AWS Networking Services

Amazon Virtual Private Cloud(VPC)

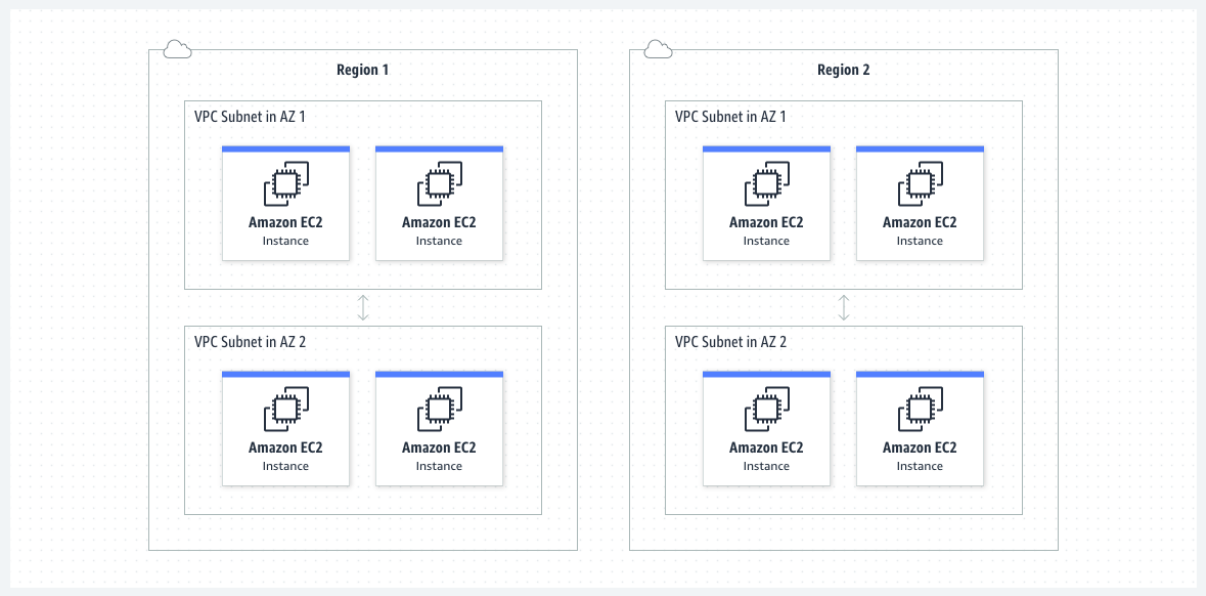
- Define and launch AWS resources in a logically isolated virtual network
- When you first create your AWS account a default VPC is created for you in each AWS region.
- By default you can create up to 5 VPCs per region.
- It is logically isolated from other virtual networks in the AWS Cloud.

Benefits of Amazon VPC

1. Increase security
2. Save time
3. Manage and control your environment

How it works

Amazon Virtual Private Cloud (Amazon VPC) gives you full control over your virtual networking environment, including resource placement, connectivity, and security. Get started by setting up your VPC in the AWS service console. Next, add resources to it such as Amazon Elastic Compute Cloud (EC2) and Amazon Relational Database Service (RDS) instances. Finally, define how your VPCs communicate with each other across accounts, Availability Zones, or AWS Regions. In the example below, network traffic is being shared between two VPCs within each Region.



Use cases

- Launch a simple website or blog
- Host multi-tier web applications
- Create hybrid connections

Components of a VPC:

- **A Virtual Private Cloud**: A logically isolated virtual network in the AWS cloud. You define a VPC's IP address space from ranges you select.
- **Subnet**: A segment of a VPC's IP address range where you can place groups of isolated resources (maps to an AZ, 1:1).
- **Internet Gateway**: The Amazon VPC side of a connection to the public Internet.
- **NAT Gateway**: A highly available, managed Network Address Translation (NAT) service for your resources in a private subnet to access the Internet.
- **Hardware VPN Connection**: A hardware-based VPN connection between your Amazon VPC and your datacenter, home network, or co-location facility.
- **Virtual Private Gateway**: The Amazon VPC side of a VPN connection.
- **Customer Gateway**: Your side of a VPN connection.
- **Router**: Routers interconnect subnets and direct traffic between Internet gateways, virtual private gateways, NAT gateways, and subnets.

