aviatrix

ACE

Aviatrix Certified Engineer

Firewall Networks (FireNet)

ACE Solutions Architecture Team

Firewalling in the Cloud

Layered Security Model - Defense in depth

Intra-Spoke Traffic – Distributed

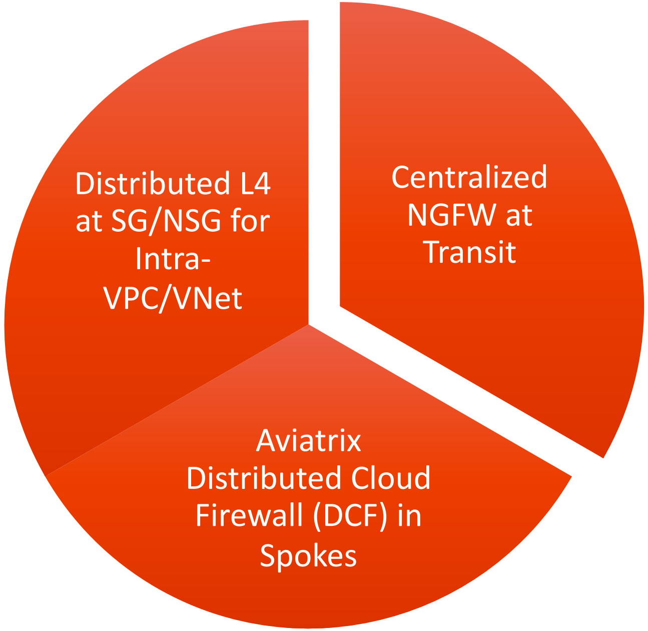
- Best handled by L4 SG/NSGs (Aviatrix can do it)
- Lifecycle tied with compute instances (CI/CD)
- Provisioned/de-provisioned by automation

E/W and N/S Inspection – Distributed

- Handle via Aviatrix L7 Firewall
- Relieves 3rd party Firewalls from processing
- Reduces cost by fewer egress charges and expensive firewalls
- Close to applications/workloads

E/W and N/S Inspection – Centralized

- Best handled via a 3rd Party Firewall
- Aviatrix provides Service Insertion, policy and life-cycle managed of 3rd party firewalls
- Centralized security policy from the 3rd party firewall platform



Distributed L4 at SG/NSG for Intra-VPC/VNet

Centralized NGFW at Transit

Aviatrix Distributed Cloud Firewall (DCF) in Spokes

Ingress/Egress From Spoke – L7 Inspection

Business and Technical Requirements

- InfoSec. mandates that certain or all traffic must go through the NGFW for L7 Inspection
  - Business Drivers: Security, Compliance, Audit, etc.
  - Technical Need: NGFW, DPI, IDS/IPS, etc.
- Existing processes and skillset on specific vendors
  - Compliance achieved using a certain design and feature set
  - Desire to maintain compliance with limited impact

Consumer/
PII Data

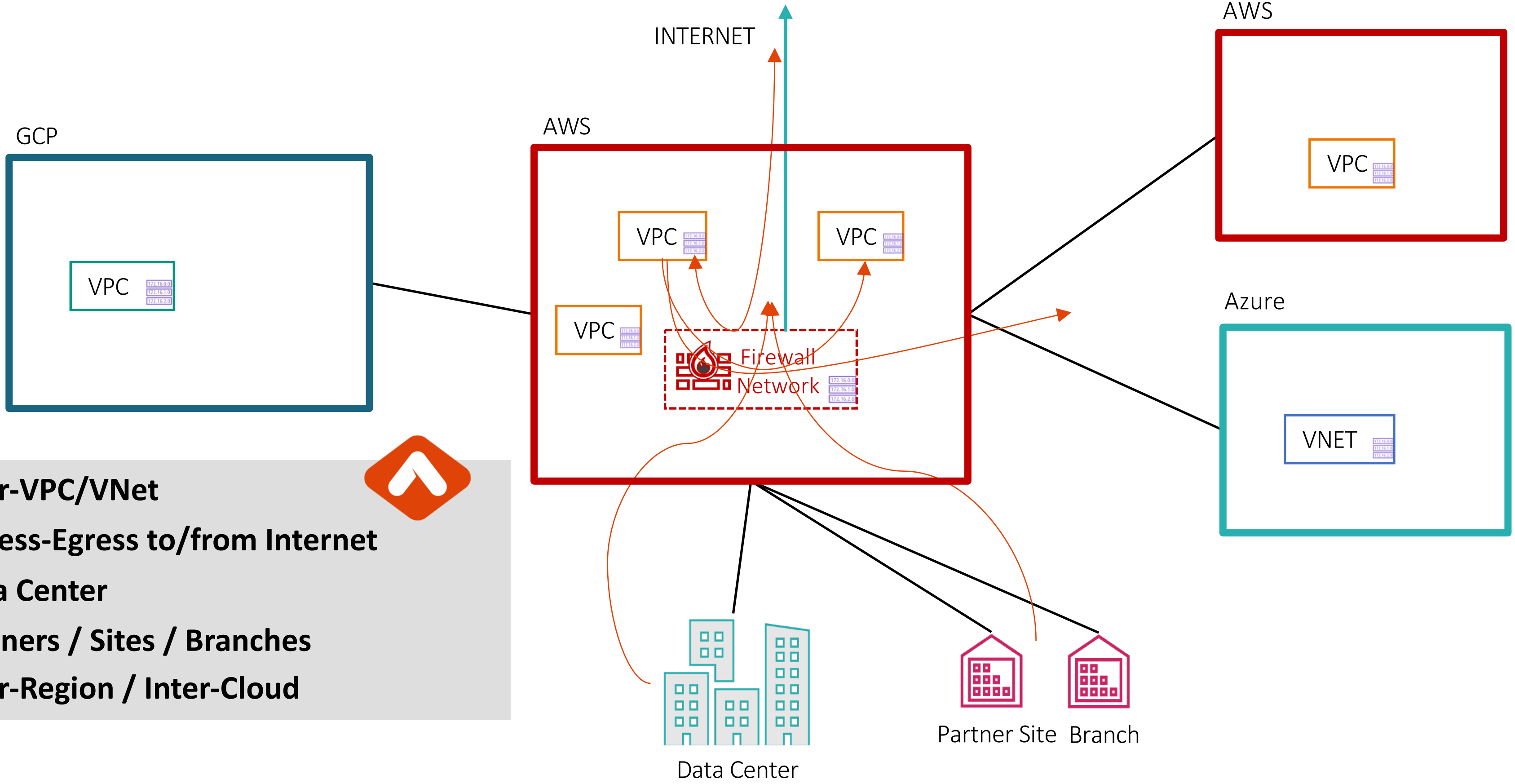
HIPAA
Health Insurance Portability
& Accountability Act

CALIFORNIA
CONSUMER
PRIVACY
ACT OF 2018

PCI DSS
COMPLIANT

General
Data
Protection
Regulation

Traffic Patterns Requiring NGFW



1. **Inter-VPC/VNet**
2. **Ingress-Egress to/from Internet**
3. **Data Center**
4. **Partners / Sites / Branches**
5. **Inter-Region / Inter-Cloud**

Challenges of Service Insertion in the Cloud

Firewall Vendors

- Firewall vendors have repackaged on-prem solutions to cloud
- Not focused to solve cloud networking and challenges
- Expect customer to own routing traffic to and from FWs

Cloud Provider

- Solution which might lack enterprise features you need
- Expect customer to figure out routing traffic to and from FWs
- Lack of visibility and troubleshooting tools

Customer

- Manually figure out routing and troubleshooting
- Many components involved that require individual config/ops (LB, NAT GWs, routes, etc.)
- Lack of visibility and troubleshooting tools reduces efficiency and increases risk

