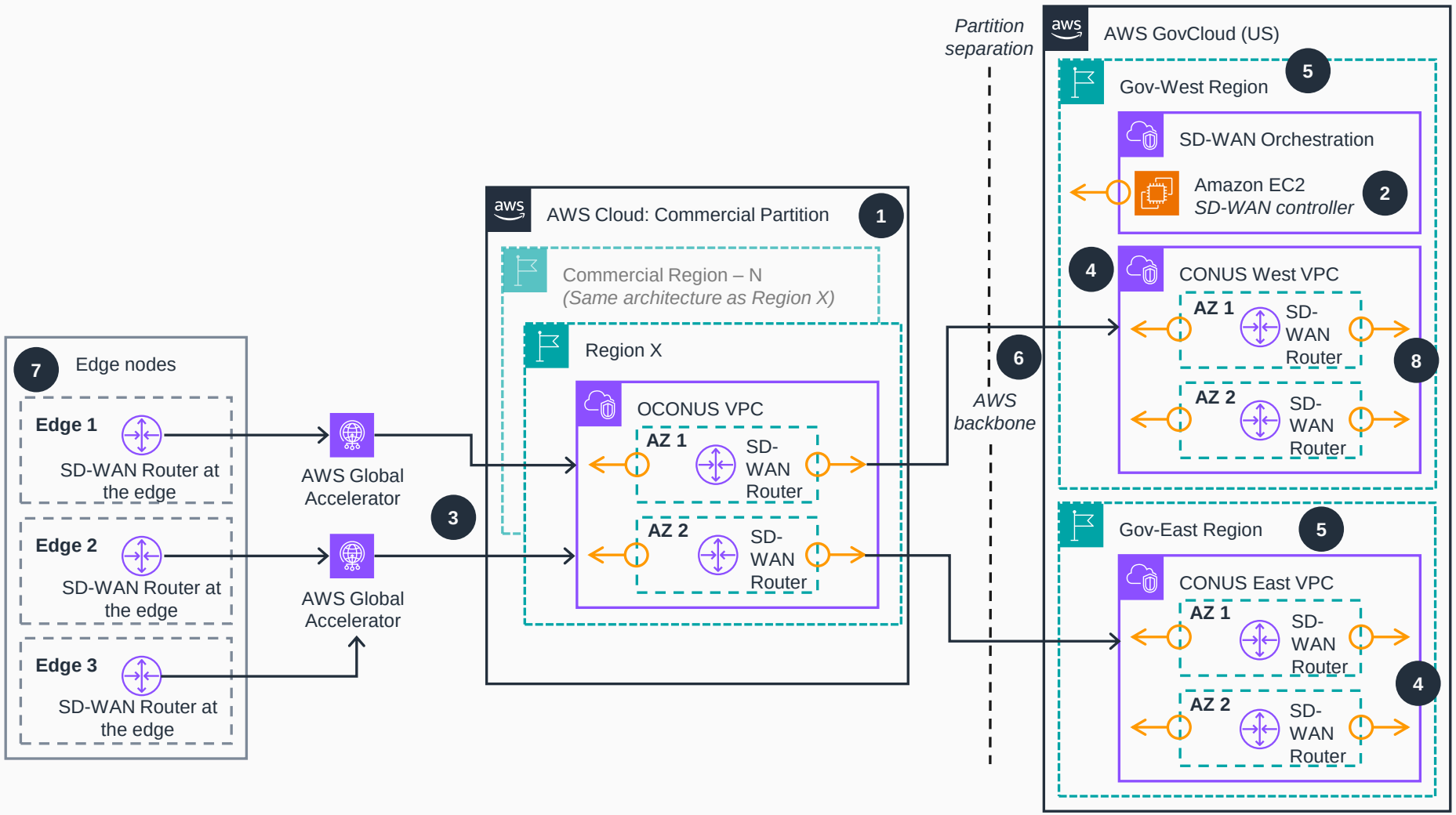
Guidance for Cloud Edge Global Access on AWS

Overview

This architecture diagram shows the high-level functional components deployed in AWS GovCloud (US) and commercial partitions. It supports up to 10 commercial AWS Regions or AWS Local Zones and a variety of interface quantities and instance sizes.



1. The AWS commercial partition contains software-defined wide area network (SD-WAN) Routers used to service edge nodes connected through internet connectivity options. These can be scaled up to 10 Regions and deployed in multiple highly available Availability Zones (AZs).

2. SD-WAN orchestration runs from the **AWS GovCloud (US)** partition. It can be deployed to be highly available in multiple AZs or multiple Regions.

3. **AWS Global Accelerator** provides rapid egress from the commercial internet onto the AWS global infrastructure for higher security, faster throughput, and lower latency.

4. SD-WAN Routers in the **AWS GovCloud (US)** partition provide direct access to Impact Level 4 or 5 (IL4 or IL5) workloads or the internet.

5. Multiple **AWS GovCloud (US)** Regions provide high availability.

6. SD-WAN Routers use the AWS backbone for secure inter-partition connectivity and can fully encrypt all traffic using Federal Information Processing Standards (FIPS).

7. The cloud-edge global access SD-WAN Routers are software-based and can be run on existing hardware or on the SD-WAN vendor's own hardware.

