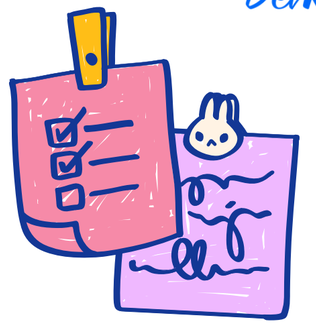
DevKTOps

ARCHITECTING ON aws

Module 5: Network Layer 1

Module Overeiw



- Amazon Virtual Private Cloud (VPC)
- Subnets
- Gateways
- Network Security

What is VPC?

Amazon VPC

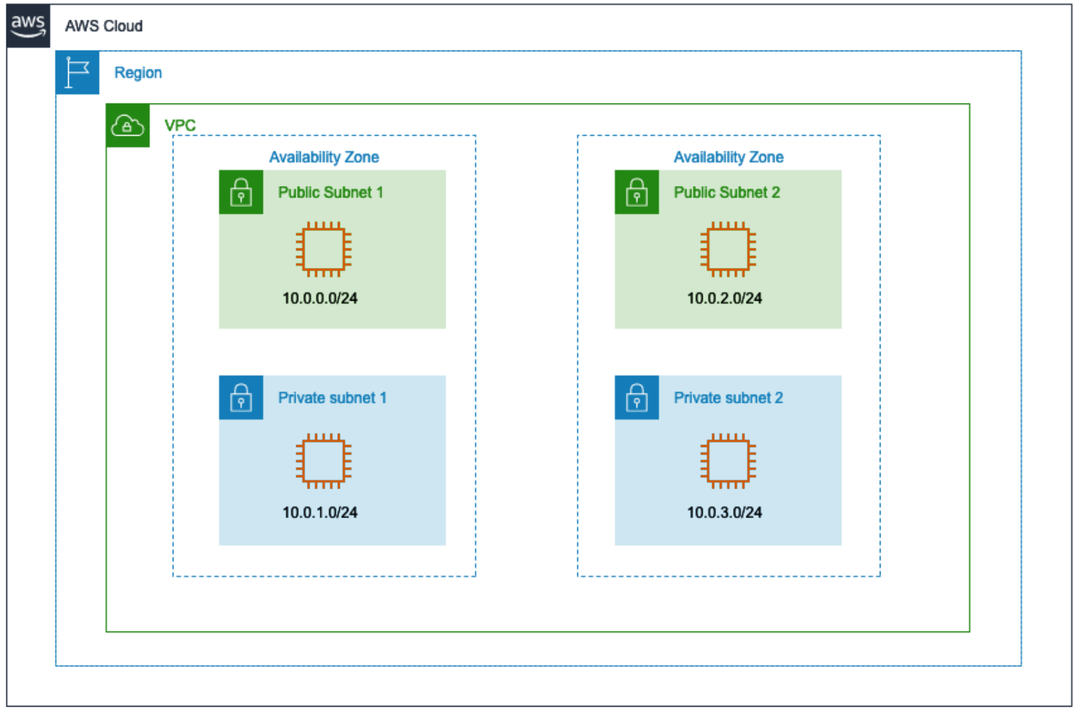
- A private, isolated section of the AWS Cloud
- A virtual network topology you can deploy and customize
- Resembles a traditional network in your own data centre
- All new accounts created post-2013 are in "Default-VPC"

Amazon VPC Specifics

Amazon VPC

- A VPC is a virtual network dedicated to your AWS account
- Requires an IPv4 address space and optionally IPv6 address ranges
- Enables you to create specific CIDR ranges for your resources to occupy
- Provides strict access rules for inbound and outbound traffic.