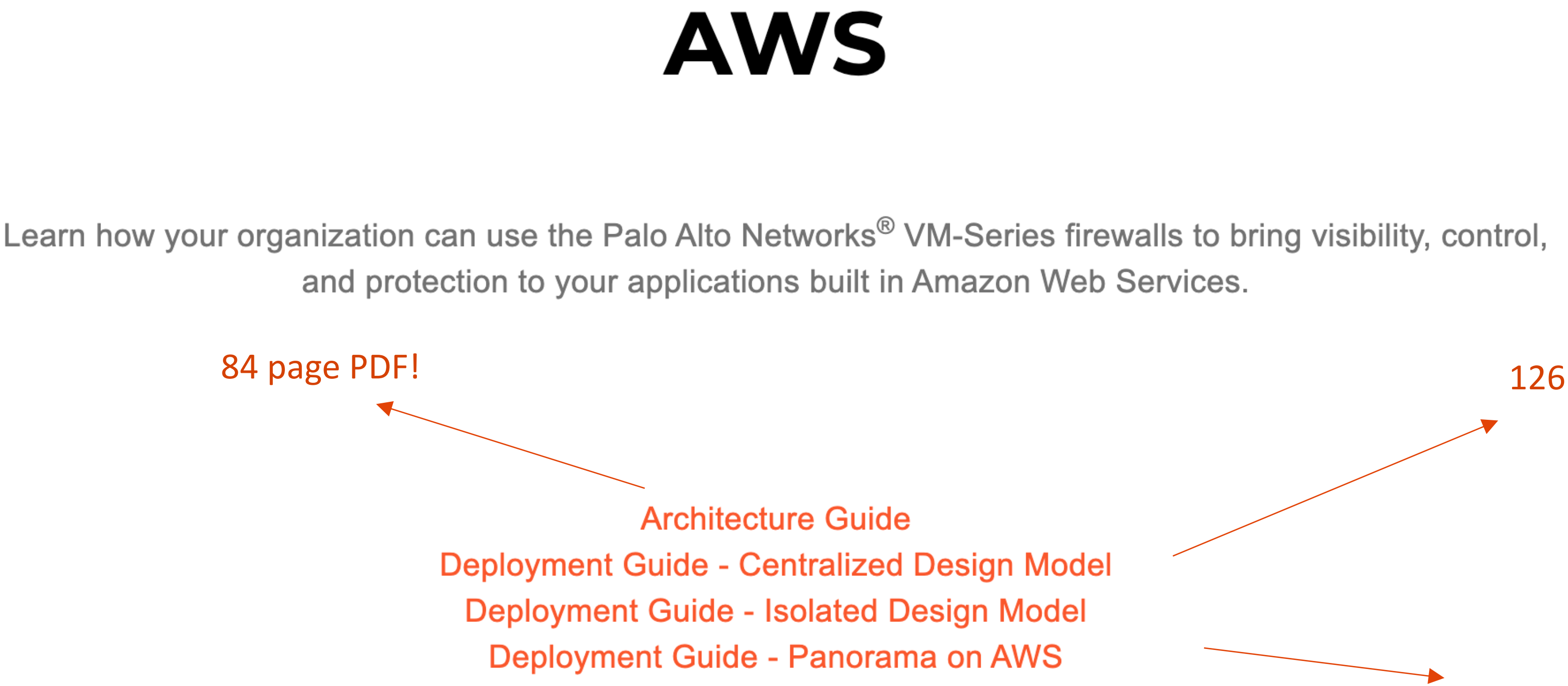
Complexity of Deploying PAN Firewalls in the Cloud

Specific to VM-Series, lots of documentation available

- Choose a cloud
- Read Reference Architecture
- Choose a Deployment Model
- Read Deployment Guide for chosen Deployment Model
- Deploy VM-Series successfully (hopefully)
- Rinse and Repeat …

https://www.paloaltonetworks.com/resources/reference-architectures

Long Reads in One Cloud…



AWS

Learn how your organization can use the Palo Alto Networks® VM-Series firewalls to bring visibility, control, and protection to your applications built in Amazon Web Services.

Architecture Guide
Deployment Guide - Centralized Design Model
Deployment Guide - Isolated Design Model
Deployment Guide - Panorama on AWS

84 page PDF!

126 page PDF!

38 page PDF!

94 page PDF!

Long Reads in Other Clouds…

Azure

Learn how your organization can use the Palo Alto Networks® VM-Series firewalls to bring visibility, control, and protection to your applications built on Microsoft Azure.

Architecture Guide
Deployment Guide - Transit VNet Design Model
Deployment Guide - Transit VNet Design Model: Common Firewall Option
Deployment Guide - Panorama on Azure

~500 pages of reading!

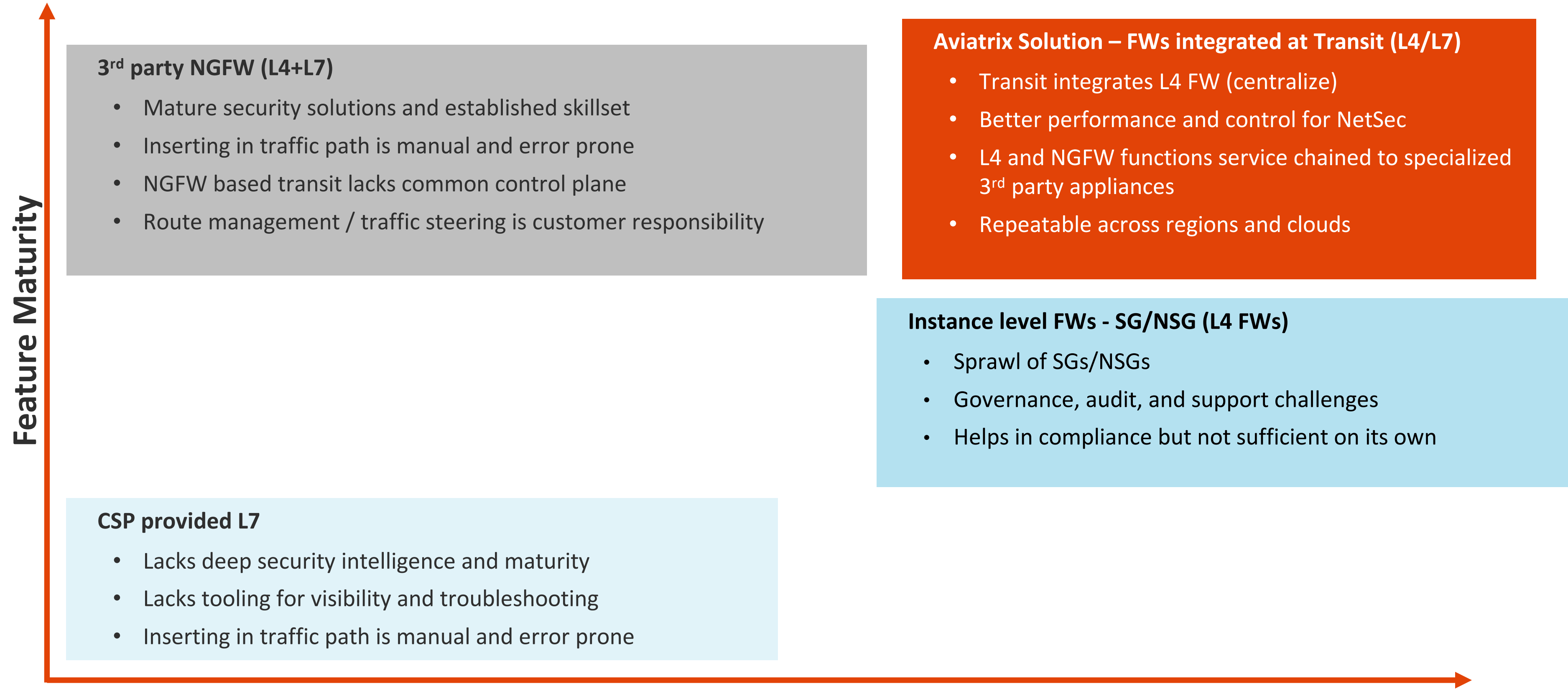
GCP

Learn how your organization can use the Palo Alto Networks® VM-Series firewalls to bring visibility, control, and protection to your applications built on GCP.

Architecture Guide
Deployment Guide - Shared VPC Design Model
Deployment Guide - VPC Network Peering Design Model
Deployment Guide - Panorama on GCP

400+ pages of reading!

