Features Overview

PART 1/2

ACE Solutions Architecture Team

Overview

Transit

Network Segmentation

Distributed Cloud Firewall

Secure Egress

High Performance Encryption

Overview

Aviatrix Cloud Network Platform Software

Not a SaaS or Managed Service. It's Yours.

Terraform Single Multicloud Provider

Centralized Automation, Orchestration and Control Plane

1 **Aviatrix Controller**

2 **Aviatrix Gateways**

Cloud Fabric (*Distributed Data Plane*)

Cloud Networking Abstraction

Native Cloud Constructs

API

3

API

Basic Cloud Network and Security

aws

ORACLE

Alibaba Cloud

FORTINET

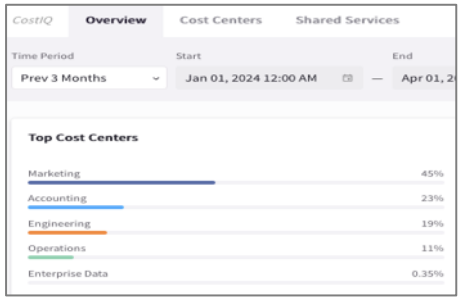
Check Point SOFTWARE TECHNOLOGIES LTD.

paloalto NETWORKS

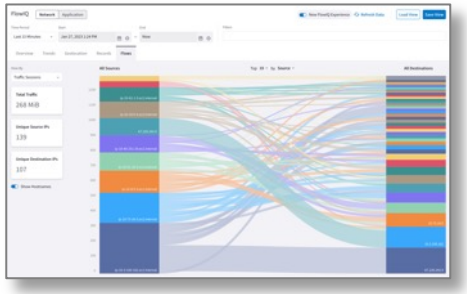
Service Insertion and Chaining

4 **Aviatrix CoPilot**

Centralized Management Plane

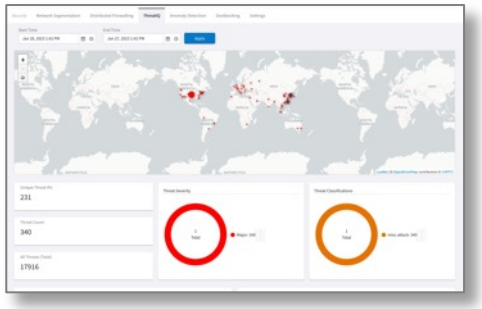


Multicloud Operational Visibility



FlowIQ Multicloud Traffic Flow Analysis

Multicloud Dynamic Topology Mapping



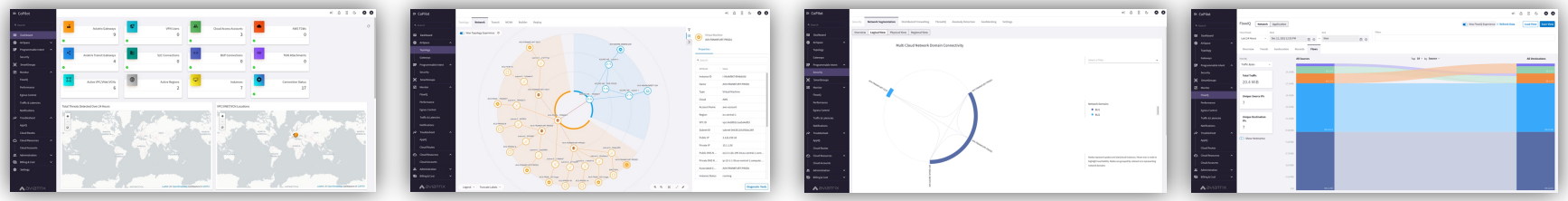
ThreatIQ with ThreatGuard Distributed Threat Visibility and Control

aviatrix

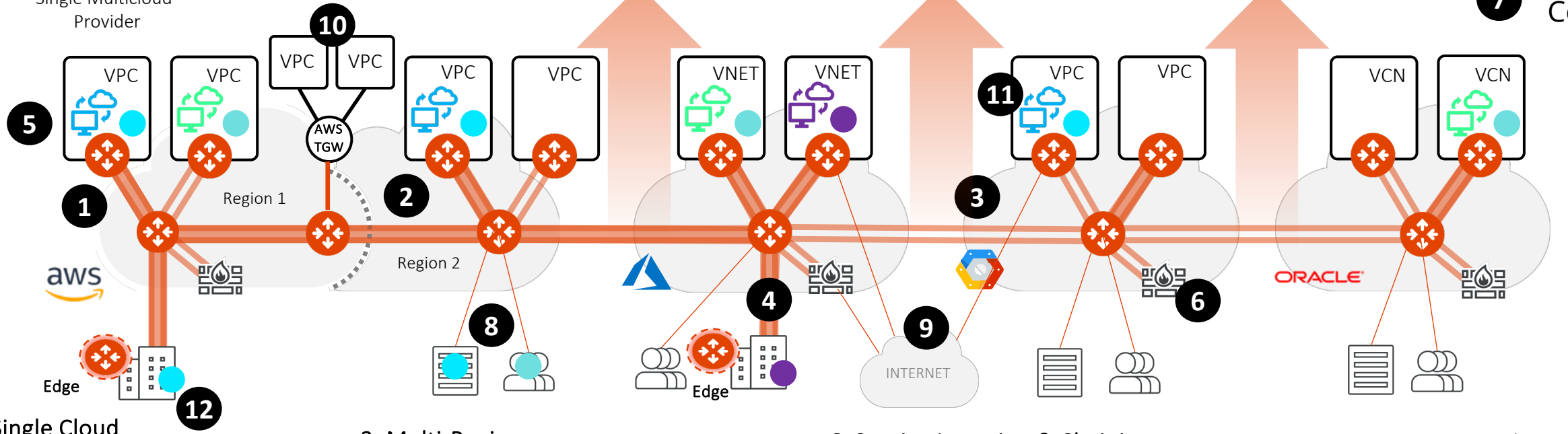
Aviatrix – Foundation of Your Multicloud Networking and Security

