AVIATRIX FIRENET FOR F5 NETWORKS SSL ORCHESTRATOR

Simplify Deployment and Maximize Performance of F5 SSL Orchestrator in Your Cloud

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 cloud.

Secure Multi-Cloud Network Transit

Aviatrix software enables enterprise IT to easily deploy a high-availability, multi-cloud network data plane with end-to-end encryption, high performance encryption, multi-cloud security domains, and operational telemetry operations teams need.

Enterprise Class Operational Visibility

The Aviatrix platform brings day-two operational visibility not available from any cloud provider to help you pinpoint traffic anomalies and suspicious behavior, resolve connectivity problems faster, and share network health metrics and dynamic network resource 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.

"Aviatrix's cloud network platform intelligently programs the native cloud network constructs and goes well beyond that by adding network segmentation policies, rich visibility, and automation that we require to support our customers. Aviatrix makes cloud networking much easier for us and our customers."

JOHN GOODSON
SVP AND GENERAL MANAGER OF PRODUCTS
VERINT

Better Together: F5 SSL Orchestrator and Aviatrix

Bring F5 security policies to the cloud with simplicity, performance and multi-cloud visibility. Aviatrix cloud network platform and FireNet reference design makes F5 SSL Orchestrator integration simpler in the public cloud. The solution leverages the Aviatrix controller for deployment automation and on-going route propagation, maximizes cloud network throughput performance, and removes the need for SNAT using bi-directional hashing to pin sessions to specific security gateways to maintain source address visibility.

What is F5 SSL Orchestrator?

F5 SSL Orchestrator is a dedicated appliance solution designed specifically to optimize SSL infrastructure, alleviate security blindspots caused by encryption by providing security devices with visibility into SSL/TLS encrypted traffic to locate and eliminate threats hidden in encryption, and maximize efficient use of their existing security investments.

This solution supports policy-based management and steering of traffic flows to dynamic service chains comprised of existing security devices. It's designed to easily integrate into existing architectures and to centralize the SSL decrypt/encrypt function, as well as delivering the latest SSL encryption technologies across the entire security infrastructure.

Simplicity and Automation with Enterprise Visibility and Control

As an enterprise IT leader, your organization is driven by business transformation and tasked to accelerate the migration to public cloud. However, large scale enterprise application and service transformations are not as simple as cloud providers would make it seem. The promise of cloud is simplicity and automation, but the reality for enterprise IT is often much more challenging – shadow IT, cloud and networking skills gaps, limited visibility, and lack of a well architected network design – all contribute to your team's everyday challenges.

Aviatrix cloud network platform is a foundation upon which you can regain visibility and control and shift your focus from managing disparate network infrastructures to controlling a consistent global cloud network that provides enterprise class networking, security and operational features that are simply not available from any cloud provider.

We understand you need the network visibility and control you enjoyed on premise, now for your cloud networks. You want day-two operations, visibility, control, regulatory compliance and other enterprise IT architectural structures that make large scale IT environments operational for the long term. But it's different, you don't want to do it the same way, you want it modernized for the cloud. That is why Aviatrix and F5 have partnered to help you bring your proven security solutions into your cloud.

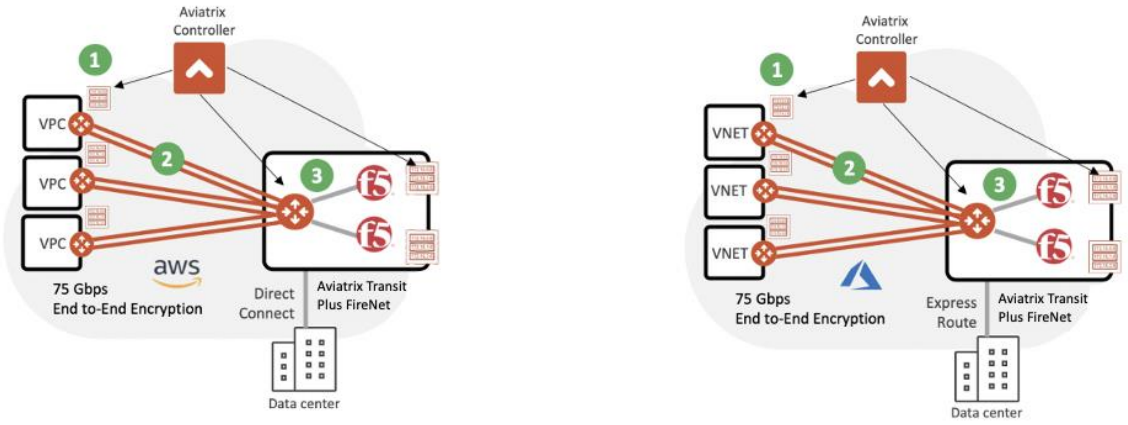

Figure 1: Eliminate deployment, performance and visibility compromises native cloud networking solutions introduce. Maximize simplicity, performance and visibility for F5 SSL Orchestrator in your cloud environment with the integration of F5 SSL Orchestrator and Aviatrix cloud networking platform. Note: There are multiple design possibilities for AWS and Azure deployments, consult an Aviatrix Solution Architect.

