# Connecting Networks

MULTI-VPC DESIGN · TRANSIT GATEWAY · VPC PEERING · SITE-TO-SITE VPN · DIRECT CONNECT · PRIVATELINK & ENDPOINTS · WELL-ARCHITECTED

STUDY & REVIEW

## 01 MUST KNOW

if you remember five things, remember these

01 **Mesh vs. hub-and-spoke: full mesh** directly links every VPC to every other — `N × (N − 1) / 2` connections (100 VPCs → 4,950), which is heavy to operate but fast and low-latency for a few VPCs. **Hub-and-spoke** routes everything through a central hub, so each node needs only one connection (100 VPCs → 100). **Transit Gateway** is the AWS hub-and-spoke router; the Well-Architected Framework prefers it over many-to-many mesh.

02 **Transit Gateway:** a **centralized, Regional router** that connects thousands of VPCs and on-premises networks through one attachment each. It is **managed and auto-scales** with traffic, supports static and dynamic routing (IPv4 and IPv6), and can be **peered** with other transit gateways across Regions and accounts. Traffic always stays on the **AWS backbone** — never the public internet. Charged per **connection-hour** plus traffic throughput.

03 **VPC peering:** a **one-to-one** private connection between two VPCs (same or different account or Region) using private IPs. The connection itself is **free** (cross-AZ and cross-Region data transfer is charged), and it is **not transitive**. The two VPCs **cannot have overlapping CIDR blocks**; for overlapping ranges or app-level access, use **AWS PrivateLink** with a Network Load Balancer.

04 **Site-to-Site VPN: IPsec-encrypted tunnels over the public internet** between an on-premises **customer gateway** and an AWS **virtual private gateway** (or transit gateway). Each connection provides **two tunnels across separate AZs** for high availability, can be ready in hours, and is charged per **VPN connection-hour**. Accelerate it with **Global Accelerator** — but only when it is attached to a **transit gateway**.

05 **Direct Connect:** a **dedicated, private 802.1Q VLAN** line from on-premises into AWS that bypasses the internet for **consistent, predictable performance**, higher bandwidth, and a **reduced data-transfer rate**. Three virtual interfaces: **public** (AWS public services), **private** (VPC via a virtual private gateway), and **transit** (VPCs via a transit gateway and Direct Connect gateway). Provisioning takes **weeks**; for HA, pair DX **primary** with a **VPN backup**.

## 02 KEY TERMS

| TERM | DEFINITION |
|---|---|
| **Full mesh architecture** | Every VPC is directly connected to every other VPC; a network of N nodes needs `N × (N − 1) / 2` connections. Fast and low-latency for a few VPCs, but operationally heavy at scale. |
| **Hub-and-spoke architecture** | A central intermediary hub manages connectivity, so each node needs only one connection to the hub; simplifies management for many VPCs at the cost of some added hub-processing latency. |
| **AWS Transit Gateway** | A centralized, Regional, hub-and-spoke router connecting VPCs and on-premises networks; managed and auto-scaling, with Transit Gateway Flow Logs (to CloudWatch Logs, S3, or Kinesis Data Firehose) for traffic visibility. |
| **Transit gateway attachment** | The reference that connects a transit gateway to a resource — a VPC (elastic network interfaces, one per AZ), a VPN, a Direct Connect gateway, or a peered transit gateway. Each attachment associates with a route table. |
| **Transit gateway peering** | A peering attachment joining two transit gateways in different Regions or accounts; a static route points traffic to the peering attachment, and inter-Region traffic is encrypted on the AWS backbone. |
| **VPC peering** | A one-to-one private connection that lets instances in two VPCs communicate by private IP as if on the same network; the connection is free, and creating it requires the peer VPC to accept the request. |
| **Transitive peering** | Routing through an intermediary peer to reach a third VPC. VPC peering does not support it — A peered to B and B peered to C does not connect A to C. |

| TERM | DEFINITION |
|---|---|
| **AWS PrivateLink** | Private, application-level connectivity from consumer VPCs to a service in a provider VPC using an interface endpoint to a Network Load Balancer; needs no peering and works with overlapping CIDR blocks. |
| **AWS Site-to-Site VPN** | Builds two encrypted IPsec tunnels (across AZs) between an on-premises customer gateway and an AWS virtual private gateway or transit gateway, over the public internet. |
| **Customer gateway / virtual private gateway** | The customer gateway is the on-premises side of a VPN (a physical or software device and its AWS representation); the virtual private gateway is the AWS side. Each needs a distinct BGP ASN. |
| **AWS VPN CloudHub** | A hub-and-spoke model using one virtual private gateway with multiple customer gateways (unique BGP ASNs) to connect several on-premises sites; the sites must not have overlapping IP ranges. |
| **AWS Direct Connect** | A dedicated, private 802.1Q VLAN connection that extends an on-premises network to AWS for consistent, predictable performance and higher bandwidth; offers public, private, and transit virtual interfaces. |

