White Paper

aviatrix

Next Generation Cloud Native Networking

Introduction

The cloud has become the default option for delivering enterprise services and applications.

To keep up with rapid prototyping, continuous development and integration, enterprise IT organizations are transforming their traditional server deployment and maintenance functions to a more strategic role that handles the selection, integration, and delivery of IT services for the cloud. Although the cloud helps enterprises get more agile, it brings in some challenges.

Q: **How can companies extend their private datacenter to the cloud and expand their cloud footprint quickly and efficiently, without compromising the security or business continuity?**

Q: **How can cloud challenges like network interoperability and performance be overcome?**

Q: **Is there a way to ensure security for connections to cloud instances, datacenters, and everything that users access?**

Good news is that the cloud fosters innovation and there are solutions to allow secure and direct access to the cloud from any where and any device. East-west connections between clouds that carry the largest proportion of cloud traffic can now be fully meshed into one secure cloud network. Applications can be deployed in the cloud and rolled out to the entire enterprise while keeping the sensitive corporate data secure.

Enterprises Embrace Cloud Networks

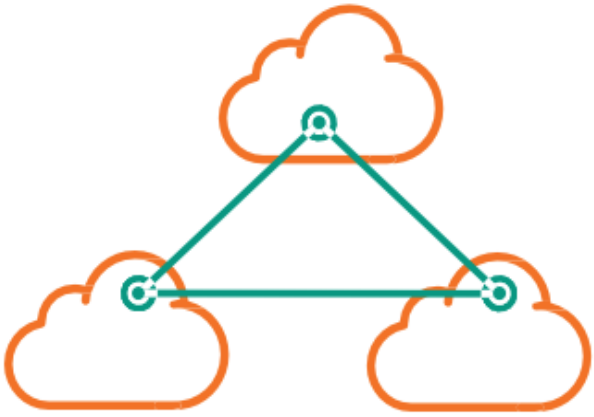
Cloud is no longer an experiment

– the largest global enterprises are in production in AWS, Azure, and Google. According to IDC, 65 percent of organizations plan to adopt a hybrid cloud deployment by 2015. Some enterprises operate entirely in the cloud; according to the Wall Street Journal, by 2022, over 20 percent of large enterprises will have cloud-only operations.

Transformation of IT departments into cloud-aware organizations, is a direct result of the impact the cloud is having on enterprise strategies.

As traditional enterprise hub and spoke network architectures change to accommodate the cloud, IT focus on cloud is a business imperative.

Networking in the Cloud



Cloud networks pose challenges on three fronts – connecting to the cloud, cloud networking to connecting within the cloud and making the enterprise, branch, and cloud part of one network with consistent policy, security, and management framework.

Connecting islands of cloud infrastructure, avoiding the shortcomings of VPNs, firewalls or proxies while managing cloud networks, and preserving enterprise security policies can be quite challenging.

Cloud Native Networking is different from traditional Enterprise Networking

Typically, IT is responsible for connecting enterprises to clouds. This phase of the cloud project is time consuming as it can get quite complex and cause business disruption as applications and services are dependent on cloud resources.

Hybrid cloud deployments come with mission-critical demands. The cloud needs to be a seamless extension of the private enterprise network. Resources launched in AWS, Azure, or Google need to interoperate with on-prem resources. As networks get increasingly global and collaborative, it is necessary to set up partner or customer accounts in the cloud and assign privileges per user to ensure that resources are managed based on business collaboration objectives.

Cloud VPN needs to go beyond traditional VPN capabilities

IT departments have expertise and deep know-how on corporate VPN and they tend to lean to these proven technologies as a way of connecting public cloud resources to on-premise applications. However, traditional corporate VPNs are unable to meet the demands of today's cloud-powered enterprise. Traditional VPNs take weeks to set up and fail to deliver on one of the main objectives of the cloud. VPNs are not designed to scale out on demand. Enterprises are forced to upgrade to new hardware - this takes time and cap ex. Security policies and edge routing configurations are complex and require deep expertise to extend into the cloud. Corporate VPNs force enterprise users to connect to the cloud via their enterprise datacenters. The result is a poor end user experience due to slow response times and long latencies to the application servers. User frustration gets amplified for collaboration and latency-sensitive real-time applications. Using a traditional VPN restricts enterprises instead of offering the scale and agility of the cloud.