Firewall Architecture Options in Public Cloud



3rd party NGFW (L4+L7)

- Mature security solutions and established skillset
- Inserting in traffic path is manual and error prone
- NGFW based transit lacks common control plane
- Route management / traffic steering is customer responsibility

Aviatrix Solution – FWs integrated at Transit (L4/L7)

- Transit integrates L4 FW (centralize)
- Better performance and control for NetSec
- L4 and NGFW functions service chained to specialized 3rd party appliances
- Repeatable across regions and clouds

Instance level FWs - SG/NSG (L4 FWs)

- Sprawl of SGs/NSGs
- Governance, audit, and support challenges
- Helps in compliance but not sufficient on its own

CSP provided L7

- Lacks deep security intelligence and maturity
- Lacks tooling for visibility and troubleshooting
- Inserting in traffic path is manual and error prone

aviatrix

ACE

Aviatrix Certified Engineer

Aviatrix Transit FireNet

Aviatrix Encrypted Transit Firewall Network

- Scale out, multi-AZ FW deployments
- Automated route management
  Segmentation and Connection Policies
- Deep visibility and operational capabilities
- Repeatable architecture, across regions and clouds

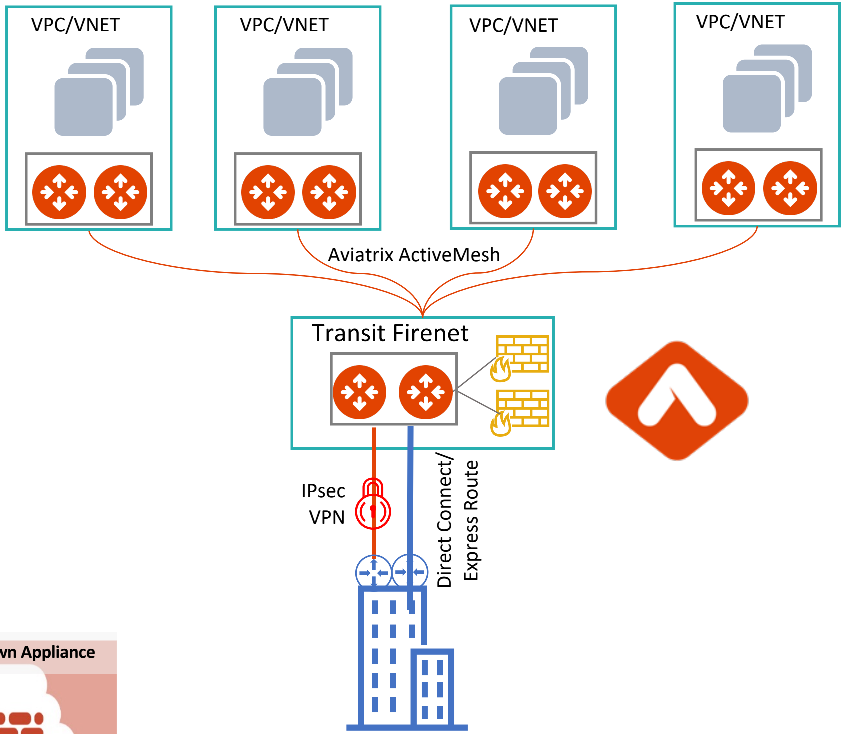
paloalto NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD

F5

FORTINET

Bring Your Own Appliance



Aviatrix Encrypted Transit Firewall Network

1. From the Aviatrix CoPilot you enable FireNet (or through TF)

2. Aviatrix Controller deploys the Firewalls

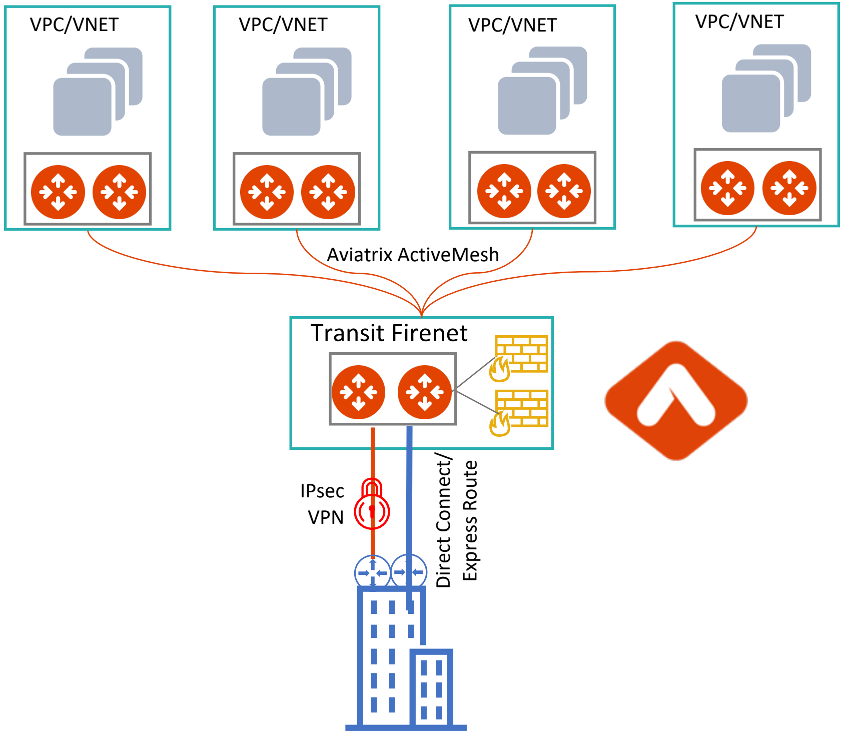
3. Aviatrix Controller configures the interfaces and routing entries at the Firewalls

4. No SNAT, IPsec, BGP, or any other elements are required to insert the FWs into the traffic path

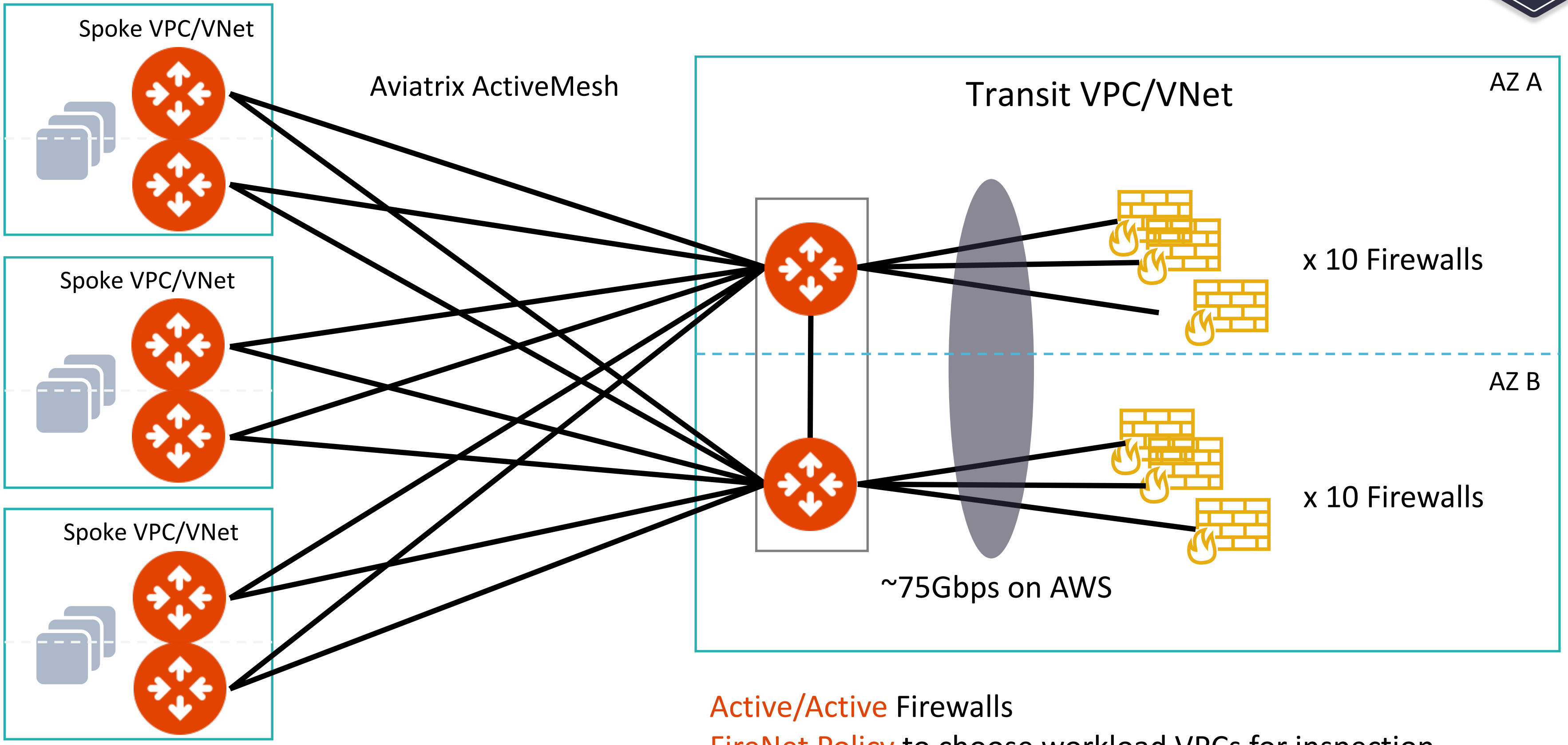
5. Aviatrix Controller ensures all the Spokes and other connected networks which are marked for inspection have their traffic inspected by the FW

