Networking

VPC FOUNDATIONS · IP ADDRESSING & CIDR · SUBNETS & ROUTE TABLES · CONNECTIVITY OPTIONS · NETWORK SECURITY · TROUBLESHOOTING

STUDY & REVIEW

01 MUST KNOW

if you remember five things, remember these

01 **The VPC is the foundation:** an **Amazon VPC** is a logically isolated virtual network you provision in the AWS Cloud, defined by an IPv4 **CIDR block from `/16` to `/28`** (16–65,536 addresses). A VPC **spans every Availability Zone** in its Region and has an **implicit router** that moves all traffic; you deploy EC2, RDS, and other resources inside it.

02 **Public vs. private is a routing decision:** a **subnet lives in exactly one Availability Zone** and its range must be a subset of the VPC's. A subnet is **public only if its route table sends `0.0.0.0/0` to an internet gateway** — otherwise it is private. AWS **reserves 5 addresses per subnet** (the first four and the last).

03 **Two firewalls, two layers:** a **security group** is **stateful**, attaches to an **instance / elastic network interface**, and holds **allow rules only** (default: deny inbound, allow outbound). A **network ACL** is **stateless**, attaches to a **subnet**, holds **allow and deny** rules evaluated by number, and defaults to allowing all traffic.

04 **Match the connection to the need: NAT gateway** → private subnet reaches the internet outbound-only · **VPC peering** → links two VPCs by private IP (no transitive routing) · **Site-to-Site VPN / Direct Connect** → on-premises networks · **VPC endpoints** → AWS services privately · **Transit Gateway** → one hub for many VPCs and networks.

05 **Troubleshoot layer by layer:** when connectivity fails, verify in order — is the **instance running** (System and Instance status checks)? Do the **security groups** allow the port and protocol? Do the **network ACLs** allow it in *both* directions? Does the **route table** point to the right target (`igw`, NAT, `vgw`, or peering)?

02 KEY TERMS

TERM	DEFINITION
Amazon VPC	A virtual network provisioned in a logically isolated section of the AWS Cloud; supports subnets, routing, and fine-grained security
Subnet	A logical segment of a VPC's address range within a single Availability Zone; required to deploy an instance
CIDR block	A range of IP addresses written as `x.x.x.x/n`, where /n is the length of the network prefix; a VPC uses /16–/28
Route table	A set of routes (destination → target) that the implicit router uses to direct traffic out of an associated subnet
Internet gateway (IGW)	A VPC component that allows communication between instances in the VPC and the internet
NAT gateway	AWS-managed device that lets private-subnet instances reach the internet outbound while blocking inbound-initiated connections
Security group	A stateful set of firewall rules at the instance / elastic network interface level; allow rules only
Network ACL (NACL)	A stateless set of allow/deny rules at the subnet level, evaluated in ascending rule-number order
VPC peering	A private connection routing traffic between two VPCs by private IP over the AWS backbone; not transitive
VPC endpoint	Privately connects a VPC to AWS services — interface endpoint (PrivateLink) or gateway endpoint (S3, DynamoDB)
Elastic network interface (ENI)	A virtual NIC attached to an instance; the primary ENI cannot be detached
Virtual private gateway (VGW)	The AWS side of a VPN connection; the customer gateway is the on-premises side

03 SECURITY GROUP VS. NETWORK ACL

the two exam workhorses

SECURITY GROUP

instance-level, stateful

- Operates at the **instance / elastic network interface** level
- **Stateful** — return traffic is automatically allowed
- **Allow rules only** (you cannot write a deny rule)
- All rules are evaluated before traffic is allowed
- Default: **denies all inbound, allows all outbound**
- Usually administered by application developers

NETWORK ACL

subnet-level, stateless

- Operates at the **subnet** level (second layer of defense)
- **Stateless** — must explicitly allow responses both ways
- **Allow and deny** rules are supported
- Rules evaluated in ascending **rule-number** order; the asterisk rule is the catch-all
- Default network ACL **allows all inbound and outbound**
- Usually administered by the network security team