Users of cloud applications demand OS- and device-agnostic services that let them access resources via any device, and the cloud needs to scale out on demand to users and workloads.

Securing public cloud infrastructure

All cloud providers talk about security in the cloud as a shared responsibility between them, the application developer, and the enterprise. The cloud needs to be highly secure to protect enterprise data. Enterprises in turn need to ensure that access to their cloud resources is restricted to authorized users.

How can you achieve all of these goals?

The security of the cloud platform is managed by the cloud service provider - AWS, Microsoft or Google. This is table-stakes and unless cloud platforms are highly secure, it affects credibility and potential of the cloud infrastructure platform. For securing access, best practices include leveraging multi-factor authentication (MFA) to grant users access to the cloud resources based on a combination of certificates, credentials, and tokens. Beyond authentication, authorization is crucial. During the development phase, it is common for developers to share root credentials, but that is not practical in production. User profiles allow administrators to manage entitlements with finer granularity. A combination of MFA and user profiles offers a much stronger entitlement management than just role-based access. Profiles can be defined by job roles, competency, or responsibility, taking into account individual needs by vertical, industry, or compliance.

What is needed to overcome these challenges is a SOLUTION that can seamlessly and securely extend the enterprise network into the CLOUD.

Next Generation Cloud Native Networking with Aviatrix

Aviatrix offers an end-to-end cloud native networking solution that is built from the ground up for the public cloud.

With Aviatrix, IT and Cloud Ops can simplify site to cloud, user to cloud, and cloud to cloud secure connectivity and access. Our solution requires no new hardware and deploys in minutes.

We enable end-to-end encrypted peering across VPCs in different regions, other clouds, and in enterprise sites. We provide Geo aware, scale out SSL VPN to VPCs with MFA from any device. Aviatrix gives greater visibility and control with comprehensive user tracking and logging capabilities such as access public-IP, multi-account billing breakdown and logging.

> “ At Aviatrix, we believe that your cloud network should be as DYNAMIC, SCALABLE, and DISPOSABLE as compute and storage. ”

Isolate

For many enterprises, life on AWS begins with a single network, a single VPC where all their instances and various AWS services reside. Subnetting and security groups within the VPC form the primary means of traffic isolation and access control. As Enterprises and their lines of businesses start to consume more cloud resources, further subnetting or further segmented sec groups do not scale. Consequently, the enterprise architects its network on AWS to create more VPCs. Some use a VPC per department or group, for instance, a VPC for game developers and another for game beta testers or to segment between enterprise users and their ecosystem partners who may have different AWS accounts.

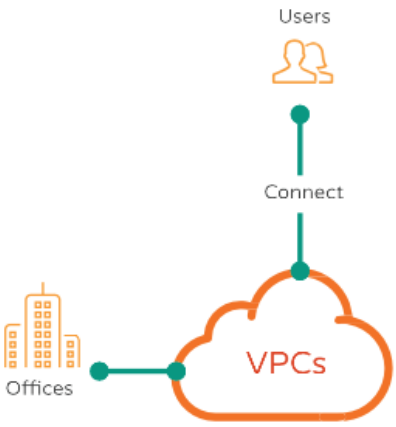
With Aviatrix, companies can micro-segment their cloud network into multiple VPCs and apply policies consistent with the security posture for all the apps across their cloud network, irrespective of the user location or the device used. Setting up and tearing down VPCs can be done in a matter of minutes.

Peer

With Aviatrix, enterprises can create an end-to-end cloud network with a single platform for multi-region and multi-cloud. Companies can scale up or down in the cloud in a snap.

Application workloads like business intelligence, analytics, or other data plane functions may need more resources, a larger CPU, more memory or storage on the same VM – this is vertical scaling. For a hardware appliance this means upgrading to the next model with higher capability, scale and of course a bigger price tag. But many cloud workloads, like web front ends or Internet of Things processes, may require load distribution across multiple, parallel VMs as users and clients grow without notice.