Aviatrix Controller

Terraform
Single Multicloud Provider



Aviatrix CoPilot



1. Single Cloud
   Multi-Account
   High-Availability (Active-Active)
   End-to-End Encryption
   Network Correctness

2. Multi-Region

3. Multicloud Repeatable Design

4. High-Performance Encryption

5. Network Segmentation

6. Service Insertion & Chaining

7. Enterprise Operational Visibility

8. Secure Cloud Access

9. Secure Ingress and Egress

10. Cloud-Native

11. Distributed Cloud Firewall

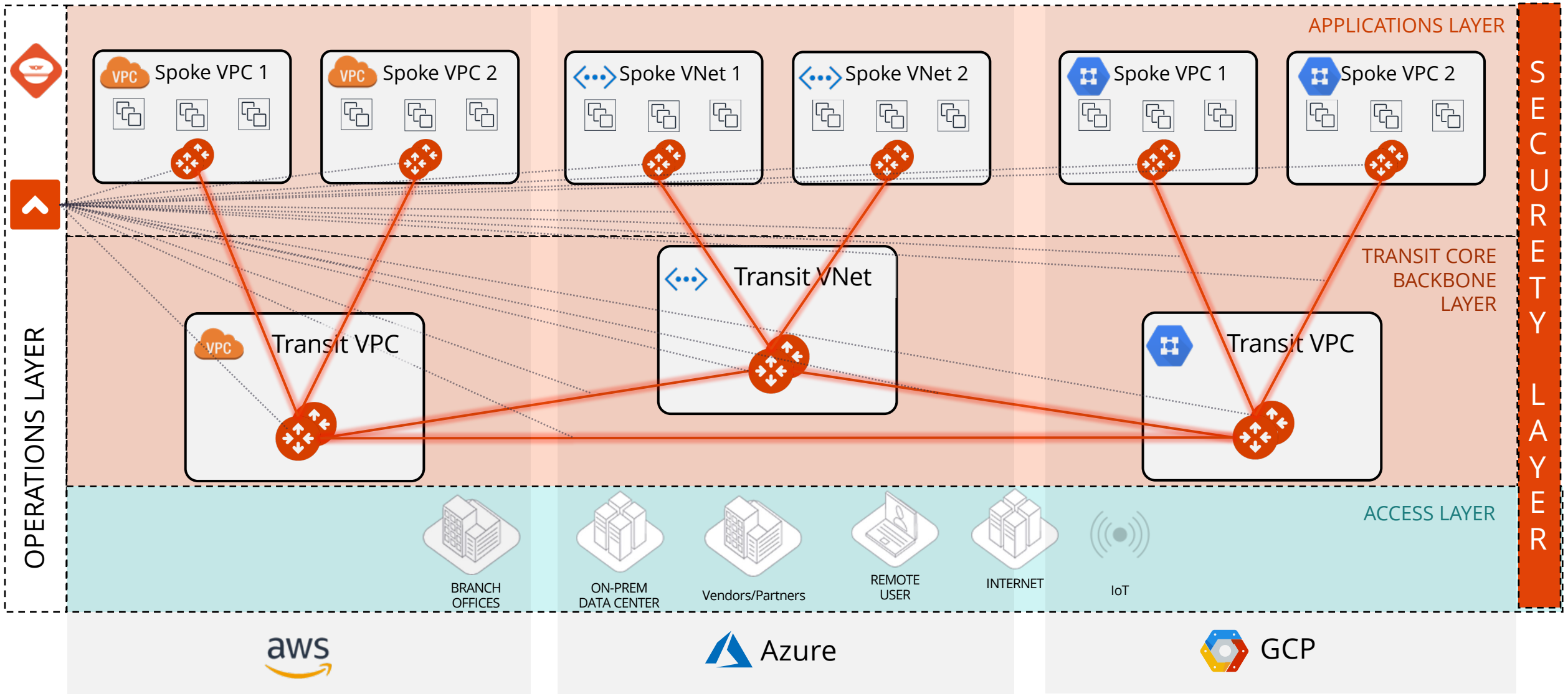
12. Aviatrix Edge

Transit Networking

With Dynamic Routing and Traffic Engineering

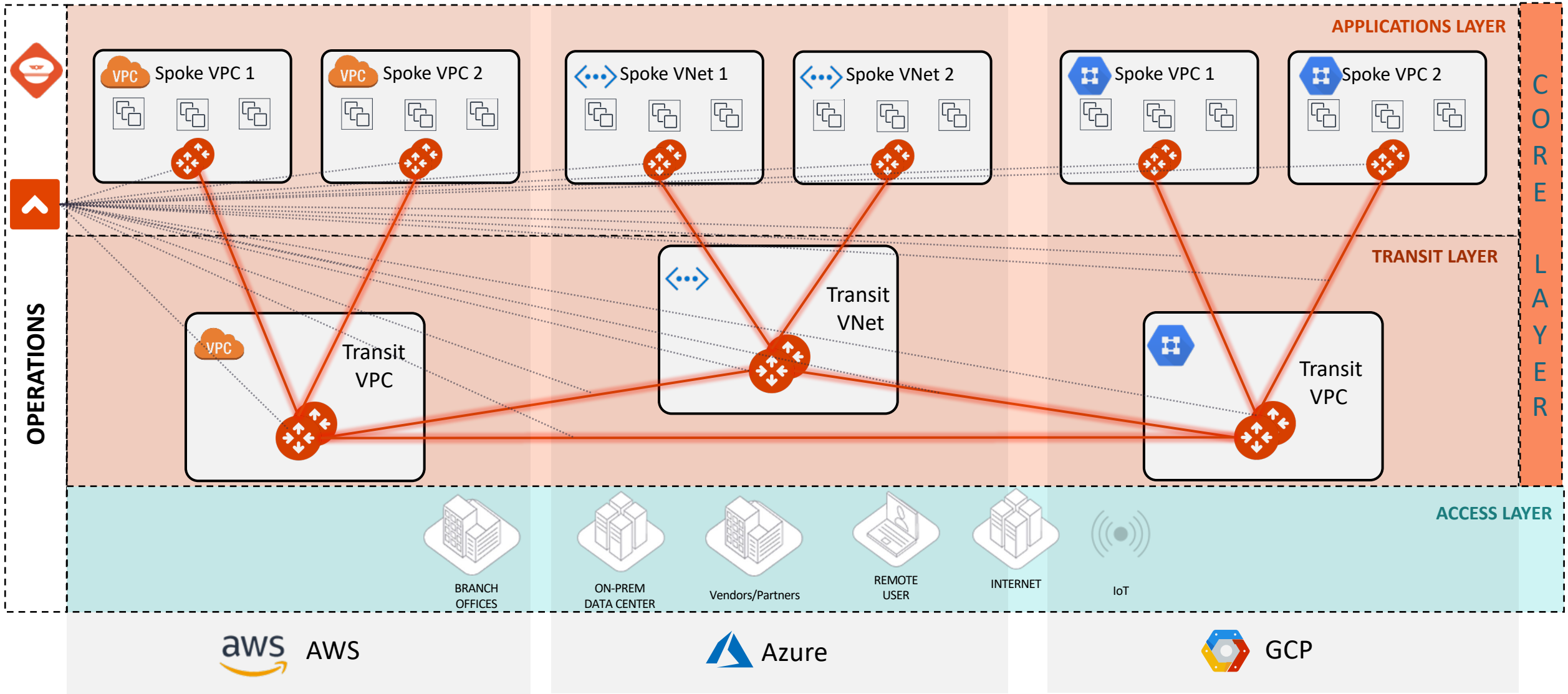
aviatrix®

Aviatrix Transit Network

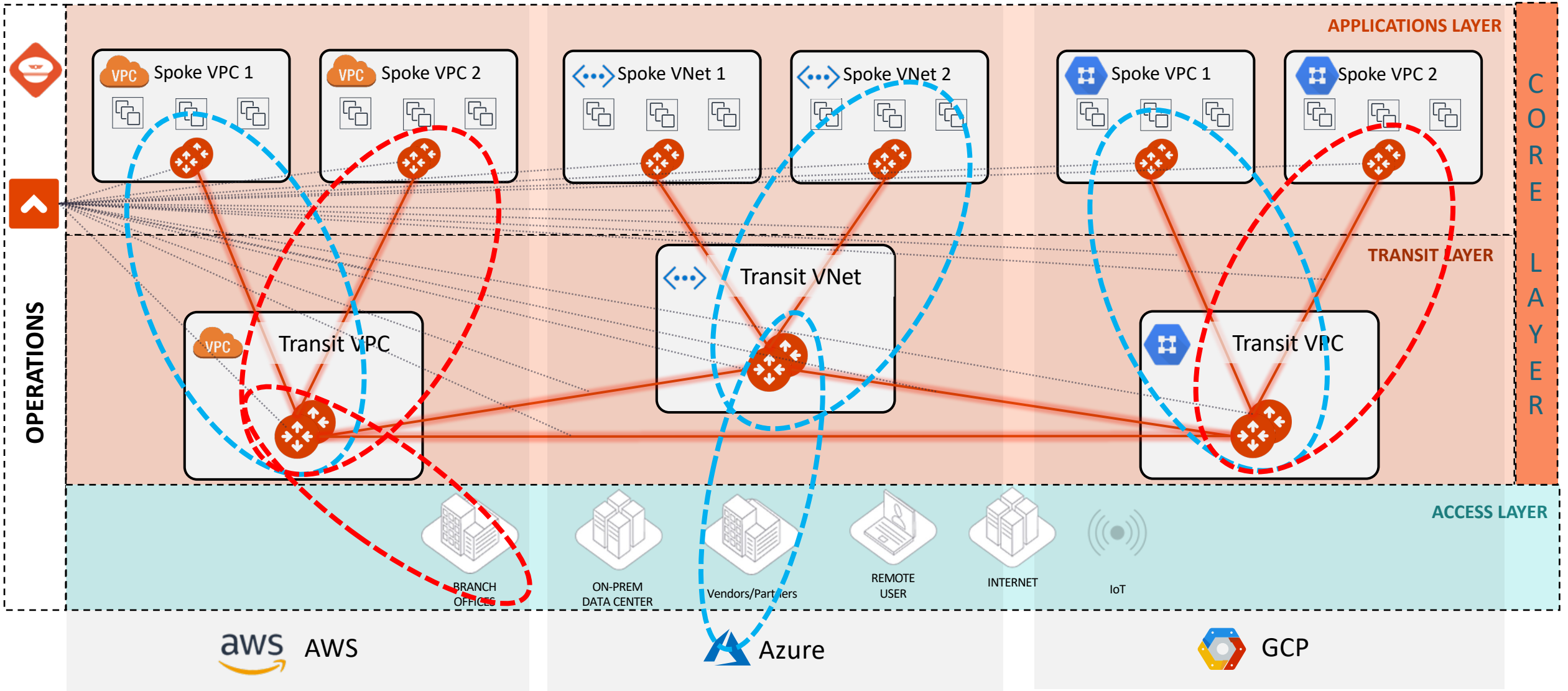


Network Segmentation

MCNA Deployment: the Foundations

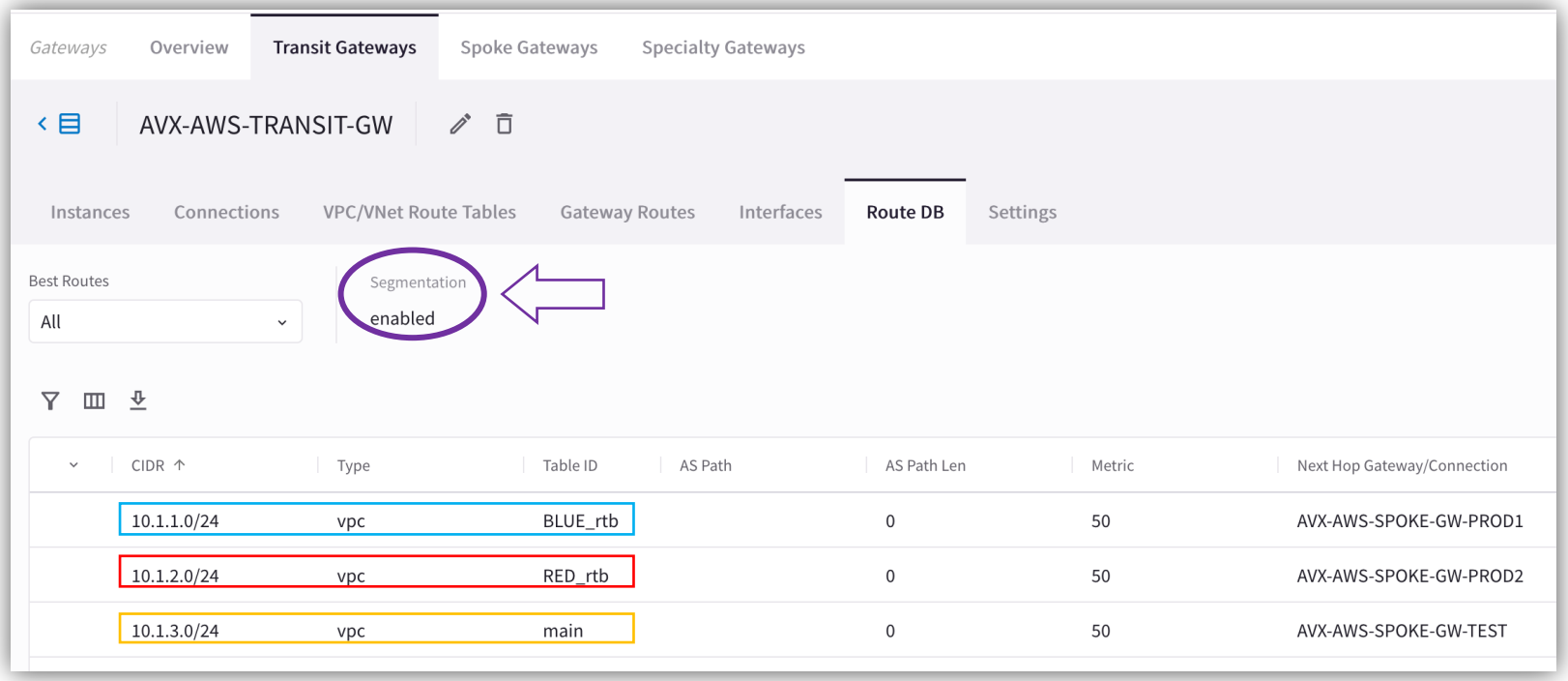


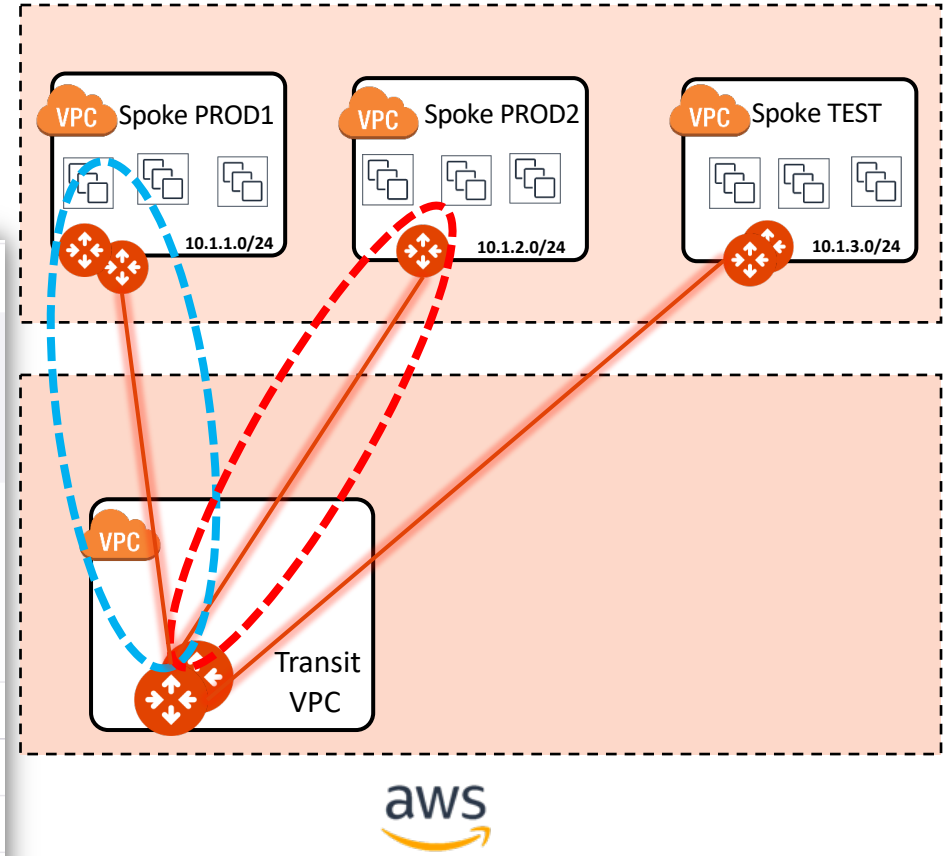
Global Segmentation with Network Domains



