aviatrix

The Security Architect's Guide to Multi-Cloud Networking

> Treat cloud networking as its own domain. Cloud networking has its own technology and operational practices and deserves focused attention.
>
> Simon Richard, Gartner Analyst May 2020

In the cloud era, the role of network security architect has become even more critical than it has ever been. Complexity and human errors have always been the banes of security professionals. As enterprise cloud computing scales, it is expected to be 10x larger in size and complexity and will be deployed 1,000x faster than data center computing.

Read on to learn how security architects and their cloud counterparts plan to embrace this exponential growth in complexity by building on security best practices around a multi-cloud network architecture that leverages the simplicity and agility of cloud with enterprise-class operations and security automation.

CONTENTS

The **Aviatrix Certified Engineer (ACE)** program is the first multi-cloud networking and security certification available to technical professionals and cloud practitioners. The ACE certification is designed for individuals who already understand basic networking concepts and prepares engineers and operations staff with the (1) working knowledge of native networking constructs in AWS, Azure, Google Cloud, and Oracle Cloud Infrastructure and (2) proficiency to build use cases and multi-cloud architectures using Aviatrix software.

Best Practices for Multi-Cloud Network Security

1 Corporate and Regulatory Compliance

Corporate and regulatory compliance teams have the power to derail your cloud network designs at the last minute. Engage them early, show them that your multi-cloud network architecture delivers data in motion protection without relying on application-based encryption and ensures secure network segmentation that is consistent across cloud environments. Highlight that your design enables secure Internet ingress and egress filtering required by industry regulations such as PCI and HIPAA and effectively eliminates human error through infrastructure as code automation.

2 End-to-End Encryption

Secure your public cloud networking traffic. Public clouds are shared infrastructure that support hundreds of thousands of customers. Your traffic operates in virtual network space that is separate from other customers, however there are risks. To ensure your data in motion is always protected, leverage end-to-end encryption between VPCs/VNets and between clouds. End-to-End encryption is often a corporate or regulatory requirement, consult your security compliance team for your businesses' policy.

3 High-Performance Encryption

To enhance end-to-end encryption, maximize encrypted network throughput on connections with aggregate throughput requirements that exceed the less than 2 Gbps throughput standard IPSec connections deliver. Leverage technology that allows you to aggregate tunnels and distribute IPSec processing overhead across multiple processor cores. Deliver wire speed IPSec throughput on data center-to-cloud links such as AWS Direct Connect, Azure Express Route and Google Cloud Interconnect and up to 90 GBps on intra-cloud connections.

4 Multi-Cloud Network Segmentation

Extend security domains and network segmentation connection policies across clouds. Reduce your overall risk profile by maintaining consistent VPC/VNET/VCN access control policies. Each cloud offers unique security group and access control services that restrict access to and between application environments within their cloud. Consistent network segmentation and connection policies across clouds simplifies secure access control and enables reliable application/data connectivity in multi-cloud environments.

5 Next Generation Firewall Service Insertion

Take advantage of your on-premises security team's familiarity with physical next generation firewall appliance rules, policies and management systems by deploying virtual version in the cloud. Simplify deployment and ongoing operations, while maximizing performance, scale and visibility by attaching virtual firewall appliances to a multi-cloud network architecture. Wherever possible leverage API-based firewall programmability and Terraform infrastructure as code automation to dramatically reduce the operational overhead of setting up routes for traffic that requires inspection.

6 Operational Visibility and Automation

Maximize operational visibility to allow security teams to easily visualize cloud network traffic patterns, trends and quickly identify anomalies. Leverage infrastructure as code automation to reduce or eliminate human configuration errors and ensure security policies are applied consistently, without draconian control that would reduce agility or service delivery speed. Enterprise cloud network environments are going to explode in scale and complexity. Plan for this exponential growth; put an architecture in place that supports multi-cloud automation and operational visibility that will support that rate of growth.

Expert Chat

Deliver Measurable Business Impact. Securely.

