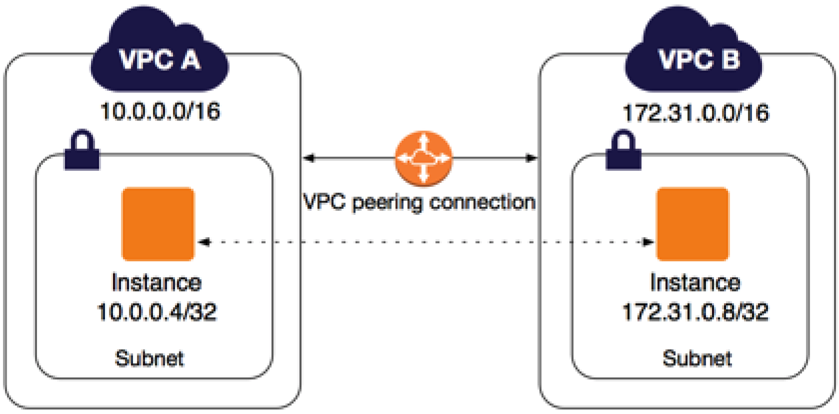
VPC- Peering

AWS VPC Peering is cool !! Where and when do you peer and why peer.

Virtual Private Cloud (VPC) enables you to launch resources into a virtual network that you've defined.

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).

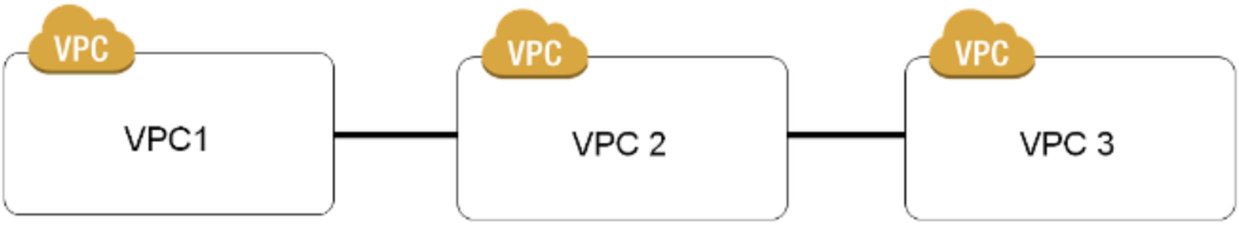


VPC Peering

AWS VPC Peering Design

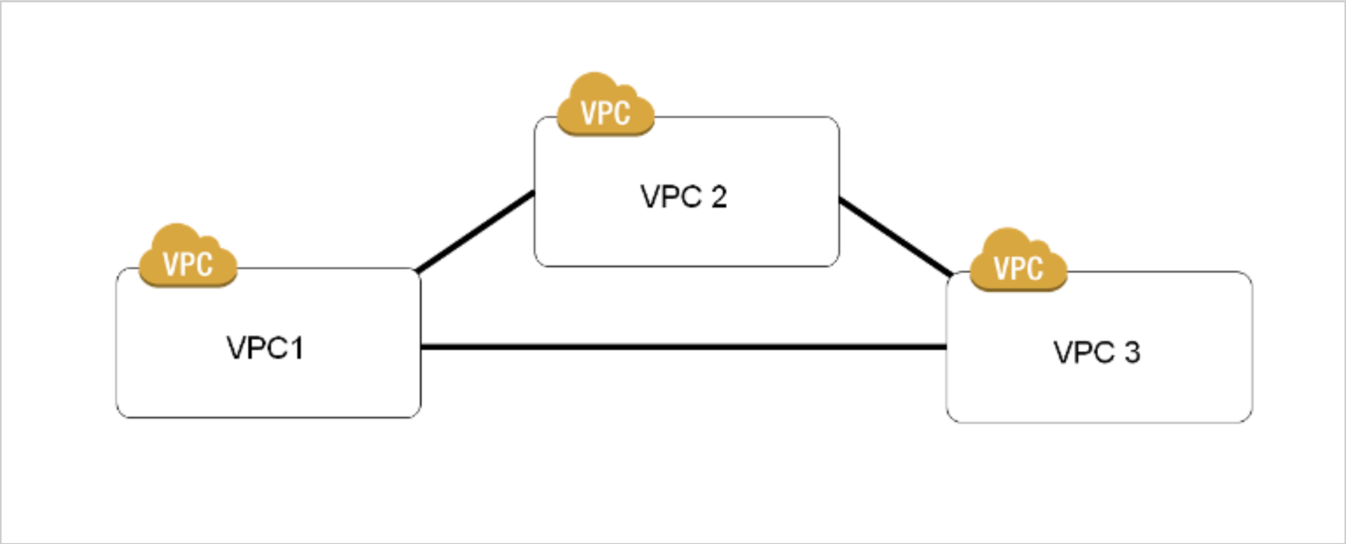
When setting up a peered connection, one VPC acts as the requester (the VPC initiating the connection) while the other acts as a peer. Before a connection can be established, the owner of the peer VPC has to acknowledge the request and accept the Peering connection. Once a connection has been established, routing between the CIDR blocks of each VPC must be added to a route table to enable resources within the networks to communicate via the private IP enable resources within the networks to communicate via the private IP address range.

