AWS NETWORK CONNECTIVITY OVER MPLS

"How do I implement connectivity to my VPC over MPLS?"

Overview

Most Amazon Web Service (AWS) customers can quickly determine the type of remote connections they want to establish (either VPN or AWS Direct Connect) between their on-premises networks and AWS. For customers who use Multiprotocol Label Switching (MPLS) to connect geographically dispersed company networks, it can be challenging to understand how to incorporate existing MPLS connectivity into their overall network design. This document provides AWS customers with best practices, recommendations, and common configurations to help build highly available, efficient connections between Amazon Virtual Private Cloud (Amazon VPC) and an MPLS network.

The following sections are applicable to customers who are looking to connect their MPLS network to their AWS resources, and assume basic knowledge of Amazon VPC, VPN connections, AWS Direct Connect, connecting and routing between remote networks, and dynamic routing protocols.

General Best Practices

Highly available, fault-tolerant network connections are key to a well-architected system. When designing remote connections, consider using redundant hardware and telecommunications providers on both sides of the network connection. It is a best practice to use dynamically routed, active/active connections for automatic load balancing and failover in each AWS Region. Additionally, provision sufficient network capacity to ensure that failure of one network connection does not overwhelm and degrade redundant connections.

Application on AWS

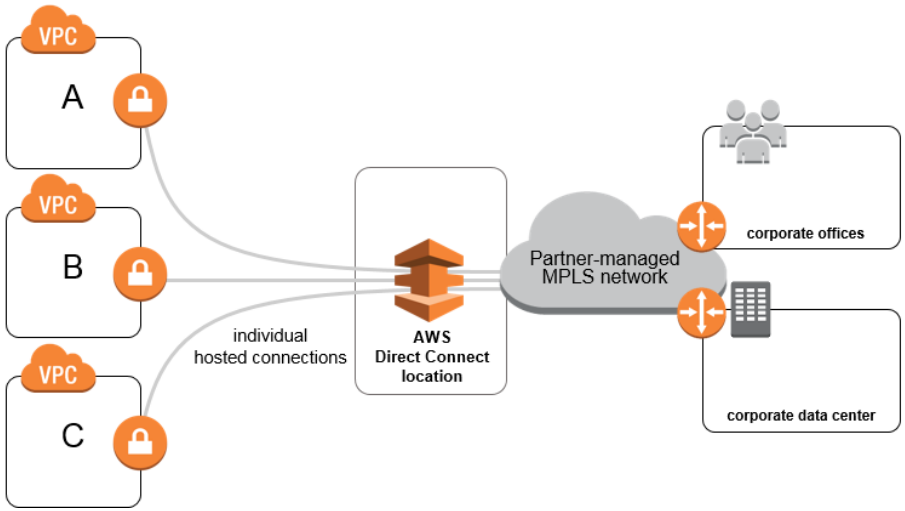
AWS customers can use different architectural approaches to extend their MPLS connectivity to their Amazon VPC networks. A company's business-availability and application requirements will help determine the most appropriate configuration for their use case. The following sections outline design options to meet different technical requirements and Amazon Partner Network (APN) and provider capabilities.

MPLS Vendor Interconnection Service

Most AWS Direct Connect partners with MPLS services also offer options for connecting their MPLS network to AWS. These are usually turnkey service offerings that leverage vendor infrastructure to quickly establish connectivity between AWS and a customer's MPLS network.

Configuration Details

Once a customer agrees to leverage a network provider's AWS interconnection service, the partner will provision a hosted AWS Direct Connect connection for each customer virtual private cloud (VPC). The customer accepts the hosted connection, associates it with a virtual private gateway (VGW), and then attaches the VGW directly to a VPC. To learn more about how to accept hosted connections, see the AWS Direct Connect User Guide.



Considerations

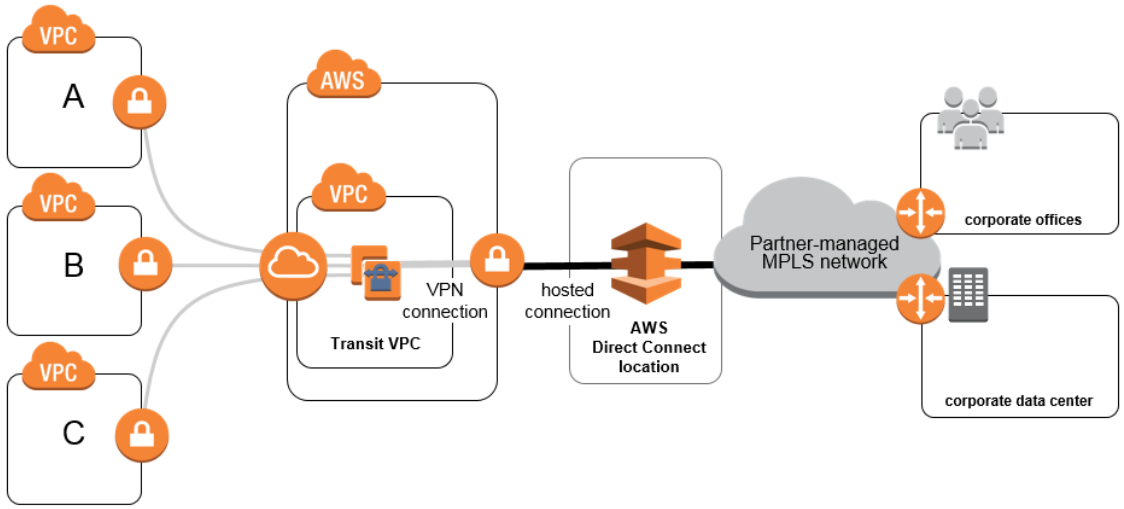
Partner-provided, turnkey MPLS connections to AWS can help customers more quickly establish connectivity to their existing network infrastructure. This option is most suitable for customers with a relatively static VPC structure. When implementing this connectivity pattern, be aware of circuit-provisioning timeframes and incorporate future requirements into your architecture to reduce the number of ad hoc requests to your MPLS provider. Also, review the network capabilities and restrictions associated with your network partner's interconnectivity service. For example, some providers require provisioning a separate MPLS circuit for each VPC, which might not scale well for some AWS customers.