6. Aviatrix Controller monitors the health of the FW instances and ensures the traffic is only forwarded to "up" Firewalls

7. Aviatrix GWs or a native cloud LB incorporated into the overall design ensure that the traffic is correctly load balanced to all available FWs, while maintaining the session stickiness



Aviatrix Transit FireNet Performance

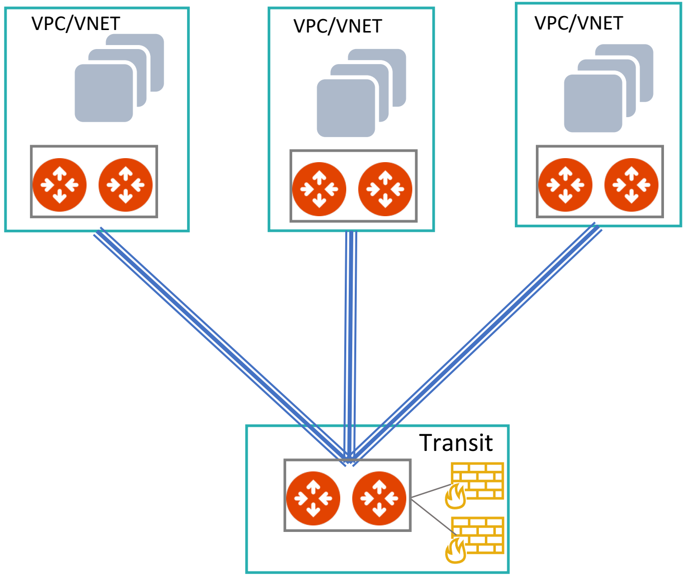


Active/Active Firewalls

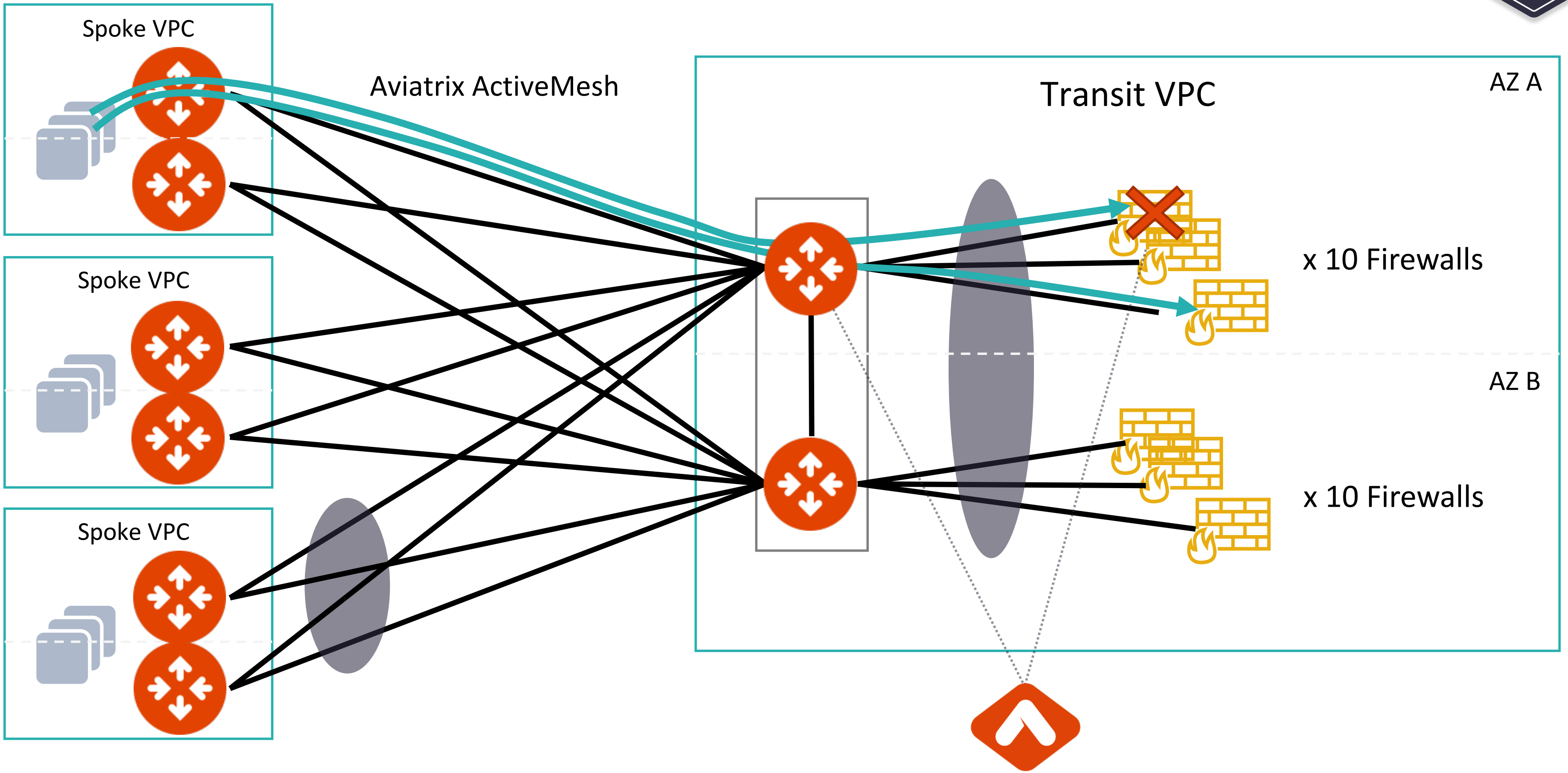
FireNet Policy to choose workload VPCs for inspection

