NETWORKING

Amazon Virtual Private Cloud Overview

Table of contents

Cloud computing continues to evolve and Amazon Web Services (AWS) is still leading the way. Large enterprises and small businesses, as well as government agencies and educational institutions, are realizing the benefits of the cloud.

As companies begin to migrate to the Amazon Cloud or extend their private datacenters to the Amazon Cloud, networking becomes a critical factor to consider.

This e-book provides a brief overview of networking with Amazon Virtual Private Cloud (VPC) and associated services.
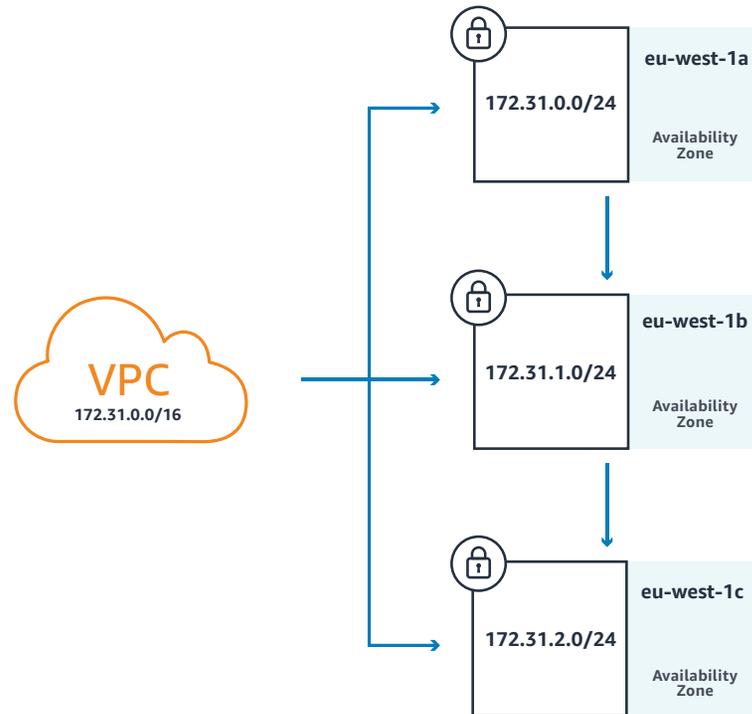
Fundamentals of Amazon Virtual Private Cloud

Amazon VPC enables you to provision a logically isolated section of the Amazon Cloud so that you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 addresses in your VPC for secure and easy access to resources and applications.

You can easily customize the network configuration for your Amazon VPC. For example, you can create a public-facing subnet for your web servers that has access to the Internet and place your backend systems, such as databases or application servers, in a private-facing subnet with no Internet access. To help control access to Amazon Elastic Compute Cloud (Amazon EC2) instances in each subnet, you can leverage multiple layers of security, including security groups and network access control lists.

If you want to leverage the Amazon Cloud as an extension of your corporate datacenter, you can create a Virtual Private Network (VPN) connection between your corporate datacenter and your VPC.

Virtual Private Cloud with subnets

VPC
172.31.0.0/16

eu-west-1a
172.31.0.0/24
Availability Zone

eu-west-1b
172.31.1.0/24
Availability Zone

eu-west-1c
172.31.2.0/24
Availability Zone
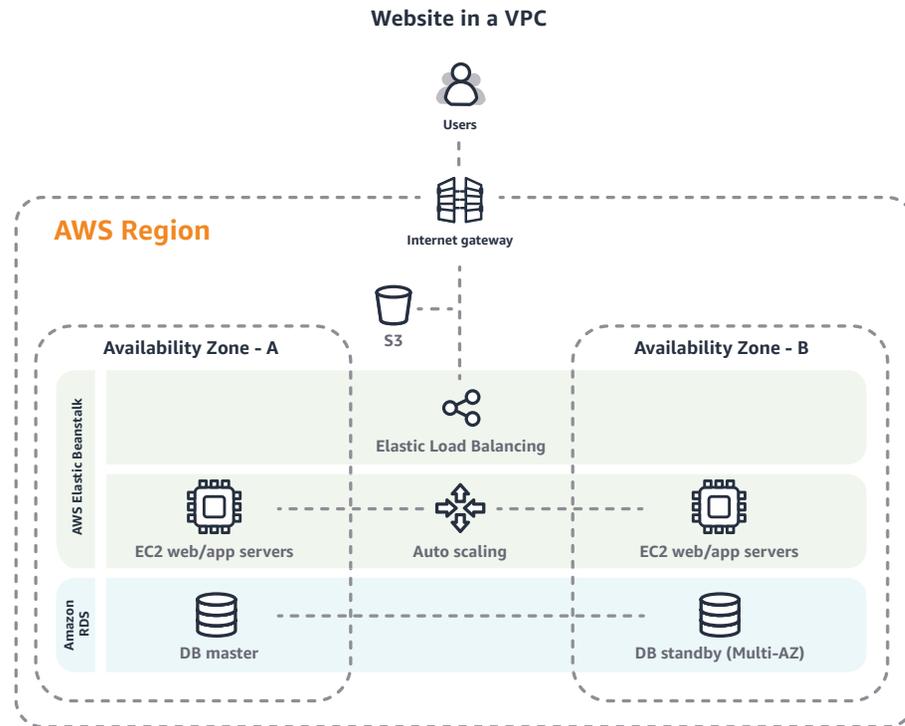
Amazon VPC use cases