Deploying a VPC



VPCs deploy into 1 of the 34 AWS Regions

A VPC can host resources from any Availability Zone within its region

Using One VPC

One VPC could be appropriate with the following limited use cases:

- Small, single applications managed by one person or a very small team
- High-performance computing
- Identity management

For most Use Cases

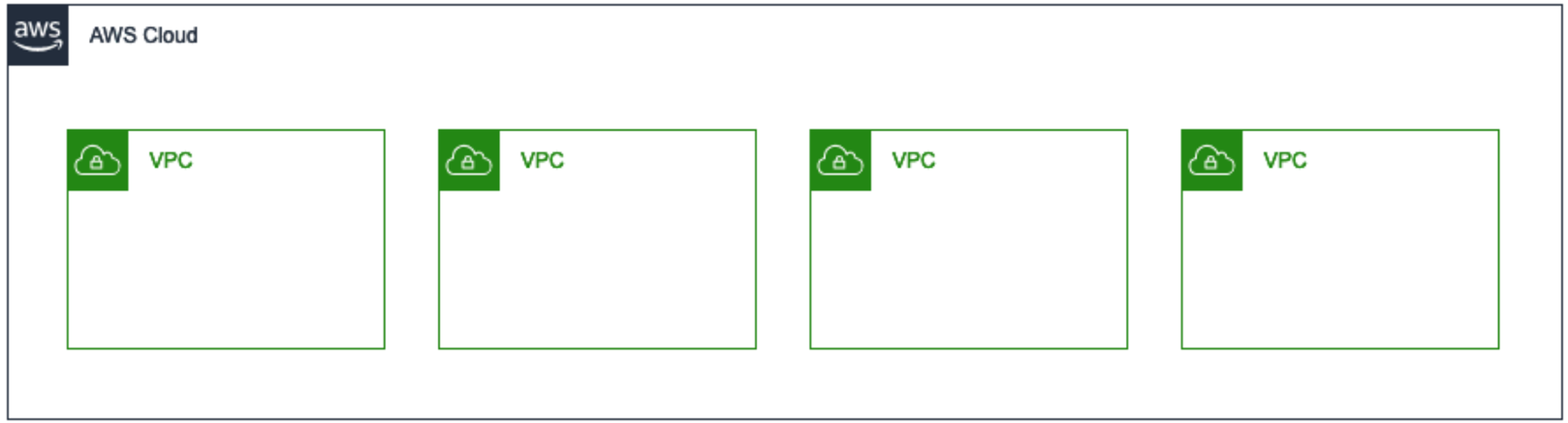
1

Multi-VPC Pattern

2

Multi-Account Pattern

Multi-VPC Pattern



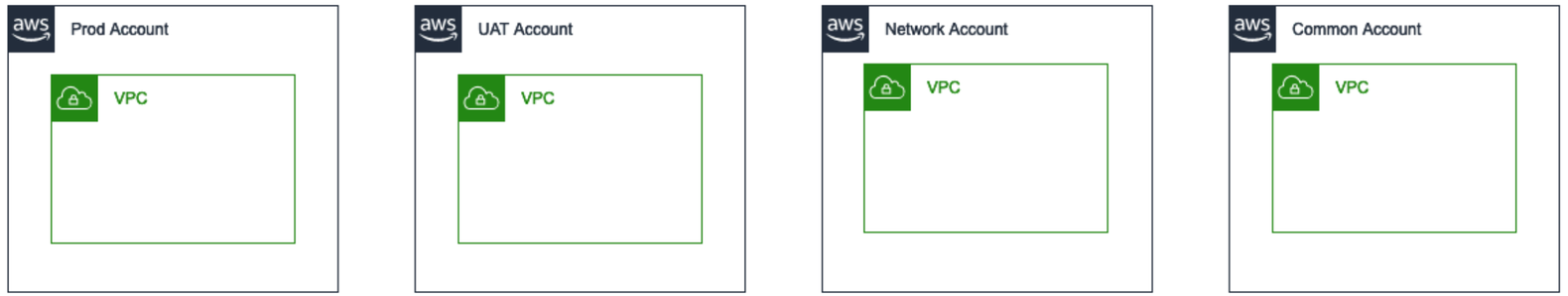
Best Suited for:

- Single team or single organizations that maintains full control over the provisioning and management of all resources in each application env.

