**VPN vs. VPC: Key Differences and Use Cases**

**Introduction**

Both Virtual Private Network (VPN) and Virtual Private Cloud (VPC) are essential networking concepts in cloud computing, but they serve different purposes. A **VPN** enables secure communication over the public internet, while a **VPC** is a logically isolated network within a cloud provider’s infrastructure.

**Key Differences**

| **Feature** | **VPN (Virtual Private Network)** | **VPC (Virtual Private Cloud)** |
| --- | --- | --- |
| **Definition** | Secure connection over the internet | Isolated network in a cloud environment |
| **Purpose** | Securely connects remote users or networks | Provides a private network for cloud resources |
| **Connectivity** | Uses tunneling protocols over public networks | Uses private networking within a cloud provider |
| **Security** | Encrypts traffic but traverses public internet | Fully isolated and secured within cloud infrastructure |
| **Use Case** | Remote access, hybrid cloud, secure communications | Hosting cloud-based applications and services |

**What is a VPN?**

A **VPN (Virtual Private Network)** is a secure communication tunnel that encrypts data while it travels between remote users or networks and a private network. It allows organizations to establish **secure remote access** to internal resources over the public internet.

**Common VPN Types:**

1. **Site-to-Site VPN** – Connects two networks securely (e.g., on-premises to cloud).
2. **Remote Access VPN** – Allows individual users to securely access a network from anywhere.

**Use Cases:**

* Secure remote access for employees.
* Connecting on-premises data centers to cloud environments.
* Encrypting internet traffic to protect sensitive data.

**What is a VPC?**

A **VPC (Virtual Private Cloud)** is a logically isolated section within a cloud provider's infrastructure where users can deploy and manage their cloud resources (e.g., virtual machines, databases, applications) with **private networking controls**.

**Key Features:**

* **Subnet Segmentation** – Allows logical division of networks.
* **Custom Routing & Security Rules** – Configurable firewalls and routing policies.
* **Private Connectivity** – Can connect to on-premises via VPN or ExpressRoute.

**Use Cases:**

* Hosting secure applications and databases in the cloud.
* Creating isolated environments for different teams or projects.
* Hybrid cloud setups where on-prem resources need cloud integration.

**VPN vs. VPC: Which One to Use?**

* Use **VPN** when you need **secure remote access** or **site-to-site connectivity** between different networks.
* Use **VPC** when you need a **private cloud environment** to host workloads securely.
* In hybrid cloud scenarios, both VPN and VPC can be used together—VPC provides the cloud network, and VPN ensures secure access.

**Conclusion**

VPN and VPC are complementary networking technologies in cloud computing. While **VPN** secures data transmission over public networks, **VPC** provides an isolated and secure cloud environment for applications and resources. Understanding their differences helps organizations choose the right approach for their cloud and networking needs.