Host a website
When you use Amazon VPC to host your basic web applications—such as blogs or simple websites—you gain the additional layers of privacy and security afforded by the AWS cloud infrastructure.
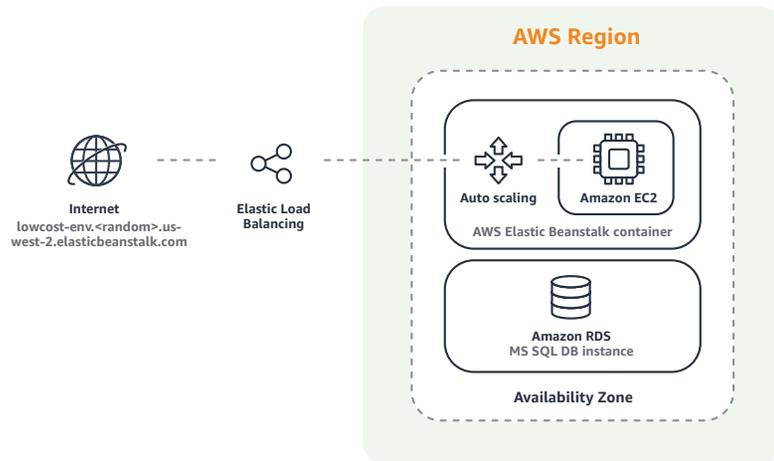
Deploy multi-tier applications
Using an Amazon VPC to host multi-tier web applications enables you to strictly enforce access and security restrictions between your web servers, application servers, and databases.

Migrate corporate applications
By connecting your Amazon VPC to your corporate network, you can move corporate applications to the cloud, add more compute capacity, or periodically back up mission-critical data. Because your VPC can be hosted behind your corporate firewall, you can move your IT resources to the cloud without changing how your users access these applications.

Website in a VPC

Users

Internet gateway

AWS Region

S3

AWS Elastic Beanstalk

Availability Zone - A

Elastic Load Balancing

EC2 web/app servers

Auto scaling

Availability Zone - B

EC2 web/app servers

Amazon RDS

DB master

DB standby (Multi-AZ)

