

AWS Cloud Security Foundations– AWS-CSF

Dr. Ibrahim Gomaa

Lecture 8: Securing your infrastructure



Lecture 8: Securing your infrastructure

Topics

- Structure of a three-tier web application
- Using a VPC
- Setting up public and private subnets and internet protocols
- Using AWS security groups
- Using AWS network ACLs
- Using AWS load balancers
- Pulling it all together
- Protecting your compute resources

Lab

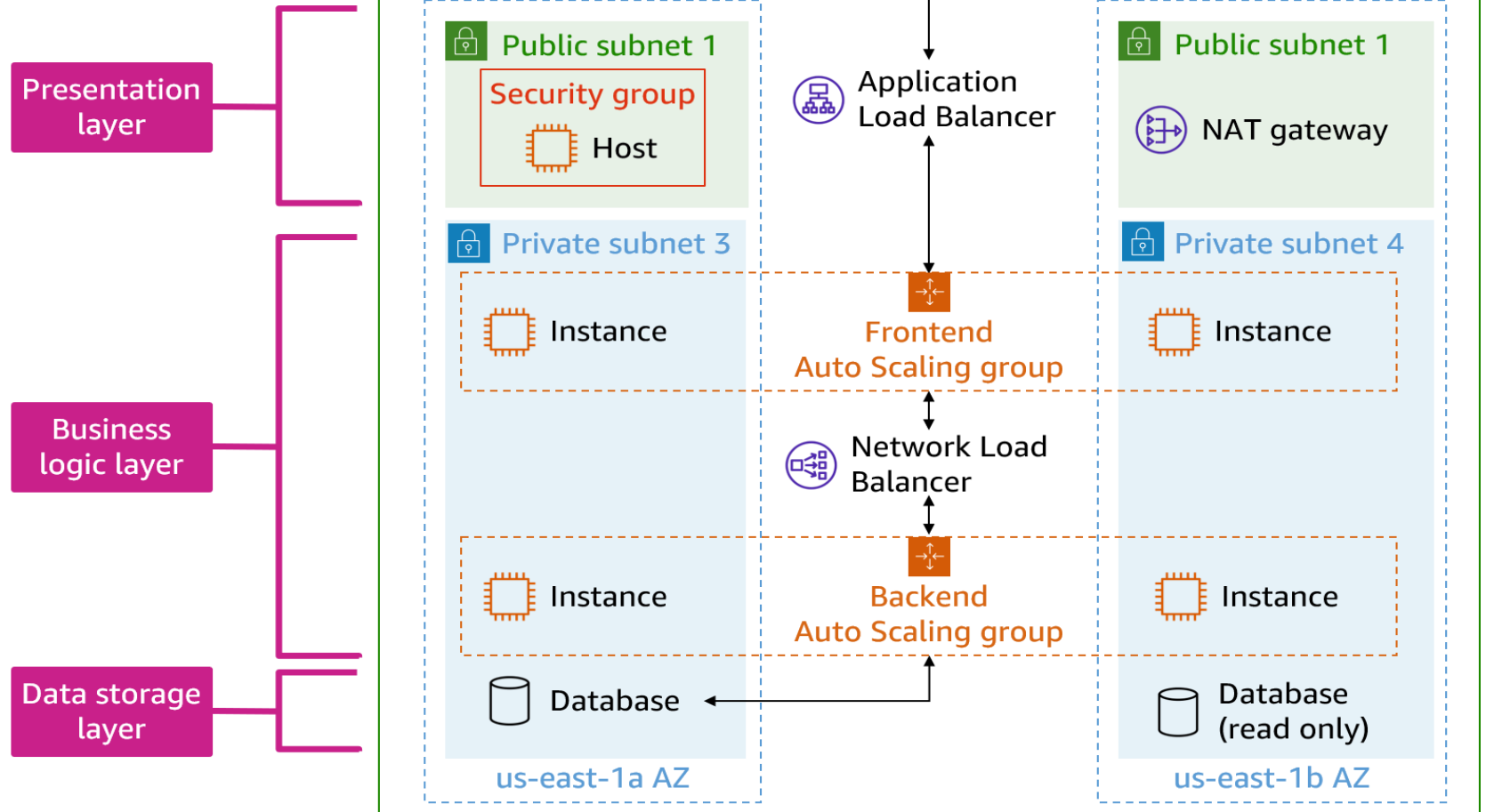
- Securing VPC Resources by Using Security Groups

Structure of a three-tier web application



Structure of a three-tier web application

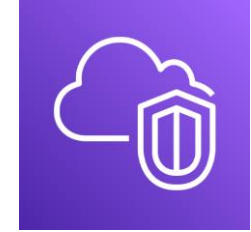
Three-tier architecture



Using a VPC



Amazon Virtual Private Cloud (Amazon VPC)

