Creating a Networking Environment

AMAZON VPC · SUBNETS & ROUTE TABLES · INTERNET & NAT GATEWAYS · SECURITY GROUPS & NETWORK ACLS · VPC ENDPOINTS · FLOW LOGS · WELL-ARCHITECTED

STUDY & REVIEW

01 MUST KNOW

if you remember five things, remember these

01 **A VPC is your private slice of a Region:** an Amazon **VPC** is a programmatically defined, logically isolated virtual network that **belongs to one Region and can span its Availability Zones**. You size it with a private-IP **CIDR block** — IPv4 ranges from `/16` (65,536 addresses) down to `/28` (16 addresses) — and it is isolated from other networks and the internet until you add configuration. Don't run production in the **default VPC**.

02 **Subnets + route tables decide public vs private:** a **subnet** belongs to **one AZ** and takes a non-overlapping segment of the VPC range; its **route table** sets reachability. Add a route `0.0.0.0/0` → **internet gateway** and give the instance a public IP to make a subnet **public**; a subnet with **no route to the internet** is **private**. The `local` route (the VPC CIDR) is added automatically and **can't be deleted**.

03 **NAT gives private resources outbound-only internet:** a **NAT gateway** (AWS-managed, hourly cost) or **NAT instance** (your own EC2) lets private-subnet resources reach the internet, other VPCs, or on-premises for tasks like patching — but **blocks unsolicited inbound connections**. Point the private route table's `0.0.0.0/0` at the NAT, place the NAT in a **public** subnet, and deploy **one per AZ**. For IPv6 use an **egress-only internet gateway**.

04 **Two firewalls, layered: security groups** are **stateful**, act at the **resource** (instance/ENI) level, and are **allow-only**; **network ACLs** are **stateless**, act at the **subnet** level, and support **allow and deny**. Use both for defense in depth. New security group: **no inbound**, all outbound allowed. Default network ACL: **all traffic allowed** both ways.

05 **Reach managed services privately with VPC endpoints: interface endpoints** (AWS **PrivateLink** — an elastic network interface with a private IP) reach many managed services but are **billed**; **gateway endpoints** use a **route-table** entry, work only for **Amazon S3 and DynamoDB**, and are **free** with no throughput limits. Both keep traffic off the public internet.

02 KEY TERMS

TERM	DEFINITION
Amazon VPC	Programmatically defined, logically isolated virtual network in one AWS Region; can span multiple AZs and is sized by a CIDR block
CIDR block	Range of private IP addresses that sizes a VPC or subnet; IPv4 VPCs run /16 (65,536 IPs) to /28 (16 IPs) and can't be changed after creation
Subnet	Segment of a VPC's IP range that belongs to one Availability Zone; a container for routing policy. Subnet CIDR blocks can't overlap
Route table	Set of routes (destination → target) the VPC router uses; the main table applies to any subnet without an explicit table
Internet gateway (IGW)	Horizontally scaled, redundant VPC component that connects a VPC to the internet and performs NAT for instances with public IPv4 addresses; one per VPC
NAT gateway	AWS-managed device in a public subnet that lets private-subnet resources initiate outbound internet traffic but blocks unsolicited inbound connections
Elastic IP address	Static, public IPv4 address you associate with an instance, load balancer, or network interface and can transfer to a healthy instance
Security group	Stateful virtual firewall at the instance/network-interface level; allow rules only, with separate inbound and outbound sets
Network ACL	Stateless, optional firewall at the subnet level; numbered allow and deny rules evaluated in order; each subnet has exactly one

TERM	DEFINITION
VPC endpoint	Private connection from a VPC to a managed AWS service; interface (PrivateLink) or gateway (S3/DynamoDB) type
Bastion host	Hardened EC2 instance in a public subnet that gives restricted administrative access (e.g., SSH) to private-subnet resources
VPC Flow Logs	Feature that captures packet-level metadata about traffic at the VPC, subnet, or network-interface level for monitoring and troubleshooting

03 PUBLIC VS PRIVATE SUBNET

the route table decides

PUBLIC SUBNET

internet-facing tier

- Route `0.0.0.0/0` → internet gateway
- Instances need a public IP or Elastic IP
- Allows direct, two-way internet access
- Hosts load balancers, bastion hosts, NAT gateways

PRIVATE SUBNET

isolated tier

- **No** route to an internet gateway
- Not reachable from the internet
- Reaches internet only via a **NAT device**
- Hosts databases, batch jobs, app servers