Multi-tier app in VPC

AWS Region

Internet
lowcost-env.<random>.us-west-2.elasticbeanstalk.com

Elastic Load Balancing

Auto scaling

Amazon EC2

AWS Elastic Beanstalk container

Amazon RDS
MS SQL DB instance

Availability Zone

Migrate corporate app

VPC

Availability Zone 1

NAT gateway

Public subnet
10.0.96.0/20

Web tier

Application tier

Database tier

Active Directory tier

Sharepoint 2016

Sharepoint 2016

SQL Server instance

Domain controller

Remote mgmt

Internet gateway

Elastic Load Balancing

Users

NAT gateway

Public subnet
10.0.96.0/20

Web tier

Application tier

Database tier

Active Directory tier

Sharepoint 2016

Sharepoint 2016

SQL Server instance

Domain controller

Availability Zone 2
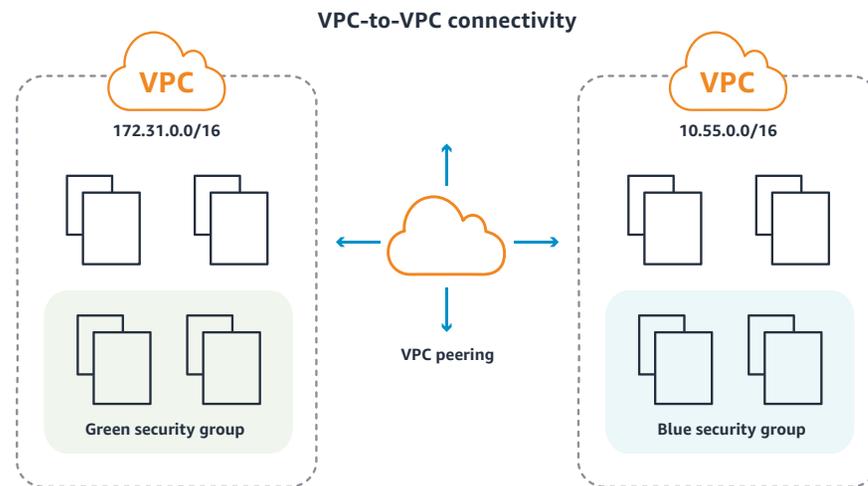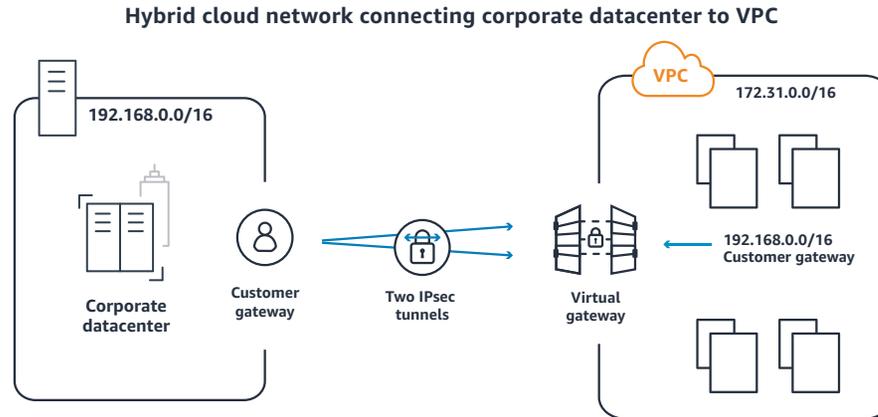
AWS Region

6

Different ways to connect your Amazon VPC

You can connect your Amazon VPC to the Internet, to your datacenter, or to other VPCs. You choose the best option based on the AWS resources that you want to expose publicly and those that you want to keep private.

You can connect your Amazon VPC to the Internet, to your datacenter, or to other VPCs.