On-demand scaling to multiple instances is the horizontal scale out typical to modern cloud workloads. Aviatrix enables vertical or horizontal scaling so cloud teams can quickly create and provision VPCs and apply consistent policy based on user profiles. The licensing model is “pay as you grow” and that makes scaling an instant and automated process. There is no new hardware to procure or complex edge routing or security policy changes.



Access

Organizations use elastic IPs to deploy servers in the cloud. Developers use SSH or Telnet to connect to these servers. Public cloud infrastructure, as a result, becomes visible and susceptible to malicious attacks.

With Aviatrix, you can connect your users and offices to a PRIVATE NETWORK OF VPCs. Jump hosts or bastion stations are not required.

Only MFA authenticated users can access cloud resources authorized for their user profiles. With this approach, infrastructure in the cloud and accesses to the cloud remain invisible – no public IP addresses involved. Geo aware cloud VPN allows users to connect to the closest region for lowest latency.

Management, visibility, and operational simplicity

It is crucial to have a central management system for the entire cloud network with a single pane of glass visibility to cloud resources. With Aviatrix, managing cloud networks is a snap and this can free up time and resources for enterprises and let them focus on revenue generating activities. No need to worry about command-line interfaces, hardware upgrades, support cycles or backwards compatibility. Aviatrix uses a simple and central control plane that allows enterprises to quickly build and easily scale and secure hybrid cloud environments. The solution includes environment stamping features with which pre-built templates allow teams to set up hybrid clouds, define and tailor security policies, and provision resources with just a few clicks.

Our dashboard displays active VPN users and a peering summary to provide Cloud Ops a clear view of usage. We provide comprehensive logging capabilities. Integrated elastic search enables easy access of sys log information. Additionally, Aviatrix supports Log stash, Splunk, rsyslog, and Sumo Logic forwarder for remote logging.

The Aviatrix solution consists of Aviatrix Gateways deployed on-prem or in the cloud and the Cloud Controller that orchestrates and manages gateways.

Aviatrix Gateway

The Aviatrix Gateway is a cloud scale out and load balanced solution that allows direct VPN access to VPCs. Built for cloud deployments with multiple VPCs/VNets, the Gateway is architected to support a distributed cloud-based deployment across multiple regions. It can be installed on-prem or in the cloud to connect, manage, and secure cloud networks.

The gateway supports multi-factor authentication (Active Directory/LDAP, DUO, Google 2-step, Okta), auto scaling to the number of users and load, and access from Chromebook, Mac, PC, iPhones, Android and Linux. The gateway offers User Profile based access to cloud resources. It enables identical IP addresses and security policies, allowing for infinite scaling of deployments. NAT capabilities connect instances in the private IP address space directly to the Internet. Source and destination based filtering and security policies can be applied at the VPC level.

The Benefits of the Gateway

- Scale-out cloud VPN that auto scales to users and load
- Multifactor authentication— Active Directory / LDAP, DUO, Google and Okta
- Multi-region, multi-cloud encrypted peering
- User profile-based access and consistent security policies
- Deployed on-prem ESX/HyperV/ KVM or in AWS, Azure, and Google
- Environmental Stamping to create cloud networks at scale

It is fully integrated with AWS, Azure, and Google native services including EC2, VPC/VNET, ELB, S3/ Blob storage, SQS, SNS, Cloud Formation, Cloud Watch, IAM and other adjacent services.

The Gateway requires the Aviatrix Cloud Controller for setup, configuration, and management. It is launched from the Aviatrix Cloud Controller.

Aviatrix Cloud Controller

The Aviatrix Cloud Controller is the central orchestration component used with the Gateways on-prem or the cloud. The Controller centralizes cloud operations and management. It is the engine that allows for automated provisioning, logging and monitoring data analytics, and flexible volume-based licensing for cloud bursting.