Do not bind your cloud network platform to a single cloud provider technology or architecture. A cloud network platform creates a cloud network abstraction layer that leverages and controls native cloud constructs and services. It then adds a superset of enterprise-class networking, security and operational visibility capabilities that operate Above the Clouds.™ This delivers compelling business value, including:

Multi-Cloud Optionality

Architect cloud networks to support existing single-cloud requirements with the option to easily expand. Having multi-cloud optionality allows Aviatrix customers to respond quickly to new customer demands or M&A integrations, which all consider a benefit.

We knew from previous experience that transit networking services offered by cloud service providers did not consistently offer the advanced networking and security controls or the ability to support the multi-cloud network architecture we envisioned. Aviatrix delivered both.

Dr. Michael Weber, Sr. Manager, Traffic Engineering, Splunk

splunk>

The Aviatrix Controller delivers the central intelligence and multi-cloud control and is the foundation for delivering measurable economic value.

Reduced Operational Overhead

Intelligent central control, increased operational visibility and control, automation, and reduced staff skills gap all contribute to a significant reduction in operational overhead.

With the Aviatrix cloud network platform, we have a standardized, repeatable network architecture that supports our transit networking and other security requirements, which means our cloud network and security engineers have the luxury of not spending time on repeatable tasks and instead can focus on driving value for our business.

David Shinnick, VP and Principal Solutions Architect, FactSet.Reduced

FACTSET

Reduced Mean Time-to-Resolution

The Aviatrix platform's operational control, critical visibility, and troubleshooting capabilities increase application uptime and end-customer satisfaction.

CoPilot's extreme visibility helps customers find the 'needle in the haystack' to more easily recognize unusual network behavior and more quickly resolve network and application connectivity issues that, in the past, would have taken much longer to resolve.

Preston Gregg, General Manager North America, Viqtor Davis

VIQTOR DAVIS
DATA CRAFTSMANSHIP

Reduced Time-to-Market

The Aviatrix platform lets IT move at cloud speed, with a multi-cloud Terraform Provider that allows cloud networking to integrate easily into enterprise infrastructure as code automation and CI/CD pipelines. All with the result of increasing IT response time to the business.

When I learned that we could run our cloud network as code, I knew it would be a game changer for us. With Aviatrix, networking has finally entered the cloud era.

David Burris, Senior DevOps Engineer at Advance Auto Parts

Advance Auto Parts

Simplicity and Agility of Cloud. Operations and Security Required by Enterprises.

Simplify Enterprise Cloud Networking

The Aviatrix cloud network platform delivers the advanced networking, security, and operational visibility services required by enterprises, while maintaining the simplicity and automation of the cloud.

Advanced Multi-Cloud Network Transit

Aviatrix software enables enterprise IT to easily deploy a high-availability, multi-cloud network data plane with end-to-end and high-performance encryption, multi-cloud security domains, and operational data IT teams need. Aviatrix Transit provides the intelligence to ensure network correctness, deliver self-healing capabilities, and deliver traffic engineering controls–functions that network architects lack with basic transit constructs delivered by the CSPs.

