Deloitte.

AUGUST 16th, 2022

AWS Cloud WAN Advances Enterprise Connectivity

Author: Ronald Bannister, Deloitte

Collaborator: Hemant Ahire, AWS

Collaborator: Cindy Liu, Deloitte

New York—National Office
30 Rockefeller Plaza, 41st floor
New York, NY., 10112-0015
United States

Phone: +1 212 492 4000

Fax: +1 212 489 1687

Introduction

1 Executive summary

Deloitte Consulting LLP announced its commitment as a Launch Partner for Amazon Web Services (AWS) Cloud WAN managed wide area networking (WAN) service. This AWS Cloud WAN offering is a substantial new capability in Cloud networking that connects resources across the cloud and on-premises environments. As a System Integrator (SI) for AWS Cloud WAN, we at Deloitte Consulting LLP., have been exploring common use-cases where AWS Cloud WAN can help our customers improve their real-world hybrid networks, both regionally and at a global scale. This white paper will explore hybrid network designs where application performance and security can be increased, complexity reduced, and reliability improved—all through the use of AWS Cloud WAN.

2 Background

2.1 Purpose

This whitepaper from Deloitte Consulting LLP., discusses the AWS Cloud WAN managed service by AWS which is designed to make it faster and easier for enterprises to build, manage, and monitor a global WAN network that efficiently connects the AWS Network and customer on-premises network environments.

2.2 Problem

Today, many enterprise WANs still service users in specific business locations with the internal network traffic routed through hardware to access applications in data centers and shared files and databases in other business locations. Connections are typically VPN tunnels or VPLS and MPLS connections provided by a telecommunications company. Deploying a new location could take weeks or even months to acquire and commission the required network hardware and connections.

Since the onset of the pandemic, enterprises went through a paradigm shift and were forced to rapidly adopt "Work from Anywhere" as a practice. A significant percentage of end-users are now accessing applications and workloads primarily hosted in on-premises data centers, on AWS, and other SaaS providers.

Additionally, enterprises are widely distributed across multiple environments, including remote users, satellite offices, on-premises data centers and AWS. Productivity gets significantly impacted if users are unable to access business applications due to poor network conditions from local WAN links.

Consequently, enterprise networking is undergoing a major transformation in securely accessing and realizing resources from their WAN infrastructure. Enterprises are increasingly looking at WANs to solve more use cases with more diverse technologies over more geographies.

3 The AWS Cloud WAN Solution

3.1 What is AWS Cloud WAN

AWS Cloud WAN is a cloud-based WAN managed solution that marries the AWS Global Network and customer networks to a single unified multi-regional or global network which removes the need to configure and manage different networks individually, even when they are running different technologies. Cloud WAN provides a full view of the on-premises and AWS networks to help visualize the health, security, and performance of the global network.

77%

of companies have at least one application or a portion of their enterprise computing infrastructure in the Cloud

92%

of companies expected to adopt SD-WAN by 2026 with most adopting for its efficiency (38%), cost savings (38%), and agility (34%)

3.2 AWS Cloud WAN Benefits

Many industry leading SD-WAN solutions are now integrated with AWS Cloud WAN, which combines a secure, high performance global network backbone with SD-WAN's capabilities of reducing costs, improving security, visibility and simplify connectivity between satellite offices and AWS cloud-based resources, both regionally and globally.

A major challenge in having multiple or even hundreds of VPCs running on AWS Cloud WAN across multiple regions and availability zones is granting access between VPCs. This is accomplished by utilizing static route tables which presents an administrative nightmare. AWS Cloud WAN removes the complexity and resource consuming task of manual configurations to provision multiple VPCs across multiple regions and availability zones through automating this process with a centrally-managed policy and dynamic routing.

Of note, AWS Cloud WAN comes with security features that are key to securing cloud connectivity in the multi-cloud ecosystems. These security capabilities can selectively route traffic to a Cloud security service while providing embedded security services such as firewalls, VPNs, and segmentation of data, applications, and users.

1. Integrate your global network with AWS's Global Network
2. Provides a unified fabric of all AWS connect Cloud Services
3. Leverage AWS's Global Network as an Internet Service Provider
4. Delivers security and a centralized security policy
5. Improved network efficiency, performance and reliability
6. Faster time-to-market for services *(in minutes)*