Order of Operations for activating the Network Segmentation

1) Enable Network Segmentation on the relevant Transit Gateway(s)
2) Create Network Domains (aka Segments)
3) Associate Spoke Gateways and/or Site2Cloud connections to the Network Domains
4) Apply the Connection Policy (*optional*)





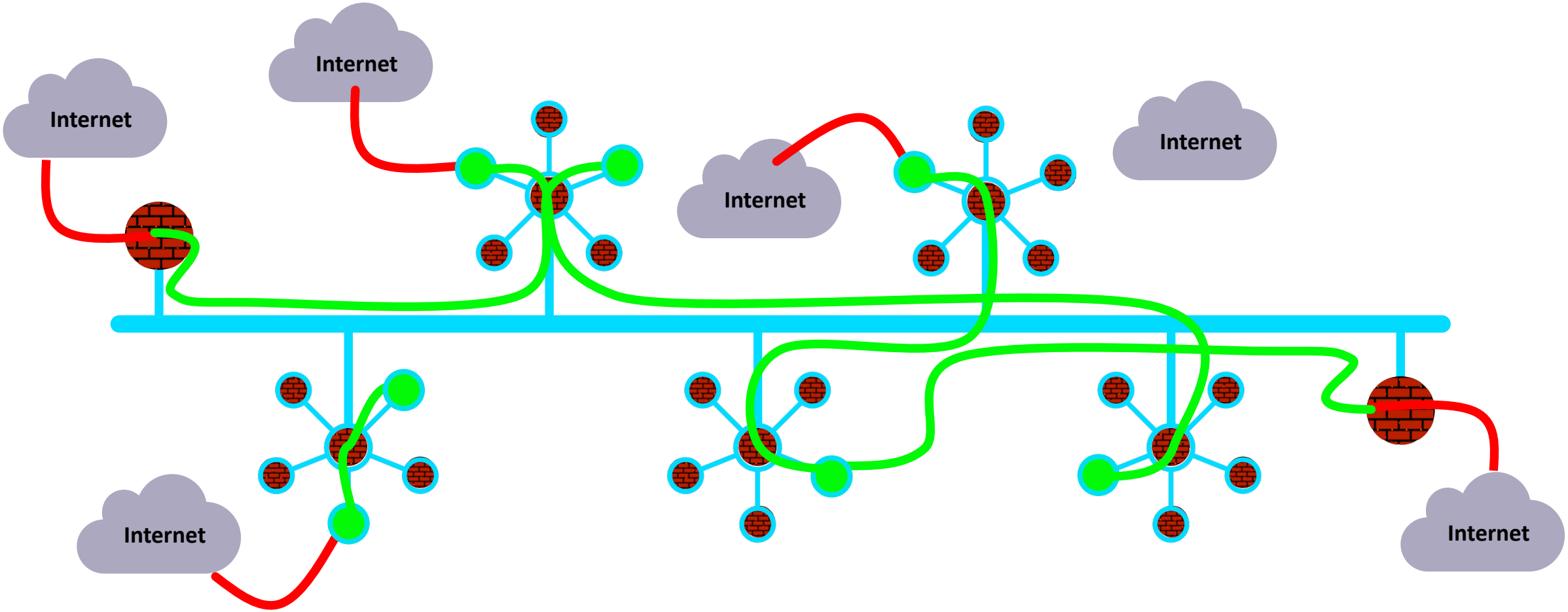
PATH: COPILOT > Cloud Fabric > Gateways > Transit Gateways > select the relevant GW > **Route DB** (equivalent of RIB)

