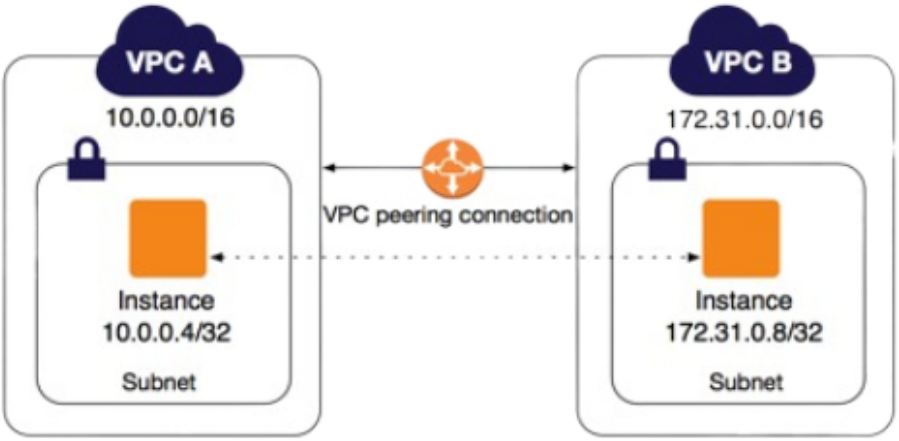
AWS VPC PEERING



Presented By
SHUBHAM CHOUHAN

OOGLELABS

What is AWS VPV Peering?

A VPC peering connection 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.

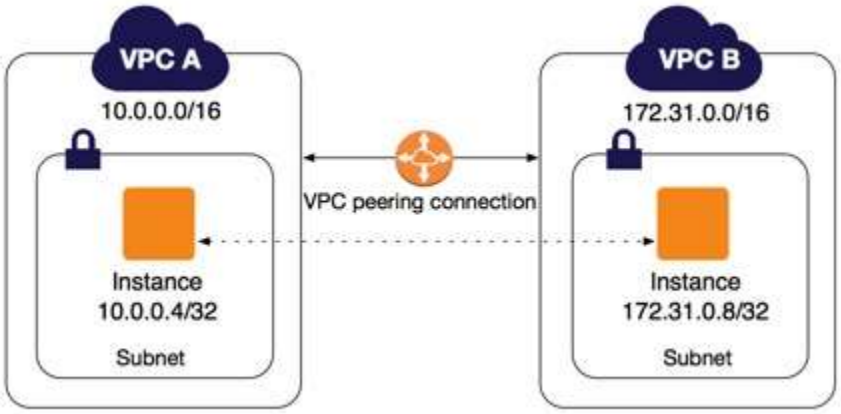
What is the difference between VPC peering and transit gateway?

TGWs across different regions can peer with each other to enable VPC communications across regions. Each spoke VPC only needs to connect to the TGW to gain access to other connected VPCs. provides simpler VPC-to-VPC communication management over VPC Peering with a large number of VPCs.

Transit Gateway Peering

- AWS Transit Gateway supports the ability to establish peering connections between Transit Gateways in the same and different AWS Regions.
- Inter-region peering enables customers to extend this connectivity and build global networks spanning multiple AWS Regions.
- Intra-region peering simplifies routing and inter-connectivity between VPCs and on-premises networks that are serviced and managed via separate Transit Gateways
- Traffic using inter-region Transit Gateway peering always stays on the AWS global network and never traverses the public internet, thereby reducing threat vectors, such as common exploits and DDoS attacks.
- Inter-region Transit Gateway peering encrypts inter-region traffic with no single point of failure.

A VPC pairing connection is a network connection between two VPCs that allows you to direct traffic between them using private IPv4 or IPv6 addresses. Instances in any VPC can communicate with each other as if they were on the same network. You can create a pairing connection between your own VPCs or with a VPC from another AWS account. VPCs can be in different regions (also known as cross-region VPC pairing connection).



AWS uses the existing VPC infrastructure to create a paired connection between VPCs; it is not a gateway nor a VPN connection and does not depend on external physical hardware. There is no single point of communication failure or a bandwidth bottleneck.

A VPC pairing connection helps you make data transfer easier. For example, if there is more than one AWS account, you can pair the VPCs between those accounts to create a file sharing network. You can also use a VPC pairing connection to allow other VPCs to access the features you have in one of your VPCs.