Challenges — Forced Compromises:

Operational Complexity.
Manual route table updates are difficult to deploy and maintain. Any change in your cloud environment (new VPCs/VNets or route updates for proper network segmentation) or on-premise (route updates from on-premises router) creates several extra manual steps in administration and introduces human error risk. At scale, you must automate this process.

Throttled Performance.
F5 SSL Orchestrator is a high-performance security solution capable of up to 10Gbps throughput. Native cloud constructs reduce this throughput to 500Mbps, resulting in a massive reduction in the product's capabilities. Why? Example: Native connections from AWS Transit Gateway to F5 SSL Orchestrator using its built in VPN function, requires IPSec tunneling. The IPSec tunnel processing overhead reduces the throughput to less than 1.25 Gbps, approximately 500Mbps bi-directional.

Scale/Visibility Trade-off.
F5 SSL Orchestrator has outstanding scale-out capabilities, but with native cloud networking constructs, if you run more than one instances using ECMP, each instance must configure Source Network Address Translation (SNAT) to ensure return traffic lands on the same instance. SNAT creates visibility compromises as customers lose source address visibility, something enterprise customers often require.

F5 with Aviatrix — No Compromises:

F5 SSL Orchestrator with Aviatrix cloud network platform simplifies public cloud deployments and allows F5 SSL Orchestrator to operate at peak performance and scale, without compromises.

Simplify F5 SSL Orchestrator Deployments and Operations.
Aviatrix Firewall Network (FireNet) combines the intelligent orchestration and automation provided by the Aviatrix Controller with advanced Aviatrix Transit capabilities to significantly simplify F5 SSL Orchestrator deployment and ongoing operations in AWS, Azure, Google Cloud and Oracle Cloud. The combined solution eliminates the need for administrators to manually propagate routes and update routing tables when changes are made to the environment

Maximize F5 SSL Orchestrator Performance.
Aviatrix eliminates the requirement for IPsec tunneling, increasing the throughput performance by over 30x to 15Gbps, maximizing F5 SSL Orchestrator performance.

Maintain Source Address Visibility
Aviatrix FireNet gateways eliminate the requirement to use SNAT when using ECMP for scale-out by providing bi-directional hashing to pin sessions to specific firewalls. By eliminating SNAT for east-west traffic inspection, spoke VPCs/VNet have complete source address visibility

Multi-Cloud Network Architecture

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

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 automation services automation across your multi-cloud environment.

Network Service 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 telemetry, but also for secure network ingress and egress filtering and external service insertion.

Operational Visibility

A key value of the Aviatrix cloud network platform is day-two operations visibility and troubleshooting. 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 central intelligence and knowledge of the controller to dynamically generate and maintain an accurate multi-cloud network topology map that includes all network resources and network configurations the controller is managing. The map includes both native network resources and Aviatrix secure transit and cloud ingress and egress control gateways.

FlowIQ – Intelligence Network Traffic Flow Analytics

Aviatrix extracts detailed network traffic flow data from the Aviatrix secure transit infrastructure including source, destination, port and protocol filtering and combined with additional meta data such as latency and tagging to deliver never before possible multi-cloud flow inspection and global traffic heat maps.

High-Availability Networking

Aviatrix secure network transit is designed with active-active high-availability and redundant pathing. Pairs of Aviatrix Gateways, often deployed in separate availability zones, establish a full mesh, multi-path connection that maximizes both throughput performance and network availability.

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, enabling multi-cloud security domains, with consistent, centrally managed, global network segmentation policy.

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 service.

Multi-Cloud Network Service Insertion

The Aviatrix secure network 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 provides load balancing to scale out connected services and ensure redundant and failover high availability.

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.

Contact your Aviatrix account executive or email info@aviatrix.com to schedule an architectural overview or design session with one of our solution architects. Learn about Aviatrix Certified Engineer (ACE) training or for more information go to aviatrix.com.