VMware Cloud on AWS – Networking Reference Architecture – 1
VMware Cloud on AWS connectivity to on-premises site using AWS Direct Connect to a virtual private gateway and AWS Site-to-Site VPNs

1. A private virtual interface (VIF) establishes connectivity to the VMware SDDC A in AWS Region A.
2. The AWS Site-to-Site VPN (over internet) provides backup connectivity to the private VIF to provide resilient connectivity to the VMware SDDC A.
3. A public VIF enables access to all AWS public services and endpoints using the public IP addresses.
4. The lack of a Direct Connect instance in Region B creates a design constraint; so a site-to-site VPN is established to the VMware SDDC B. This VPN leverages the public VIF from the Direct Connect instance in Region A. Also, Site-to-Site VPNs over a public VIF can be used to establish a more consistent network experience compared to internet-based VPNs. Alternatively, redundant Site-to-Site VPNs (not shown) can be established for resiliency.
5. A private VIF to the AWS Direct Connect gateway (DXGW) enables the DXGW to establish on-premises communication to Amazon VPCs in different Regions by associating the DXGW to the virtual private gateways (VGW).
6. The private VIF to DXGW cannot be used for gateway associations to a VMware SDDC. This feature is not supported on a VMware Cloud on AWS instance.
7. Gateway associations can be established between the DXGW and the VGW to enable on-premises communication with Amazon VPCs in multiple Regions.
8. Site-to-Site VPNs are configured as a backup to the DXGW-VGW associations for more resilient connectivity to Amazon VPCs.
VMware Cloud on AWS – Networking Reference Architecture – 2

VMware Cloud on AWS connectivity to on-premises site using dual AWS Direct Connect instances with Direct Connect Gateway and AWS Transit Gateway

1. The Private VIF from the AWS Direct Connect instance in Region A establishes connectivity from the on-premises site to the SDDC in Region A. Similarly, the Private VIF from the AWS Direct Connect instance in Region B establishes connectivity from the on-premises site to the SDDC in Region B.

2. Dual Transit VIFs establish redundant, resilient connectivity from the on-premises site to the DXGW.

3. The DXGW is associated with AWS Transit Gateway in both Regions to provide on-premises connectivity to Amazon VPCs.

4. The Transit Gateway is a Regional virtual router that is capable of transitive routing between networks connected to it using the following attachments:
   - VPC attachments
   - VPN attachments
   - DXGW attachments
   - Peering attachments (inter-region)

   Amazon VPC attachments enable VPCs to establish communication with other VPCs and networks connected to the Transit Gateway.

5. The Transit Gateway peering attachment enables cross-Region communication between networks connected to Transit Gateway A and Transit Gateway B.

6. The Transit Gateway VPN attachments extend the communication between the VPCs and SDDCs in their respective AWS Regions, and also between the compute networks residing on SDDC A and SDDC B over the Peering attachment. However, the VPN attachments do not support VMkernel traffic, including ESXi Mgmt., vMotion, vSphere Replication, and HCX Interconnects. The SDDCs use the Direct Connect private VIFs to connect to the on-premises site.

AWS Reference Architecture

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Reviewed for technical accuracy 8/30/2021
VMware Cloud on AWS – Networking Reference Architecture – 4

VMware Cloud on AWS connectivity using a Transit VPC to connect AWS Transit Gateway and VMware Transit Connect in the same Region

1. Transit VIFs from two separate AWS Direct Connect connections in different Regions are used to establish resilient and fault-tolerant connectivity to AWS Regions A and B.

2. Each DXGW is associated with a AWS Transit Gateway and the VMware Transit Connect (VTG) to provide on-premises connectivity.

3. The AWS Transit Gateway is a regional virtual router that is capable of transitive routing between networks connected to it using the following attachments:
   - VPC attachments
   - VPN attachments
   - DXGW attachments
   - Peering attachments (inter-Region)

4. The SDDC group uses a VTGW to provide high-bandwidth, low-latency connectivity between:
   - SDDCs in an SDDC Group
   - SDDCs and one or more VPCs
   - SDDCs and on-premises via DXGW
   - SDDCs in other Regions (inter-Region)

5. Static routes in a Transit VPC are used to enable intra-Region transitive routing between VMware Transit Connect and AWS Transit Gateway in the same Region.

5a. A VPC attachment connects the AWS Transit Gateway to the Transit VPC. Static routes to the SDDC are configured in the AWS Transit Gateway route tables on the VPC attachment.

5b. Another VPC attachment connects the VMware Transit Connect to the Transit VPC. Static routes to the Customer VPCs are configured in the VMware Transit Connect route tables on this VPC attachment.