SOLUTION BRIEF

Fortinet and Aviatrix Cloud Security Solution

Enhance Application Security With Advanced Cloud Networking, Visibility, and Control in the Public Cloud

Executive Summary

The Aviatrix Firewall Network Service (FireNet) allows enterprises to bring firewall solutions to the public cloud and easily integrate with cloud-native constructs. Aviatrix FireNet supports the Fortinet FortiGate Next-Generation Firewall (NGFW) for inspection of all, or specified, traffic flows with a zero-trust policy-based model. It provides complete orchestration and control with maximum performance and scale-out architecture, while providing the high performance demanded by enterprises.

Challenges

Implementing and operationalizing any NGFW in a public cloud can be challenging for organizations, not because of the NGFW itself, but because of networking restrictions, lack of centralized architecture, and complex operating models. Understanding cloud networking limitations to ensure a successfully designed and maintained NFGW deployment in the cloud is not a small task. It comes with performance, scale, and visibility trade-offs that must be tackled for enterprise security needs.

Organizations are also challenged by the lack of visibility that creates blind spots. Moreover, operationalizing the NGFW in the public cloud without familiar tools, Day-2 operations best practices, and consistent security polices for compliance and audit is another hurdle faced by single- or multi-cloud enterprises.

Solution Description

Aviatrix and Fortinet partnered to deliver an industry-leading security solution to address the above challenges. The integration of the Aviatrix platform and FortiGate virtual machines (VMs) is enabled through the Fortinet Fabric-Ready Partner Program in the Fortinet Open Fabric Ecosystem. It delivers a framework to successfully insert FortiGate NGFWs in single or multiple clouds by eliminating all the complexities, blind spots, and trade-offs. The partnership ensures a smooth transition and adoption for existing and new customers to protect cloud and on-premises applications.

Solution Components

- Fortinet FortiGate Next-Generation Firewall
- Aviatrix secure cloud network platform

Solution Benefits

- Simplicity with cost optimization for single and multi-cloud architectures
- Automation and orchestration
- Maximize scale with high-performance encryption
- Visibility, troubleshooting, and compliance
- Self-healing with zero-trust policy-based model
- Enhanced app security with east-west, north-south, egress traffic inspection

FORTINET FABRIC-READY

Solution Components

The Aviatrix platform is deployed under an organization's public cloud accounts, subscriptions, and projects. This ensures that enterprises have complete control, compliance, and visibility with dedicated cloud-native instances and services. The Aviatrix platform comprises three products:

Aviatrix Controller: The controller is deployed as an instance (VM) from the public cloud marketplace. It provides centralized and cloud-agnostic control, management, and automation plane.

Aviatrix Gateways: The data plane is built using Aviatrix cloud-agnostic gateways. The controller utilizes a standard architecture using Aviatrix Gateways to provide advanced networking and security services.

Aviatrix CoPilot: CoPilot is a Day-2 component providing centralized logging, visualization, visibility, and troubleshooting for compliance, audit, and reporting.

Fortinet FortiGate NGFWs deliver industry-leading enterprise security for any edge at any scale with full visibility and threat protection. Organizations can weave security deep into the hybrid IT architecture and build security-driven networks to achieve:

- Ultrafast security, end to end
- Consistent real-time defense with FortiGuard security services
- Excellent user experience with security processing units
- Operational efficiency and automated workflows

FortiGate-VM virtual appliances allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. FortiGate-VM virtual appliances feature all of the security and networking services common to traditional hardware-based FortiGate appliances. With the addition of virtual appliances from Fortinet, you can deploy a mix of hardware and virtual appliances, operating together and managed from a common centralized management platform.

Solution Integration

Aviatrix Controller deploys the FortiGate-VMs in a security/DMZ VPC/Vnet/VCN. It manages the health and life cycle of FortiGate-VMs. All the necessary route programming and propagation to the VPC/Vnet route table and NGFW are done by the Aviatrix Controller based on the inspection policy. This also includes routes learned dynamically from on-premises data centers and branches, and seamless integration with continuous integration/continuous deployment (CI/CD) pipeline with comprehensive Terraform support.

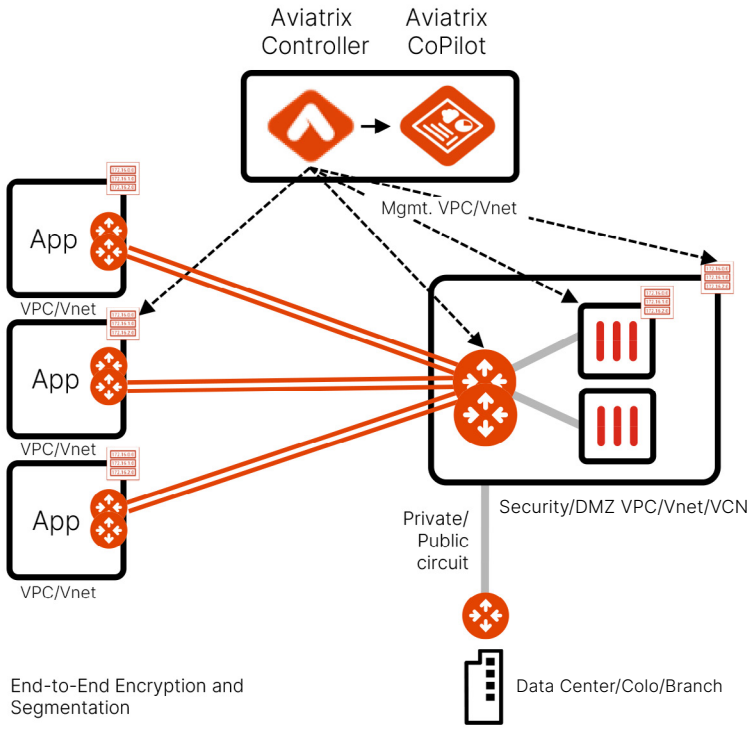

Figure 1. Aviatrix Controller manages the health and life cycle of FortiGate-VMs

Microsegmentation, inline threat detection, and remediation allow granular policies based on Content Security Policy (CSP) tags and other attributes. Geofencing blocks malicious IPs based on regions, which allows enforcement closest to the source of the threat. The architecture is simple yet powerful without using source network address translation (SNAT) or complex Border Gateway Protocol (BGP)/Virtual Extensible LAN (VXLAN)/Geneve overlays. Excellent NGFW performance results in higher ROI for organizations.

Use Cases

Use case #1 – Protect internet-facing applications using FortiGate NGFWs in multiple clouds, using a consistent and repeatable architecture, so that enterprises can eliminate the skills gap problem, increase visibility, and reduce mean time to remediation (MTTR).

Use case #2 – Uncompromised and automated deep-packet inspection for east-west, egress, and north-south traffic. The solution also caters traffic flows between on-premises data centers, edges, and SD-WAN branches. The NGFWs are deployed in a centralized security/DMZ VPC/Vnet catering to low-latency applications' needs with a policy-based zero-trust model.

About Aviatrix

Aviatrix is a leader in secure cloud networking for single and multi-cloud enterprises. The Aviatrix secure cloud network platform delivers a single, common platform for multi-cloud networking, regardless of public cloud providers used. Aviatrix delivers the simplicity and automation enterprises expect in the cloud with the operational visibility and control they require. The Aviatrix Certified Engineer (ACE) program is the industry's first and only multi-cloud networking certification and training program. Email info@aviatrix.com for more information.

September 2, 2022 10:34 AM

1725007-0-0-EN