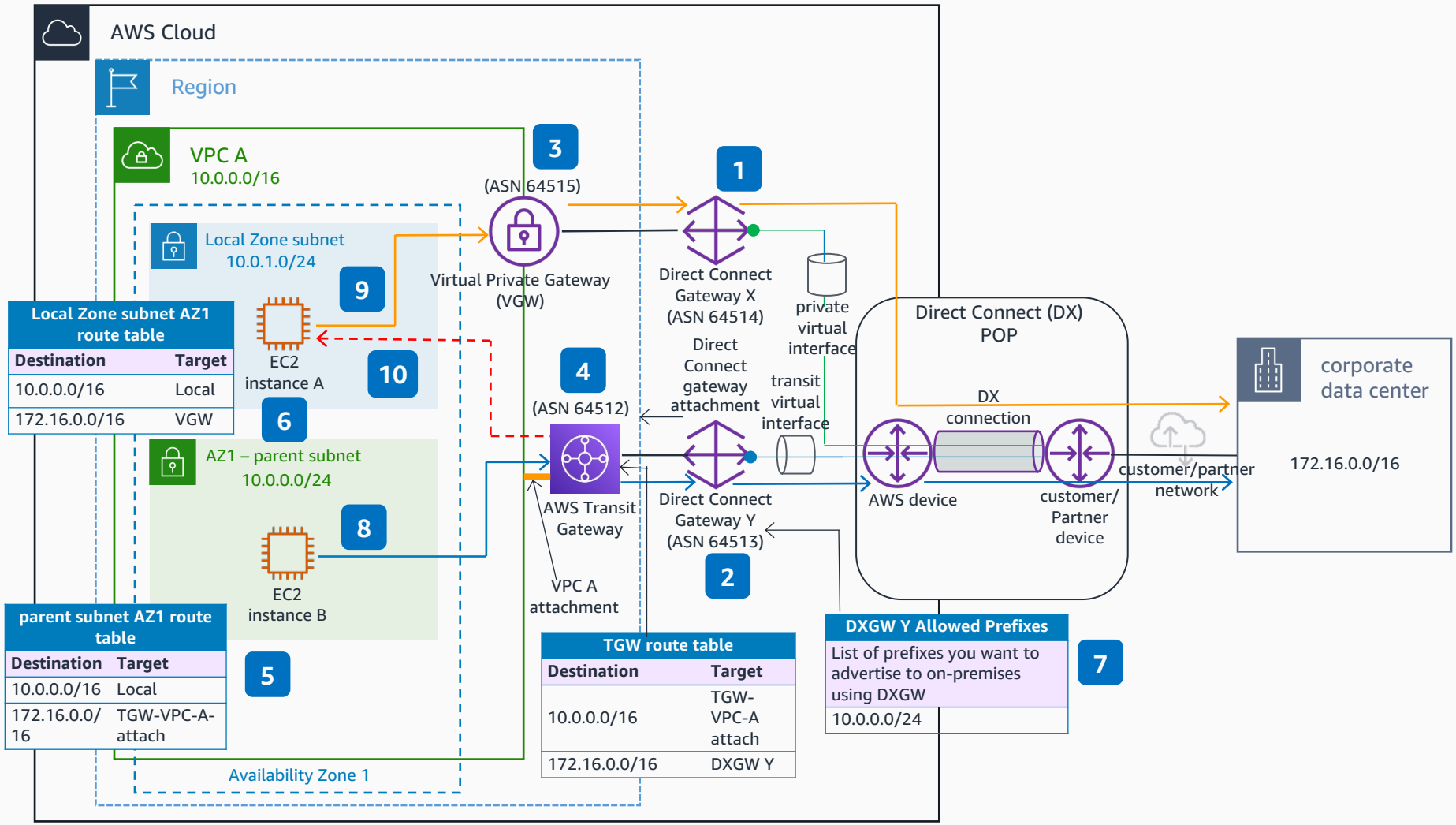
AWS Direct Connect Traffic Flow with AWS Local Zone

This reference architecture shows traffic flows from an on-premises data center to an AWS Local Zone using Direct Connect for latency applications.



1. Create **AWS Direct Connect** gateway (DXGW) "X" and assign a unique autonomous system number (ASN). Attach the Private Virtual Interface (VIF) to DXGW X.
2. Create DXGW "Y" and assign a unique ASN. Attach the Transit VIF to DXGW Y.
3. Create a Virtual Private Gateway (VGW) and attach to DXGW X. Assign a unique ASN to VGW. Attach the VGW to VPC A.
4. Create a AWS Transit Gateway (TGW) and attach to DXGW Y using DXGW attachment, and to VPC A using VPC A attachment, respectively.
5. Create a parent subnet (10.0.0.0/24) with **Amazon Elastic Compute Cloud** (Amazon EC2) instance B in an Availability Zone (AZ1) and associate it with a route table.
6. Create another subnet (10.0.1.0/24) in the AWS Local Zone (LZ) where the latency sensitive app will be running (EC2 instance A). Associate this to a separate LZ route table.
7. Add the the AZ1 parent subnet (10.0.0.0/24) in in the DXGW Y "Allowed Prefixes" list.
8. The AZ1 parent subnet (10.0.0.0/24) is advertised using TGW and DXGW Y back to on-premises. Traffic destined to the parent subnet (routes that fall inside /24) follow the TGW path.
9. Any traffic destined to the Local Zone subnet (10.0.1.0/24) follow a shorter VGW path, without hairpinning through the Local Zone's parent Region (routes that fall outside /24).
10. We don't recommend any resource accessing the local zone subnet from on-premises through **Transit Gateway**, as traffic using this path would hairpin through the parent Region.

Reviewed for technical accuracy September 29, 2022

AWS Reference Architecture