Amazon Virtual Private Cloud

Overview

Amazon Virtual Private Cloud (VPC) gives you control over your virtual networking environment including resource placement, connectivity, and security. The first step is to create your VPC. Then you can add resources to it, such as Amazon Elastic Compute Cloud (EC2) and Amazon Relational Database Service (RDS) instances. Finally, you can define how your VPCs communicate with each other, across accounts, Availability Zones (AZs), or Regions.

Features

Amazon VPC provides features that you can use to increase and monitor the security for your virtual private cloud:

Reachability Analyzer: Reachability Analyzer is a static configuration analysis tool that enables you to analyze and debug network reachability between two resources in your VPC.

VPC Flow Logs: You can monitor your VPC flow logs delivered to Amazon S3 or Amazon CloudWatch to help you gain operational visibility into your network dependencies and traffic patterns, detect anomalies and prevent data leakage, or troubleshoot network connectivity and configuration issues.

VPC Traffic Mirroring: VPC traffic mirroring enables you to copy network traffic from an elastic network interface of Amazon EC2 instances and then send the traffic to out-of-band security and monitoring appliances for deep packet inspection.

Ingress Routing: This enables you to route all incoming and outgoing traffic flowing to/from an Internet Gateway (IGW) or Virtual Private Gateway (VGW) to a specific EC2 instance’s Elastic Network Interface. With this feature, you can configure your virtual private cloud to send all traffic to an IGW, VGW or EC2 instance before the traffic reaches your business workloads.

Security Groups: Security groups act as a firewall for associated Amazon EC2 instances, helping to control both inbound and outbound traffic at the instance level. When you launch an instance, you can associate it with one or more security groups that you've created. Each instance in your VPC could belong to a different set of security groups. If you don't specify a security group when you launch an instance, the instance is automatically associated with the default security group for the VPC.

Network Access Control List: A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets.