MULTIPLE REGION MULTI-VPC CONNECTIVITY

“How do I connect multiple VPCs in different AWS Regions?”

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 that reside in different AWS Regions. It includes best practices and guidance, and outlines the most commonly used cross-region VPC network configurations. For guidance on connecting VPCs in the same AWS Region, see the Single Region Multi-VPC Connectivity Solution Brief.

The following sections address key considerations and recommendations for connecting VPCs in different regions, and assume basic knowledge of Amazon VPC, VPN connections, HA remote network connectivity, network addressing, subnetting, routing, Amazon Elastic Compute Cloud (Amazon EC2), and AWS Direct Connect.

General Best Practices

When connecting multiple VPCs in different AWS Regions, 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.
- Use network equipment that supports IPsec VPN tunnels and Border Gateway Protocol (BGP), when applicable.
- Connect only those VPCs that really need to communicate with each other.

Application on the AWS Platform

The following sections offer prescriptive advice for connecting VPCs in different AWS Regions using either non-AWS networks, such as the Internet or a customer's existing network backbone, or AWS-managed networks. Customers who have already established AWS Direct Connect or VPN connections from on-premises networks to their VPCs typically prefer to reuse existing connections, while customers without existing network infrastructure usually opt for AWS-managed networks. 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.

1 See the Resources section for related documentation.
Routing Over Non-AWS Networks

Many AWS customers have invested heavily in on-premises networks, and use VPN connections or AWS Direct Connect to connect to AWS. These customers often prefer to leverage their existing infrastructure investments to route VPC traffic across regions, either by establishing new VPN connections or using their own corporate network backbone. AWS customers in this scenario often start by connecting on-premises networks to the closest AWS Region, and then look to expand to additional AWS Regions.

Internet-Based VPN

This approach enables customers to leverage Internet-based VPN connections and their on-premises infrastructure in a single region to route VPC traffic between regions. This option is best suited for customers who do not have existing network infrastructure investment in the remote region and want to leverage their existing VPN investments to connect VPCs.

Configuration Details

This design pattern creates a network hub to route traffic between spoke VPCs in different AWS Regions. Intra-region network connectivity is established using either a VPN connection or AWS Direct Connect (both options are portrayed in the diagram), and cross-region connectivity is established with Internet-based VPN connections.

Considerations

This design leverages existing on-premises network equipment and wide area network (WAN) connections to route network traffic between VPCs. It establishes cross-region VPC connectivity using existing Internet connectivity and allows customers to apply additional on-premises network monitoring and controls to inter-VPC traffic. Note that the cross-region network traffic is subject to the specific latency, variability, and available bandwidth of the existing Internet connections.

Corporate Network Backbone

This approach enables customers to route cross-region VPC traffic over existing corporate networks. This option is best suited for customers who can leverage existing global infrastructure and networks, such as a multinational customer with network connectivity between data centers in multiple locations. It is also appropriate for customers who want to ensure their VPC traffic never traverses a public network.

Configuration Details

As in the previous approach, this design also establishes intra-region network connectivity to existing network infrastructure using either a VPN connection or AWS Direct Connect. Cross-region connectivity leverages existing wide area network (WAN) connections by propagating VPC network advertisements within the company’s internal network. Finally, network routing in each VPC must be configured (through either dynamic BGP advertisements or static routes) to route cross-region traffic over the existing network backbone.
Considerations
This design leverages existing on-premises network equipment and wide area network (WAN) connections to route network traffic between VPCs. It also allows customers to apply additional on-premises network monitoring and controls to inter-VPC traffic. Note that the cross-region network traffic is subject to the specific latency, variability, and available bandwidth of the existing private network connections.

Routing Over AWS Networks
AWS provides high bandwidth, global network infrastructure to support customers’ regional networking needs. AWS Regions are connected to multiple Internet Service Providers (ISPs) as well as to a private global network backbone, which provides lower cost and more consistent cross-region network latency when compared with the public Internet. AWS customers with small on-premises network footprints, limited regional network connectivity, or who simply want to leverage AWS networks often choose one of the following options to connect VPCs in different regions. These options use public IP addresses to route network traffic between regions, using the AWS global network backbone by default. However, use of AWS private network infrastructure is provided on a best effort basis and network connectivity will failover to AWS ISP networks in the unlikely event that private network connectivity between AWS Regions is not available.2

Software VPN Appliances
This approach leverages the Amazon VPC capability to create VPN tunnels between EC2 instances in order to route traffic between VPCs in different regions. This option uses customer- or AWS Partner Network (APN) member-managed, EC2-based software VPN appliances and is best suited to customers who want to manage both ends of VPN connections using their preferred VPN software provider.

This design optimizes cross-region network transfer costs, however it requires customers to design and manage their own HA configuration for EC2 network instances.

Configuration Details
This design uses Elastic IP addresses and VPC Internet gateways to facilitate communication between the software VPN appliances. Although EC2 instances are configured with public IP addresses, network traffic between AWS Regions traverse the AWS global network backbone by default, which typically provide more consistent, lower latency network connectivity than equivalent Internet-based connections. AWS Marketplace provides multiple third-party and open source options3 for implementing software VPN appliances. Ocedo AutoVPN currently provides advanced network automation for launching, managing, and configuring software-based VPN appliances to connect multiple VPCs and full-mesh VPN networks.

Considerations
Products available in the AWS Marketplace provide additional network control features for monitoring and controlling traffic between VPCs. These include additional security features such as enhanced monitoring, network-protocol-aware firewall rules, or universal threat management capabilities. Note that customers must run network appliances in each VPC, which results in additional EC2 and, potentially, third-party license charges. These EC2 instances can also introduce a single point of failure into the network architecture, and a potential network bottleneck, so be sure to choose a VPN appliance instance size that will meet cross-region network routing requirements. Finally, leverage Auto Recovery for EC2 or other network monitoring and recovery options to decrease the time to recover failed VPN appliances.

2 Note that, for simplicity, the diagrams in this section depict use of AWS backbone network connections and do not depict network failure scenarios where traffic might briefly be routed over public ISP networks.

3 These include products from Cisco, Fortinet, Ocedo, OpenSWAN, OpenVPN, Palo Alto Networks, Sophos, and Vyatta.
Transit VPC

This approach creates a resilient, highly available transit network that supports multiple VPCs and on-premises networks. It uses a dedicated transit VPC(s) hosting EC2-based VPN appliances to route traffic between VPC virtual private gateways (VGWs) in multiple regions and, optionally, on-premises networks.

This option is best suited to customers who want to leverage AWS-provided, automated HA network connectivity features and also optimize their investments in third-party product licensing. Additionally, this design enables customers to control cross-region network traffic using AWS and third-party network security products.

Configuration Details

This design pattern creates dynamically routed VPN connections between spoke VPC VGWs and VPN appliances in one or more transit VPCs (and optionally to on-premises network equipment). The best practice for making a transit network highly available and scalable is to use dynamically routed VPN connections to take advantage of VGW native HA capabilities and reduce network single points of failure. Note that in the diagrams above, all communication with the VPN appliances uses transit VPC Internet gateways and Elastic IP addresses. Additionally, AWS highly recommends the use of Auto Recovery for EC2 or Auto Scaling for automatic recovery of failed EC2-based VPN instances.

Considerations

Customers can use a transit VPC not only to provide direct network routing between VPCs and on-premises networks, but also to implement more complex routing rules such as network address translation between overlapping network ranges, or to add additional network-level packet filtering or inspection. However, this approach requires the customer to configure and manage the EC2-based VPN instances deployed in the transit VPC. AWS highly recommends leveraging virtual network appliances available in the AWS Marketplace to significantly reduce the level of effort to establish and maintain these VPN connections. This design will result in additional EC2 and, potentially, third-party license charges. Also, be aware 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.

4 For recommended products, search AWS Marketplace for one of the following terms: Cisco CSR 1000V, Fortinet FortiGate, Palo Alto Networks, Sophos UTM, Vyatta
## Resources

<table>
<thead>
<tr>
<th>Single Region Multi-VPC Connectivity</th>
<th><a href="https://d0.aws.awsstatic.com/aws-answers/AWS_Single_Region_Multi_VPC_Connectivity.pdf">https://d0.awsstatic.com/aws-answers/AWS_Single_Region_Multi_VPC_Connectivity.pdf</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Solution Brief on connecting VPCs within a single AWS Region</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Single Data Center HA Network Connectivity</th>
<th><a href="https://d0.awsstatic.com/aws-answers/AWS_Single_Data_Center_HA_Network_Connectivity.pdf">https://d0.awsstatic.com/aws-answers/AWS_Single_Data_Center_HA_Network_Connectivity.pdf</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Solution Brief describing options for creating HA connections from a single data center to AWS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multiple Data Center HA Network Connectivity</th>
<th><a href="https://d0.awsstatic.com/aws-answers/AWS_Multiple_Data_Center_HA_Network_Connectivity.pdf">https://d0.awsstatic.com/aws-answers/AWS_Multiple_Data_Center_HA_Network_Connectivity.pdf</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Solution Brief describing options for creating HA connections from multiple data centers to AWS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Multiple-VPC VPN Connection Sharing</th>
<th><a href="https://d0.awsstatic.com/aws-answers/AWS_Multiple_VPC_VPN_Connection_Sharing.pdf">https://d0.awsstatic.com/aws-answers/AWS_Multiple_VPC_VPN_Connection_Sharing.pdf</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Solution Brief on shared VPN connections with information on designing a transit VPC</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AWS Direct Connect Product Website</th>
<th><a href="https://aws.amazon.com/directconnect">https://aws.amazon.com/directconnect</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon VPC Documentation</td>
<td><a href="https://aws.amazon.com/documentation/vpc/">https://aws.amazon.com/documentation/vpc/</a></td>
</tr>
<tr>
<td></td>
<td>AWS webpage with links to VPC technical documentation, including introductory material (<em>Getting Started Guide</em>), component and strategy overviews (<em>User Guide</em>), and more robust technical documentation (<em>Network Administrator Guide</em>)</td>
</tr>
</tbody>
</table>