From a design perspective, you cannot daisy chain VPCs together and expect them to communicate across one large network. Each AWS VPC will only communicate with its 'requester' or 'peer.' For example, if you have a peering connection between VPC 1 and VPC 2, and another connection between VPC 2 and VPC 3 as below



Then VPC 1 and VPC 2 could communicate with each other directly, as can VPC 2 and VPC 3. However, because you cannot route through one VPC to get to another, VPC 1 and VPC 3 could not communicate directly.

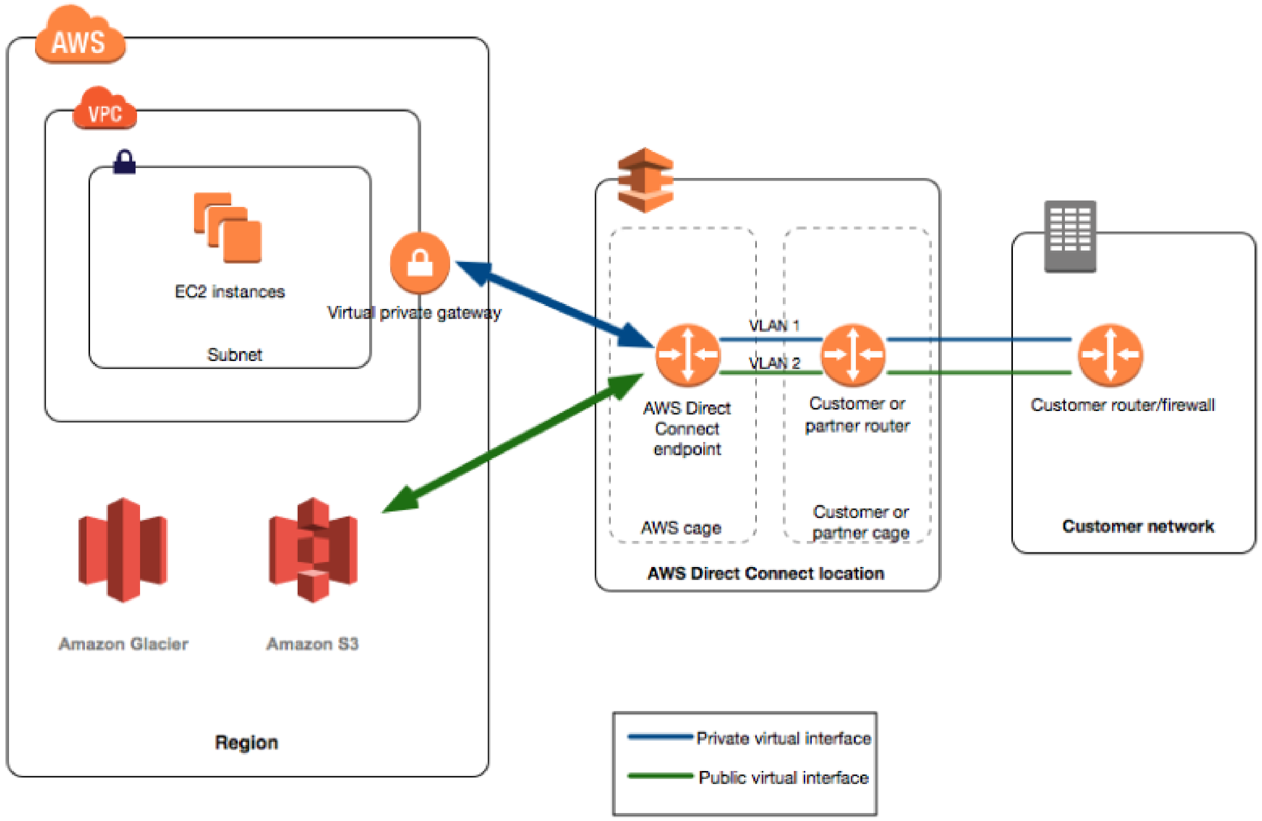
To enable direct communication between VPC 1 and VPC 3, you would have to implement a separate peering connection between the two, as shown below :-



WS VPC peering provides an excellent secure and trusted connection between VPCs for enhanced management and resource sharing. Depending on how you have configured your VPCs, you may want to incorporate such an architecture into your environment.

Direct Connect:

Makes it easy to establish a dedicated network connection from your premises to AWS. Using Direct connect you can establish private connection between AWS and your data center.



VPN vs Direct Connect

VPN: Can be configured in minutes and are a good solution if you have an immediate need. You are susceptible to having your data passed via the internet – i.e. low bandwidth, packet drop etc.

Direct Connect: Does not involve the internet it uses dedicated private network connections between your intranet and Amazon VPC.

1. Increase Reliability
2. Higher Bandwidth
3. Takes longer to set up