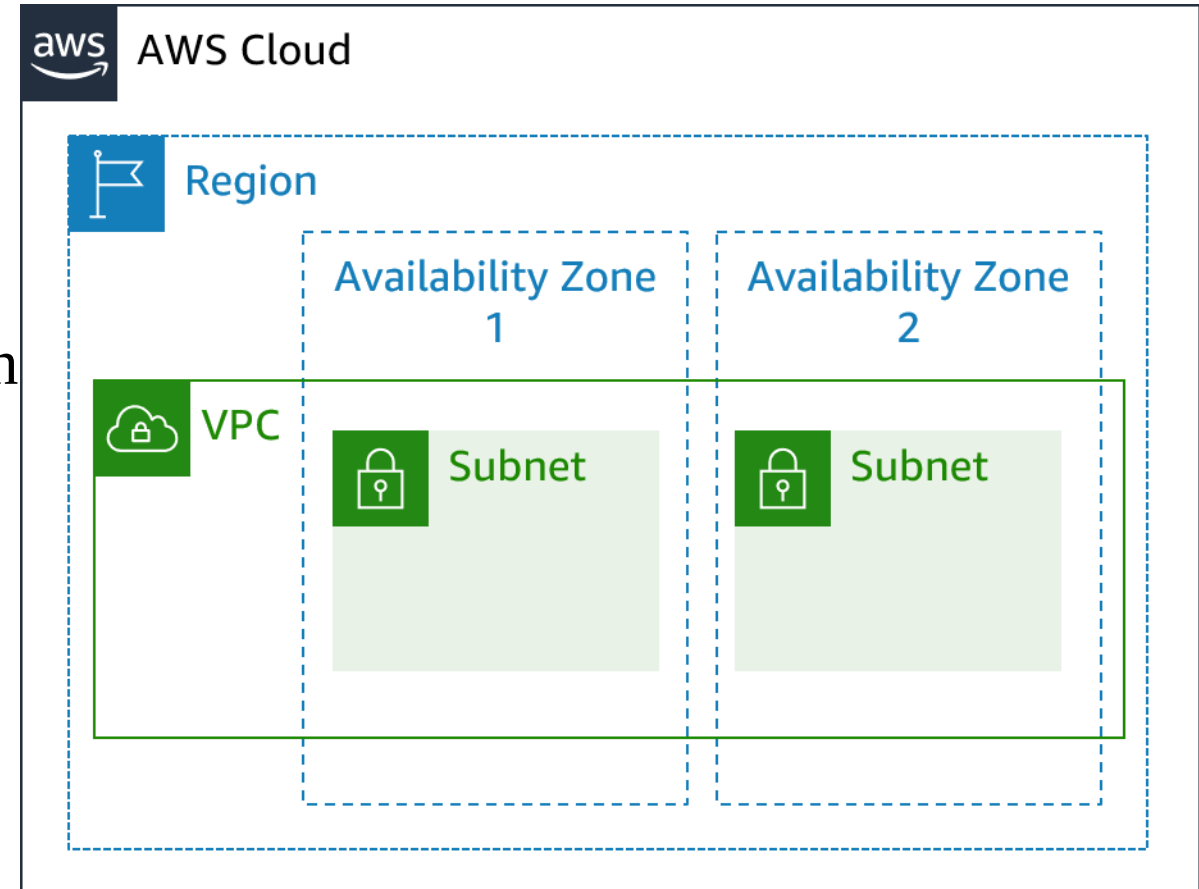


Amazon Virtual Private
Cloud (Amazon VPC)

- Provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define.
- Control your virtual networking resources, including the following:
 - Select the IP address range.
 - Create subnets.
 - Configure route tables and network gateways.
- Customize the network configuration for your VPC.
- Use multiple layers of security.

VPCs and subnets

- VPC
 - Is logically isolated from other VPCs
 - Is dedicated to your AWS account
 - Belongs to a single AWS Region and can span multiple Availability Zones
- Subnet
 - Is a range of IP addresses that divide a VPC
 - Belongs to a single Availability Zone
 - Is classified as public or private



Setting up public and private subnets and internet protocols



Internet gateway

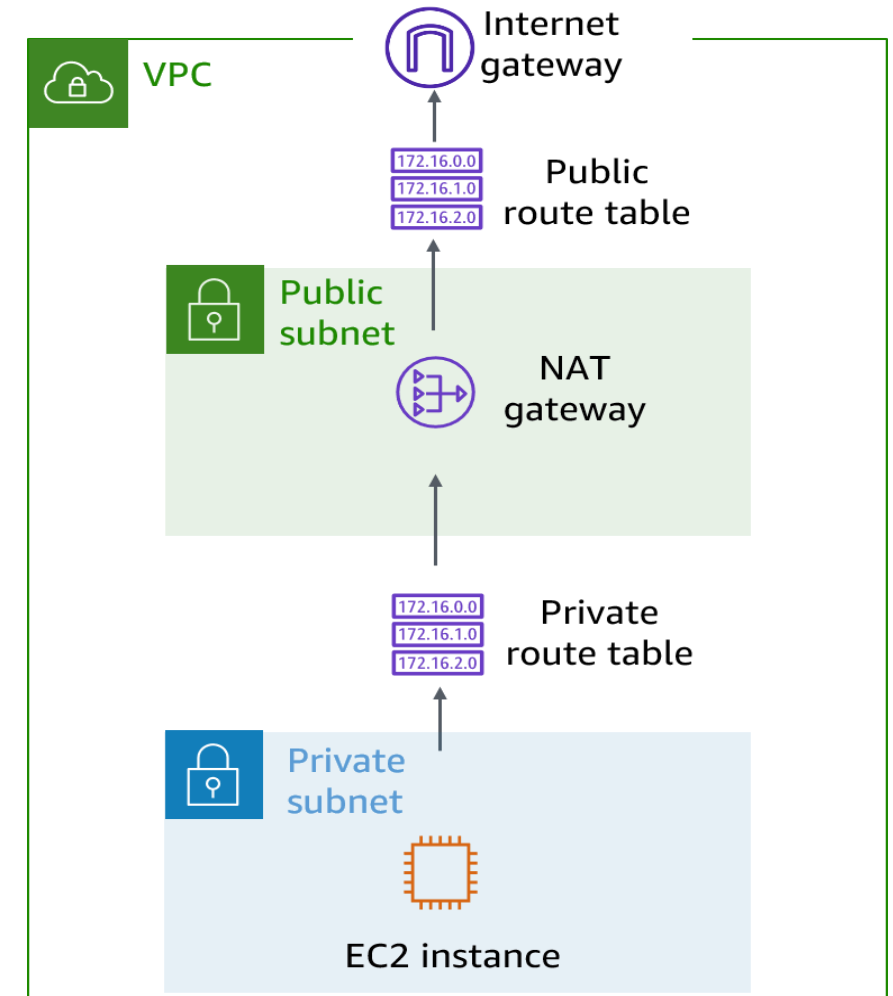
- Provides a target in your VPC route tables for internet-routable traffic
- Performs network address translation (NAT) for instances that have been assigned public IPv4 addresses
- Supports IPv4 and IPv6 traffic
- Doesn't incur an additional charge in your account