04 SECURITY GROUP VS NETWORK ACL

run both = defense in depth

BEHAVIOR	SECURITY GROUP	NETWORK ACL
Scope	Resource (instance/ENI)	Subnet
Rule types	Allow only	Allow and deny
State	Stateful — return auto-allowed	Stateless — return needs a rule
Evaluation	All rules evaluated	Numbered order; stops at match
New/default inbound	None allowed (new SG)	All allowed (default NACL)
New/default outbound	All allowed	All allowed

05 LAYERED DEFENSE — THE REQUEST PATH

internet → in, each layer filters

`01` Client app over **TLS/HTTPS** → `02` **Internet gateway** → `03` **Route table** layer → `04` **Network ACL** layer → `05` **Subnet** layer → `06` **Security group** layer → `07` **EC2 instance**

06 INTERFACE VS GATEWAY VPC ENDPOINT

S3 supports both — pick on cost/reach

FACTOR	INTERFACE ENDPOINT	GATEWAY ENDPOINT
Backed by	AWS PrivateLink (ENI + private IP)	Route-table entry (prefix list)
Services	Many managed AWS services	**Amazon S3 and DynamoDB only**
Cost	Billed (hourly + data)	No charge
On-prem / other Region	Allowed	Not allowed
Bandwidth	≤10 Gbps per AZ, scales to 100 Gbps	No limit

07 EXAM TRAPS

where the knowledge check gets you

- × “A private subnet with a NAT gateway can be reached from the internet.” — A NAT device allows only **outbound-initiated** traffic and **blocks unsolicited inbound connections**, so resources stay private and undiscoverable.
- × “Security groups can block (deny) specific traffic.” — Security groups have **allow rules only**. To explicitly **deny** an IP or CIDR, you need a **network ACL**.
- × “Security groups are stateless, so you must add a return rule.” — Security groups are **stateful**: return traffic for an allowed connection is automatically permitted. **Network ACLs** are the stateless layer that needs explicit return rules.
- × “A brand-new security group blocks everything.” — A new security group allows **no inbound** traffic but permits **all outbound** by default; remove that rule to restrict outbound.
- × “The default network ACL behaves like a new security group and blocks traffic.” — The **default** network ACL **allows all** inbound and outbound; only a **custom** network ACL starts with just the deny-all catch-all rule.
- × “The `local` route can be deleted to isolate subnets.” — The default `local` route for the VPC CIDR is added automatically and **can't be deleted**; every resource in the VPC can reach every other by default.
- × “A subnet can span multiple Availability Zones.” — A **VPC** spans AZs, but each **subnet belongs to exactly one AZ**. Spread subnets across AZs for availability.
- × “Gateway VPC endpoints work for any AWS service.” — Gateway endpoints support **only Amazon S3 and DynamoDB**; every other supported service uses an **interface endpoint** (PrivateLink).

08 SELF-QUIZ

answers are upside-down below

Q1 What is the range of private IP addresses that sizes a VPC or subnet called?

Q2 What are the largest and smallest IPv4 VPC netmasks, and how many addresses does each hold?

Q3 How many IP addresses does AWS reserve in each subnet CIDR block, and which ones?

Q4 Which single route entry turns a subnet into a public subnet, and what must its instances also have?

Q5 Which device lets resources in a private subnet reach the internet without accepting unsolicited inbound connections?

Q6 Which traffic control is stateful and operates at the resource level — a security group or a network ACL?

Q7 By default, what inbound and outbound traffic does a brand-new security group allow?

Q8 Which two AWS services can a gateway VPC endpoint connect to?

Q9 Which VPC endpoint type is powered by AWS PrivateLink and creates an elastic network interface in your subnet?

Q10 Sample exam: EC2 instances in private subnets must download internet patches but stay unreachable from the internet. Which two actions achieve this?

ANSWER KEY (rotate the page)

Q1 a CIDR block **Q2** /16 is largest (65,536 addresses); /28 is smallest (16 addresses) **Q3** five — the first four addresses and the last address **Q4** 0.0.0.0/0 targeting the internet gateway ID; the instance needs a public IP address **Q5** a NAT gateway (or NAT instance) **Q6** a security group **Q7** no inbound traffic; all outbound traffic **Q8** Amazon S3 and Amazon DynamoDB **Q9** an interface VPC endpoint **Q10** create a NAT gateway in a public subnet, and update the private subnet route tables to send 0.0.0.0/0 to the NAT gateway