AVIATRIX TRANSIT FIRENET FOR F5 NETWORKS SSL OFFLOAD

Introduction

Aviatrix Transit FireNet (Firewall Network) solution delivers flexible NextGen Firewall service insertion to simplify the inspection of traffic leaving a VPC/VNet. This capability can be extended to include advance service chaining using F5 Big-IP, which can be inserted in front of NGFW, IPS and other service appliances. To keep this tech brief short, we will focus on F5 Big-IP's SSL Offload feature and use AWS for single cloud example. The same design principles apply for Azure and other public cloud environments. We will also look at multi-cloud deployments covering both AWS and Azure. This tech brief overviews three proven designs for service insertion:

1. SSL Offloading by F5 Big-IP for all traffic
2. SSL Offloading by F5 Big-IP for Ingress traffic only
3. Multi-Cloud SSL Offloading by F5 Big-IP
    a. For Ingress traffic only
    b. For all traffic in AWS and Ingress traffic only in Azure

Advance Service Insertion: SSL Decryption + NGFW + IPS

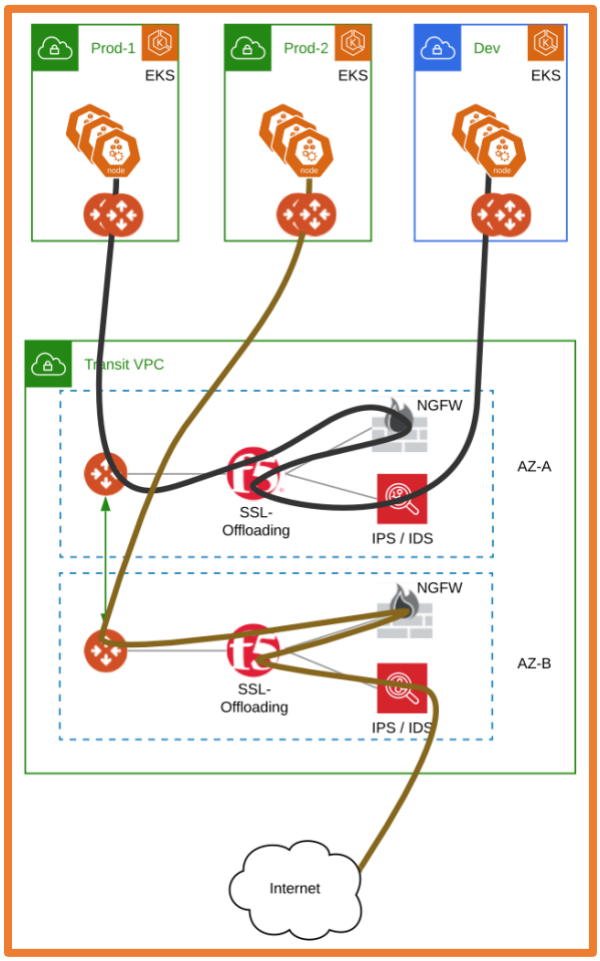
Service insertion in public cloud usually means inspecting traffic that is initiated by applications in VPCs to various destinations such as other VPCs, on-prem and internet. This can be handled via collapsed design where a single Transit FireNet facilitates all traffic paths, and also via scale-out design where one Transit FireNet handles E-W and On-Prem traffic and a dedicated Transit FireNet handles Egress to Internet.

In either case, as most of this traffic may be encrypted, payload inspection requires in-line decryption. Most NGFW offer SSL decryption capabilities but their performance may take a hit while doing so hence it's optimal to offload SSL decryption to a specialized appliance that can decrypt the traffic and hand it off to the NGFW.

In more security sensitive environments, just NFGW is not enough on its own, and there are requirements to chain multiple types of security appliances in the path. When put together, the requirement from security and compliance teams look like:

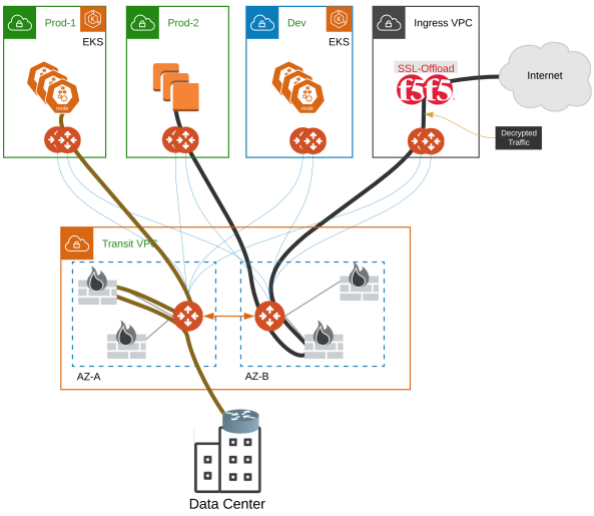
1. A way to transparently redirect interesting traffic to an SSL Offloading appliance.
2. Chain multiple security appliances (NGFW, IPS/IDS, Packet Capture) behind the SSL Offloading appliance.
3. Load balancing, managing health, scale and failover of the SSL-Offloading appliance which will in turn load balance, manage health and scale the security appliances.