NAT gateway

- Supports instances in a private subnet to connect to the internet or other AWS services
- Prevents the internet from initiating a connection to those instances
- Requires that you specify the following at creation:
 - Public subnet in which the NAT gateway should reside
 - An Elastic IP address to associate with the NAT gateway
- After creation, requires that you update the route table for one or more of your private subnets to direct internet-bound traffic to the NAT gateway

Private subnet

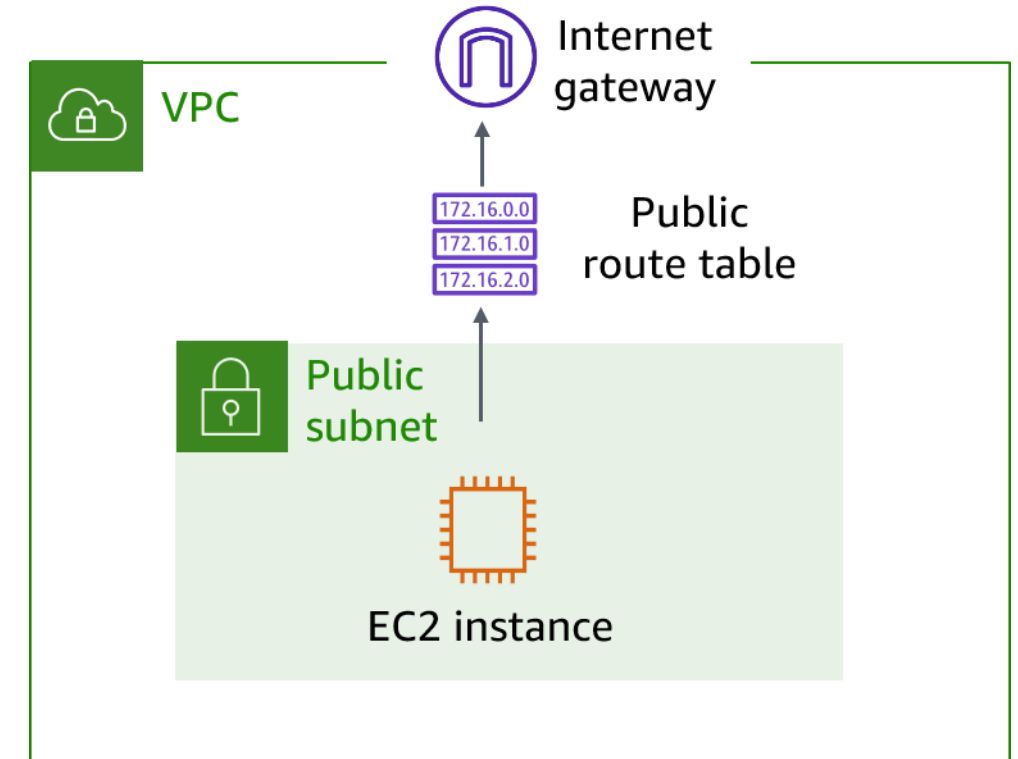
- All subnets consist of a contiguous range of IP addresses.
- Interfaces that are attached to instances in private subnets cannot be reached from outside the parent VPC.
- Private subnets are often used to host database instances that don't need to be accessed through the public internet.



Setting up public and private subnets and internet protocols

Public subnet

- When external traffic needs to reach an interface, such as an Amazon Elastic Compute Cloud (Amazon EC2) instance, the interface requires the following:
 - A public IP address must be assigned to an EC2 instance.
 - The subnet's route table must include an entry to the interface.
- With these two factors in place, the subnet is considered to be a public subnet.



IP addressing

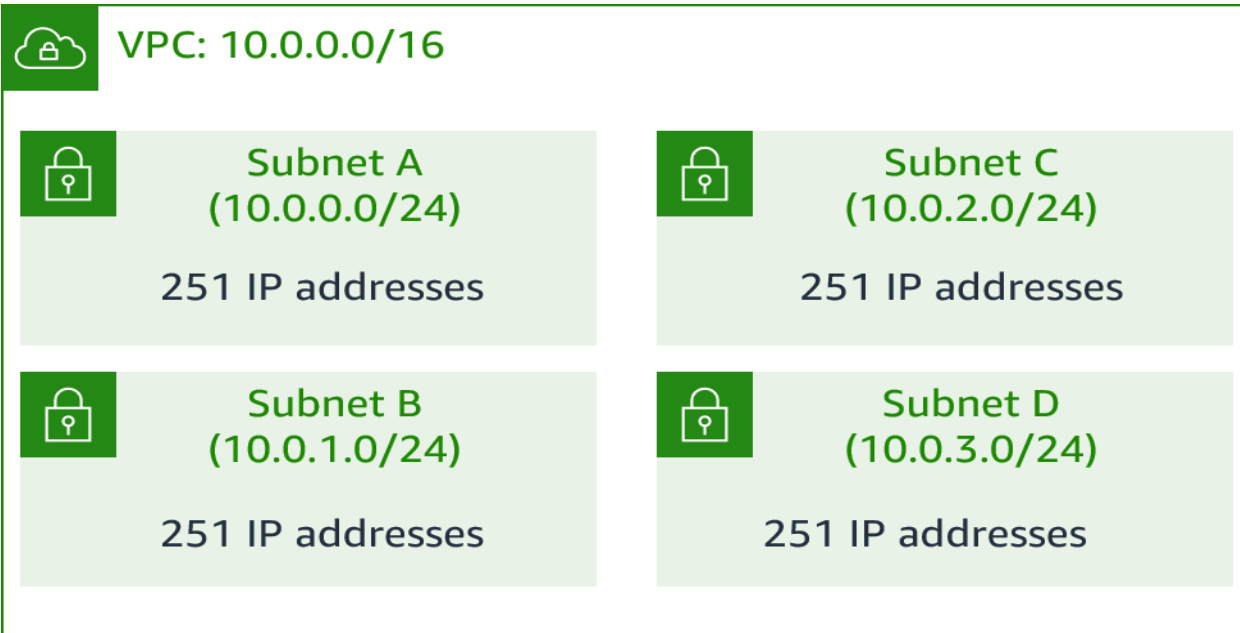
- When you create a VPC, you assign a CIDR range (a range of private addresses).
- You cannot change the range in a VPC or subnet, but you can add more CIDR ranges to your VPC.
- The largest CIDR block size is /16, and the smallest is /28.
- The CIDR ranges of subnets shouldn't overlap.