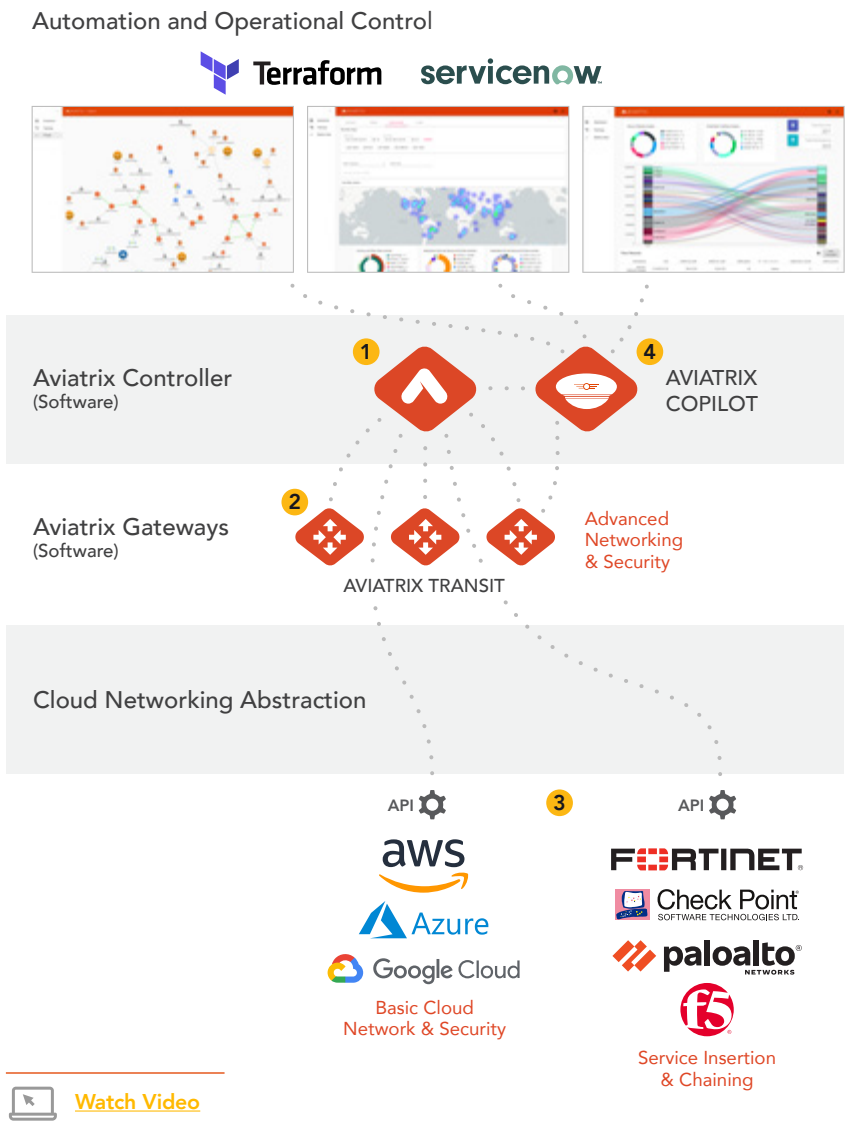
Enterprise-Class Operational Visibility

The Aviatrix platform brings day-two operational visibility not available from any cloud provider. This helps pinpoint traffic anomalies and suspicious behavior, resolve connectivity problems faster, and share network health metrics and dynamic network topology maps with staff and management.

Multi-Cloud Network Training

Aviatrix offers hands-on Aviatrix Certified Engineer (ACE) training and certifications to quickly bring your whole team up to speed on native AWS, Azure, and GCP networking, multi-cloud reference architectures, and the Aviatrix cloud network platform.

The Aviatrix Cloud Network Platform



Watch Video

1 Centralized Controller

The Aviatrix controller is the brain of the cloud network platform. The platform leverages the centralized intelligence and knowledge of the controller to dynamically program both native cloud network constructs and Aviatrix's own advanced services. Our single Terraform provider enables network and security Infrastructure-as-Code automation across your multi-cloud environment.

2 Gateways

Aviatrix gateways deliver advanced cloud networking and security services. Gateways are primarily deployed to deliver transit network and security services such as intelligent dynamic routing, active-active network high-availability, end-to-end and high-performance encryption and collect operational visibility data, but also for secure network ingress and egress filtering and external service insertion.

3 Native Cloud Constructs

The Aviatrix Controller leverages and controls native cloud constructs through public APIs, allowing the platform to be part of the cloud network, while adding critical network, security and operational visibility enterprises require.

4 Aviatrix CoPilot

Enterprise network operations teams must have deep visibility into network activity. CoPilot leverages the intelligence of the Aviatrix Controller and network flow analytics from Aviatrix Gateways to deliver multi-cloud visibility that is simply not available from any cloud provider.

Cloud Networking and Security Beyond Cloud Boundaries

Multi-Cloud Network Architecture

Aviatrix helps enterprise cloud network architects create a multi-cloud network architecture. It also offers a cloud network platform that provides the software and services required to plan, dzeploy, and operate a secure enterprise multi-cloud network.

High-Availability Networking

Aviatrix secure network transit's design includes active-active, high-availability, and redundant pathing. Pairs of Aviatrix Gateways, deployed in separate availability zones, establish a full mesh, multi-path connection that maximize both throughput performance and network availability.

Infrastructure as Code

The Aviatrix multi-cloud Terraform Provider leverages the multi-lingual capability of the Aviatrix Controller, which enables a single Terraform module to deploy repeatable network designs and security policies across all clouds. This allows cloud networking to integrate easily into enterprise infrastructure as code automation and CI/CD pipelines.

