VPC Peering

## Service Overview

[***VPC peering connection***](https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html) *is a networking connection between two VPCs that enables you to route traffic between them privately. 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, with a VPC in another AWS account, or with a VPC in a different AWS Region. AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor an AWS Site-to-Site 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.*

*You can establish peering relationships between VPCs across different AWS Regions (also called Inter-Region VPC Peering). This allows VPC resources including EC2 instances, Amazon RDS databases and Lambda functions that run in different AWS Regions to communicate with each other using private IP addresses, without requiring gateways, VPN connections, or separate network appliances. 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.*

*Instead of using VPC peering, you can use an* [***AWS Transit Gateway***](https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html) *that acts as a network transit hub, to interconnect your VPCs and on-premises networks*

## Use cases / Considerations

* *Your company has a VPC for the finance department, and another VPC for the accounting department. The finance department requires access to all resources that are in the accounting department, and the accounting department requires access to all resources in the finance department.*
* *Your company has multiple IT departments, each with their own VPC. Some VPCs are located within the same AWS account, and others in a different AWS account. You want to peer together all VPCs to enable the IT departments to have full access to each others' resources.*
* *Your company's IT department has a VPC for file sharing. You want to peer other VPCs to that central VPC, however, you do not want the other VPCs to send traffic to each other.*
* *Your company has a VPC that you want to share with your customers. Each customer can create a VPC peering connection with your VPC, however, your customers cannot route traffic to other VPCs that are peered to yours, nor are they aware of the other customers' routes.*
* *You have a central VPC that is used for Active Directory services. Specific instances in peer VPCs send requests to the Active Directory servers and require full access to the central VPC. The central VPC does not require full access to the peer VPCs; it only needs to route response traffic to the specific instances.*

## Governance

## Cautions

* *You cannot create a VPC peering connection between VPCs with matching or overlapping IPv4 CIDR blocks.*
* *If the VPCs have multiple IPv4 CIDR blocks, you cannot create a VPC peering connection if any of the CIDR blocks overlap (regardless of whether you intend to use the VPC peering connection for communication between the non-overlapping CIDR blocks only).*
* *This limitation also applies to VPCs that have non-overlapping IPv6 CIDR blocks. Even if you intend to use the VPC peering connection for IPv6 communication only, you cannot create a VPC peering connection if the VPCs have matching or overlapping IPv4 CIDR blocks.*
* *Active VPC peering connections per VPC 50. The maximum quota is 125 peering connections per VPC. The number of entries per route table should be increased accordingly; however, network performance might be impacted.*
* *Outstanding VPC peering connection requests – 25. This is the quota for the number of outstanding VPC peering connection requests that you've requested from your account.*
* *Expiry time for an unaccepted VPC peering connection request - 1 week (168 hours). This quota cannot be increased.*

## Pricing considerations

*https://aws.amazon.com/vpc/pricing/*

## More details

[Unsupported VPC peering configurations - Amazon Virtual Private Cloud](https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html)

[What is VPC peering? - Amazon Virtual Private Cloud](https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html)