VPC

x.x.x.x/16 or 65,536 addresses
(max)
to
x.x.x.x/28 or 16 addresses (min)

Reserved IP addresses

Example: A VPC with an IPv4 CIDR block of 10.0.0.0/16 has 65,536 total IP addresses. The VPC has four subnets, all with /24 CIDR blocks. Although each subnet has 256 IP addresses, only 251 IP addresses are available for use in each.



IP Addresses for CIDR Block 10.0.0.0/24	Reserved for
10.0.0.0	Network address
10.0.0.1	Internal communication
10.0.0.2	Domain Name System (DNS) resolution
10.0.0.3	Future use
10.0.0.255	Network broadcast address

Public IP address

- A public IP address is an IP address that is used to access the internet.
- A public IP address can be automatically assigned if you modify the subnet's auto-assign public IP address properties.
- Public IP addresses are dynamic. If you stop or start your instance, a new public IP is assigned. For production projects, use an Elastic IP address rather than an assigned public IP, which will be dissociated if you stop the instance.

Elastic IP address

- Is associated with an AWS account
- Is static and doesn't change over time
- Comes from Amazon's pool of IPv4 addresses
 - If you unassign an Elastic IP address, you are charged until you remove it completely.

Elastic IP addresses get allocated to your account and stay the same. Use an Elastic IP address when you work on a long-term project and configuring IP addresses can be time-consuming.

Elastic network interface

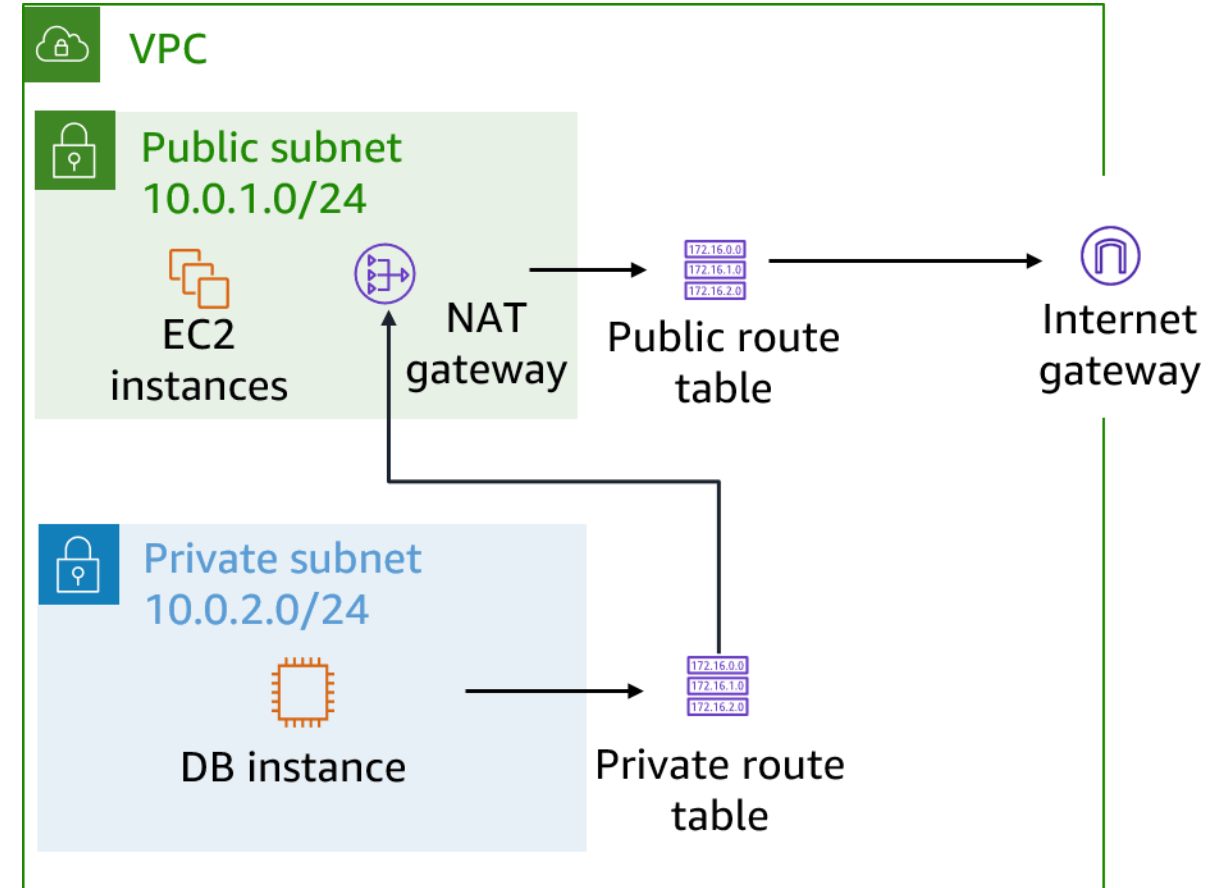
- An elastic network interface is a virtual network interface. You can do the following:
 - Attach it to an instance.
 - Detach it from the instance, and attach it to another instance to redirect network traffic.
- Its attributes follow when it is reattached to a new instance.
- Each instance in your VPC has a default network interface, which can be assigned a private IPv4 address from your VPC's range.