The design pattern shown here is a collapsed design where single Transit FireNet facilitates all E-W, On-Prem and Egress to Internet traffic. Aviatrix orchestrates F5 Big-IP in a scale-out fashion performing SSL-Offloading to multiple appliances service chained and load balanced behind it. An example could be Palo Alto Networks VM-Series performing NGFW and Cisco Firepower used as NG-IPS appliance.



Advance Service Insertion: SSL Decryption for Ingress Only + NGFW

In some instances, the SSL-Offloading is only required for traffic coming in from the internet or another untrusted domain but not needed for east-west or traffic to on-prem. In such cases, we can setup a dedicated VPC to handle Ingress Traffic where the F5 Big-IP type of specialized SSL-Offloading appliance can decrypt the traffic before it proceeds to the application. Aviatrix transit will handle the traffic and redirect the decrypted traffic to a NextGen Firewall for inspection. Once inspected and allowed, the traffic can proceed to the application. Some benefits of this approach include:



- Simplified offloading of SSL to specialized appliance
- Transparent offloading
- Transparent NGFW inspection
- Selectively choose which traffic needs to be inspected
- Operational visibility and troubleshooting

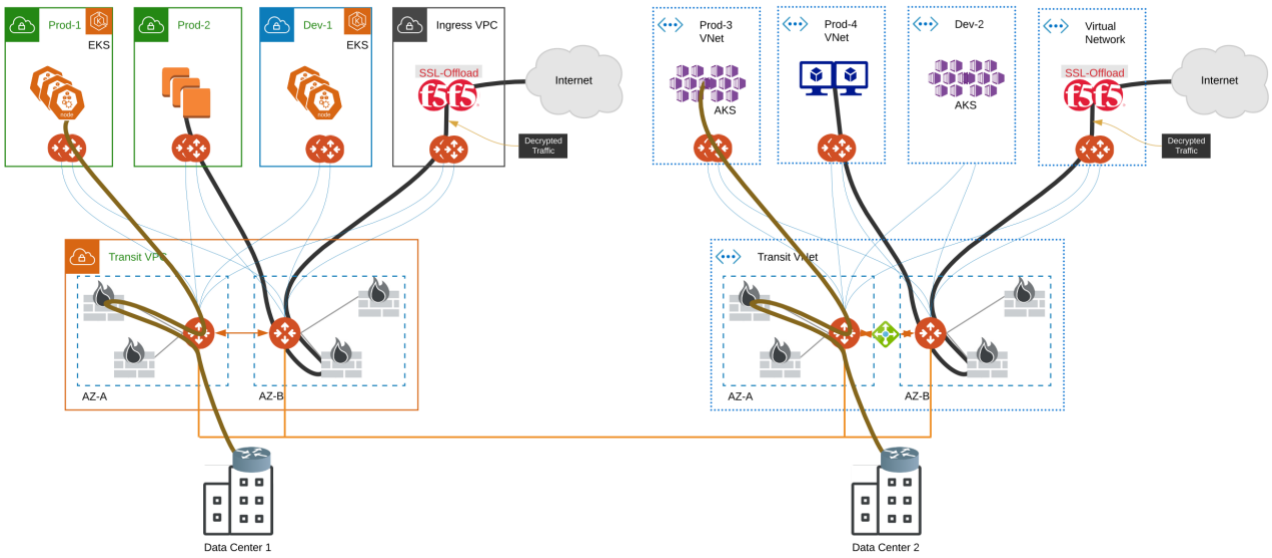
Multi-Cloud SSL Offloading by F5 Big-IP

Enterprise production deployments usually have a mix of requirements that warrant multiple Transit architecture. For ex, Production traffic may not share the same transit as Test environments; Multiple environments using overlapping IP addresses; Environments that need to be segmented from each other. Similarly, security requirements won't be same for all environments. Some environments requiring complete decryption of packet for payload inspection whereas some traffic pattern may only need L4 inspection. Aviatrix Transit offers the repeatable flexibility even in a single region where you can provision multiple transits to provide individual control and scale that different environments and applications may need.

