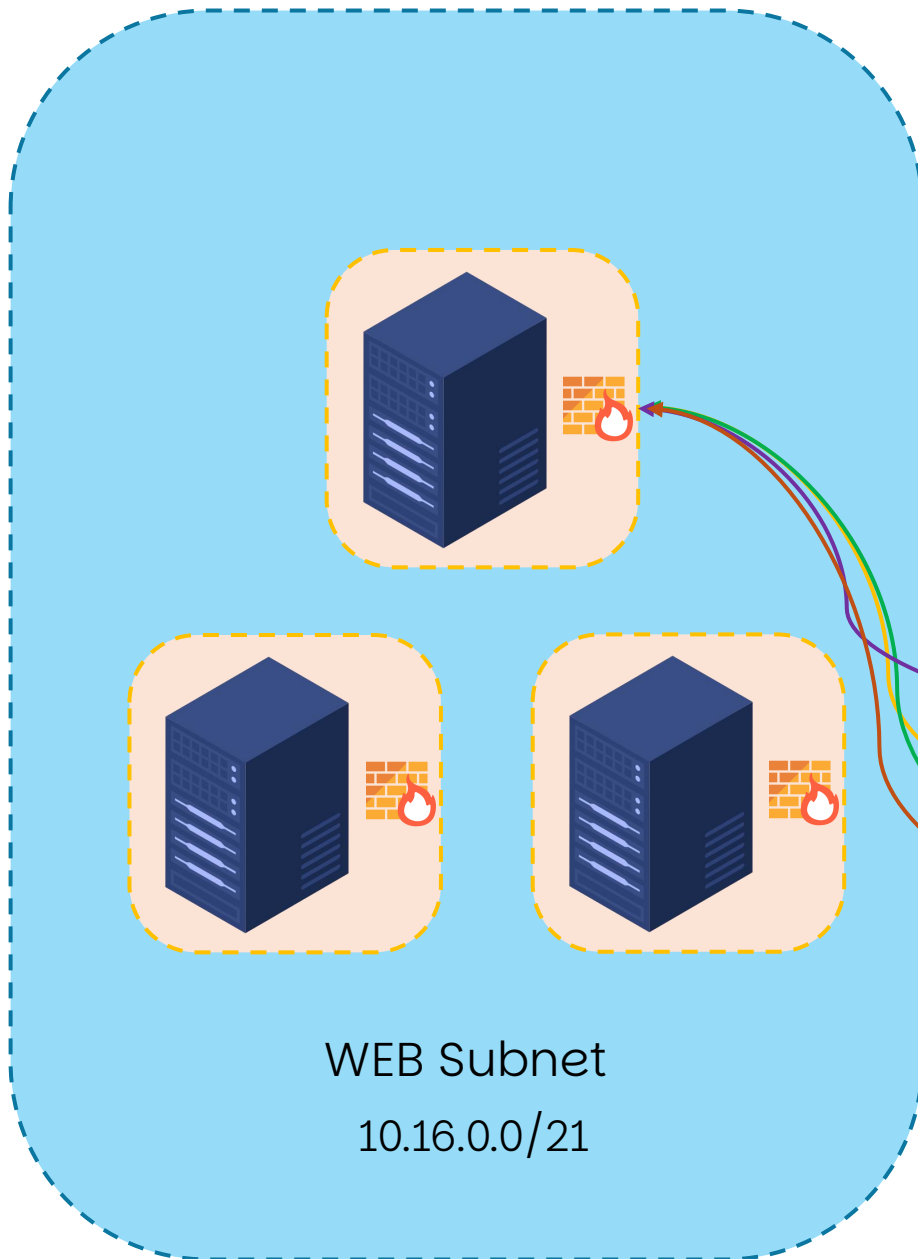




Security Groups

- Operates on infrastructure directly
- Stateful
- Don't need to define both inbound rules and outbound rules

Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	203.0.113.5/32



- Customer needs a VPC for their banking application.
- Web, app and database components.
- At max, they will have running together:
 - 150 web servers serving the website
 - 1250 web servers serving the app logic
 - 300 database instances
- Large growth expected.
- Known hacking attempts from IP Addresses 185.219.143.0 – 185.219.143.7 (185.219.143.0/29)

- As large growth is expected, keep $\frac{2}{3}$ of available IP allocations empty.
- 3 subnets

Min. 5632 IP Addresses Required

Banking App - VPC

10.16.0.0/19

150 instances

×3 (for future growth)

= 450 required IP
Addresses

Round to nearest power of 2

$2^9 = 512$
512 IP Address allocations

/23 CIDR

WEB Subnet
10.16.0.0/23

1250 instances

×3 (for future growth)

= 3750 required IP
Addresses

Round to nearest power of 2

$2^{12} = 4096$
4096 IP Address allocations

/20 CIDR

APP Subnet
10.16.2.0/20

300 instances

×3 (for future growth)