Setting up public and private subnets and internet protocols

Route tables and routes

- A route table contains a set of rules (or routes), which you can configure to direct network traffic from your subnet.
- Each route specifies a destination and a target.
- By default, every route table contains a local route for communication within the VPC.
- Each subnet should have its own route table.

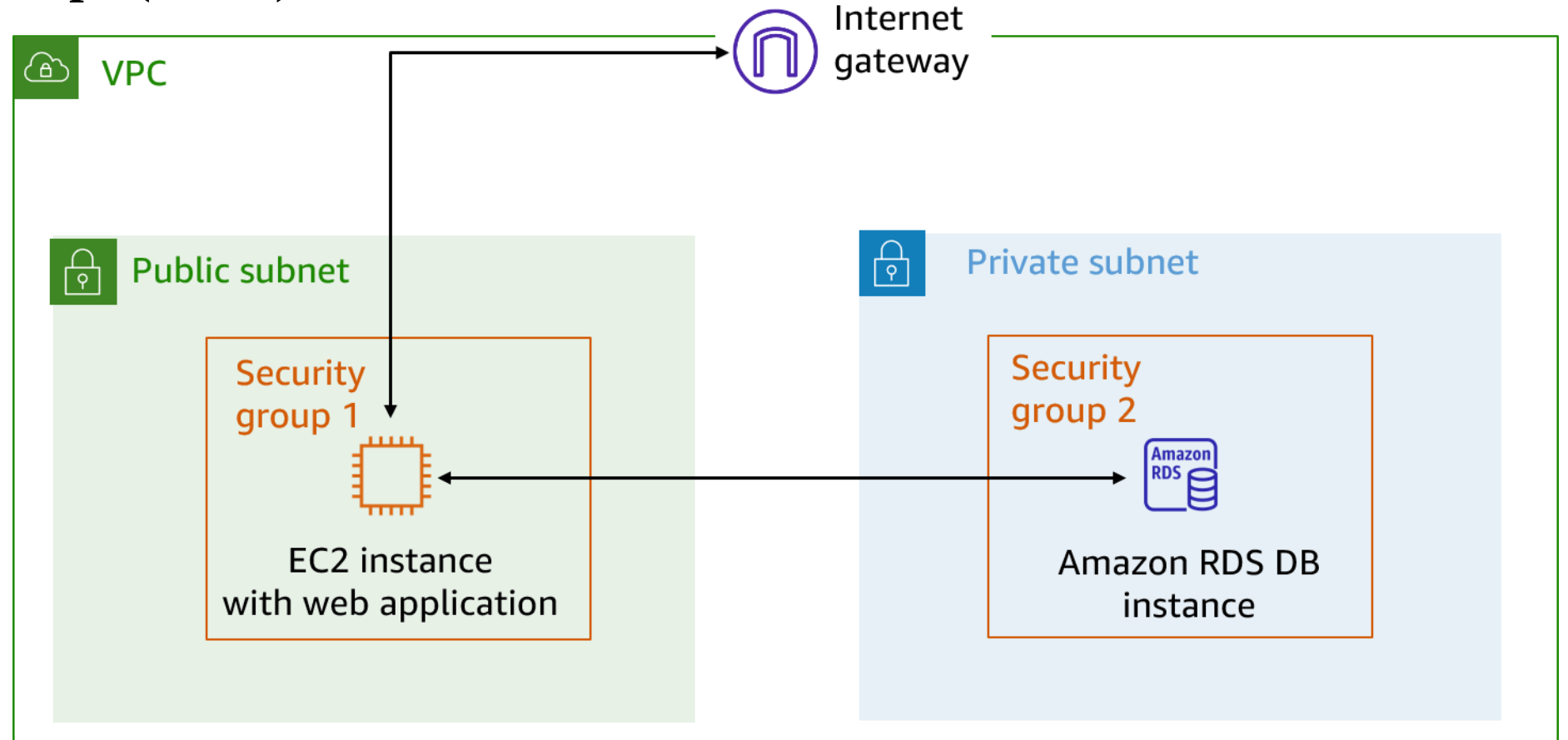


Using AWS security groups



Security groups (1 of 2)

A **security group** acts as a virtual firewall for an EC2 instance, and controls inbound and outbound traffic for the instance. Security groups act at the **instance level**, not the subnet level.



Security groups (2 of 2)

- Security groups have rules that control inbound and outbound instance traffic.
- Default security groups deny all inbound traffic and allow all outbound traffic. This is considered *stateful*.

Inbound

Source	Protocol	Port Range	Description
sg-xxxxxxx	All	All	Allow inbound traffic from network interfaces that are assigned to the same security group.