Distributed Cloud Firewall

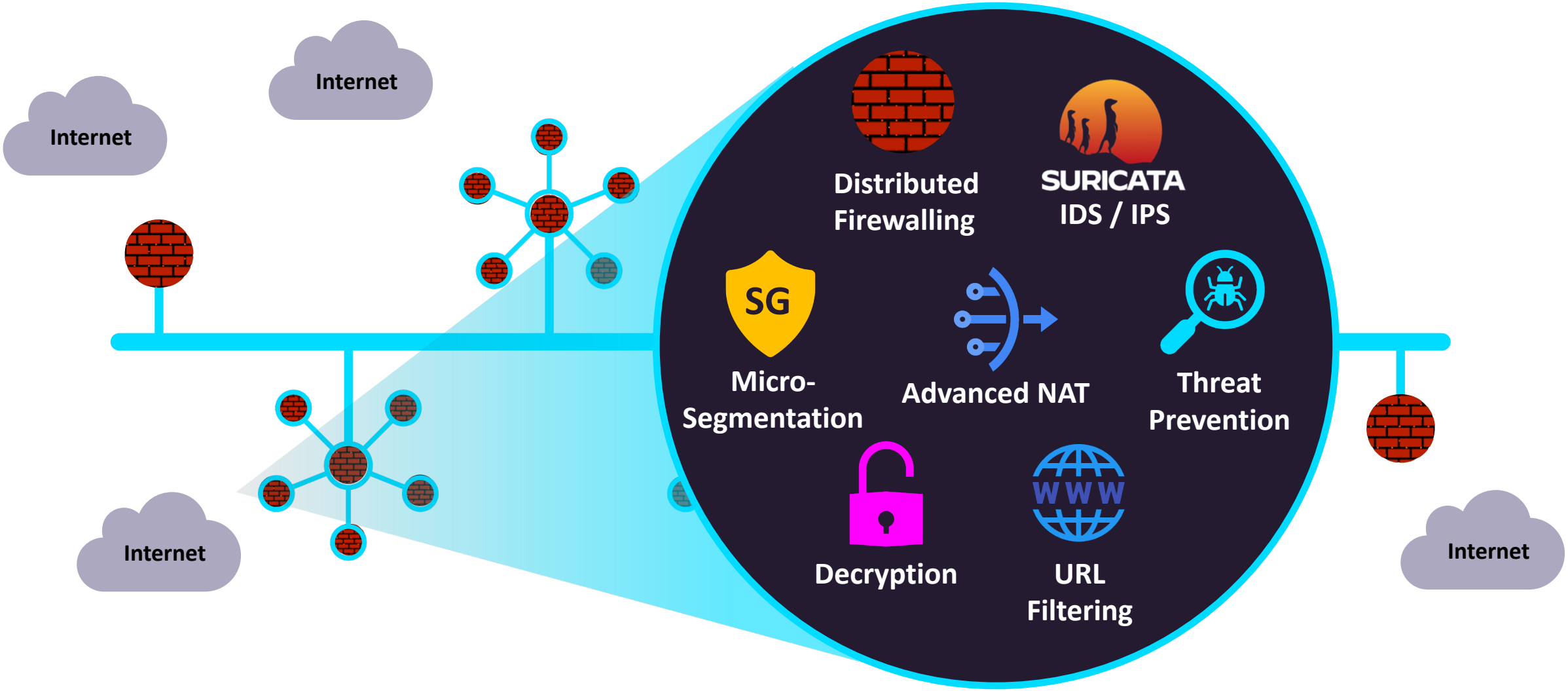
Aviatrix DCF

aviatrix

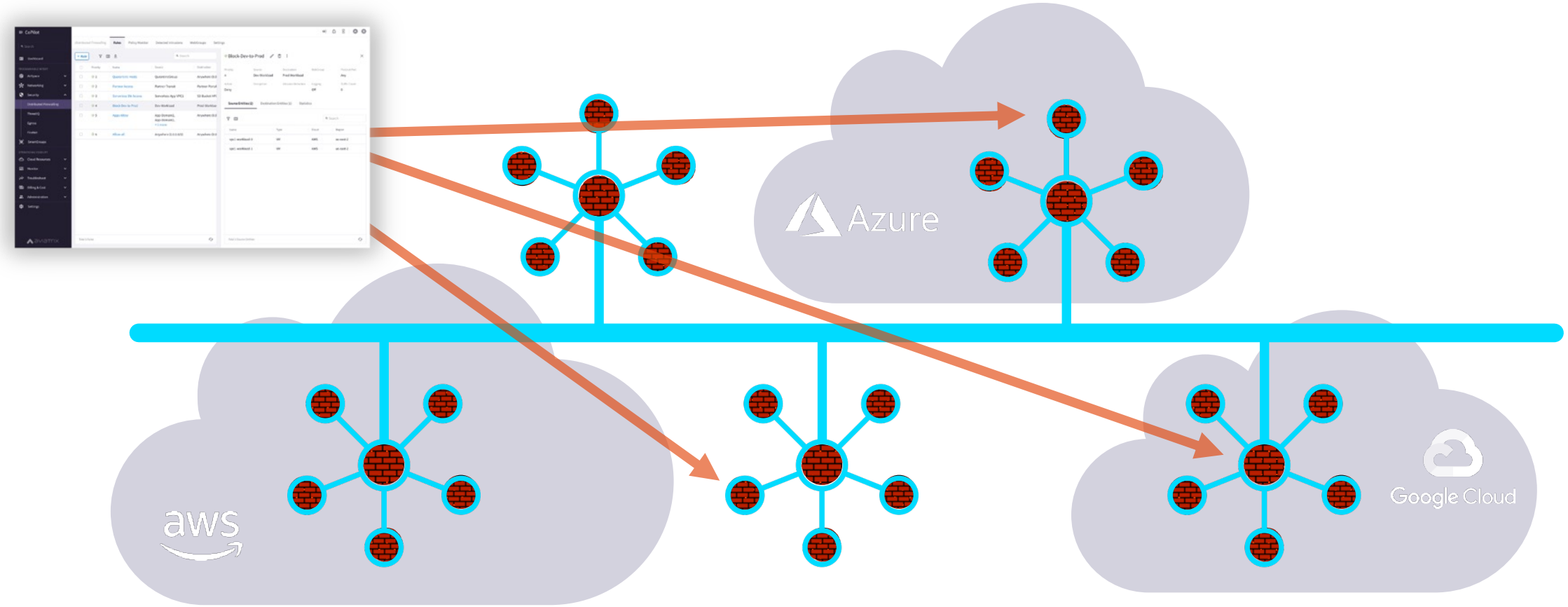
Aviatrix DCF Centrally Managed, with Distributed Inspection & Enforcement…



