SINGLE REGION MULTI-VPC CONNECTIVITY *"How do I connect multiple VPCs within the same AWS Region?"*

Overview

Amazon Virtual Private Cloud (Amazon VPC) offers a comprehensive set of virtual networking capabilities that provide AWS customers with many options for designing and implementing networks on the AWS cloud. With Amazon VPC, customers can provision logically isolated virtual networks to host their AWS resources. Customers can create multiple VPCs within the same region or in different regions, in the same account or in different accounts. This is useful for customers who require multiple VPCs for security, billing, regulatory, or other purposes, and want to integrate AWS resources between their VPCs more easily. More often than not, these different VPCs need to communicate privately and securely with one another for sharing data or applications.

This document provides AWS customers with high-level connectivity options for multiple VPCs within the same AWS Region using VPC peering or AWS Direct Connect connections. It includes best practices and guidance, and outlines the most commonly used multiple-VPC connection configurations within a region. For guidance on connecting VPCs in different AWS Regions, see the Multiple Region Multi-VPC Connectivity Solution Brief.

The following sections address key considerations and recommendations for connecting VPCs in the same region, and assume some basic knowledge of VPC peering, network addressing, subnetting, routing,[1] and AWS Direct Connect.

General Best Practices

When connecting multiple VPCs in a single AWS Region, there are some universal network-design principles to consider:

- Ensure that your VPC network ranges (CIDR blocks) do not overlap.
- Make sure the solution you choose is able to scale according to your current and future VPC connectivity needs.
- Ensure you implement a highly available (HA) design with no single point of failure.
- Consider your data-transfer needs, as this will affect the solution you choose. Some solutions proposed below may prove to be more expensive than others based on the amount of data transferred.
- Connect only those VPCs that really need to communicate with each other.

Application on the AWS Platform

The following sections offer prescriptive advice and guidelines to help connect VPCs within a single AWS Region. We describe three possible solutions for connecting VPCs, and briefly introduce a fourth design strategy that accommodates transitive routing. Keep in mind that VPC designs that adhere to networking best practices can be easily changed from one configuration to another, so select the option that makes most sense for your current networking needs.

Partially Meshed Network (VPC Peering)

This approach allows customers to connect VPCs as appropriate, and is a common strategy for customers who have a central VPC that contains shared resources. In the shared-services VPC scenario, customers use VPC peering to connect selected VPCs to the central VPC in a hub-and-spoke formation. The central VPC might require full or partial access to the spoke VPCs, and the spoke VPCs might require full or partial access to the central VPC. Note that the following solution addresses VPCs in the same region as the central VPC.

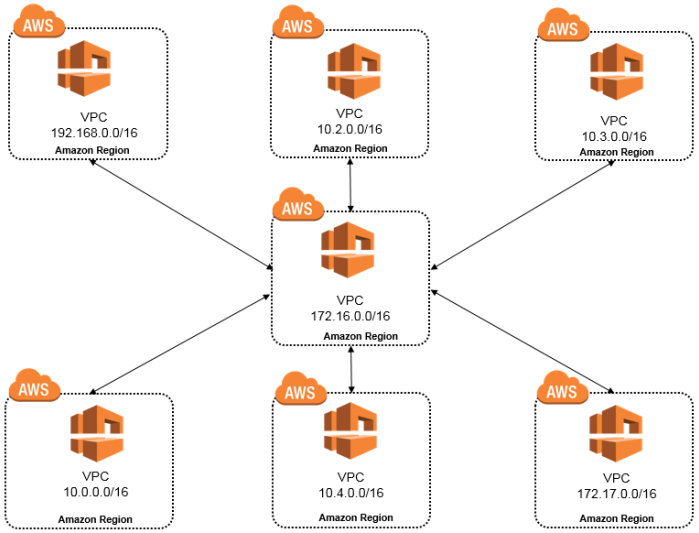
[1] Please see the Wikipedia article on CIDR address allocation for background information: https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

This option is best suited for customers with the following use case/requirements:

- They do not require full connectivity between all of their VPCs.
- They would benefit from a central VPC to host shared services such as Active Directory or a central repository.
- They have multiple VPCs that need access to shared resources but do not need access to each other.
- They require fewer than 125 peering connections per VPC.[2]
- They have a business need to allow other AWS customers to connect to their VPC, such as a SaaS provider who wants to share resources with customers. Each customer can create a VPC peering connection to the central VPC, but they cannot route traffic to other peered VPCs, nor are they aware of the other customers' routes.

Configuration Details

The diagram to the right shows a shared-services VPC configuration, which is the most common partial-mesh configuration. This design pattern creates peering connections between the central VPC and each spoke VPC, but not from one spoke VPC to another.



Specific instances in the peer VPCs send requests to the central 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 or to exchange data.