Aviatrix Transit FireNet Load Balancing and Failover

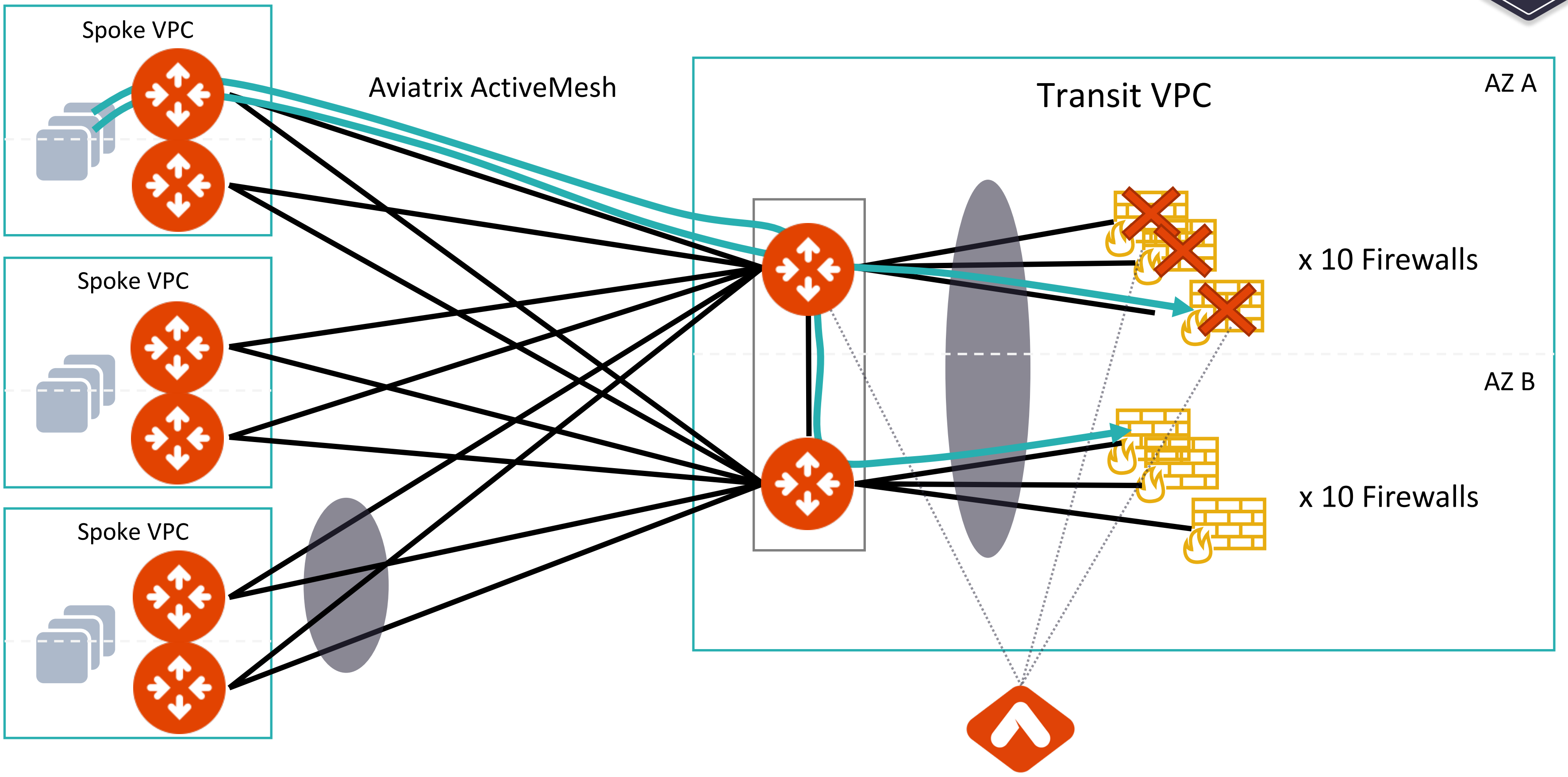
- The Aviatrix Controller monitors the health of the Firewalls
- Controller periodically checks Firewall instance health
- Session stickiness is maintained
  - Existing sessions on working firewalls are not disturbed
  - AKA resilient hashing