04 VPC CONNECTIVITY OPTIONS

pick the service for the scenario

IF YOU NEED TO…	CONSIDER USING	CATEGORY
Connect a private subnet to the internet	NAT gateway or NAT instance	EC2 instance connectivity
Connect a VPC to another VPC	VPC peering	VPC to VPC
Connect a VPC to an on-premises network	Site-to-Site VPN · Direct Connect + VPN · VPN CloudHub	Network to VPC
Reach AWS services without leaving AWS	PrivateLink interface endpoint · gateway endpoint	VPC endpoints
Connect many VPCs and networks via one hub	AWS Transit Gateway	Network / VPC to VPC

05 RESERVED IP ADDRESSES IN EVERY SUBNET

example subnet `10.0.0.0/24`

ADDRESS	WHY AWS RESERVES IT
10.0.0.0	Network address
10.0.0.1	Reserved for the VPC router
10.0.0.2	Amazon DNS — base of the range **plus two**, reserved in every subnet
10.0.0.3	Reserved by AWS for future use
10.0.0.255	Network broadcast address (a VPC does not support broadcast)

06 CREATING A VPC PEERING CONNECTION

`01` Requester VPC owner **sends** the peering request → `02` Accepter VPC owner **accepts** it (request expires after 7 days) → `03` **Both** owners add route-table entries for the peer's CIDR → `04` Adjust **security group** rules if needed → `05` Optionally enable **DNS hostname resolution**

07 EXAM TRAPS

where the knowledge check gets you

- × “A subnet can span multiple Availability Zones.” — False. A **subnet lives in exactly one AZ**; it is the *VPC* that spans all AZs in the Region.
- × “An auto-assigned public IP is permanent like an Elastic IP.” — False. A public IP is **not static** — it is released when the instance is stopped or terminated. Only an **Elastic IP** stays fixed.
- × “Security groups can deny specific traffic.” — False. Security groups hold **allow rules only**; if you need explicit deny rules, that is a **network ACL** at the subnet level.
- × “Security groups are stateless.” — Reversed. **Security groups are stateful** (responses flow back automatically); **network ACLs are stateless** and need an explicit rule for return traffic.
- × “VPC peering is transitive.” — False. If A peers with B and B peers with C, **A cannot reach C** through B. Peer A and C directly, and no route may lead through a peer to its internet gateway or NAT.
- × “You can peer VPCs with overlapping CIDR ranges.” — False. Peered (and VPN-connected) VPCs must have **non-overlapping IP ranges**.
- × “A gateway endpoint works for any AWS service.” — False. A **gateway endpoint reaches only Amazon S3 and Amazon DynamoDB**; every other supported service uses a **PrivateLink interface endpoint**.
- × “A NAT gateway lets the internet start connections to private instances.” — False. NAT allows only **outbound-initiated** traffic; it forwards the instance's request and returns the response, but the internet cannot initiate a connection inward.

08 SELF-QUIZ

answers are upside-down below

Q1 What is the smallest and largest CIDR prefix length allowed for a VPC?

Q2 What single configuration determines whether a subnet is public or private?

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

Q4 Which firewall is stateful and at what level does it operate; which is stateless and where?

Q5 Can a single subnet exist in more than one Availability Zone?

Q6 Which NAT device does AWS recommend, and why?

Q7 Is VPC peering transitive?

Q8 Which two AWS services can a VPC gateway endpoint reach?

Q9 What service connects thousands of VPCs and on-premises networks through a single hub?

Q10 What are the two endpoints of a Site-to-Site VPN connection?

ANSWER KEY (rotate the page)

Q1 /16 (largest, up to 65,536 addresses) to /28 (smallest, 16 addresses) **Q2** Its route table — a route sending 0.0.0.0/0 to an internet gateway makes it public **Q3** Five — the first four addresses and the last (broadcast) address **Q4** Security group = stateful, instance/ENI level; network ACL = stateless, subnet level **Q5** No — a subnet exists in exactly one Availability Zone **Q6** The NAT gateway — better availability and bandwidth, and it is a managed service (no administration) **Q7** No — peering is one-to-one; VPCs must be peered directly and traffic cannot transit a peer **Q8** Amazon S3 and Amazon DynamoDB **Q9** AWS Transit Gateway **Q10** A virtual private gateway on the AWS side and a customer gateway on the on-premises side