## 03 NETWORK CONNECTIVITY OPTIONS AT A GLANCE

match the option to the connection you need

| OPTION | CONNECTS | MODEL AND KEY TRAITS | COST |
|---|---|---|---|
| **VPC peering** | Two VPCs (any account or Region) | One-to-one, private IPs, **not transitive**, no overlapping CIDRs; update both route tables | Connection is **free**; cross-AZ/Region data transfer charged |
| **Transit Gateway** | Thousands of VPCs and on-prem to one hub | Regional hub-and-spoke router; auto-scales; peer across Regions/accounts; stays on AWS backbone | Per **connection-hour** + traffic throughput |
| **Site-to-Site VPN** | On-prem to a VPC over the internet | Two **IPsec** tunnels across AZs; ready in hours; BGP or static routing | Per **VPN connection-hour** |
| **Direct Connect** | On-prem to AWS via a private line | Dedicated **802.1Q VLAN**; predictable performance, more bandwidth; weeks to provision | Reduced **DX data-transfer rate** vs. internet |
| **AWS PrivateLink** | Consumer VPC to a service (app level) | Interface endpoint to a Network Load Balancer; **no peering**; allows overlapping CIDRs | — (no VPC peering charge) |

## 04 SITE-TO-SITE VPN VS. DIRECT CONNECT

the two ways to reach AWS from on-premises

### SITE-TO-SITE VPN

*encrypted tunnels over the public internet*

- IPsec-encrypted; two tunnels terminating in separate AZs for HA
- Rides the public internet — availability is not guaranteed
- Fast to set up — can be available in hours
- Charged per VPN connection-hour
- Accelerate with Global Accelerator (transit gateway attachment only)

### DIRECT CONNECT

*dedicated private VLAN line into AWS*

- Dedicated or hosted 802.1Q VLAN; does not traverse the internet
- Consistent, predictable performance and higher dedicated bandwidth
- Reduced Direct Connect data-transfer rate
- Needs planning and physical provisioning — typically weeks
- Still enforce encryption in transit (TLS/IPsec); pair DX + VPN backup for HA

## 05 DIRECT CONNECT VIRTUAL INTERFACES (VIFS)

know which VIF reaches what

| VIRTUAL INTERFACE | PROVIDES ACCESS TO | THROUGH |
|---|---|---|
| **Public VIF** | Public AWS services (for example, Amazon S3) | Direct Connect endpoint → public services |
| **Private VIF** | Your VPC | A virtual private gateway |
| **Transit VIF** | Your VPCs | A transit gateway, via a Direct Connect gateway |

## 06 CREATING A SITE-TO-SITE VPN CONNECTION

six steps, on-prem side and AWS side

01 Create the **customer gateway** (BGP ASN if supported) → 02 Create the **virtual private gateway** (distinct ASN) — or use a transit gateway → 03 Configure routing to the VGW (enable route propagation) → 04 Update **security groups** (SSH, RDP, ICMP, ...) → 05 Create the **VPN connection** — two tunnels, separate AZs → 06 Download config file → configure the customer gateway device

## 07 EXAM TRAPS

where the knowledge check gets you

- × "VPC peering is transitive." — It is **not**. If A↔B and B↔C are peered, A still cannot reach C unless A and C are explicitly peered. This isolation limits the blast radius.
- × "You can peer VPCs with overlapping CIDR blocks." — Peering requires **non-overlapping** CIDRs. For overlapping ranges (or application-level access), use **AWS PrivateLink** with a Network Load Balancer.
- × "You can reach Amazon S3 over a Site-to-Site VPN." — You **cannot** connect to S3 by VPN. Use a **gateway VPC endpoint** for S3 — private, no additional cost, no bandwidth or packet-size limits.
- × "Transit Gateway (or peering) traffic can cross the public internet." — Transit Gateway traffic **always stays on the AWS backbone**; inter-Region peering and transit-gateway peering traffic is encrypted and never traverses the internet.
- × "A Site-to-Site VPN connection gives you one tunnel." — Each connection provides **two IPsec tunnels** across separate AZs; use one as primary and one for redundancy.
- × "Global Accelerator can accelerate a VPN attached to a virtual private gateway." — Acceleration is supported **only for VPNs attached to a transit gateway**, not a virtual private gateway.
- × "Direct Connect can be turned up in hours like a VPN." — DX needs planning and physical provisioning and typically takes **weeks**. VPN is the fast option (hours).
- × "For many VPCs, full mesh peering is the recommended design." — Well-Architected prefers **hub-and-spoke** (Transit Gateway) over many-to-many mesh; avoid VPC peering for more than two VPCs.

## 08 SELF-QUIZ

answers are upside-down below

Q1 In a full mesh of N VPCs, what formula gives the number of connections required?

Q2 Which AWS service is a centralized, Regional, hub-and-spoke router that connects VPCs and on-premises networks?

Q3 VPC peering does not support which routing relationship, so A↔B and B↔C does not connect A to C?

Q4 If two VPCs that must connect have overlapping CIDR blocks, which feature (with a Network Load Balancer) provides connectivity?

Q5 How many IPsec tunnels does each Site-to-Site VPN connection provide, and why?

Q6 In a Site-to-Site VPN, what is the on-premises side called and what is the AWS side called?

Q7 Global Accelerator can accelerate a Site-to-Site VPN only when the VPN is attached to what?

Q8 Name the three Direct Connect virtual interface types.

Q9 Which virtual interface connects a Direct Connect location to a transit gateway through a Direct Connect gateway?

Q10 To privately access Amazon S3 from EC2 by the most efficient route (no internet), what do you use?

ANSWER KEY (rotate the page)

Q1 N × (N − 1) / 2 Q2 AWS Transit Gateway Q3 transitive peering Q4 AWS PrivateLink (an interface VPC endpoint) Q5 two tunnels across separate Availability Zones, for high availability Q6 customer gateway (on-prem); virtual private gateway or transit gateway (AWS) Q7 a transit gateway (not a virtual private gateway) Q8 public, private, and transit Q9 the transit virtual interface Q10 a gateway VPC endpoint for Amazon S3