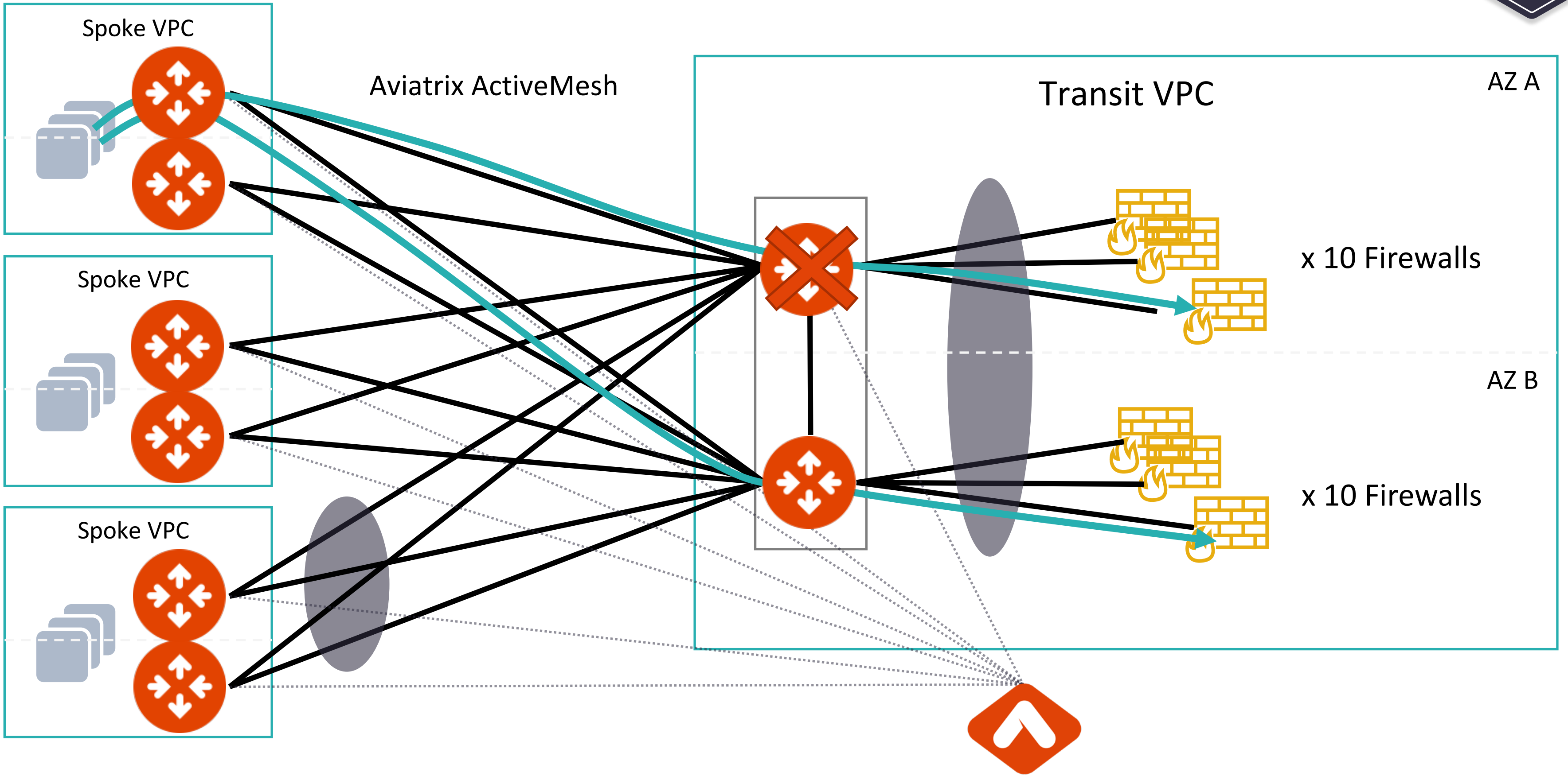
Aviatrix Transit FireNet Failover



Aviatrix Transit FireNet Failover



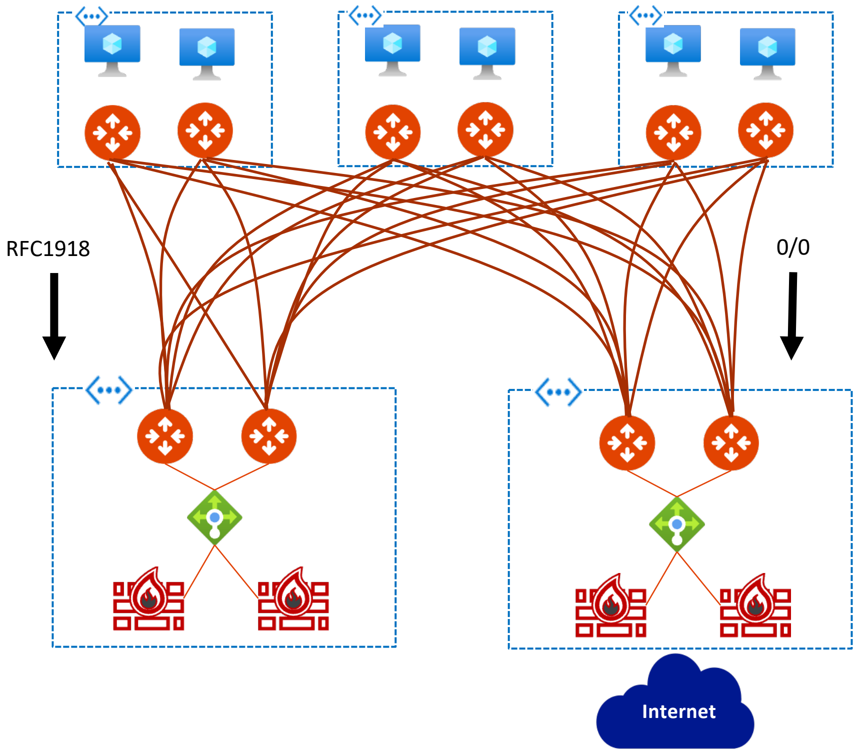
Aviatrix Transit FireNet Failover



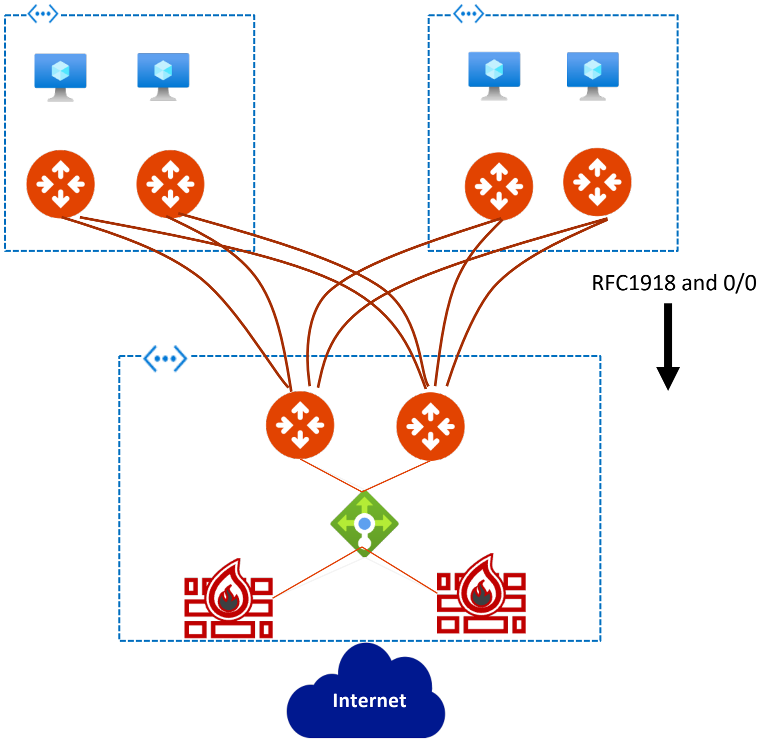
FireNet Architecture Options (Azure Example)

Each firewall set can scale independently based on need

Dual Hub FireNet



Single Hub FireNet



Aviatrix Multicloud Service Insertion/Chaining

Multiple Design Patterns

- Single Transit FireNet (E-W, Ingress and Egress)
- Dedicated FireNets for E-W and Egress (shown)
- Dedicated Ingress VPC via E-W FW (purple box)

Firewall Service Insertion

- E-W / Egress / Ingress / all traffic
- High Performance Encryption (HPE)
- Active / Active – Across AZs
- No IPsec / No BGP / No SNAT required

Automated Control and Management

- Repeatable architecture across regions/clouds
- Centralized firewall deployment
- Vendor API integration
- UDR and VPC Route propagation

Improved Failure Detection and Failover

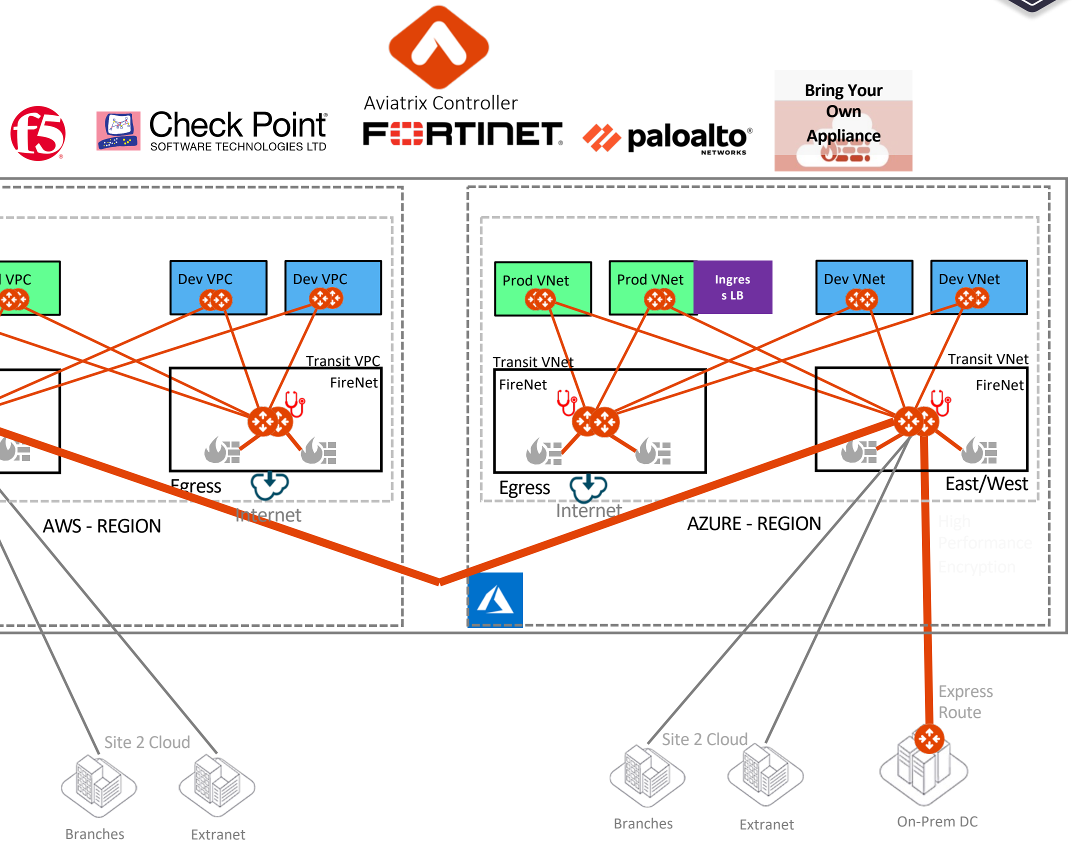
- Health Check monitoring

Forwarding Algorithm Options

- Intelligent traffic steering and firewalling based on traffic type
- 5-tuple and 2-tuple

Firewall Bootstrap Support

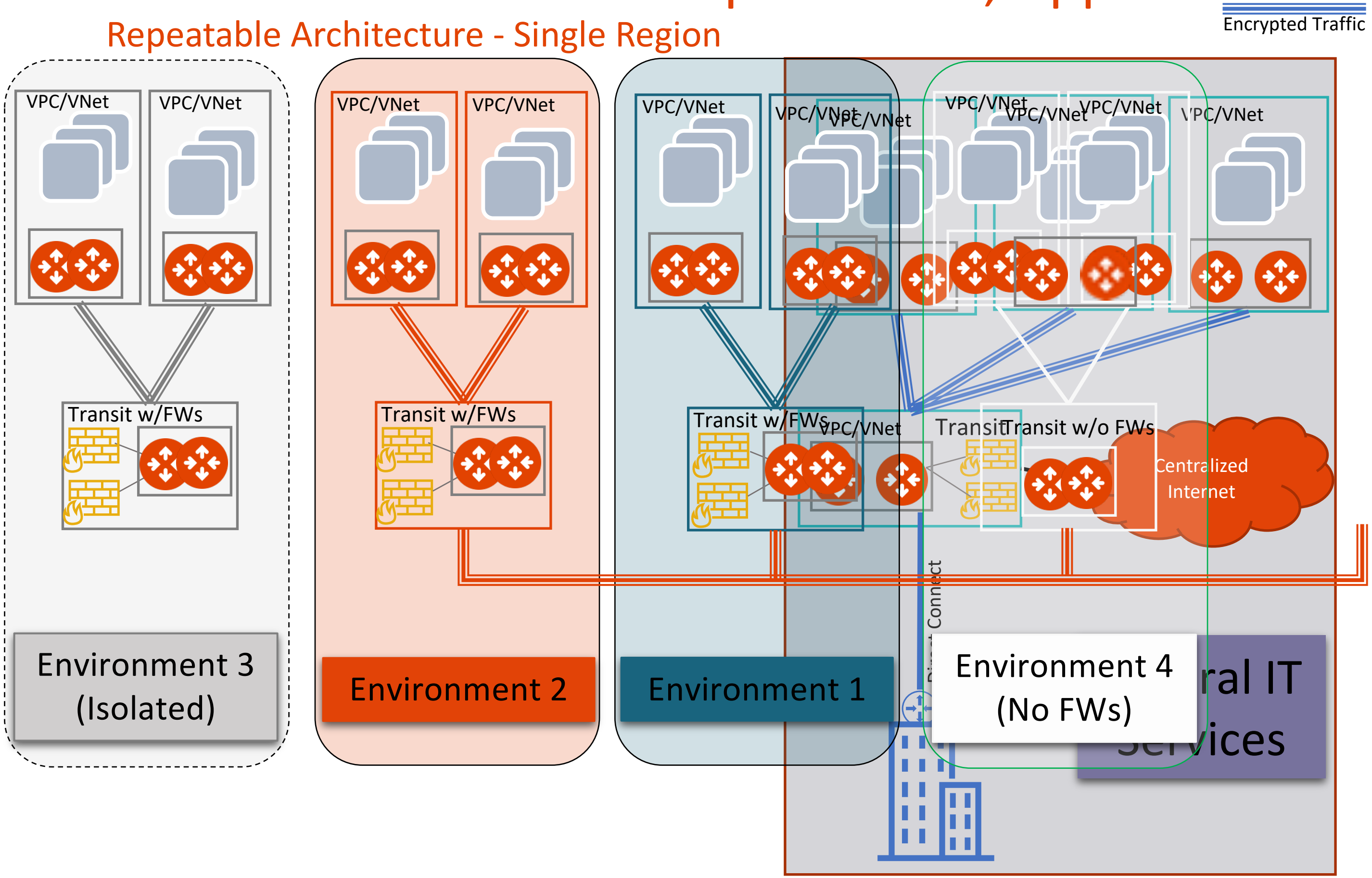
- Firewall zero-touch deployment capability in Azure and AWS