Outbound

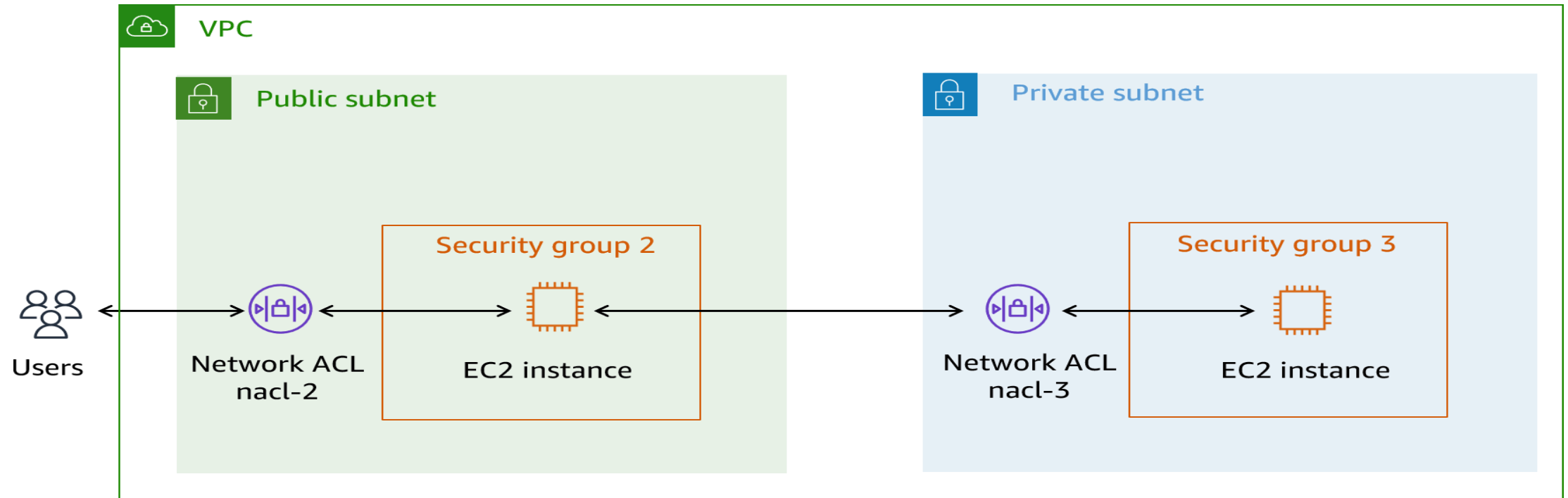
Destination	Protocol	Port Range	Description
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic.

Using AWS network ACLs



Network ACLs (1 of 2)

A **network access control list (ACL)** is an optional layer of security for your VPC. A network ACL acts as a firewall to control traffic in and out of one or more subnets. To add another layer of security to your VPC, you can set up network ACLs with rules that are similar to your security group rules



Network ACLs (2 of 2)

- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic. Network ACLs are stateless.
- Each VPC automatically comes with a modifiable default network ACL. By default, it allows all inbound and outbound IPv4 traffic.
- You can create a custom network ACL and associate it with a subnet. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.

Default inbound and outbound rules

Rule	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

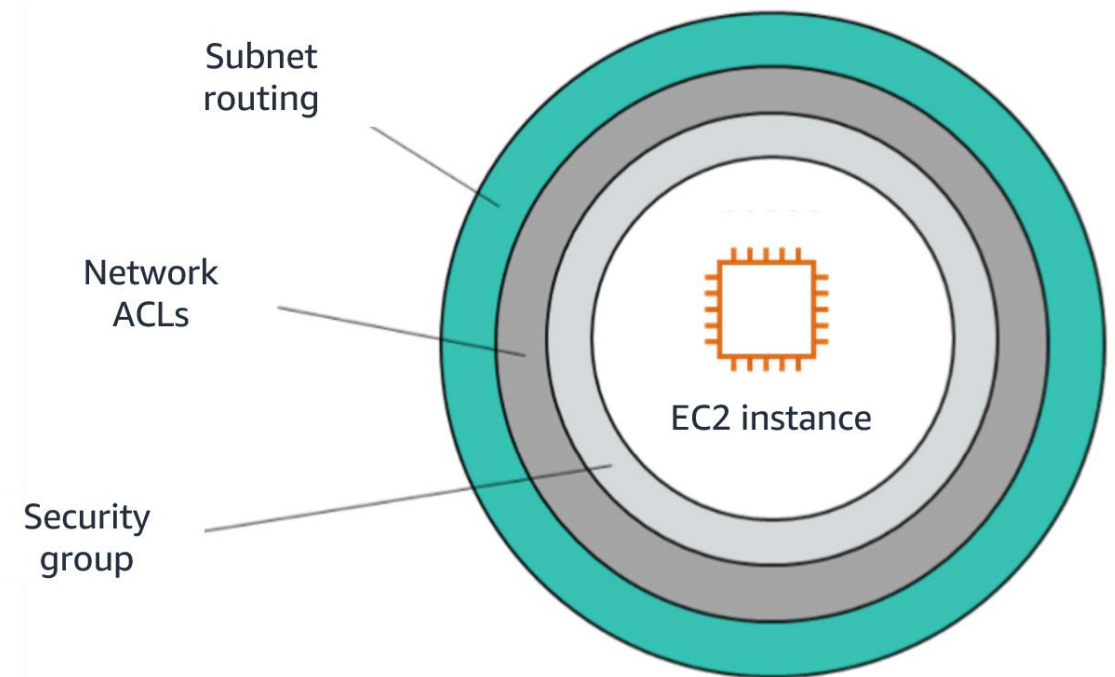
Comparing security groups and network ACLs

Attribute	Security Groups	Network ACLs
Scope	Instance or interface level	Subnet level
Supported Rules	Allow rules only	Allow and deny rules
State	Stateful (return traffic is automatically allowed, regardless of rules)	Stateless (return traffic must be explicitly allowed by rules)
Order of Rules	All rules are evaluated before a decision is made to allow traffic	Rules are evaluated in number order before a decision is made to allow traffic