4 AWS Cloud WAN Architecture Use-Cases

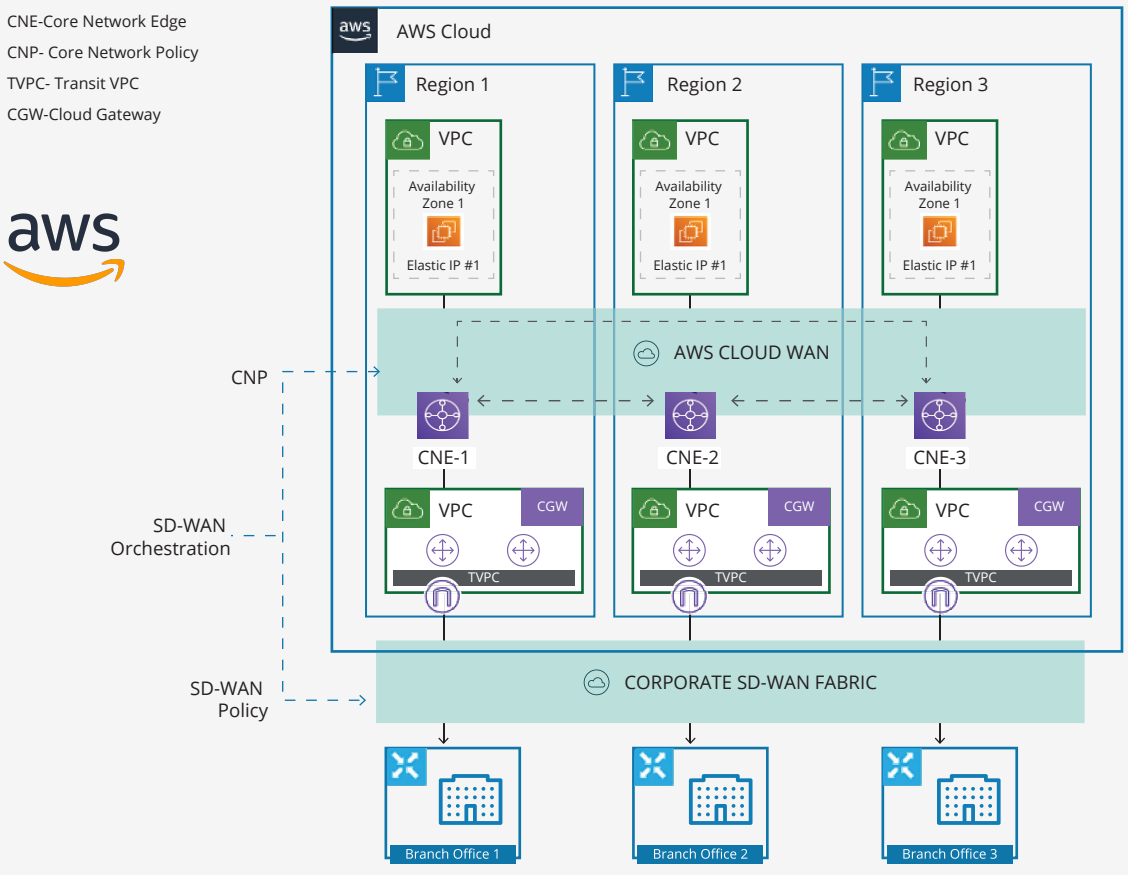
4.1 AWS Cloud WAN & SD-WAN Uni ied Architecture Use-Case

AWS Cloud WAN can be used by satellite offices, remote users, mobile users, and data-centers to simplify Site-to-Cloud, Site-to-Site, and inter-region secure access to the AWS global backbone, even if you are not hosting data or running workload in VPCs. Integrating SD-WAN with AWS Cloud WAN simplifies operations by enabling visibility for the SD-WAN overlay and AWS Cloud WAN underlay within a single pane of glass.

As shown in this example architecture, satellite offices can connect directly to the AWS Global Network backbone by encrypted SD-WAN tunnels to utilize the AWS Cloud WAN for multi-regional VPC access. Traditionally, an AWS Transit Gateway is used to inter-connected other regional Transit Gateways for access between VPCs in other regions. As additional regions are added this Transit Gateway, design becomes significantly more complex.

Utilizing AWS Cloud WAN enables businesses to build a multi-Region global WAN network on the AWS backbone using policy statements without relying on the complexity of multi-transit gateway design.

Figure 1—AWS Cloud WAN Multi-Region Architecture



4.2 AWS Cloud WAN Multi-Region Use-Case

Access to network segments between regions is managed by a cloud WAN security policy. Security policies can be created to segment shared services such as service directories, authentication services, and allowing or denying Internet access from a network segment.

AWS Cloud WAN automation makes it easy to build in and attach new VPCs and network connections without requiring approval of each change manually. This can be done by tagging attachments and defining network polices to map attachments automatically with a specific tag to a specific network segment. Tagging identifies which attachments can join a segment automatically, which segments require manual approval, and whether attachments within the same network segment can communicate with each other. The following reference architecture illustrates a multi-region access and segmentation between US-EAST-1, EU-WEST-1, AP-SOUTH-1, and External Account by using AWS Cloud WAN. The Security Policy is setup allowing the following communication and segmentation between regions and services.