High-Performance Encryption

Standard IPSec encryption is limited to 1.25 Gbps. Aviatrix's high-performance encryption distributes processing across multiple cores and aggregates IPSec tunnels to achieve wire-speed encryption, up to 75 Gbps.

Multi-Cloud Network Segmentation

Some clouds enable the creation of security domains. Aviatrix extends secure network segmentation beyond cloud boundaries to enable multi-cloud security domains with consistent, centrally managed, global network segmentation, and connection policies.

Secure Cloud Ingress and Egress Controls

Aviatrix gateways offer both ingress and egress L4 and Fully Qualified Domain Name (FQDN) filtering. Centrally managed filter groups ensure consistent multi-cloud security for any cloud application communicating with Internet-based resources and services.

Multi-Cloud Network Service Insertion

Aviatrix Transit provides a secure point of access for network and security services such as next-generation firewalls, IDS/IPS, and SD-WAN cloud edge connections. Aviatrix gateways provide load balancing to scale-out connected services and ensure redundant and failover high availability.

Operational Visibility

Enterprise network operations teams must have deep visibility into network activity. Native public cloud networks are opaque. Even basic analytics must be obtained from multiple sources and require skilled human correlation to become actionable. Multi-cloud visibility is simply not available from any cloud provider.

Dynamic Network Mapping

Aviatrix leverages the controller's central intelligence and knowledge to dynamically generate and maintain an accurate multi-cloud network topology map. This includes all network resources and network configurations the controller manages. The map includes both native network resources and Aviatrix's secure transit and cloud ingress and egress control gateways.

FlowIQ – Intelligence Network Traffic Analytics

Aviatrix extracts detailed network traffic flow data from Aviatrix Transit infrastructure, including source, destination, port, and protocol filtering. This combined with additional metadata, such as latency and tagging, delivers never before possible multi-cloud flow inspection and global traffic heat maps.

AppIQ – End-to-End Application Path Analysis

Allowing network teams to work more closely with their application teams, AppIQ provides a detailed analysis of traffic and systems which form the path between two application endpoints, including gateway performance, network latency, route table analysis, security domains and more.

More

Additional advanced networking features include BGP propagation, traffic engineering, optimal path routing, and more.

Learn More

Try Aviatrix Today or Schedule an Architectural Review Session

Aviatrix is simple to deploy; our intelligent central controller is launched from cloud provider marketplaces and automates the deployment of additional network and security services, as required. Most customers launch and begin using Aviatrix services in an afternoon, easy to try and evaluate. We have experts available to help you.

Schedule Demo

Schedule Meeting

About Aviatrix

Aviatrix is a cloud network platform that brings multi-cloud networking, security, and operational visibility capabilities that go beyond what any cloud service provider offers. Aviatrix has over 450 enterprise customers who leverage it's proven multi-cloud network reference architecture to design, deploy and operate a repeatable network and security architecture that is consistent across public clouds. Aviatrix software leverages AWS, Azure, GCP and Oracle Cloud APIs to interact with and directly program native cloud networking constructs, abstracting the unique complexities of each cloud to form one network data plane, and adds advanced networking, security and operational features enterprises require.

Aviatrix.com

aviatrix

CUSTOMER FLIGHT PLANS

THE JOURNEY TO MULTI-CLOUD

Watch Steve talk candidly with Aviatrix customers

Steve Mullaney teams up with innovative cloud architects and executives for an entertaining and in-depth look into the future of enterprise infrastructure in the cloud.

Watch the series

Meet our CEO

Steve Mullaney is an industry visionary and proven leader. Ten years ago, Steve led Nicira and VMware to transform data center networking with SDN and network virtualization. Three years ago, Steve saw that the approaching next wave of enterprise digital transformation, the "all in" shift to public cloud services. He knew this would require networking as we knew it to transform as well. Two years ago, he took the helm at Aviatrix. Today some of the largest enterprise businesses in the world look to Steve as the industry's thought leader and have partnered with him and the team at Aviatrix to deliver the foundation of their next generation multi-cloud network infrastructure.

aviatrix