And, What If it was more than just firewalling…

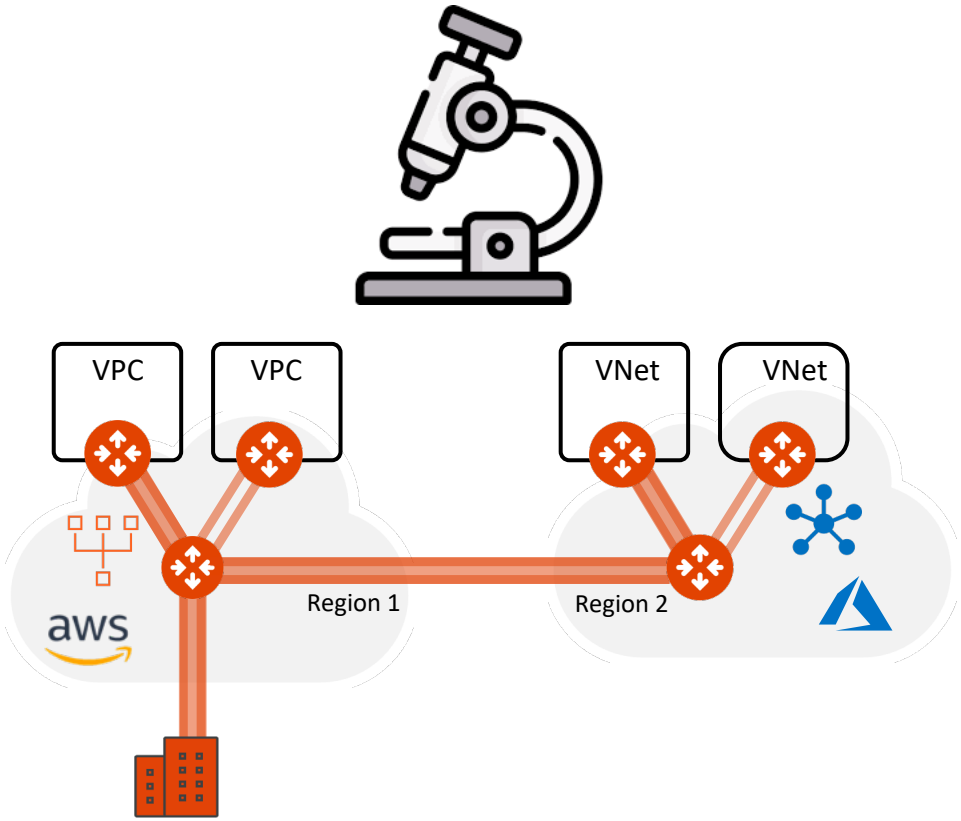


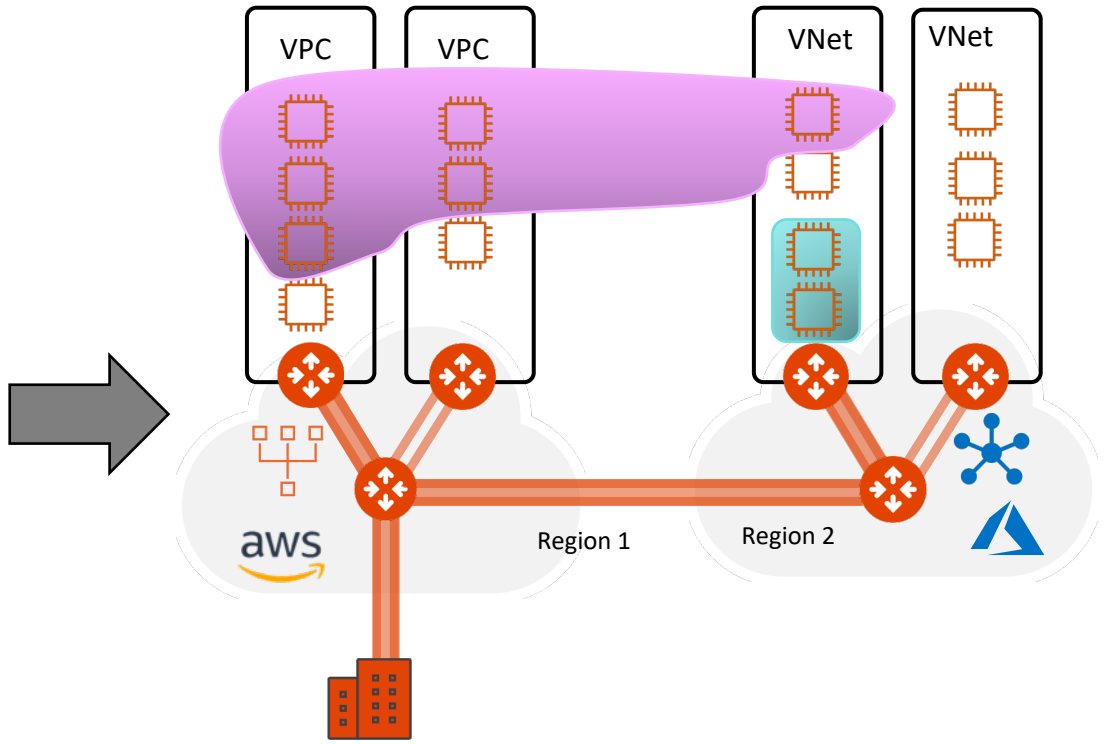
A Distributed Cloud Firewall…

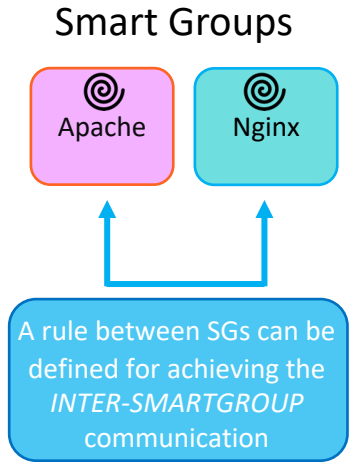


Where and How Policies Are Enforced Is Abstracted…

Distributed Firewalling: Intra-rule vs. Inter-rule



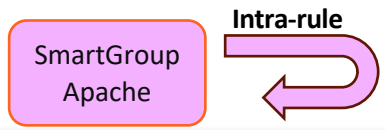


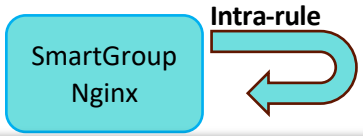


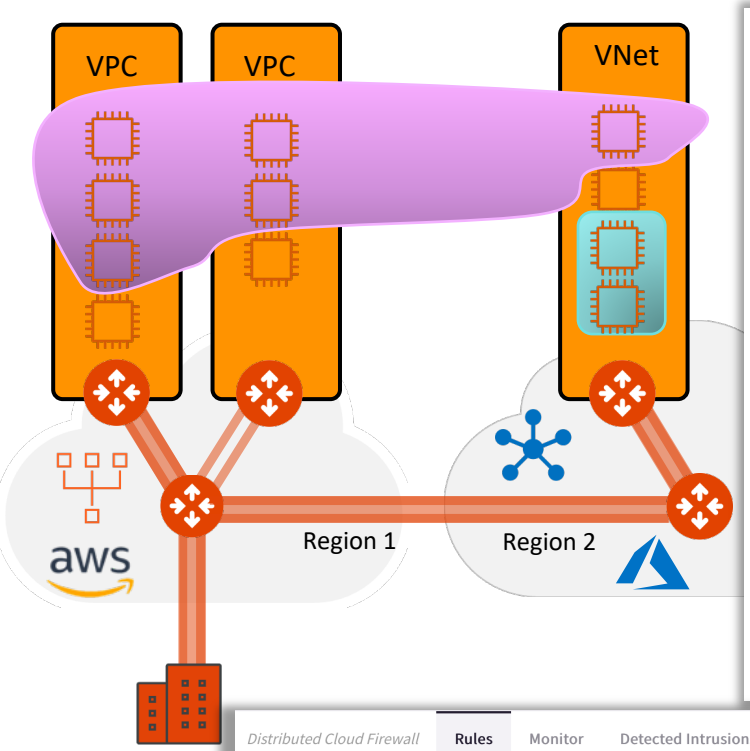