FireNet Terraform Demo: https://youtu.be/FFuDo8AZxmo

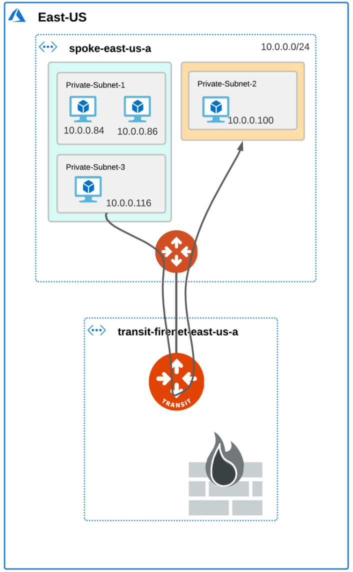
Isolation and Control for Departments, Apps and BUs

Repeatable Architecture - Single Region

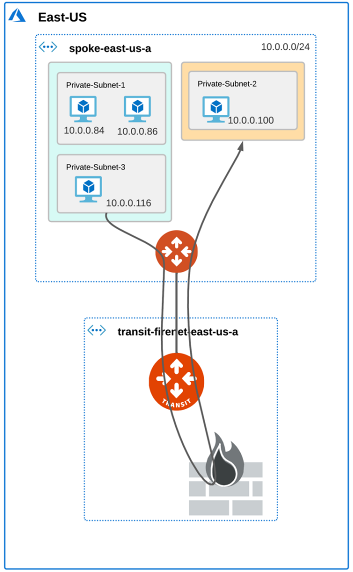


Subnet-level Inspection in Azure (released in 6.6.5404)

- *Subnet Groups* -- Logical grouping of subnets in a VNet
- Local to VNet -- unlike segmentation domains, does not span across VNets
- Subnet Group name does not have to be unique across VNets
- Subnet Groups may or may not have an inspection policy



No Inspection Policy



Inspection Policy

- ○ If a group has inspection policy, traffic redirected to firewall, otherwise it just traverses the transit gateway

https://docs.aviatrix.com/HowTos/transit_subnet_inspection_azure.html

aviatrix

ACE

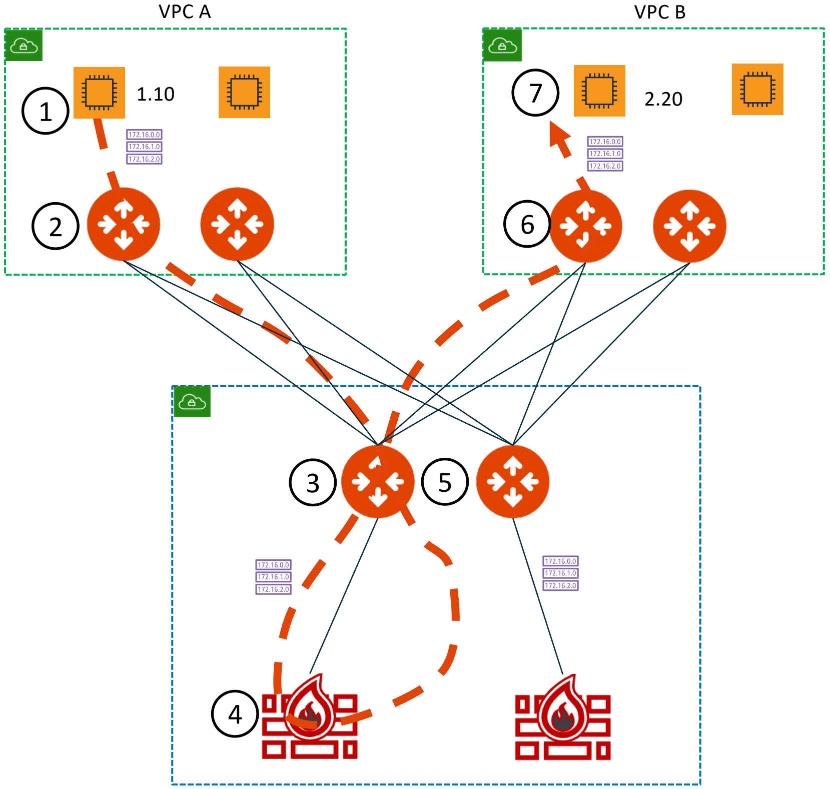
Aviatrix Certified Engineer

Aviatrix Transit FireNet Packet Walk

FireNet Packet Walkthrough – AWS Example

A Host 1.10 communicating with 2.20 with VPC A inspected via FireNet

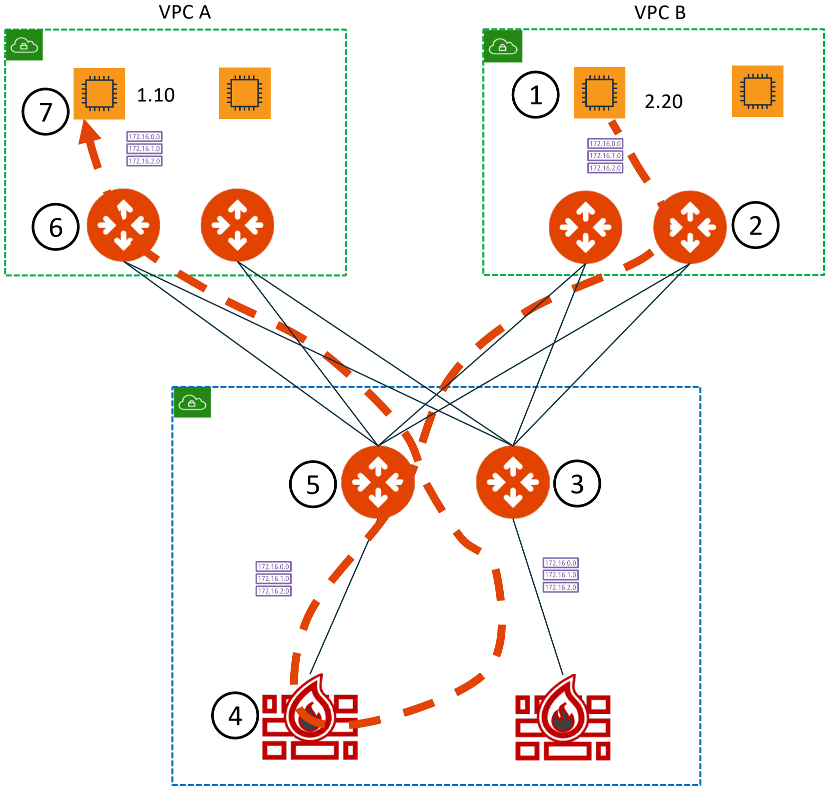
1. The local route table for 1.10 has RFC1918 routes pointed to its local gateway
2. The local Aviatrix spoke gateway will ECMP traffic with 5-tuple hash to one of the Aviatrix Transit Gateways
3. The Aviatrix Transit Gateway receiving the flow will check PBR rules to determine if either source or destination requires FireNet. If a match, traffic is redirected to the one of the available FWs (it can be in the same AZ or a different AZ – when it's in a different AZ, Transit GW sends the traffic first to the other Transit GW).
4. The Firewall selected will process the packet and send the traffic back to its local Transit Gateway.
5. The Aviatrix Transit Gateway will receive the processed packet and PBR this traffic back into the egress interface and ECMP traffic with 5-tuple hash towards the destination spokes.
6. The spoke gateway will receive the traffic and route the traffic out its local interface to the VPC route table. Note that this GW may not be in the same AZ as the destination instance.
7. The destination will receive the original traffic and see this as native VPC communication flow.