Exception:

- Governance and compliance standards may require greater workload isolation regardless of organizational complexity

Multi-Account Pattern

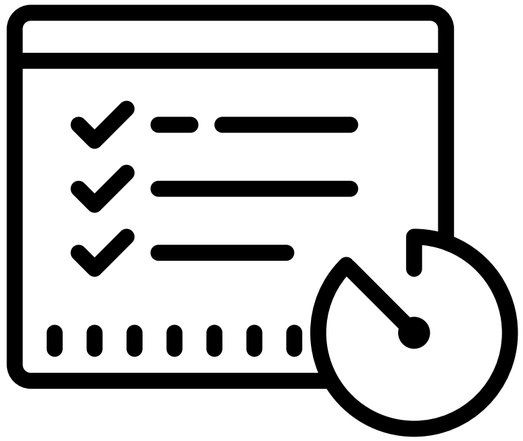


Best Suited for:

- Large organizations and organizations with multiple IT teams
- Medium-sized organizations that anticipate rapid growth

Managing access and standards can be more challenging in more complex organizations

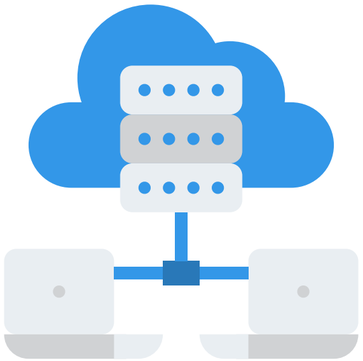
VPC Limits



You can have multiple VPCs in the same region but

Service limit : **5** VPCs per region per account

CIDR?



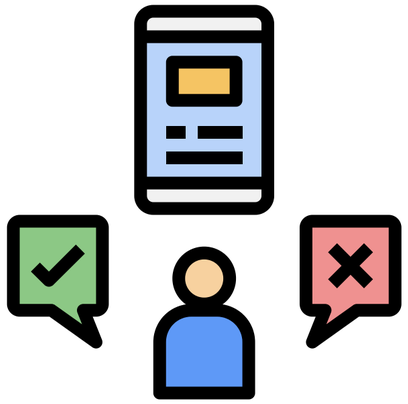
0.0.0.0/0	= All IPs
10.22.33.44/32	= 10.22.33.44
10.22.33.0/24	= 10.22.33.*
10.22.0.0/16	= 10.22.*.*

CIDR	Total IPs
/28	16
...	...
/20	4,096
/19	8,192
/18	16,384
/17	32,768
/16	65,536

VPC IP Addressing

- Internal to VPC
  - VPCs can be between /16 and /28
  - VPCs support subnetting
  - VPC CIDRs cannot be modified once created
  - Additional CIDRs can be added to a VPC
- External
  - Support IPv4 and IPv6
  - Support bringing your own IP space

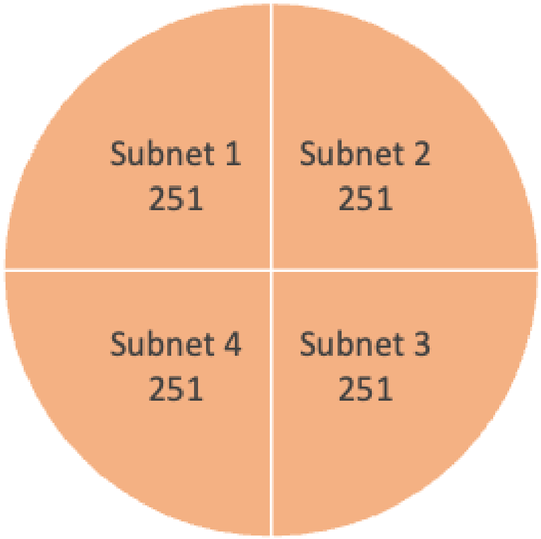
VPC IP Address Considerations



Plan your IP space before creating it

- Overlapping IP spaces = future headache
- Consider using multiple VPCs
- Consider future AWS region expansion
- Consider future connectivity to corporate networks
- Consider subnet design