- **INTRA-RULE**: is defined within a Smart Group, for dictating what kind of traffic is allowed/prohibited among all the instances that belong to that Smart Group

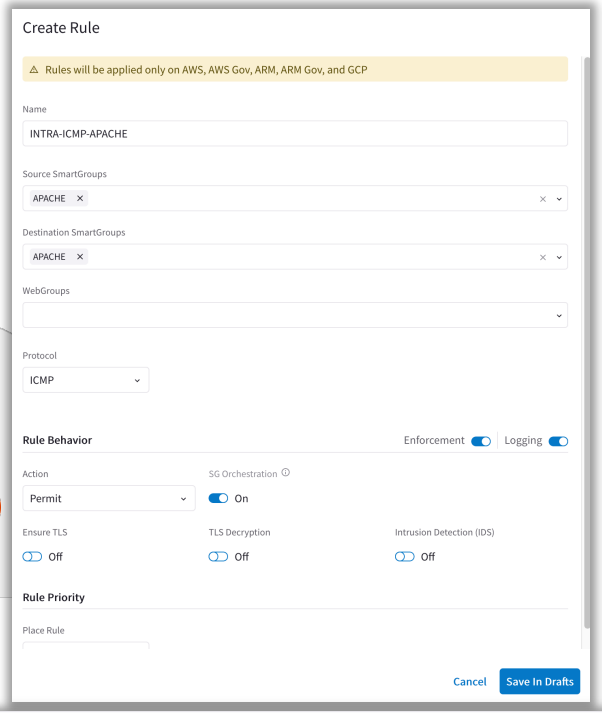
- **INTER-RULE:** is defined among Smart Groups, for dictating what kind of traffic is allowed/prohibited among two or more Smart Groups.

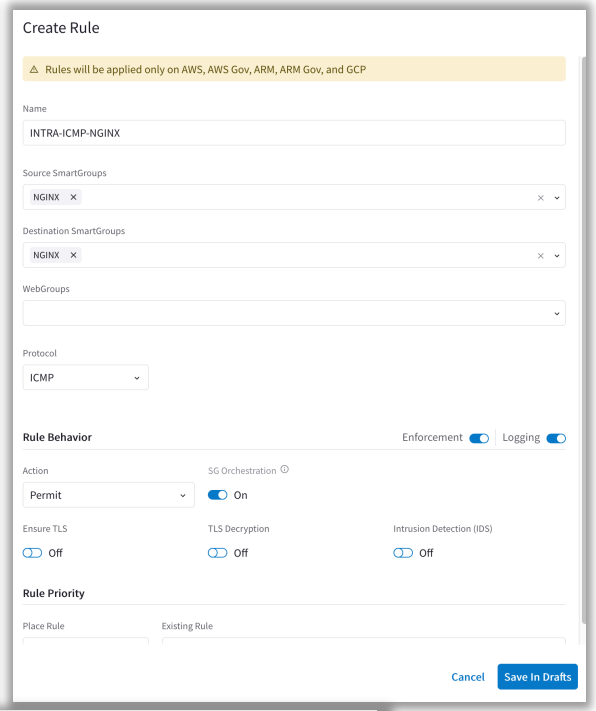
Micro-Segmention: SmartGroups, Intra-Rules and Inter-Rules (5)

