Building a scalable and secure multi-VPC AWS network infrastructure

Prabhnoor Kaur (8856211)

**Cloud Technologies, Conestoga College**

Digital Solutions Management 1524G

Fadi Abd Ulhamid

02 October 2023

Table of Contents

[Abstract 3](#_Toc147156299)

[Introduction 3](#_Toc147156300)

[Best practices for developing large-scale networks 3](#_Toc147156301)

[Network Connectivity 3](#_Toc147156302)

[Network Security 4](#_Toc147156303)

[DNS Management 5](#_Toc147156304)

[Key Services 6](#_Toc147156305)

[Equivalent Services of Azure, Google Cloud and AWS 7](#_Toc147156306)

[References 8](#_Toc147156307)

# Abstract

AWS customers depend on VPCs to segment its workloads and expand their footprint. The large scale of applications built on AWS often overcome the big challenge of enabling resource sharing, inter-VPC connections and on-premises to VPC connection.

# Introduction

AWS services become increasingly important to monitor in terms of cost, access, and easier environmental management. Large-scale networks in AWS demand a well-thought-out strategy, encompassing VPC (Virtual Private Cloud) architecture, connectivity options, and security measures.

# Best practices for developing large-scale networks

This research paper outlines best practices for architecting and operating large-scale networks using AWS services, considering factors like scalability, security, and cost-effectiveness. This paper delves into key best practices for network development in the AWS cloud in terms of:

* Network Connectivity
* Network Security
* DNS Management

## Network Connectivity

In the realm of developing large-scale networks, customers on Amazon Web Services (AWS) can choose between two primary VPC flow patterns, namely many-to-many and hub-and-spoke, which offer distinct connectivity options. In the many-to-many model, individual connections manage traffic between each VPC, while the hub-and-spoke approach funnels inter-VPC traffic through a central resource guided by established rules.

VPC peering emerges as the simplest method to connect two VPCs, enabling full bidirectional connectivity between them, and it can even span across AWS accounts and regions. However, it lacks transitive routing capabilities, necessitating direct VPC peering for some scenarios. For more complex setups, the Transit VPC Solution introduces a hub-and-spoke design, facilitating transitive routing and leveraging third-party software appliances for advanced security features. On the other hand, AWS Transit Gateway provides an efficient and scalable hub-and-spoke model, simplifying network management by consolidating VPN connections for large-scale environments.

AWS PrivateLink enables secure unidirectional access in client-server configurations, while Amazon VPC Sharing streamlines connectivity for organizations seeking better resource utilization and reduced costs. In terms of hybrid connectivity, VPN and Direct Connect options are explored. VPN connections work well for smaller setups and can be consolidated on Transit Gateway for efficient management.

The choice of network connectivity practices depends on the scale, security, and complexity of the AWS environment, and often, a combination of these approaches may be employed to achieve optimal results.

## Network Security

When building large-scale networks with AWS services, implementing robust network security practices is essential for large scale AWS networks. One of these practices involves centralized egress to the internet, which is essential for ensuring secure outbound traffic. Organizations can utilize Network Address Translation (NAT) gateways or EC2 instances configured with Source NAT (SNAT) as the next hop for all egress internet access which is particularly crucial for applications that require outbound connectivity for tasks such as downloading libraries, patches, or OS updates.

Using NAT Gateways is a common approach, but deploying one in each spoke VPC can become costly due to hourly charges. For high availability, it's recommended to use two NAT Gateways, one in each Availability Zone (AZ). AWS provides a 99.9% availability SLA for NAT Gateways within an AZ. AWS provides safety from redundancy against component failure under the SLA agreement.

Furthermore, for VPC-to-VPC and on-premises-to-VPC traffic control, AWS considers implementing third-party software appliances running on EC2 instances alongside Transit Gateway. By removing blackhole routes and configuring VPN or Direct Connect attachments, implementing security zones and defining communication rules, organizations can selectively inspect and control traffic, enhancing overall network security.

## DNS Management

When establishing large-scale network architectures with AWS services, implementing careful management of DNS within the Virtual Private Cloud (VPC) environment becomes crucial. AWS provides private DNS hostnames for instances in non-default VPCs, and custom DNS mappings can be achieved using Amazon Route 53.

For optimal DNS resolution, consider enabling 'enableDnsSupport' and 'enableDnsHostnames' attributes, which provide DNS resolution particularly beneficial for achieving internal DNS resolution and connecting instances by their private DNS hostnames within the VPC via Route 53 Resolver.

Hybrid network environments, which integrate AWS with on-premises resources, require a specific approach where AWS recommends setting up Route 53 Resolver inbound and outbound endpoints. In the inbound endpoint setup, it handles DNS queries forwarded from on-premises networks to your AWS resources, while the outbound endpoint forwards selected queries from your VPCs to your on-premises DNS servers. These configurations ensure seamless DNS resolution across hybrid environments.

# Key Services

**Amazon VPC:** Amazon Virtual Private Cloud (Amazon VPC) is a fundamental building block of AWS cloud computing. It allows you to create isolated network environments within the AWS cloud. With VPC, you can define your own IP address range, configure route tables, and control inbound and outbound network traffic

**AWS PrivateLink:** AWS PrivateLink is a service that enhances security by allowing you to access AWS services over a private network connection, rather than the public internet. With PrivateLink, you can connect to various AWS services, such as S3 and EC2, from within your Amazon VPC or on-premises network, keeping your data traffic isolated and secure.

**AWS Direct Connect Gateway:** AWS Direct Connect Gateway simplifies network connectivity for businesses with multiple geographically distributed AWS regions. It allows you to establish connections to AWS resources across different AWS Direct Connect locations. This means you can create a global network backbone that spans multiple regions and share Direct Connect connections more efficiently.



A screenshot of a computer program

Description automatically generatedA screenshot of a computer

Description automatically generated

# Equivalent Services of Azure, Google Cloud and AWS

A screenshot of a computer

Description automatically generated

# References

1. *Google Cloud documentation  |  Documentation*. (n.d.). Google Cloud. <https://cloud.google.com/docs/>
2. Google Cloud Architecture Framework. (2023). *Google Cloud*. <https://cloud.google.com/architecture/framework>
3. TimG. (2019, February 22). How to build a scalable architecture with AWS - We’ve moved to freeCodeCamp.org/news - Medium. *Medium*. <https://medium.com/free-code-camp/how-to-build-a-fully-scalable-architecture-with-aws-5c4e8612565e>
4. <https://www.coursehero.com/file/21283928/AWS/>
5. *Building a scalable and secure Multi-VPC AWS network infrastructure - Building a scalable and secure Multi-VPC AWS network infrastructure*. (n.d.). <https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/welcome.html>
6. *Amazon Web Services Cloud - Overview of Amazon Web Services*. (n.d.). <https://docs.aws.amazon.com/whitepapers/latest/aws-overview/amazon-web-services-cloud-platform.html>