MPLS Vendor Interconnection Service with a Transit VPC

Some customers want to maintain a partner-managed MPLS network, but require the flexibility to modify their AWS networks without provider involvement at every step. In this scenario, a customer can add a transit VPC as the interface for a single hosted AWS Direct Connect connection. A transit VPC serves as a network hub to facilitate routing between multiple "spoke" VPCs and an MPLS provider's hosted connection. This option can make it easier to add (and remove) VPCs to an MPLS network and reduces costs associated with individual circuit provisioning.

Configuration Details

This configuration requires a transit VPC that hosts a pair of third-party virtual router or firewall appliances to facilitate routing between multiple VPCs. As in the previous scenario, the MPLS provider provisions a single hosted AWS Direct Connect connection that the customer then associates with a detached VGW. The customer then establishes VPN connections to connect this VGW, as well as the attached VGW of each spoke VPC, to the transit VPC.



Considerations

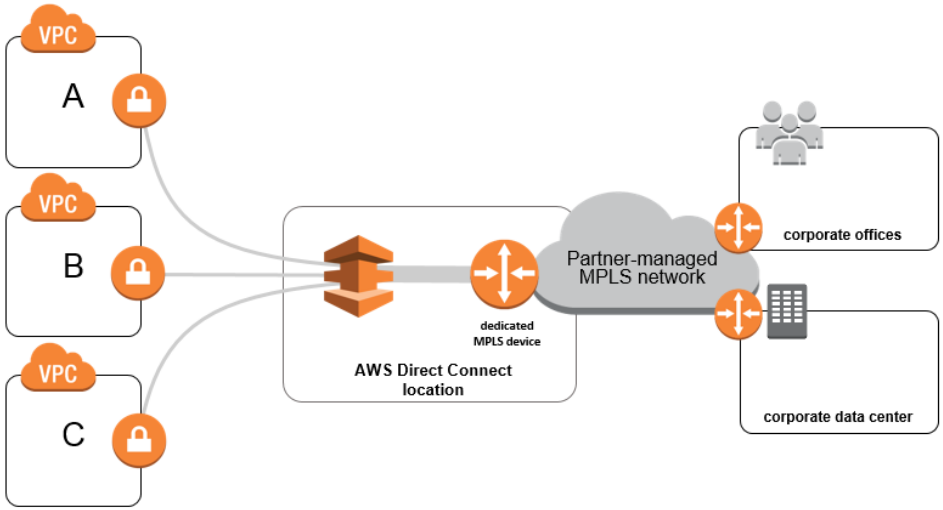
This strategy supports scalability and agility of AWS networks without the need to provision multiple AWS Direct Connect connections or MPLS circuits. It is important to consider the additional responsibilities of designing and managing the transit network, as well as third-party product license fees. This approach is appropriate for customers who have up to 1 Gbps AWS Direct Connect connections.

MPLS Colocated Hardware with AWS Direct Connect

Some AWS customers require a high level of network configuration control, flexibility, and scalability, and choose to colocate dedicated MPLS devices in an AWS Direct Connect location. This option minimizes dependencies on an MPLS provider for change control activities and offers the highest level of control over network configuration to accommodate changing requirements.

Configuration Details

Customers can choose to colocate their own MPLS devices, or request dedicated equipment from a managed network service provider who already has colocation presence in an AWS Direct Connect location. Either the customer or the managed network provider will work with AWS to establish an AWS Direct Connect cross connection and then connect it to the MPLS devices, which also serve as the gateway to the MPLS network. Once the physical connection is established, the customer (or their provider) configures the necessary virtual interfaces, circuits, and network paths to connect the MPLS network to their VPCs. This option also supports provisioning additional AWS Direct Connect connections to provide additional bandwidth with minimal MPLS vendor involvement.



Considerations

This topology offers the highest level of control, agility, and scalability. For example, it provides the most flexible options for including additional security hardware appliances or NAT capabilities for more complex networks. It is also the most appropriate option for 10 Gbps AWS Direct Connect connections. However, this approach requires the highest level of customer involvement when managing networks. This option is applicable to customers who already manage their own MPLS network connectivity and require a high level of visibility into all of their network connections. Consider the cost and general overhead of managing a colocation facility, and leverage your MPLS provider's existing relationships with AWS, if possible.

Resources

AWS Global Transit Network	https://aws.amazon.com/answers/networking/aws-global-transit-network/
AWS Direct Connect Website	https://aws.amazon.com/directconnect/
AWS Direct Connect Documentation	https://aws.amazon.com/documentation/direct-connect/
Amazon VPC Documentation	https://aws.amazon.com/documentation/vpc/