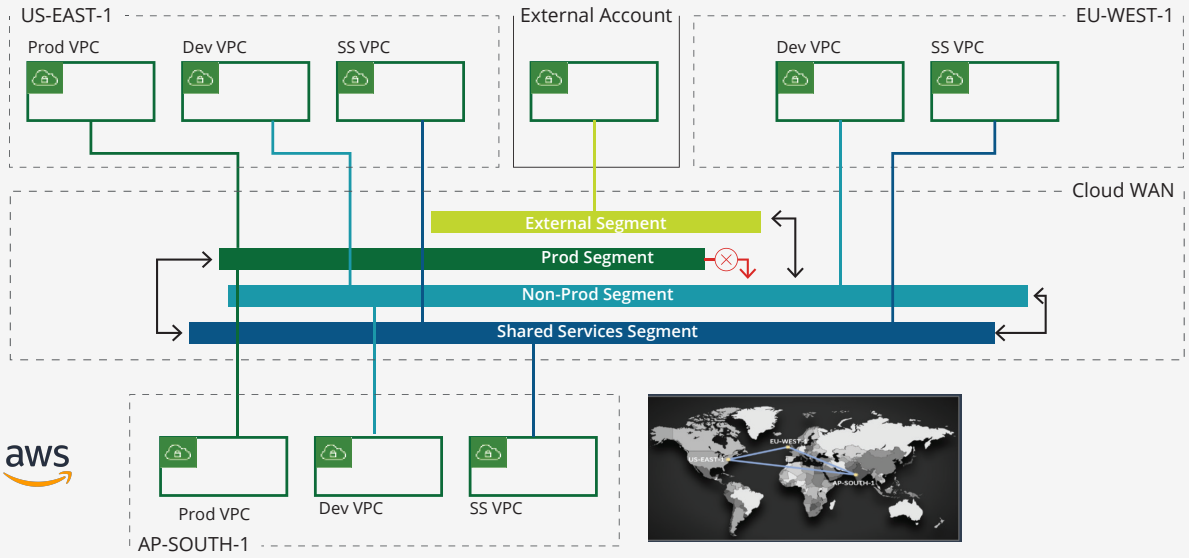
4.2.1 AWS Cloud WAN Global Architecture

- Three regions - US-EAST-1, EU-WEST-1, AP-SOUTH-1
- Non-Production – Segment for Development environments which is available in US-EAST-1, EU-WEST-1, AP-SOUTH-1
- Prod – Segment for production environments which is available inUS-EAST-1 and AP-SOUTH1
- Shared Services – Segment for Shared Services like centralized NAT egress and is available in US-EAST-1, EU-WEST-1, AP-SOUTH-1
- External Account – Segment for VPC's from accounts outside the organization like partner account and is available in US-EAST-1, EU-WEST-1, AP-SOUTH-1

4.2.2 AWS Cloud WAN Security Policy

- DevNetwork (Development) VPCs can communicate with each other
- Production VPC's can communicate with each other.
- Production segment is not approved for use in Eu-WEST-1
- No communication is authorized between DevNetwork and Production segments
- Share service segment is shared with DevNetwork and Production segments only
- Each region will use its local shared services attachment to access shared services
- VPC's in Shared Services segment cannot communicate
- External segment is shared with Non-Production only

Figure 2—AWS Cloud WAN Multi-Region Reference Architecture



Conclusion

The demand for cloud computing services continues to grow every year with most enterprises adopting a cloud-first strategy. The cloud has made the current traditional legacy WAN technologies are out-of-date and an impediment to the digital transformation for today's enterprises. AWS's Cloud WAN offers a more robust and scalable solution to link complex, multi-account, multi-region AWS environments.

About the Authors

Ronald Bannister, Deloitte Consulting LLP

Ronald Bannister is a Manager in Deloitte's Platforms & Infrastructure Service. Ronald Assists organizations in Cloud adoption, Network & Security Transformations to help clients achieve their business objectives.

Cindy Liu, Deloitte Consulting LLP

Cindy Liu is a Manager in Deloitte's Platforms & Infrastructure Service. Cindy assists customers in aligning tbusiness and IT objectives for cloud adoption.

Richard Johnson, Deloitte Consulting LLP

Richard Johnson is a National Practice Lead for Network and Cloud Modernization in Deloitte's Cloud Engineering practice. Rich has over 25 years of IT strategy and transformation experience across multiple industries.

Hemant Ahire, AWS

Hemant Ahire is an AWS Global Migrations and Modernization Leader, Sr. Partner SA. Hemant assists customers in Cloud Strategy and Transformations, large scale Cloud migrations and building solution architectures to address business imperatives.