

# Types of VPC Connection


## Types of VPC Connections

Here's a breakdown of the most common types:

---

### 1. Internet Gateway (IGW)

- Allows resources in your VPC (like EC2) to **connect to the internet**.
- Required for **public subnets**.

 One VPC ↔ Internet (public access)

---

### 2. NAT Gateway / NAT Instance


- Allows **private subnets** (no public IP) to **access the internet** for updates, downloads, etc.
- **No inbound connections** from the internet are allowed.

 Private subnet ↔ Internet (outbound only)

---

### 3. VPC Peering

- Connects two VPCs **privately** using AWS's backbone network.
- No need to use public IPs or VPNs.
- Supports **cross-account** and **cross-region** (with limitations).

 VPC A ↔ VPC B (1-to-1, transitive peering not allowed)

---

### 4. Site-to-Site VPN

- Creates an **encrypted IPsec tunnel** between your **on-premises** network and your VPC.
- Uses a **Virtual Private Gateway** on AWS side and a **Customer Gateway** on your side.

 On-prem network ↔ AWS VPC (via secure tunnel)

---

## 5. ⚡ AWS Direct Connect

- Provides a **dedicated physical fiber connection** from your data center to AWS.
- More reliable and consistent than VPN.
- Can be used alone or with VPN for **high availability**.

 On-prem ↔ AWS VPC (via private link)

---

## 6. 🏠 Transit Gateway


- Acts as a **central hub** to connect **multiple VPCs, VPNs, and Direct Connect**.
- Supports **transitive routing**, unlike peering.

 Many-to-many VPC connectivity (VPC ↔ TGW ↔ VPC, VPN, DX)

---

## 7. 📦 VPC Endpoints (Interface & Gateway)

- Allows **private connection to AWS services** (like S3, DynamoDB, etc.) **without going through the internet**.
- Two types:
  - **Interface Endpoint** (ENI) — for most AWS services
  - **Gateway Endpoint** — for S3 and DynamoDB

 VPC ↔ AWS Services (via private network)

---

## 8. 👤 Client VPN

- A **user-level VPN service** that lets individual users connect securely to a VPC (e.g., developers working remotely).
- Uses OpenVPN protocol.

 Individual clients ↔ AWS VPC

---

## Summary Table

VPC Connection Type	Purpose	Internet Required	Encrypted Transitive?	
Internet Gateway (IGW)	Public access to/from VPC	Yes	No	N/A
NAT Gateway/Instance	Outbound access for private subnets	Yes	No	N/A
VPC Peering	Private VPC-to-VPC comms	No	No	✗
Site-to-Site VPN	Connect VPC to on-prem	Yes	✓	✗
AWS Direct Connect	Dedicated line from on-prem	No	Optional	✗
Transit Gateway (TGW)	Hub for multiple connections	No	Optional	✓
VPC Endpoint	Private access to AWS services	No	✓	N/A
Client VPN	Remote user access to VPC	Yes	✓	N/A