To enable the flow of traffic between VPCs, the central VPCs route table must contain a route that points to all or part of the CIDR block of each spoke VPC. Similarly, each spoke VPC must have a route that points to the IP address range of the central VPC.

Considerations

Note that Amazon VPC does not support directly routing from one VPC to another through an intermediary VPC's peered connections. For example, if VPC A is peered with VPC B, and VPC B is peered with VPC C, VPC A will not have access to VPC C unless a new peering connection is established between them. Each peering connection requires modifications to the associated VPCs' route tables and, as the number of VPCs grows, this can be difficult to maintain. And keep in mind that AWS recommends a maximum of 125 peering connections per VPC. Customers can create VPC peering connections between VPCs in the same account, or with VPCs in a different AWS account, as long as the VPCs are in the same region.

Fully meshed VPC Peers (VPC Peering)

This approach creates multiple peering connections to facilitate the sharing of information between resources in different VPCs.

This option is best suited for customers with the following use case/requirements:

- Their AWS resources are logically separated across different VPCs for each business or IT unit, but different departments might need to be able to route to any other group's resources. For example, finance and accounting departments often require access to one another's data.
- They require fewer than 125 peering connections per VPC.[2]
- There is no one centralized shared-services VPC to serve as a hub for hosting shared resources.

[2] Consider using AWS Direct Connect, especially if you have an existing relationship with an AWS Direct Connect provider.

Configuration Details

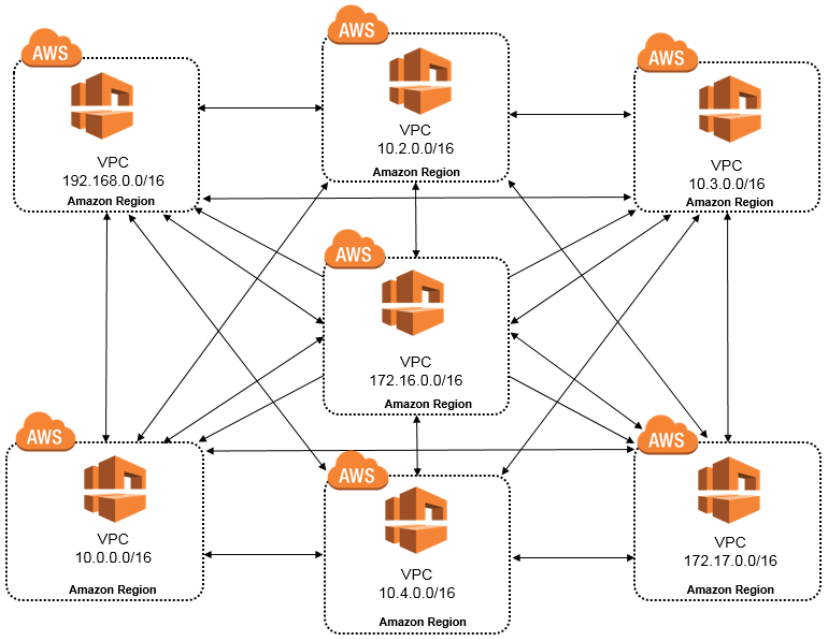
This design connects multiple VPCs in a fully meshed configuration, with peering connections between each pair of VPCs. With this configuration, each VPC has access to the resources in all other VPCs.

To enable the flow of traffic between VPCs, each VPC route table must contain entries that point to the IP address ranges of all the other VPCs in the fully meshed configuration. This design is more complicated to set up than a partially meshed configuration, but it enables communication across all VPCs in the system.

Considerations

Each peering connection requires modifications to all the other VPCs' route tables and, as the number of VPCs grows, this can be difficult to maintain. And keep in mind that AWS recommends a maximum of 125 peering connections per VPC.

Customers can create VPC peering connections between VPCs in the same account, or with VPCs in a different AWS account, as long as the VPCs are in the same region.



VPCs connected with AWS Direct Connect

This approach is a good alternative for customers who need to connect a high number of VPCs to a central VPC or to on-premises resources, or who already have an AWS Direct Connect connection in place. This design also offers customers the ability to incorporate transitive routing into their network design. For example, if VPC A and VPC B are both connected to an on-premises network using AWS Direct Connect connections, then the two VPCs can be connected to each other via AWS Direct Connect.