Subnets



A VPC with CIDR/22 includes 1,024 total IPs

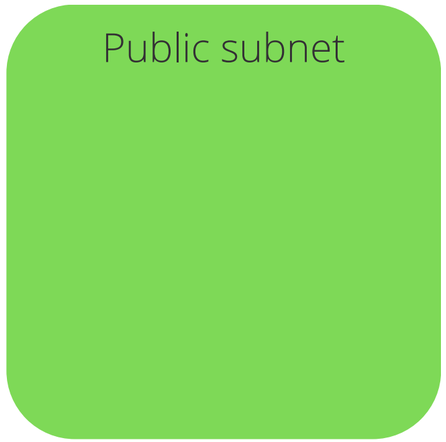
- VPCs span a region
- Subnets are allocated as a subset of the VPC CIDR range and span a specific AZ
- You can have multiple subnets in each VPC and each AZ
- Implicit route between all subnets within a VPC
- AWS will reserve five IP addresses from each subnet
  - For example, CIDR 10.0.0.0/24,
  - 10.0.0.0: network address
  - 10.0.0.1: Reserved by AWS for the VPC router
  - 10.0.0.2: Reserved by AWS (for DNS)
  - 10.0.0.3: Reserved by AWS for future use
  - 10.0.0.255: Network broadcast address

Route Tables

Destination	Target
10.0.0.0/16	local

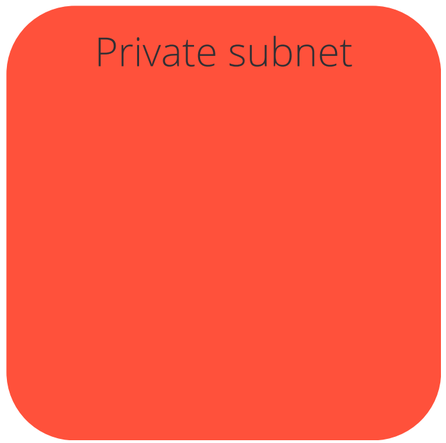
- Each subnet has associated routing table
- Routing tables can be associated with multiple subnets
- Required to direct traffic between VPC resources
- Each VPC has a main (default) route table
- You can create custom route tables
- All subnets must have an associated route table

Different Levels of Subnets



Public subnets

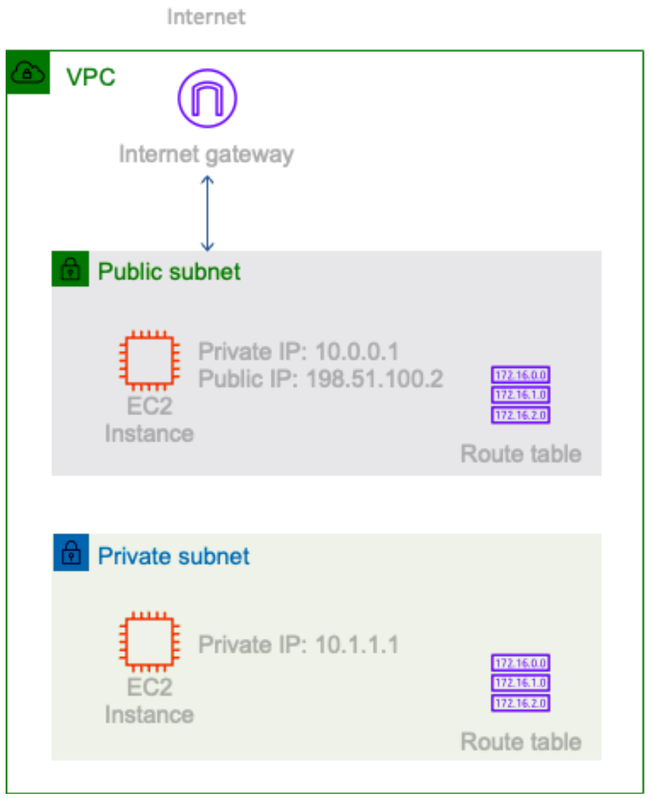
- Include a routing table entry to an internet gateway to support inbound/outbound access to the public internet



Private subnets

- Do not have a routing table entry to an internet gateway
- Are not directly accessible from the public internet
- Typically use a NAT gateway to support restricted, outbound public internet access

