Securing Your Infrastructure

VPC & SUBNETS · ROUTING & GATEWAYS · SECURITY GROUPS · NETWORK ACLS · LOAD BALANCERS · COMPUTE PROTECTION

STUDY & REVIEW

01 MUST KNOW

if you remember five things, remember these

01 **Your half of the model:** under the **shared responsibility model**, AWS secures the *cloud itself* — the foundation compute, storage, database, and networking services plus the global infrastructure. The customer secures things *in* the cloud, and this module is the customer's job: **operating system, network, and firewall configuration**, and **network traffic protection**.

02 **VPC contains, subnet divides:** a **VPC** is a logically isolated virtual network *dedicated to one AWS account* (an account boundary), belongs to a single **Region**, and can span multiple **Availability Zones**. A **subnet** is a slice of the VPC's IP range that lives in *one* AZ and is **public** or **private**. Put subnets in different AZs for high availability.

03 **Security group = instance firewall:** a **stateful** virtual firewall attached at the **instance/ENI level** with **allow rules only**. Return traffic to an allowed request is permitted automatically, and **all rules are evaluated** before traffic is allowed. A new group has no inbound rules and one allow-all outbound rule.

04 **Network ACL = subnet firewall:** a **stateless**, optional firewall at the **subnet level** that supports both **allow and deny** rules, evaluated in **number order** (first match wins) ending in a * deny. **Every subnet must be associated with exactly one** network ACL, and return traffic needs its own explicit rule.

05 **Layer the defenses:** stack controls from the outside in — **route tables and subnets → network ACLs → security groups** closest to the instance. Control **inbound and outbound** at every layer, **limit exposure** to the minimum required, and watch traffic with **VPC Flow Logs**. No single control is enough.

02 KEY TERMS

TERM	DEFINITION
Amazon VPC	A logically isolated section of the AWS Cloud, dedicated to your account, where you launch resources in a virtual network you define; belongs to one Region and can span multiple Availability Zones
Subnet	A range of IP addresses that divides a VPC; belongs to a single Availability Zone and is classified as public or private
CIDR block	The range of private IP addresses assigned to a VPC or subnet; largest is /16 (65,536 addresses), smallest is /28 (16). You can't change a range, but you can add more ranges to a VPC
Internet gateway (IGW)	VPC component that gives route tables a target for internet-bound traffic and performs NAT for instances with public IPv4 addresses; supports IPv4/IPv6 at no additional charge
NAT gateway	Managed service placed in a public subnet (with an Elastic IP) that lets private-subnet instances make outbound connections while blocking connections the internet tries to initiate
Route table	A set of routes (each a destination + a target) that directs a subnet's traffic; every table has an undeletable local route, and any subnet not explicitly associated uses the VPC's main route table
Elastic IP address	A static, public IPv4 address allocated to your account that stays constant across stop/start; you're billed for it while it is allocated but unassigned
Elastic network interface (ENI)	A virtual network interface you can attach, detach, and move between instances to redirect traffic; its attributes follow it. The primary ENI can't be detached
Security group	A stateful virtual firewall at the instance/interface level; supports allow rules only, and all rules are evaluated before traffic is allowed
Network ACL	A stateless firewall at the subnet level; supports allow and deny rules evaluated in number order; each subnet must be associated with one

TERM	DEFINITION
Elastic Load Balancing (ELB)	Service that distributes incoming traffic across multiple healthy targets (EC2, containers, IP addresses, Lambda); offered as Application, Network, and Classic load balancers
VPC Flow Logs	Feature that captures IP-traffic metadata to and from network interfaces — down to the interface level — and publishes it to Amazon CloudWatch Logs or Amazon S3

03 SECURITY GROUPS VS. NETWORK ACLS

the module's single most tested comparison

ATTRIBUTE	SECURITY GROUP	NETWORK ACL
Scope	Instance or interface (ENI) level	Subnet level
Rules	Allow rules only	Allow and deny rules
State	Stateful — return traffic is auto-allowed	Stateless — return traffic needs its own rule
Rule order	All rules evaluated before allowing	Evaluated in number order; first match wins
Defaults	New group: no inbound, allow-all outbound	Default NACL allows all; custom NACL denies all until you add rules

04 PUBLIC SUBNET VS. PRIVATE SUBNET

what makes each, and how each reaches the internet

PUBLIC SUBNET

internet-reachable

- An instance has a **public IP** (or Elastic IP)
- Route table has a route to an **internet gateway**
- Hosts internet-facing resources — AWS recommends a **load balancer** here, forwarding to private web servers