You can establish pairing relationships between VPCs between different AWS regions (also called interregion VPC pairing). 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 separate gateways, VPN connections, or network equipment. The traffic remains in the private IP space. All interregion traffic is encrypted with no single point of failure or bottleneck in bandwidth. Traffic always stays on the global AWS backbone and never traverses the public internet, which reduces threats such as common breaches and DDoS attacks. Pairing intra-region VPCs provides a simple and cost-effective way to share resources across regions or replicate data for geographic redundancy.

VPC peering basics

To establish a VPC peering connection, you do the following:

1. The owner of the requester VPC sends a request to the owner of the accepter VPC to create the VPC peering connection. The accepter VPC can be owned by you, or another AWS account, and cannot have a CIDR block that overlaps with the CIDR block of the requester VPC.
2. The owner of the accepter VPC accepts the VPC peering connection request to activate the VPC peering connection.
3. To enable the flow of traffic between the VPCs using private IP addresses, the owner of each VPC in the VPC peering connection must manually add a route to one or more of their VPC route tables that points to the IP address range of the other VPC (the peer VPC).
4. If required, update the security group rules that are associated with your instance to ensure that traffic to and from the peer VPC is not restricted. If both VPCs are in the same region, you can reference a security group from the peer VPC as a source or destination for ingress or egress rules in your security group rules.
5. With the default VPC peering connection options, if EC2 instances on either side of a VPC peering connection address each other using a public DNS hostname, the hostname resolves to the public IP address of the instance. To change this behavior, enable DNS hostname resolution for your VPC connection. After enabling DNS hostname resolution, if instances on either side of the VPC peering connection address each other using a public DNS hostname, the hostname resolves to the private IP address of the instance.

VPC peering connection lifecycle

A VPC peering connection goes through various stages starting from when the request is initiated. At each stage, there may be actions that you can take, and at the end of its lifecycle, the VPC peering connection remains visible in the Amazon VPC console and API or command line output for a period of time.

- **Initiating-request:** A request for a VPC peering connection has been initiated. At this stage, the peering connection can fail, or can go to pending-acceptance.
- **Failed:** The request for the VPC peering connection has failed. While in this state, it cannot be accepted, rejected, or deleted. The failed VPC peering connection remains visible to the requester for 2 hours.
- **Pending-acceptance:** The VPC peering connection request is awaiting acceptance from the owner of the accepter VPC. During this state, the owner of the requester VPC can delete the request, and the owner of the accepter VPC can accept or reject the request. If no action is taken on the request, it expires after 7 days.
- **Expired:** The VPC peering connection request has expired, and no action can be taken on it by either VPC owner. The expired VPC peering connection remains visible to both VPC owners for 2 days.
- **Rejected:** The owner of the accepter VPC has rejected a pending-acceptance VPC peering connection request. While in this state, the request cannot be accepted. The rejected VPC peering connection remains visible to the owner of the requester VPC for 2 days, and visible to the owner of the accepter VPC for 2 hours. If the request was created within the same AWS account, the rejected request remains visible for 2 hours.
- **Provisioning:** The VPC peering connection request has been accepted, and will soon be in the active state.
- **Active:** The VPC peering connection is active, and traffic can flow between the VPCs (provided that your security groups and route tables allow the flow of traffic). While in this state, either of the VPC owners can delete the VPC peering connection, but cannot reject it. Note If an event in a region in which a VPC resides prevents the flow of traffic, the status of the VPC peering connection remains Active.
- **Deleting:** Applies to an inter-Region VPC peering connection that is in the process of being deleted. The owner of either VPC has submitted a request to delete an active VPC peering connection, or the owner of the requester VPC has submitted a request to delete a pending-acceptance VPC peering connection request. 3 Amazon Virtual Private Cloud VPC Peering Multiple VPC peering connections
- **Deleted:** An active VPC peering connection has been deleted by either of the VPC owners, or a pending-acceptance VPC peering connection request has been deleted by the owner of the requester VPC. While in this state, the VPC peering connection cannot be accepted or rejected. The VPC peering connection remains visible to the party that deleted it for 2 hours, and visible to the other party for 2 days. If the VPC peering connection was created within the same AWS account, the deleted request remains visible for 2 hours.