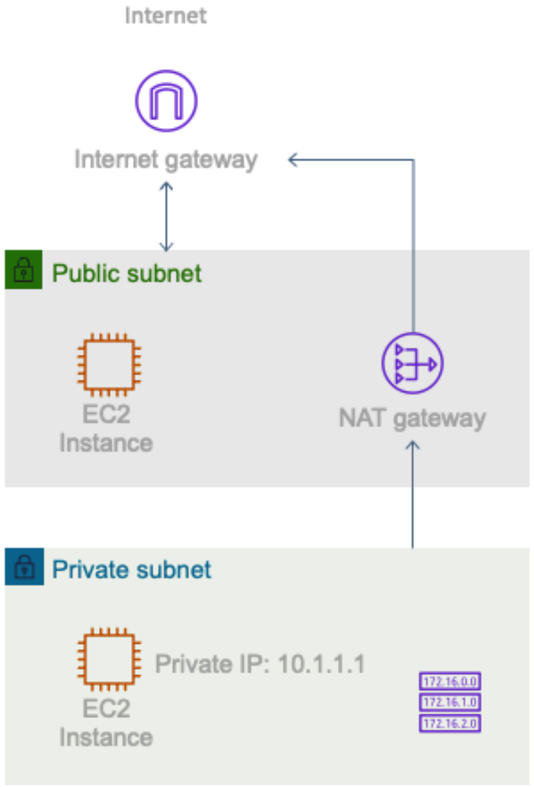
VPC to Internet via Public Subnets



Internet Gateways

- Allow communication between instances in your VPC and the internet
- Are horizontally scaled, redundant, and highly available by default
- Provide a target in your subnet route tables for internet-routable traffic
- Must be referenced on the Route Table
- Performs 1:1 NAT between Public and Private IP Addresses

VPC to Internet via Private Subnets



NAT Gateways

- Enable instances in the private subnet to initiate outbound traffic to the internet or other AWS services.
- Prevent private instances from receiving inbound traffic from the internet.
- Fully managed by AWS
- Highly available
- Up to 45Gbps aggregate bandwidth
- Supports TCP, UDP, and ICMP protocols
- Network ACLs apply to NAT gateway traffic

Elastic Network Interfaces

An elastic network interface is a virtual network interface that can be moved across EC2 instances in the same Availability Zone.

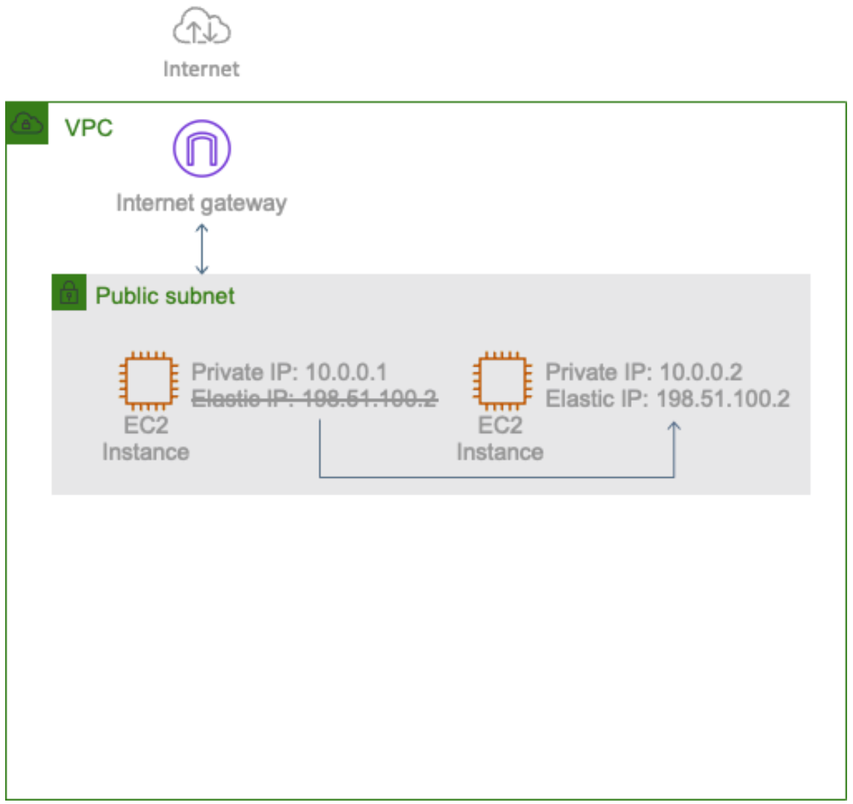
When moved to a new instance, a network interface maintains its:

- private IP address
- Elastic IP address
- MAC address

Why have more than one ENI on an instance?