VPC security features

- Security groups
- Network ACLs
- Subnets
- Route tables



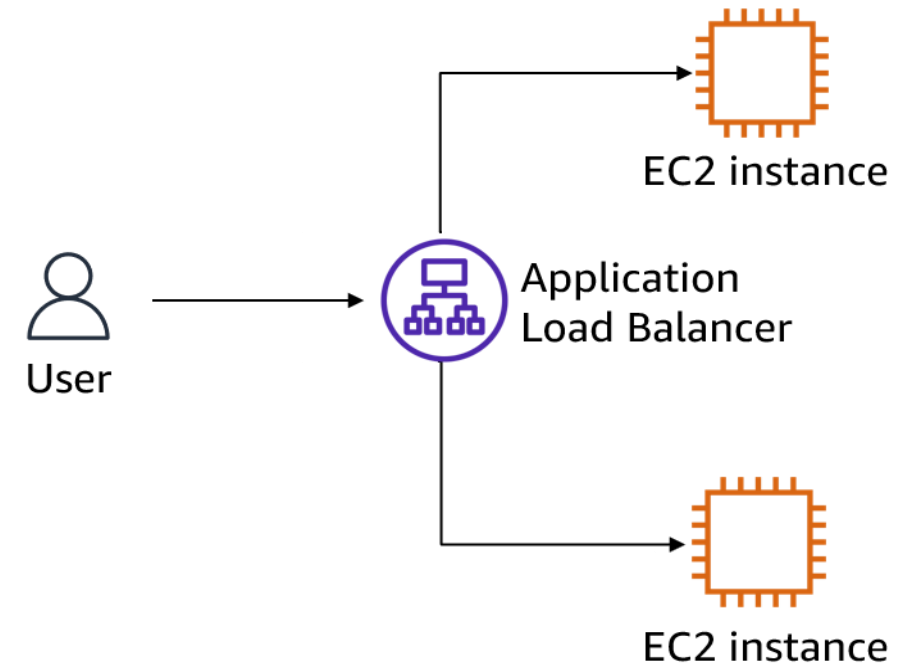
Note: VPC Flow Logs can log activity down to the interface level.

Using AWS load balancers



Elastic Load Balancing (ELB)

- Distributes incoming application traffic
- Supports high availability
- Performs health checks on instances
- Provides the following:
 - Application Load Balancer
 - Network Load Balancer
 - Classic Load Balancer



