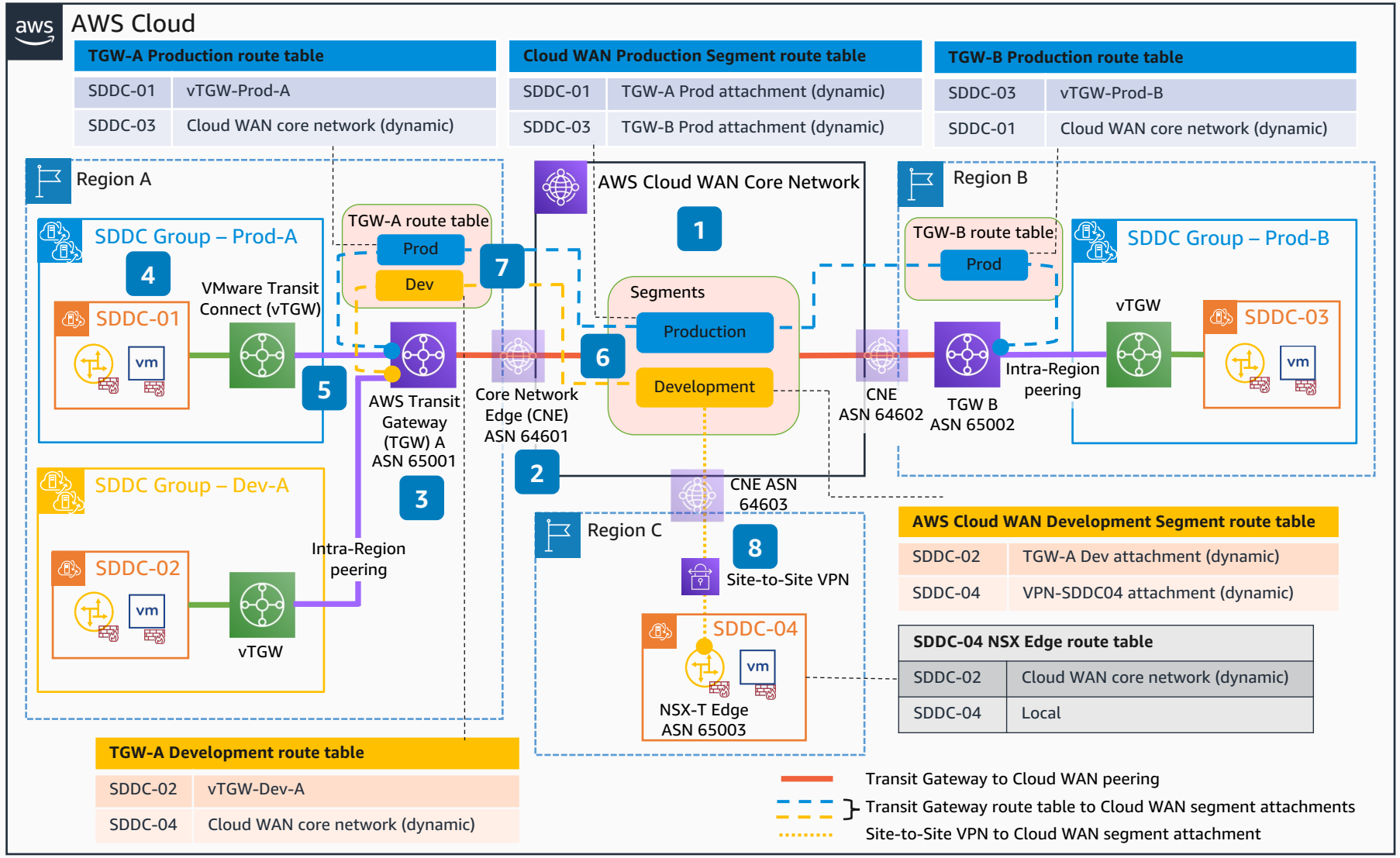
VMware Cloud on AWS – AWS Cloud WAN Reference Architecture

This architecture details how to connect VMware Cloud on AWS Software-Defined Data Centers (SDDCs) across different AWS Regions to the AWS Cloud WAN global network using VMware Transit Connect, AWS Transit Gateway, and Site-to-Site Virtual Private Network (VPN) connections.



1. An **AWS Cloud WAN** global network is created to expand across all AWS Regions where the customer's **VMware Cloud on AWS** Software-Defined Data Centers (SDDCs) are deployed. The Cloud WAN global network consists of a core network that is logically partitioned into multiple network segments based on environment segregation requirements.
2. Within the Cloud WAN core network, a Core Network Edge (CNE) is automatically provisioned in each defined Region as a connection point for Regional network attachments.
3. Deploy an **AWS Transit Gateway** (TGW) with multiple route tables following the same segmentation strategy. Refer to this reference architecture for detailed examples.
4. For each environment (such as Prod, Dev), deploy a SDDC into a dedicated SDDC Group. This automatically builds a VMware Transit Connect (VMware-managed Transit Gateway, or vTGW) to establish high-speed, resilient connections between SDDCs within the group and other resources, including AWS networking services.
5. Build an intra-Region peering attachment from each SDDC group (vTGW) to customer-managed TGW, and associate each peering attachment to its corresponding **Transit Gateway** route table. On each vTGW, configure static routes for SDDCs in the remote Regions toward the TGW. Refer to this reference architecture for more details.
6. Configure a **Transit Gateway** peering connection to the local CNE in the Cloud WAN core network. Cloud WAN uses Border Gateway Protocol (BGP) over peering, so your TGW and Cloud WAN BGP autonomous system number (ASN) must be unique.
7. To maintain end-to-end traffic segmentation for different environments, create separate **Transit Gateway** route table attachments mapped to their respective Cloud WAN segments. Routes are automatically propagated bidirectionally between TGW route tables and Cloud WAN segments.
8. Alternatively, configure an IPsec Site-to-Site VPN connection (with BGP routing) from the NSX edge in a SDDC to the local CNE, and create a VPN attachment to the corresponding Cloud WAN segment. Routes are dynamically exchanged using BGP over the VPN connection.

Reviewed for technical accuracy January 19, 2023

AWS Reference Architecture