= 900 required IP
Addresses

Round to nearest power of 2

$2^{10} = 1024$
1024 IP Address allocations

/22 CIDR

DB Subnet
10.16.18.0/22

Min. 5632 IP Addresses Required

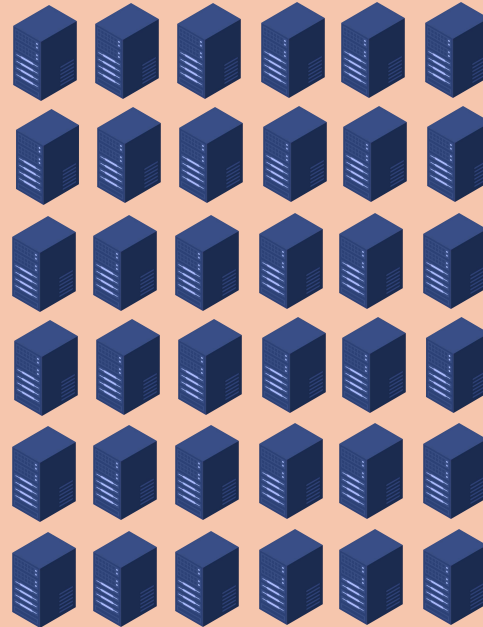
Banking App - VPC

10.16.0.0/19



/23 CIDR

WEB Subnet
10.16.0.0/23



/20 CIDR

APP Subnet
10.16.2.0/20



/22 CIDR

DB Subnet
10.16.18.0/22

WEB Subnet
10.16.0.0/23

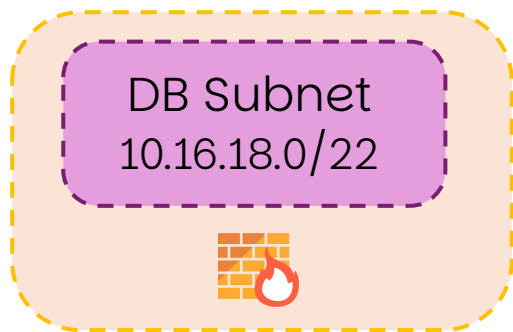
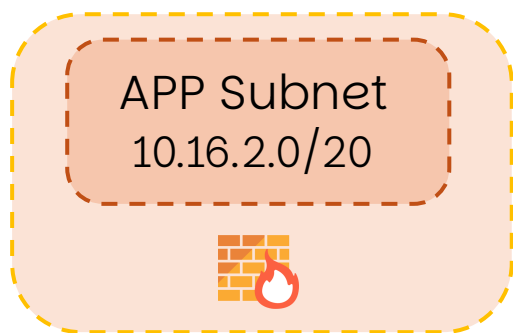
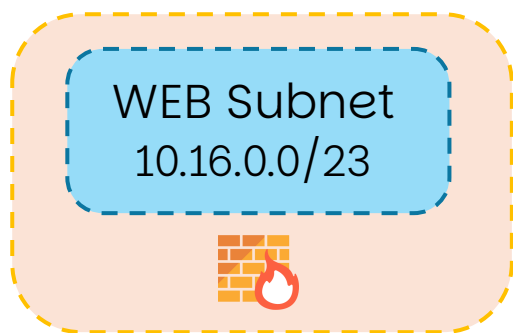
Destination	Target
10.16.0.0/19	local
0.0.0.0/0	internet-gateway

APP Subnet
10.16.2.0/20

Destination	Target
10.16.0.0/19	local

DB Subnet
10.16.18.0/22

Destination	Target
10.16.0.0/19	local



Inbound Rules

Rule #	Protocol	Port Range	Source	A/D
100	ALL	ALL	185.219.143.0/29	DENY
110	TCP	80, 443	0.0.0.0/0	ALLOW
120	TCP	1024-65535	10.16.2.0/20	ALLOW
200	ALL	ALL	*	DENY

Rule #	Protocol	Port Range	Source	A/D
100	ALL	ALL	185.219.143.0/29	DENY
110	TCP	443	10.16.0.0/23	ALLOW
120	TCP	3306	10.16.18.0/22	ALLOW
200	ALL	ALL	*	DENY

Rule #	Protocol	Port Range	Source	A/D
100	ALL	ALL	185.219.143.0/29	DENY
110	TCP	3306	10.16.2.0/20	ALLOW
200	ALL	ALL	*	DENY

Outbound Rules

Rule #	Protocol	Port Range	Source	A/D
100	ALL	ALL	185.219.143.0/29	DENY
110	TCP	1024-65535	0.0.0.0/0	ALLOW
120	TCP	443	10.16.2.0/20	ALLOW
200	ALL	ALL	*	DENY

Rule #	Protocol	Port Range	Source	A/D
100	ALL	ALL	185.219.143.0/29	DENY
110	TCP	3306	10.16.18.0/22	ALLOW
120	TCP	443	0.0.0.0/0	ALLOW
200	ALL	ALL	*	DENY

Rule #	Protocol	Port Range	Source	A/D
100	ALL	ALL	185.219.143.0/29	DENY
110	TCP	1024-65535	10.16.2.0/20	ALLOW
200	ALL	ALL	*	DENY



Thanks for reading!

 @hamdivazim

Check out the video at
<https://youtube.com/@hamdivazim>!

 [@hamdivazim](#)

 <https://hamdivazim.hamdtel.co.uk>