FireNet Packet Walkthrough – AWS Example

Return Flow: 1.10 communicating with 2.20 with VPC A inspected via FireNet

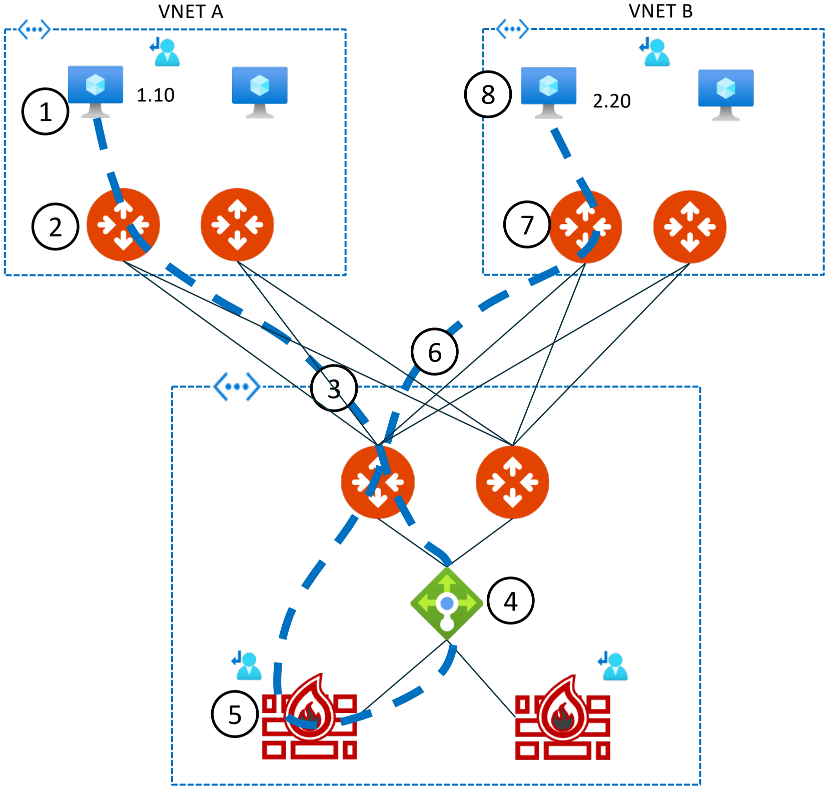
1. The local route table for 2.20 has RFC1918 routes pointed to its local spoke gateway for return traffic.
2. The local Aviatrix spoke gateway will ECMP traffic with 5-tuple hash to one of the Aviatrix Transit Gateways
3. The Aviatrix Transit Gateway receiving the traffic will pass the traffic to the the same FW which handled the initial flow to maintain symmetry (directly or via another Transit GW).
4. The stateful Firewall will process the return traffic and route the traffic back to its designated gateway.
5. The Aviatrix gateway will ECMP traffic with 5-tuple hash to one of the destination spoke gateways.
6. The destination spoke gateway will route this traffic out its local interface to the native VPC route table.
7. The original source will receive the return traffic and see this as native VPC communication flow.



FireNet Packet Walkthrough – Azure Example

A Host 1.10 communicating with 2.20 with VNET A inspected via FireNet

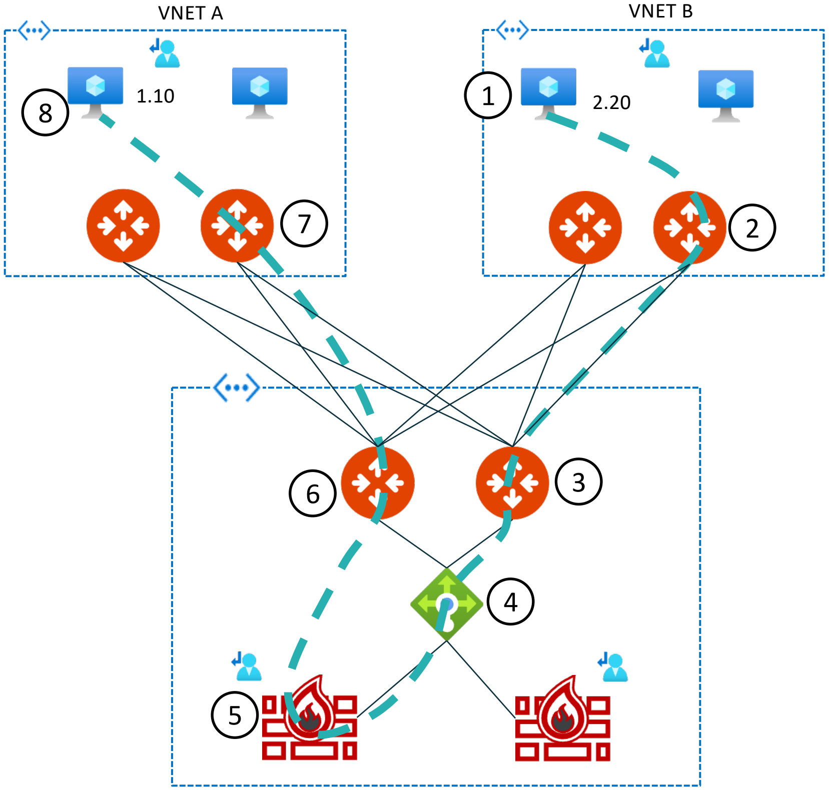
1. The local route table for 1.10 has RFC1918 routes pointed to its local gateway
2. The local Aviatrix spoke gateway will ECMP traffic with 5-tuple hash to one of the Aviatrix Transit Gateways
3. The Aviatrix Transit Gateway receiving the flow will check PBR rules to determine if either source or destination requires FireNet. If a match, traffic is redirected to Azure ILB.
4. The Azure ILB will perform a 5-tuple hash to send the traffic to one of the backend pool members.
5. The Firewall selected will process the packet and send the traffic back to its defined Transit Gateway.
6. The Aviatrix Transit Gateway will receive the processed packet and PBR this traffic back into the egress interface and ECMP traffic with 5-tuple hash towards the destination spokes.
7. The spoke gateway will receive the traffic and route the traffic out its local interface to the Azure VNET route table.
8. The destination will receive the original traffic and see this as native Azure communication flows.



FireNet Packet Walkthrough – Azure Example

Return Flow: 1.10 communicating with 2.20 with VNET A inspected via FireNet

1. The local route table for 2.20 has RFC1918 routes pointed to its local spoke gateway for return traffic.
2. The local Aviatrix spoke gateway will ECMP traffic with 5-tuple hash to one of the Aviatrix Transit Gateways
3. The Aviatrix Transit Gateway receiving the traffic will pass the traffic to the ILB. The gateway will PBR the traffic back to the ILB for FireNet.
4. The Azure load balancer will hash the traffic however, the reverse flow hash will match the initial flow to ensure symmetry.
5. The stateful Firewall will process the return traffic and route the traffic back to its designated gateway.
6. The Aviatrix gateway will ECMP traffic with 5-tuple hash to one of the destination spoke gateways.
7. The destination spoke gateway will route this traffic out its local interface to the native Azure route table.
8. The original source will receive the return traffic and see this as native Azure communication flows.



aviatrix

ACE

Aviatrix Certified Engineer

Next: Lab 7 - FireNet