8. Traffic egresses from the cloud-edge global access SD-WAN Routers to on-premises data-centers or the internet, depending on the mission's needs.

NOTE: SD-WAN Routers are provided by their respective companies, such as Juniper Networks.

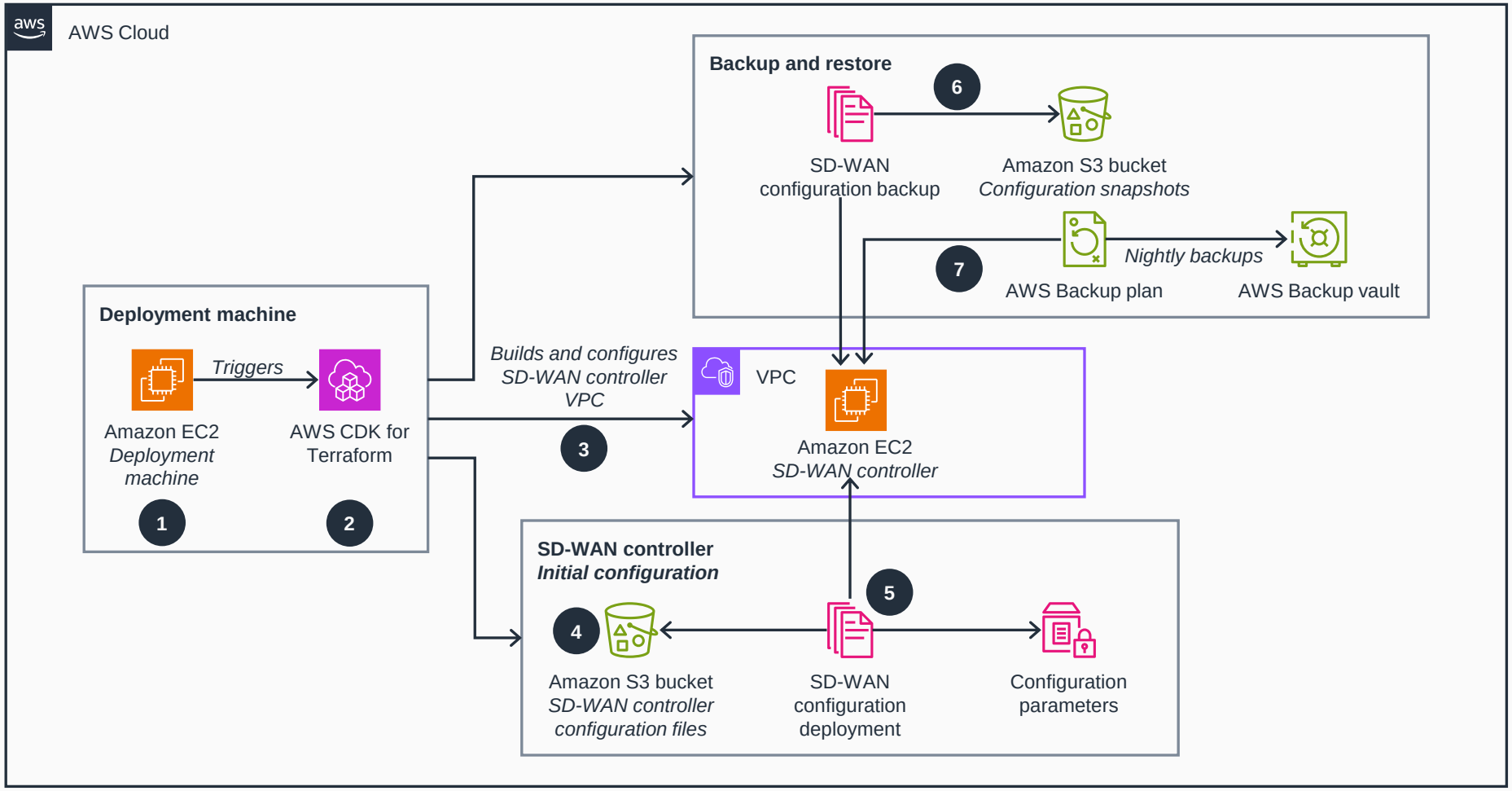
Reviewed for technical accuracy December 12, 2024

AWS Reference Architecture

Guidance for Cloud Edge Global Access on AWS

Core orchestration flow

This architecture diagram shows the core orchestration flow for the deployment of an SD-WAN controller. Because all routers running in the cloud are provisioned before step 4, you can fully build out the configurations using the “as build” details from those routers. This diagram also provides steps for data protection.



1. The **Amazon Elastic Compute Cloud (Amazon EC2)** deployment machine runs an **AWS Cloud Development Kit (AWS CDK)** for Terraform.
2. **AWS CDK** for Terraform is used to deploy into AWS partitions.
3. The SD-WAN controller is provisioned from an Amazon Machine Image (AMI) through the **AWS CDK** for Terraform.
4. The automation builds vendor-specific SD-WAN configuration files.
5. The SD-WAN controller is configured using **AWS Systems Manager** documents.
6. Configuration snapshots are automated and stored in **Amazon Simple Storage Service (Amazon S3)**.
7. **AWS Backup** provides snapshots to the SD-WAN controller disk.

Reviewed for technical accuracy December 12, 2024

AWS Reference Architecture