Create a VPC peering connection

To create a VPC peering connection, first create a request to peer with another VPC. You can request a VPC peering connection with another VPC in your account, or with a VPC in a different AWS account. For an inter-Region VPC peering connection where the VPCs are in different Regions, the request must be made from the Region of the requester VPC. To activate the request, the owner of the accepter VPC must accept the request. For an inter-Region VPC peering connection, the request must be accepted in the Region of the accepter VPC. For more information, see

- Create with VPCs in the same account and Region.
- Create with VPCs in the same account and different Regions.
- Create with VPCs in different accounts and the same Region.
- Create with VPCs in different accounts and Regions.
- Create a VPC peering connection using the command line.

Create with VPCs in the same account and Region

To create a VPC peering connection with VPCs in the same account and Region

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Peering connections. 6 Create with VPCs in the same account and different Regions
3. Choose Create peering connection.
4. Configure the following information, and choose Create Peering Connection when you are done:

- Peering connection name tag: You can optionally name your VPC peering connection.
- VPC (Requester): Select the VPC in your account with which you want to create the VPC peering connection.
- Under Select another VPC to peer with: Ensure My account is selected, and select another of your VPCs.
- (Optional) To add a tag, choose Add new tag and enter the tag key and value.

5. In the confirmation dialog box, choose OK.
6. Select the VPC peering connection that you've created, and choose Actions, Accept Request.
7. In the confirmation dialog, choose Yes, Accept. A second confirmation dialog displays; choose Modify my route tables now to go directly to the route tables page, or choose Close to do this later.

Create with VPCs in the same account and different Regions

To create a VPC peering connection with VPCs in the same account and different Regions

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Peering connections.
3. Choose Create peering connection.
4. Configure the following information, and choose Create Peering Connection when you are done:

- Peering connection name tag: You can optionally name your VPC peering connection. Doing so creates a tag with a key of Name and a value that you specify.
- VPC (Requester): Select the requester VPC in your account with which to request the VPC peering connection.
- Account: Ensure My account is selected.
- Region: Choose Another region, select the Region in which the accepter VPC resides.
- VPC (Accepter): Enter the ID of the accepter VPC.

5. In the confirmation dialog box, choose OK.
6. In the Region selector, select the Region of the accepter VPC.
7. In the navigation pane, choose Peering Connections. Select the VPC peering connection that you've created, and choose Actions, Accept Request.
8. In the confirmation dialog, choose Yes, Accept. A second confirmation dialog displays; choose Modify my route tables now to go directly to the route tables page, or choose Close to do this later.

Create with VPCs in different accounts and the same Region

To request a VPC peering connection with VPCs in different accounts and the same Region

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Peering connections. 3. Choose Create peering connection.
3. Configure the information as follows, and choose Create Peering Connection when you are done:

- Peering connection name tag: You can optionally name your VPC peering connection. Doing so creates a tag with a key of Name and a value that you specify. This tag is only visible to you; the owner of the peer VPC can create their own tags for the VPC peering connection.
- VPC (Requester): Select the VPC in your account with which to create the VPC peering connection.
  • Account: Choose Another account.
- Account ID: Enter the AWS account ID of the owner of the accepter VPC.
- VPC (Accepter): Enter the ID of the VPC with which to create the VPC peering connection.

4. In the confirmation dialog box, choose OK.

Create with VPCs in different accounts and Regions

To request a VPC peering connection with VPCs in different accounts and Regions

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Peering connections.
3. Choose Create peering connection.
4. Configure the information as follows, and choose Create Peering Connection when you are done:

- Peering connection name tag: You can optionally name your VPC peering connection. Doing so creates a tag with a key of Name and a value that you specify. This tag is only visible to you; the owner of the peer VPC can create their own tags for the VPC peering connection.
- VPC (Requester): Select the VPC in your account with which to create the VPC peering connection.
- Account: Choose Another account.
- Account ID: Enter the AWS account ID of the owner of the accepter VPC. • Region: Choose Another region, select the Region in which the accepter VPC resides. • VPC (Accepter): Enter the ID of the VPC with which to create the VPC peering connection.

5. In the confirmation dialog box, choose OK.