PRIVATE SUBNET

no inbound from the internet

- Interfaces are **not reachable** from outside the VPC
- Outbound only, via a **NAT gateway** (e.g., OS patching); responses are allowed back
- Hosts databases and backend servers

05 ELASTIC LOAD BALANCING — THE THREE TYPES

match the load balancer to the traffic

LOAD BALANCER	LEVEL	IDEAL FOR	REMEMBER
Application (ALB)	Request · Layer 7	HTTP/HTTPS, content-based routing, microservices	Enforces the latest SSL/TLS
Network (NLB)	Connection · Layer 4	TCP/UDP, sudden volatile traffic	Millions of req/s, ultra-low latency; static IP per AZ
Classic (CLB)	Request + connection	Legacy EC2-Classic apps	Basic load balancing

06 HOW AN INBOUND REQUEST REACHES A PUBLIC INSTANCE

outside-in through the layered defenses

01 Client on the internet → 02 **Internet gateway** (route-table target) → 03 **Route table** directs the subnet's traffic → 04 **Network ACL** — subnet firewall (stateless) → 05 **Security group** — instance firewall (stateful) → 06 EC2 instance

07 EXAM TRAPS

where the knowledge check gets you

- × “Security groups and network ACLs are the same firewall.” — No. A **security group** is stateful, at the instance level, allow-only; a **network ACL** is stateless, at the subnet level, and supports allow *and* deny.
- × “I can block one bad IP with a security group deny rule.” — Security groups have **no deny rules**. To explicitly deny a specific IP address, use a **network ACL**.
- × “Network ACLs are stateful like security groups.” — They are **stateless**: responses to inbound traffic are subject to the *outbound* rules (and vice versa), so return traffic must be explicitly allowed.
- × “A subnet is public unless it holds a database.” — A subnet is public **only** when an instance has a public IP **and** the route table has a route to an internet gateway. Without both, it's private.
- × “Instances in a private subnet have no internet access at all.” — Through a **NAT gateway** they can make **outbound** requests (like patching); the internet just can't **initiate** inbound connections.
- × “Put the NAT gateway in the private subnet.” — The NAT gateway lives in a **public subnet** and needs an **Elastic IP**; you point the *private* subnet's route table at it.
- × “A /24 subnet gives me all 256 addresses.” — AWS reserves **5** per subnet (network, VPC router, DNS, future use, broadcast), so a /24 leaves **251** usable.
- × “A VPC lives in one Availability Zone.” — A VPC belongs to a single **Region** and **spans** multiple AZs; the **subnet** is the AZ-scoped unit.

08 SELF-QUIZ

answers are upside-down below

Q1 At what level does a security group act as a virtual firewall, and what property lets it automatically allow return traffic?

Q2 At what level does a network ACL act as a firewall, and what property means return traffic must be explicitly allowed?

Q3 Which of the two VPC firewalls supports deny rules to block a specific IP address?

Q4 What two conditions must both be true for a subnet to be considered public?

Q5 What VPC component lets private-subnet instances make outbound internet requests while blocking inbound connections from the internet?

Q6 In which subnet must a NAT gateway reside, and what address must be associated with it?

Q7 How many IP addresses does AWS reserve per subnet, leaving how many usable in a /24 block?

Q8 What are the largest and smallest CIDR block sizes allowed for a VPC?

Q9 In what order does a network ACL evaluate its rules, and what does the catch-all rule numbered ∗ do?

Q10 Which ELB type does AWS recommend for HTTP/HTTPS (request-level) traffic, and which for TCP/UDP (connection-level) traffic?

ANSWER KEY (rotate the page)

Q1 the instance/ENI level; it is stateful **Q2** the subnet level; it is stateless **Q3** the network ACL (security groups are allow-only) **Q4** an instance has a public IP address, and the subnet's route table has a route to an internet gateway **Q5** a NAT gateway **Q6** a public subnet; an Elastic IP address **Q7** 5 reserved; 251 usable **Q8** largest /16 (65,536 addresses), smallest /28 (16 addresses) **Q9** ascending rule-number order (first match wins); the ∗ rule denies any packet that matched no numbered rule **Q10** Application Load Balancer for HTTP/HTTPS; Network Load Balancer for TCP/UDP