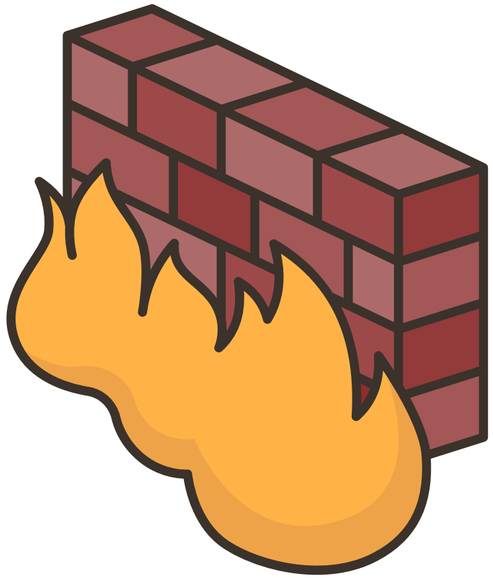
- Create a management network
- Use network and security appliances in your VPC
- Create dual-homed instances with workloads/roles on distinct subnets

Elastic IP Address



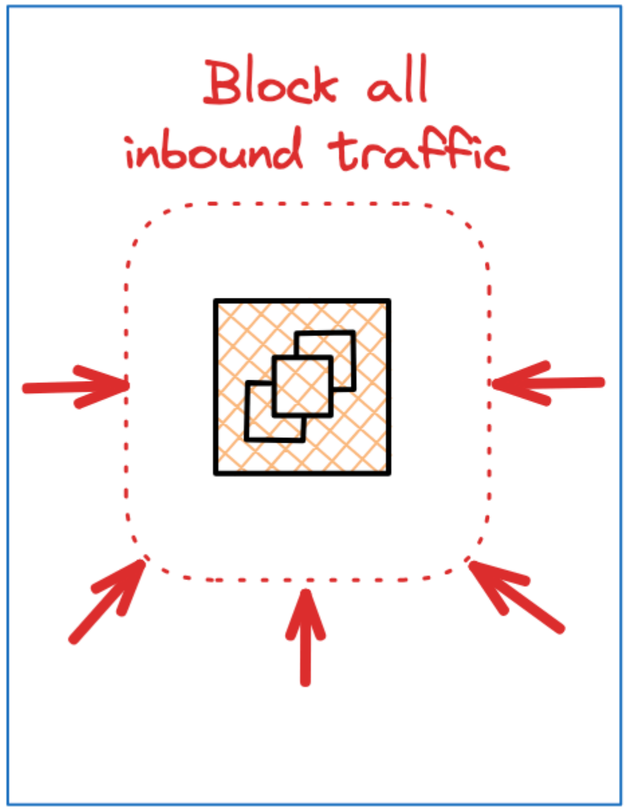
- Static, Public IPv4 address, associated with your AWS account
- Dynamically assigned
- Specific to a region
- Can be associated with an instance or network interface
- Can be remapped to another instance in your account
- Useful for redundancy when Load Balancers are not an option
- Five allowed per AWS Region (But you can increase it)

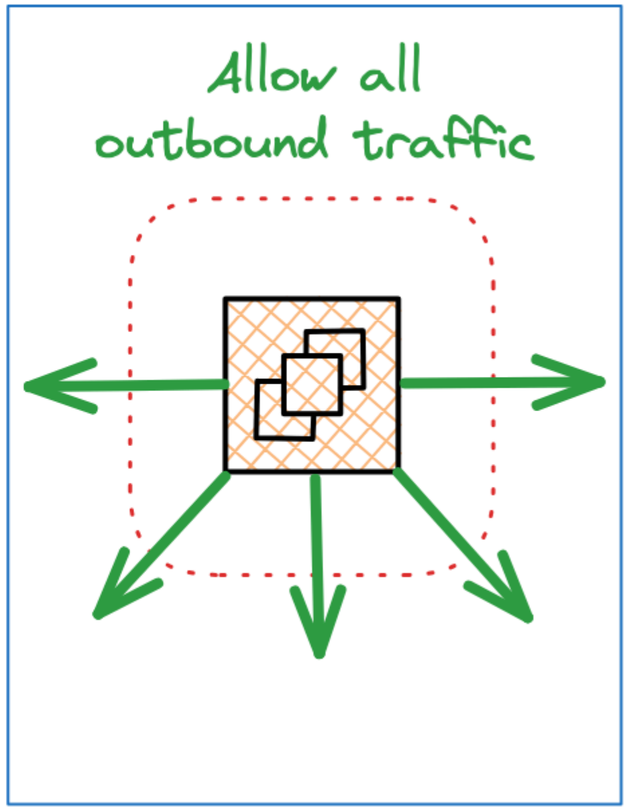
Security Groups



- Virtual firewalls that control inbound and outbound traffic into AWS resources
- Traffic can be allowed by any IP protocol, port, or IP address
- Rules are stateful