Hybrid cloud network connecting corporate datacenter to VPC

192.168.0.0/16

VPC

172.31.0.0/16

Corporate datacenter

Customer gateway

Two IPsec tunnels

Virtual gateway

192.168.0.0/16
Customer gateway

VPC-to-VPC connectivity

VPC

172.31.0.0/16

Green security group

VPC peering

VPC

10.55.0.0/16

Blue security group

Connecting Amazon VPC to a corporate datacenter with AWS Direct Connect

By connecting your VPC to your corporate network with AWS Direct Connect, you can move corporate applications to the cloud, launch additional web servers, and add more compute capacity to your network. When you connect with AWS Direct Connect, your VPC is hosted behind your corporate firewall, which means you can move your IT resources into the Amazon Cloud without changing how your users access these applications.
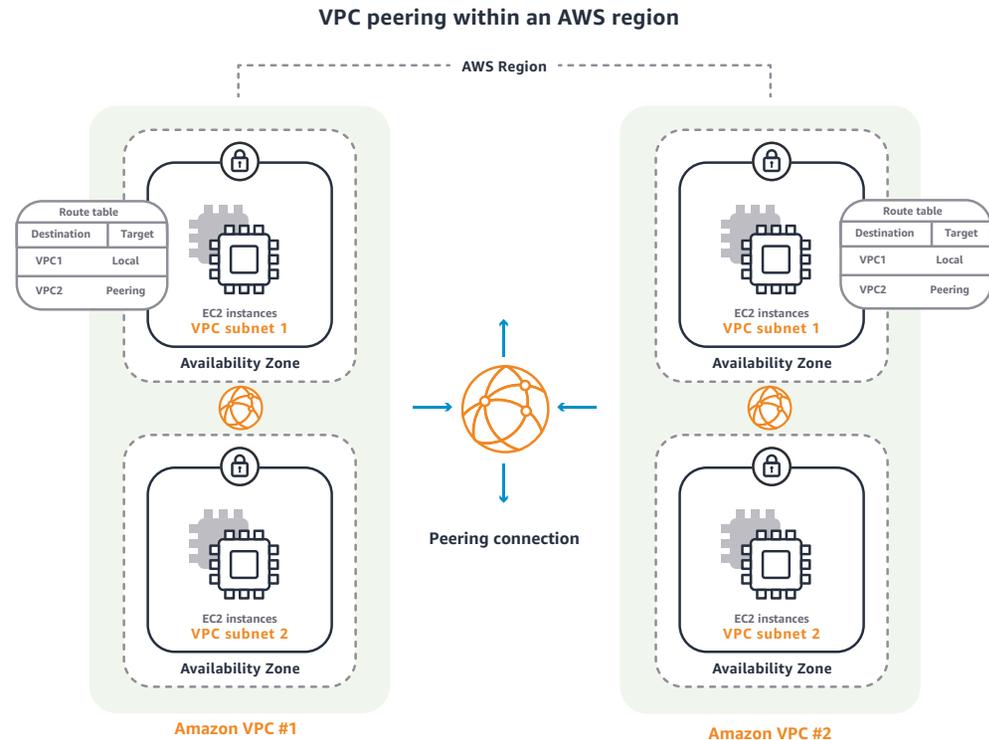
Hybrid cloud connectivity with Amazon VPC and Direct Connect
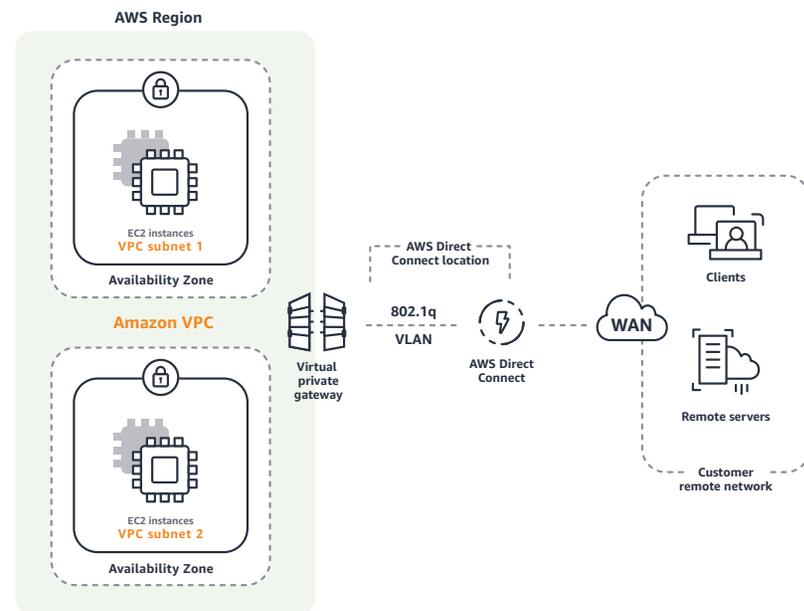
VPC peering

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 or IPv6 addresses. Instances in either VPC can communicate with each other as if they were within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The peered VPCs can be in the same or different regions.
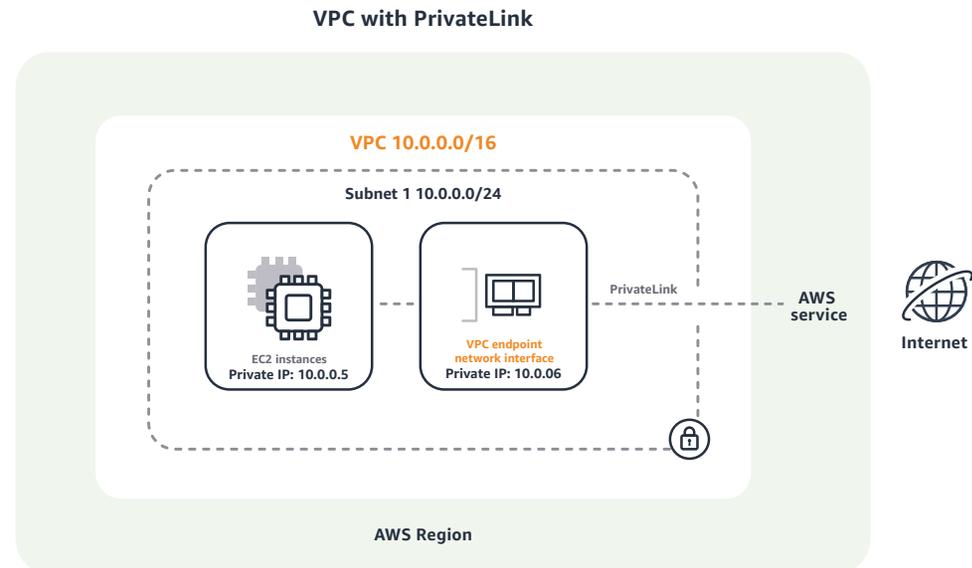
A VPC peering connection is a network connection between two VPCs that enables you to route traffic between them using either IPv4 or IPv6 addresses.