This option is best suited for customers with the following use case/requirements:

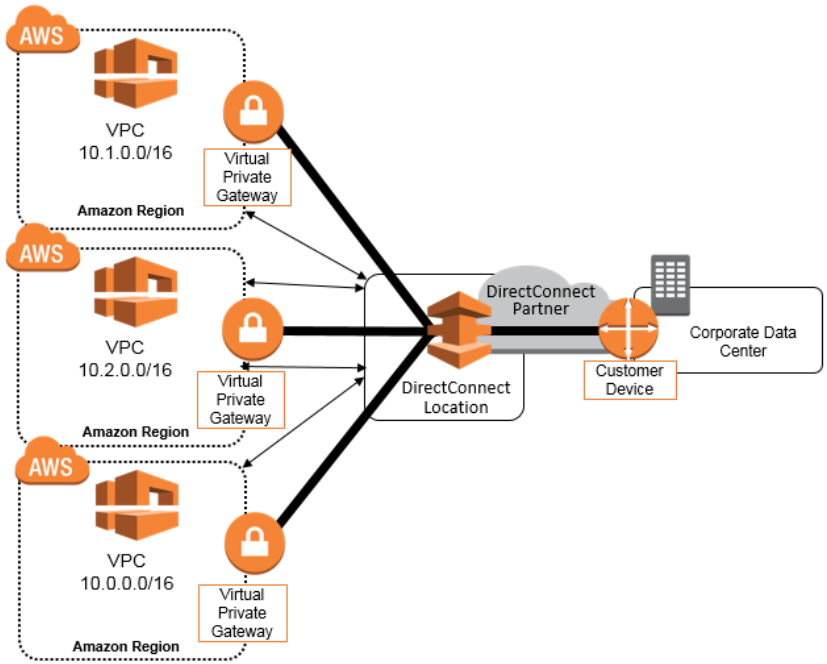
- They have an existing AWS Direct Connect connection.
- They can use the AWS Direct Connect connection for transitive routing between VPCs.
- They need to create more than 125 connections per VPC.

Configuration Details

This design pattern leverages AWS Direct Connect to route traffic between VPCs. In the diagram to the right, a single physical AWS Direct Connect connection is divided into multiple logical connections, called *virtual interfaces*. On the AWS side, a Virtual Private Gateway (VGW) is configured for each VPC in the network.

Considerations

VPC and VGW route tables support a maximum of 100 routes. Therefore, this approach will require VPCs to either use a default route, or perform route summarization with AS override on the customer device, to connect more than 100 AWS Direct Connect routed VPCs.



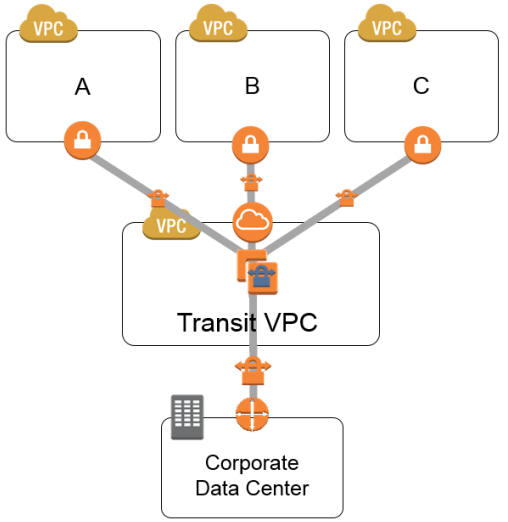
Transit VPC

This approach uses customer-managed Amazon Elastic Compute Cloud (Amazon EC2) VPN instances in a dedicated transit VPC with an Internet gateway. The EC2 instances initiate the VPN connections and route traffic between multiple VPCs and shared-services VPCs. The spoke VPCs can leverage VPC peering to circumvent the transit VPC, providing more scalable, direct access between VPCs.

This design requires the customer to deploy, configure, and manage EC2-based VPN appliances, which will result in additional EC2, and potentially third-party product and licensing charges. Therefore, it is best suited for customers who have already implemented a transit VPC and want to leverage it to manage more advanced connection types, such as inter-region connectivity, or multi-VPC connectivity to on-premises resources.

Note that this design will generate additional data transfer charges for traffic traversing the transit VPC: data is charged when it is sent from a spoke VPC to the transit VPC, and again from the transit VPC to the on-premises network or a different AWS Region.

For additional details on this solution, see the Multiple-VPC VPN Connection Sharing Solution Brief.



Resources

AWS Direct Connect Documentation	https://aws.amazon.com/documentation/direct-connect/ AWS webpage with links to AWS Direct Connect technical documentation, including the product *User Guide*, which describes features and configuration details, and an *API Reference*
Amazon VPC Documentation	https://aws.amazon.com/documentation/vpc/ AWS webpage with links to Amazon VPC technical documentation, including introductory material (*Getting Started Guide*), component and strategy overviews (*User Guide*), and more robust technical documentation (*Network Administrator Guide*)
VPC Peering	http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html AWS documentation on VPC peering
Multiple Region Multi-VPC Connectivity	https://d0.awsstatic.com/aws-answers/AWS_Multiple_Region_Multi_VPC_Connectivity.pdf AWS Solution Brief describing options for connecting VPCs in different AWS Regions
Multiple-VPC VPN Connection Sharing	https://d0.awsstatic.com/aws-answers/AWS_Multiple_VPC_VPN_Connection_Sharing.pdf AWS Solution Brief describing options for sharing a single VPN connection with multiple VPCs