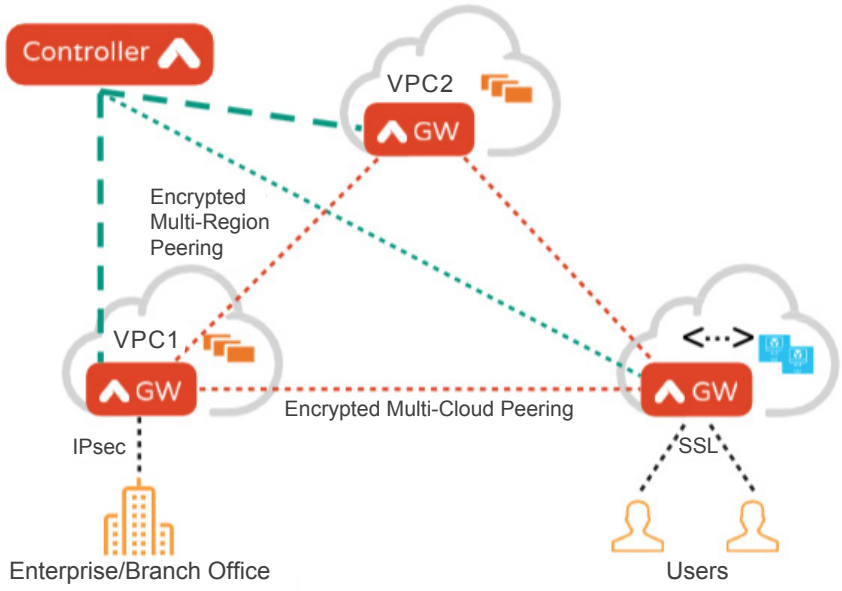


Fig 1. Aviatrix connects, secures, and manages your cloud network

The Benefits of Aviatrix Cloud Controller

- Central Orchestration and provisioning
- Extensive access logging and monitoring for compliance and audit
- Multi-region, multi-cloud encrypted peering
- Flexible volume-based licensing to enable burst usage

Use Case

How Aviatrix Solves one Common Cloud Challenge

When put into action, the Aviatrix solution is well suited for a variety of use cases, including hybrid cloud networks, direct and secure cloud-scale VPN access, delivering applications as a service over public clouds, and building geo aware secure networks that minimize application latency. Let's look at one use case in detail.

Connecting Users and Offices to the Cloud

Problem:

A large company has many employees that never work in an office. The enterprise would usually install a corporate VPN for these employees to access enterprise resources.

Solution:

With Aviatrix, the company can go beyond corporate VPN and quickly set up direct and secure cloud access so that employees could work from anywhere and from any client - Chromebooks to Macs, PCs, iPhones, Android and even Linux tablets. No local infrastructure is required so the company is able to save money and IT resources.

As the company continues to deepen its operations into the cloud, Aviatrix can provide the security and access to data and resources that employees need. By setting up MFA with user profile-based access, the company has complete visibility and control over what users access in the cloud. With more granularity, IT administrators can craft access-based policy to each user. The result - Aviatrix improves mobility for the vast workforce while reducing the security attack surface and enabling access to only trusted users and managing entitlements based on their function.

Conclusion

At Aviatrix we believe that your cloud network should be as dynamic, scalable, and disposable as compute and storage. We free you up from the complexity of securing and maintaining highly-scalable and highly-available cloud networks.

Aviatrix is a pioneer in cloud native networking with a solution built from the ground up for the public cloud.

Simplify the way you enable site to cloud, user to cloud and cloud to cloud secure connectivity and access. The Aviatrix solution requires no new hardware and deploys in minutes.

We enable end to end encrypted peering across VPCs in different regions, other clouds and in enterprise sites. We provide Geo aware, scale out SSL VPN to VPCs with MFA from any device. We give you greater visibility and control with comprehensive user tracking and logging capabilities such as access public-IP, multi-account billing breakdown and logging.

About Aviatrix

Aviatrix is a Cloud Native Networking startup that simplifies scaling in the cloud, enables connectivity across a wide range of cloud architectures, and delivers end to end network security. Our solution is built from the ground up for AWS, Azure, and Google based on software defined architecture that enables enterprises to realize the benefits of agility, scale and mobility from deploying applications in the cloud. To learn more about Aviatrix solutions, please visit the website, call +1.844.262.3100, follow us on Twitter, or connect with us on LinkedIn.