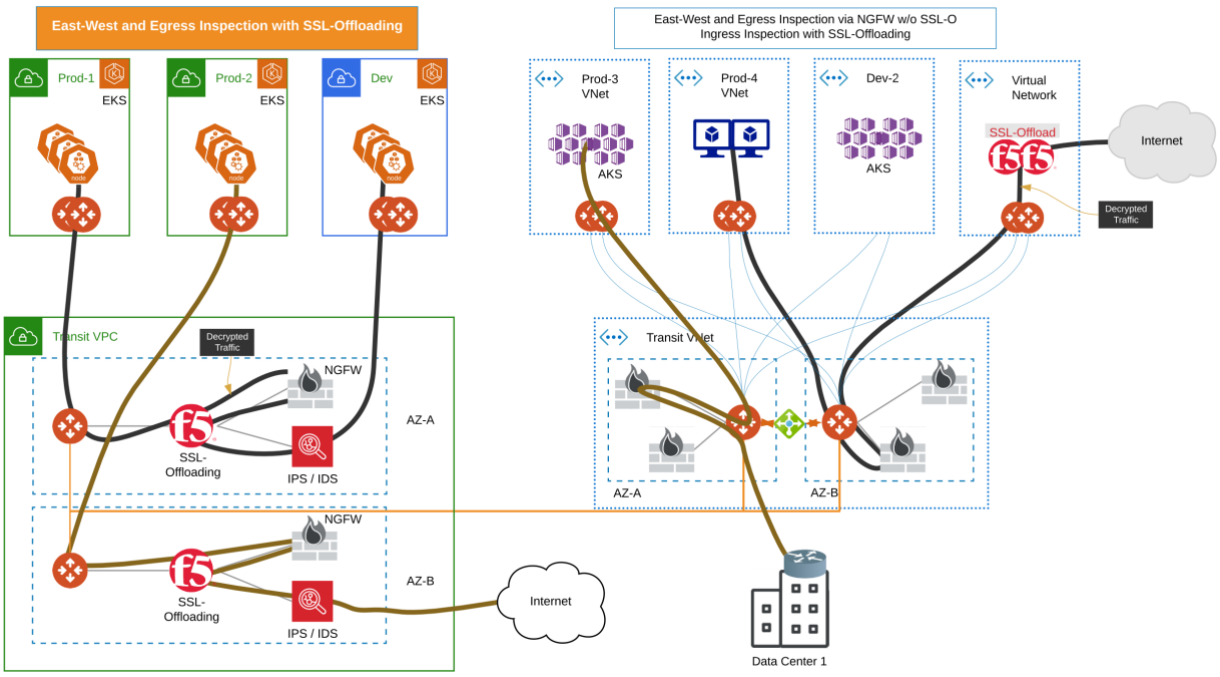
The previous two designs in an AWS example demonstrated the flexibility Aviatrix provides in steering traffic thru desired path while providing visibility and control. Next we will demonstrate the repeatability aspect of the platform such that the same design that worked in AWS also works in Azure and there can be mix and match or modifications based on requirements.

The next two designs highlight how, leveraging the repeatable multi-cloud network designs capabilities of the Aviatrix cloud network platform, we can easily extend into Azure and modify traffic flows to fit enterprise needs.

A. Multi-Cloud with SSL-Offloading for Ingress traffic only design:



B. Multi-Cloud with SSL-Offloading for all traffic in AWS and Ingress traffic only in Azure:

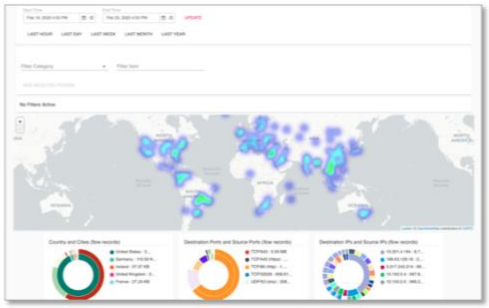


Day-Two Operational Visibility – Aviatrix CoPilot

The Aviatrix cloud network platform provides the data and intelligent analytics required to deliver deep, enterprise-class visibility and troubleshooting capabilities, not offered by any cloud service provider. The Aviatrix CoPilot visualization platform provides a detailed view into what's going on your public cloud network. It provides dynamic topology mapping, intelligent flow analytics, traffic flow heat maps, visibility into cloud routes and overall environment health.

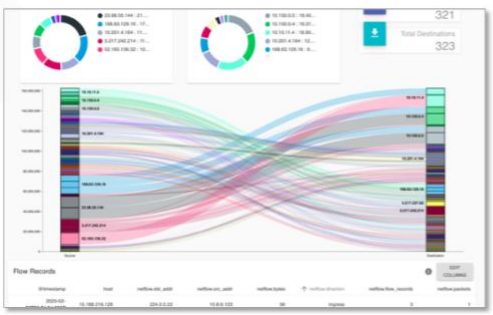
Link here to view a CoPilot Demo

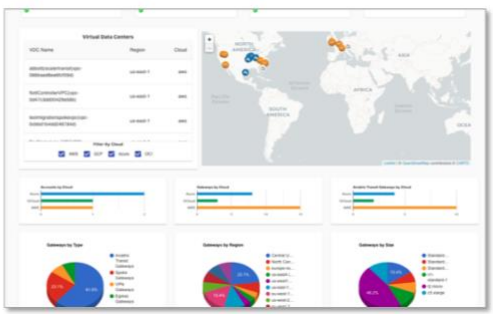
Multi-Cloud Dynamic Topology Mapping



Global Network Traffic Flow Heat Maps

FlowIQ Intelligent Traffic Analytics





Multi-Cloud Network Health Dashboard