# **What is VPC peering**

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. You can launch AWS resources, such as Amazon EC2 instances, into your VPC.

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different Regions (also known as an inter-Region VPC peering connection).


            A VPC peering connection
        

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck.

A VPC peering connection helps you to facilitate the transfer of data. For example, if you have more than one AWS account, you can peer the VPCs across those accounts to create a file sharing network. You can also use a VPC peering connection to allow other VPCs to access resources you have in one of your VPCs.

When you establish peering relationships between VPCs across different AWS Regions, resources in the VPCs (for example, EC2 instances and Lambda functions) in different AWS Regions can communicate with each other using private IP addresses, without using a gateway, VPN connection, or network appliance. The traffic remains in the private IP space. All inter-Region traffic is encrypted with no single point of failure, or bandwidth bottleneck. Traffic always stays on the global AWS backbone, and never traverses the public internet, which reduces threats, such as common exploits, and DDoS attacks. Inter-Region VPC peering provides a simple and cost-effective way to share resources between regions or replicate data for geographic redundancy.

**Benefits of VPC Network Peering**

VPC Network Peering has the following benefits:

* Network Latency: Connectivity that uses only internal addresses provides lower latency than connectivity that uses external addresses.
* Network Security: Service owners do not need to have their services exposed to the public Internet and deal with its associated risks.
* Network Cost: Google Cloud charges egress bandwidth pricing for networks using external IP addresses to communicate even if the traffic is within the same zone. If however, the networks are peered they can use internal IP addresses to communicate and save on those egress costs. Regular network pricing still applies to all traffic.

**Specifications**

VPC Network Peering has the following specifications:

General specifications:

* VPC Network Peering works with Compute Engine, GKE, and App Engine flexible environment.
  + By default, VPC Network Peering with GKE is supported when used with IP aliases. If you don't use IP aliases, you can export custom routes so that GKE containers are reachable from peered networks.
* Only VPC networks are supported for VPC Network Peering. Peering is not supported for legacy networks.
* VPC Network Peering supports both IPv4 and IPv6 connectivity. You can configure VPC Network Peering on a VPC network that contains dual-stack subnets. However, for IPv6, only dynamic routes are exchanged.
* A given VPC network can peer with multiple VPC networks, but there is a limit.

Administrative separation:

* Peered VPC networks remain administratively separate. Routes, firewalls, VPNs, and other traffic management tools are administered and applied separately in each of the VPC networks.
* To establish peering connectivity, a Network Administrator for each VPC network must create a peering connection to the other VPC network. A Network Administrator for either VPC network can disconnect a peering connection.
* Each side of a peering association is set up independently. Peering will be active only when the configuration from both sides matches. Either side can choose to delete the peering association at any time.
* Creating a peering connection does not grant you any IAM roles on the other VPC network. For example, if you have the Compute Network Admin role or the Compute Security Admin role for one network, you don't become a Network Administrator or a Security Administrator for the other network.