Data protection in ELB



Single point of
contact



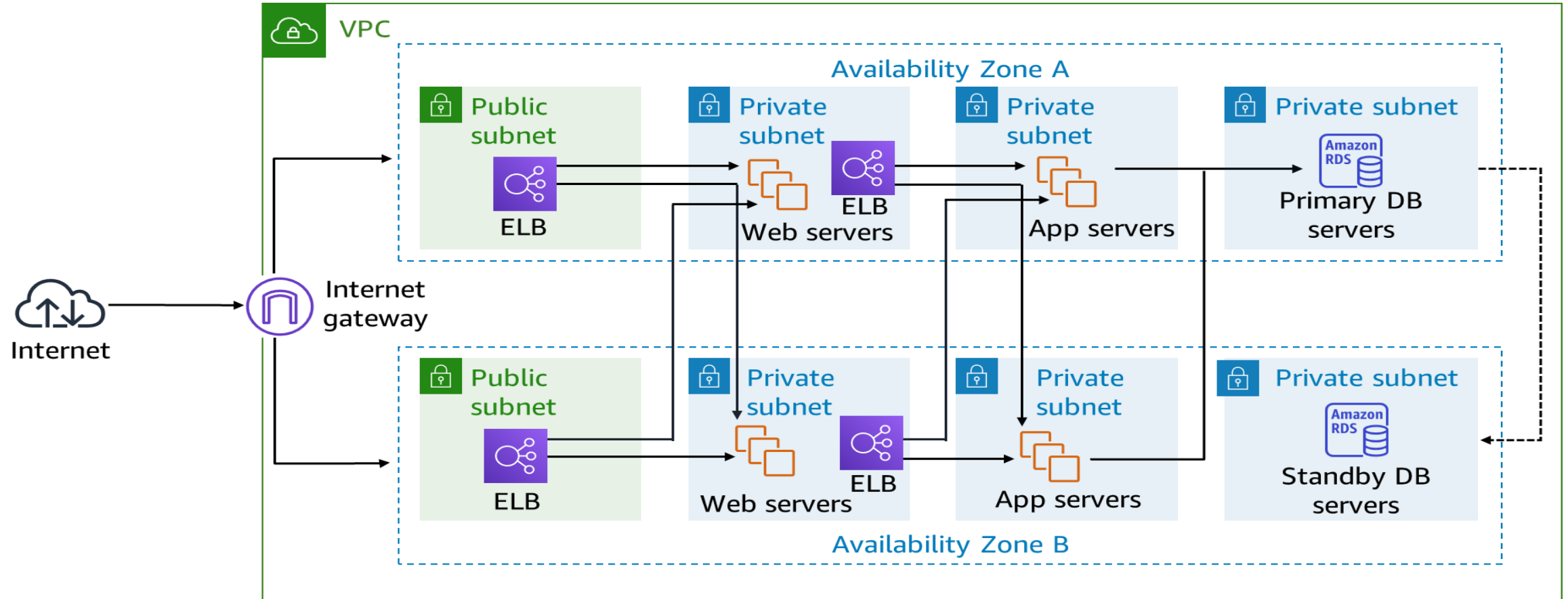
Encryption
at rest



Encryption
in transit

Using AWS load balancers

Load balancers in action

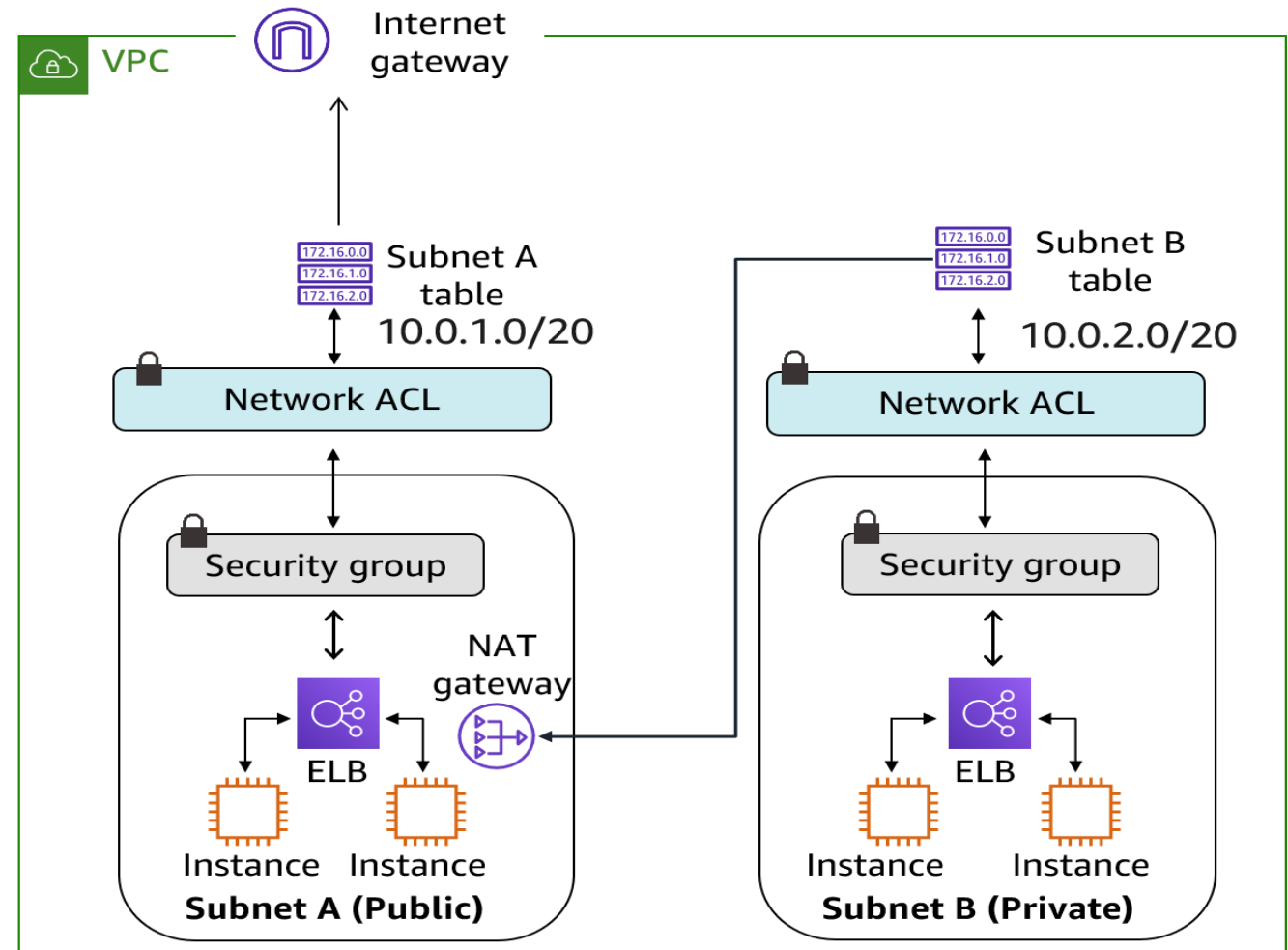


Pulling it all together



Workflow

VPC
10.0.0.0/16 (IPv4)
2001:db8:1234:1a00::/56 (IPv6)



Best practices to protect your network

- Control traffic at all layers.
- Inspect and filter your traffic at the application level.
- Automate network protection.
- Limit exposure by only allowing the minimum required access.



Protecting your compute resources



Amazon Inspector

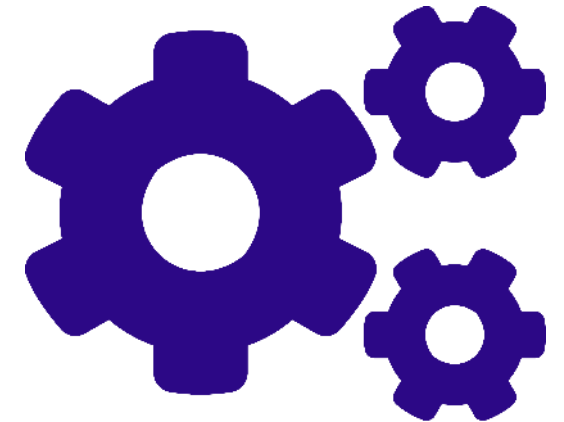
- Run automated security assessments on EC2 instances and applications.
- Identify application security issues.
- Enforce security standards and best practices.
- Generate assessment reports.



Amazon Inspector

Security benefits of Amazon Inspector

- Automate tasks to help you respond to security issues
- Regularly monitor your resources
- Benefit from AWS security expertise
- Integrate security into DevOps



AWS Systems Manager

- AWS Systems Manager gives you visibility and control of your infrastructure on AWS. The service includes capabilities that help you automate management tasks. You can collect system inventory, apply operating system patches, maintain up-to-date antivirus definitions, and configure operating systems and applications at scale.
- Amazon Inspector uses the widely deployed AWS Systems Manager Agent (SSM Agent) to collect the software inventory and configurations from your EC2 instances.
- The collected application inventory and configurations are used to assess workloads for vulnerabilities.



AWS Systems Manager

Thanks