VPC peering within an AWS region

AWS Region

Route table	
Destination	Target
VPC1	Local
VPC2	Peering

EC2 instances
VPC subnet 1
Availability Zone

EC2 instances
VPC subnet 2
Availability Zone

Amazon VPC #1

Peering connection

Route table	
Destination	Target
VPC1	Local
VPC2	Peering

EC2 instances
VPC subnet 1
Availability Zone

EC2 instances
VPC subnet 2
Availability Zone

Amazon VPC #2

AWS PrivateLink with VPC endpoints

AWS PrivateLink is designed to enable customers to access and scale AWS services fast, while keeping all the network traffic within the AWS network. When you create endpoints for AWS services powered by PrivateLink, these service endpoints appear in your VPCs as Elastic Network Interface (ENI) with private IPs. With PrivateLink, you do not need to whitelist public IPs or manage Internet connectivity using an internet gateway, network address translation (NAT) devices, or firewall proxies to connect to AWS services. AWS services available on PrivateLink also support private connectivity over AWS Direct Connect, so that applications in corporate datacenters can connect to AWS services.

VPC with PrivateLink

VPC 10.0.0.0/16

Subnet 1 10.0.0.0/24

EC2 instances
Private IP: 10.0.0.5

VPC endpoint network interface
Private IP: 10.0.06

PrivateLink

AWS service

Internet

AWS Region

Benefits of Amazon Virtual Private Cloud

Simple

Create a VPC quickly and easily using the AWS Management Console. Select one of the common network setups that best matches your needs and press "Start VPC Wizard." Subnets, IP ranges, route tables, and security groups are automatically created to enable you to create the applications to run in the VPC.
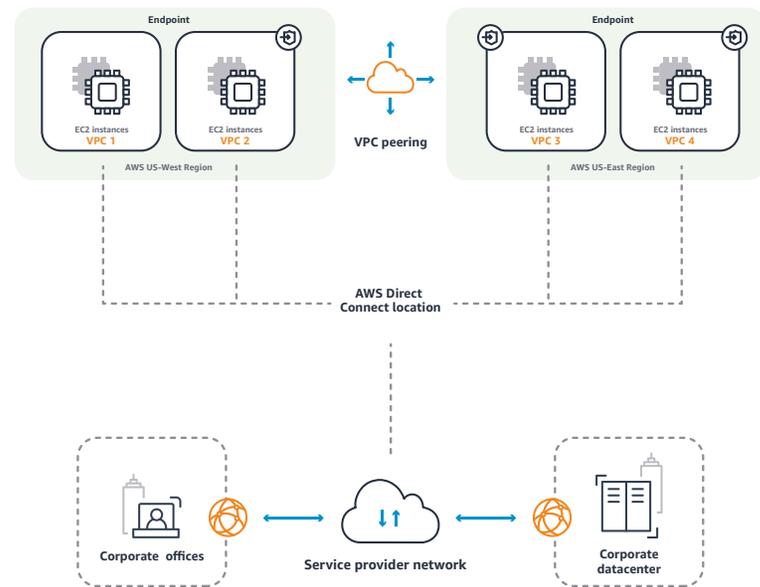
Secure

Amazon VPC provides advanced security features, such as security groups and network access control lists, to enable inbound and outbound filtering at the instance level and subnet level. In addition, you can store data in Amazon Simple Storage Service (S3) and restrict access so that it's accessible only from instances in your VPC.

Scalable

Amazon VPC provides all of the same benefits as the rest of the AWS platform. You can instantly scale your resources up or down, select Amazon EC2 instance types and sizes that are right for your applications, and pay only for the resources you use —all within Amazon's proven cloud infrastructure.

Hybrid Cloud Network connecting corporate datacenter to Amazon VPC

Networking is key to company performance today. With its advanced security features, wide array of connecting options, and simple setup and management, Amazon Virtual Private Cloud delivers reliable networking you can easily customize and scale to your company's needs.

For secure, customizable networking with the high availability and scalability of the AWS Cloud, choose Amazon Virtual Private Cloud.

Get more details at aws.amazon.com/vpc.
Or contact a sales representative