Subnets

After creating a VPC, you can add one or more subnets in each Availability Zone.

When you create a subnet, you specify the CIDR block for the subnet, which is a subset of the VPC CIDR block.

Each subnet must reside entirely within one Availability Zone and cannot span zones.

Firewalls

Network Access Control Lists (ACLs) provide a firewall/security layer at the subnet level.

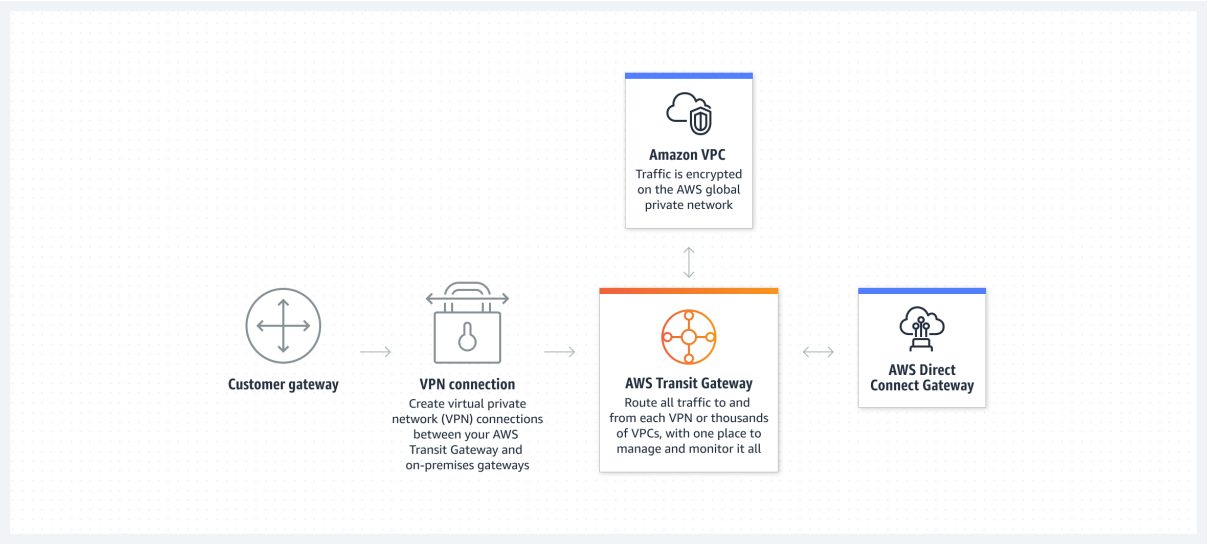
Security Groups provide a firewall/security layer at the instance level.

AWS Transit Gateway

- Connect Amazon VPCs, AWS accounts, and on-premises networks to a single gateway.

How it works

AWS Transit Gateway connects your Amazon Virtual Private Clouds (VPCs) and on-premises networks through a central hub. This connection simplifies your network and puts an end to complex peering relationships. Transit Gateway acts as a highly scalable cloud router—each new connection is made only once.



Use cases

1. Deliver applications around the world
2. Rapidly move to global scale
3. Smoothly respond to spikes in demand
4. Host multicast applications on AWS

AWS PrivateLink

- Establish connectivity between VPCs and AWS services without exposing data to the internet
- AWS PrivateLink provides private connectivity between virtual private clouds (VPCs), supported AWS services, and your on-premises networks without exposing your traffic to the public internet. Interface VPC endpoints, powered by PrivateLink, connect you to services hosted by AWS Partners and supported solutions available in AWS Marketplace.