Security Groups: Default



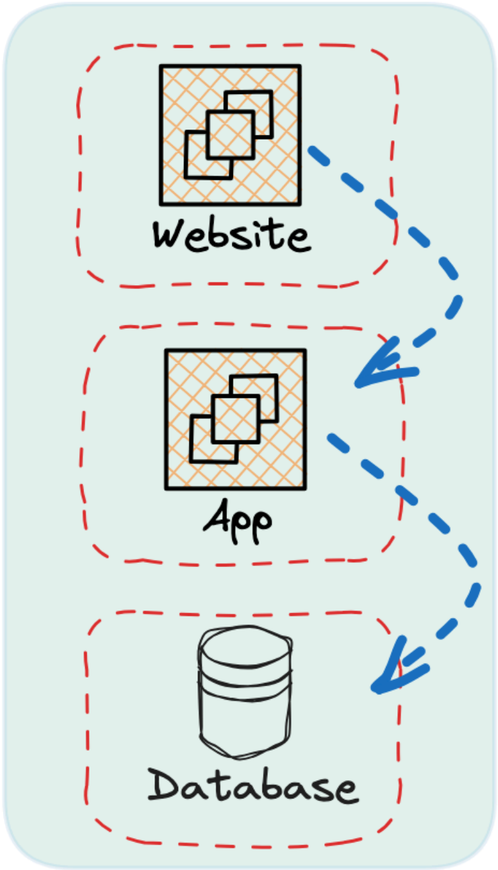


Security Groups Sample

Web Tier
Security Group

Application
Security Group

Database
Security Group

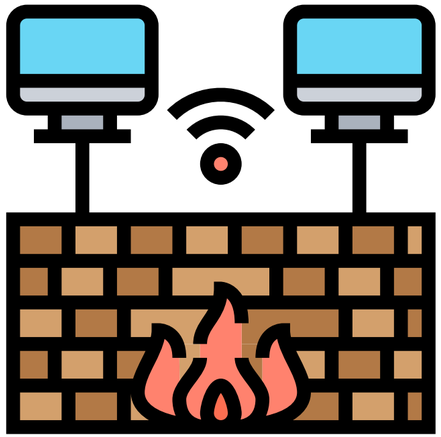


Inbound Rule
Allow HTTPS port 443
Source: 0.0.0.0/0 (Any)

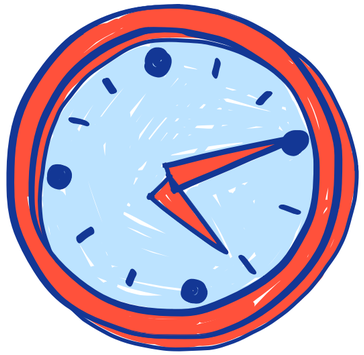
Inbound Rule
Allow HTTP port 80
Source: Web Tier

Inbound Rule
Allow TCP port 3306
Source: App Tier

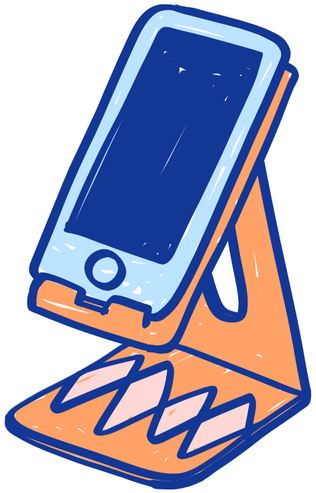
Network Access Control Lists (NACLs)



- Firewalls at the subnet boundary
- Will allow all inbound and outbound traffic by default
- Are stateless



THANK YOU



See you in next lecture!