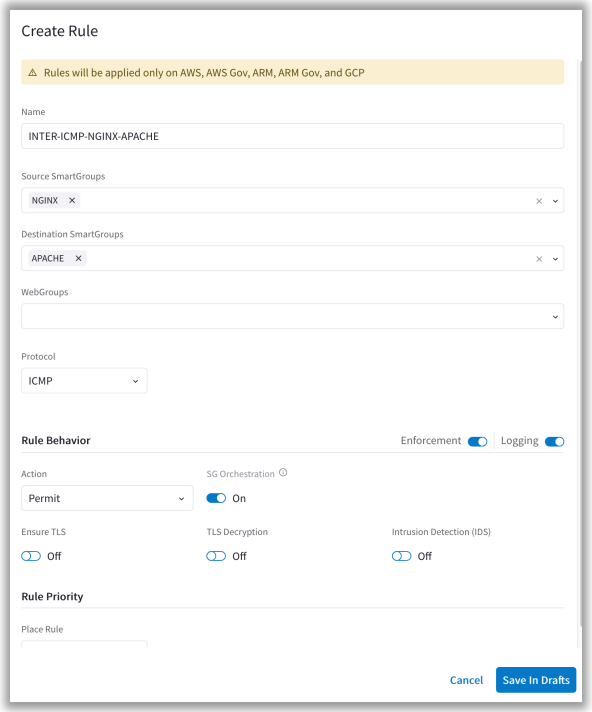


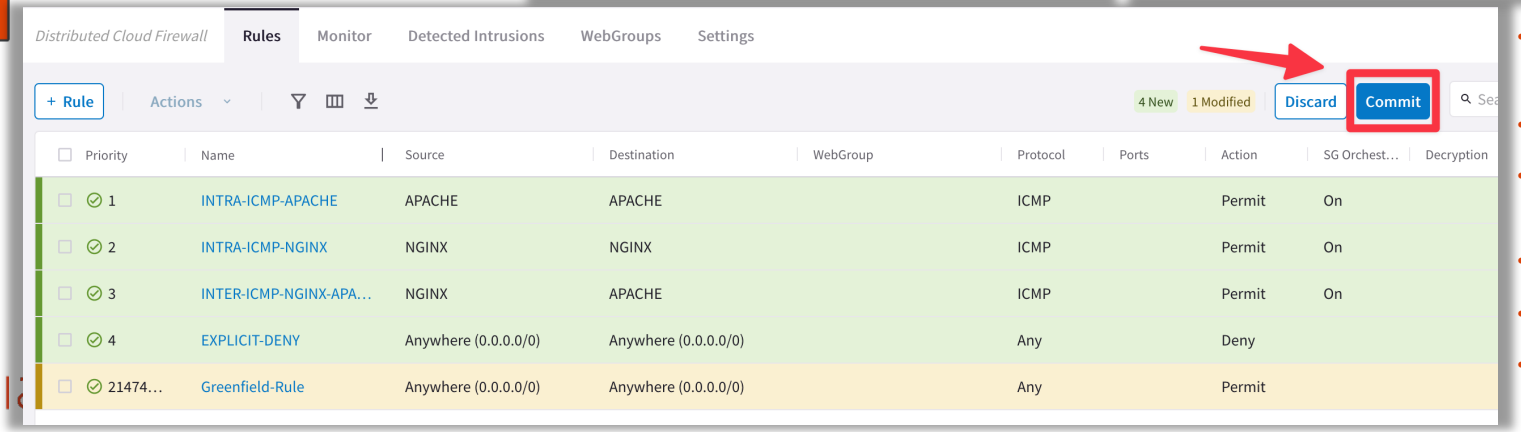












- **What is the Micro-Segmentation?** It's a combination of SmartGroups and DCF Rules
- Rule changes are saved in **Draft** state
- When you apply a rule to a SmartGroup, please keep in mind that there is an **Invisible Hidden Deny** at the very bottom.
- To save the changes click on "**Commit**"
- **Discard** will trash the changes
- Rule is **stateful**, this means that the return traffic is allowed automatically

Distributed Secure Egress

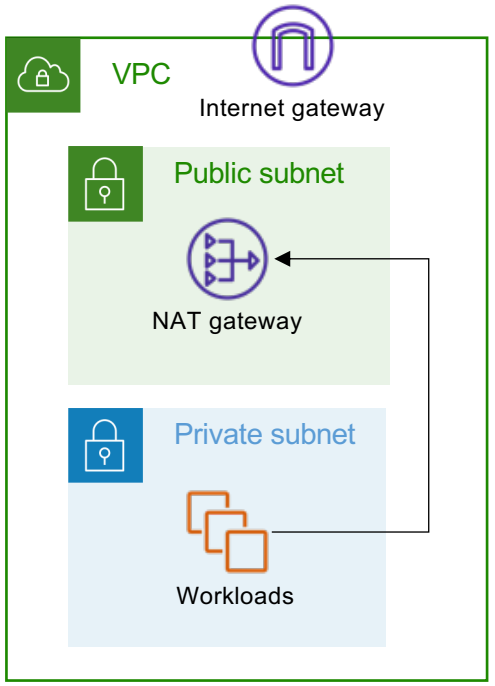
Problem Statement

Private workloads need internet access

- **SaaS integration**
- **Patching**
- **Updates**

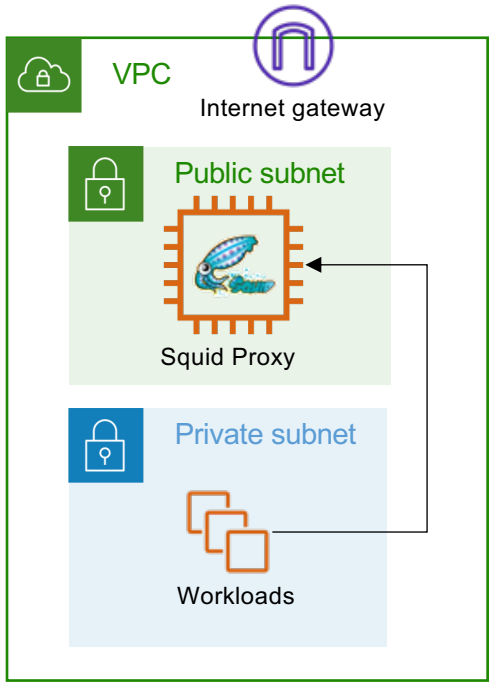
NAT Gateway

- NACLs management
- Layer-4 only



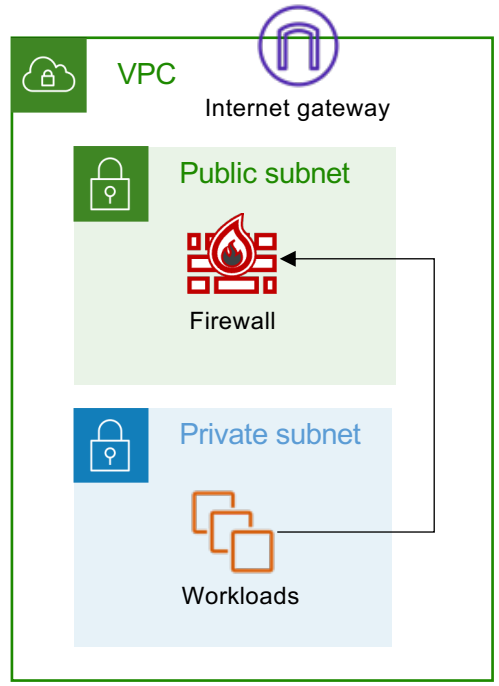
Squid Proxy

- Hard to manage
- Scale and HA issues

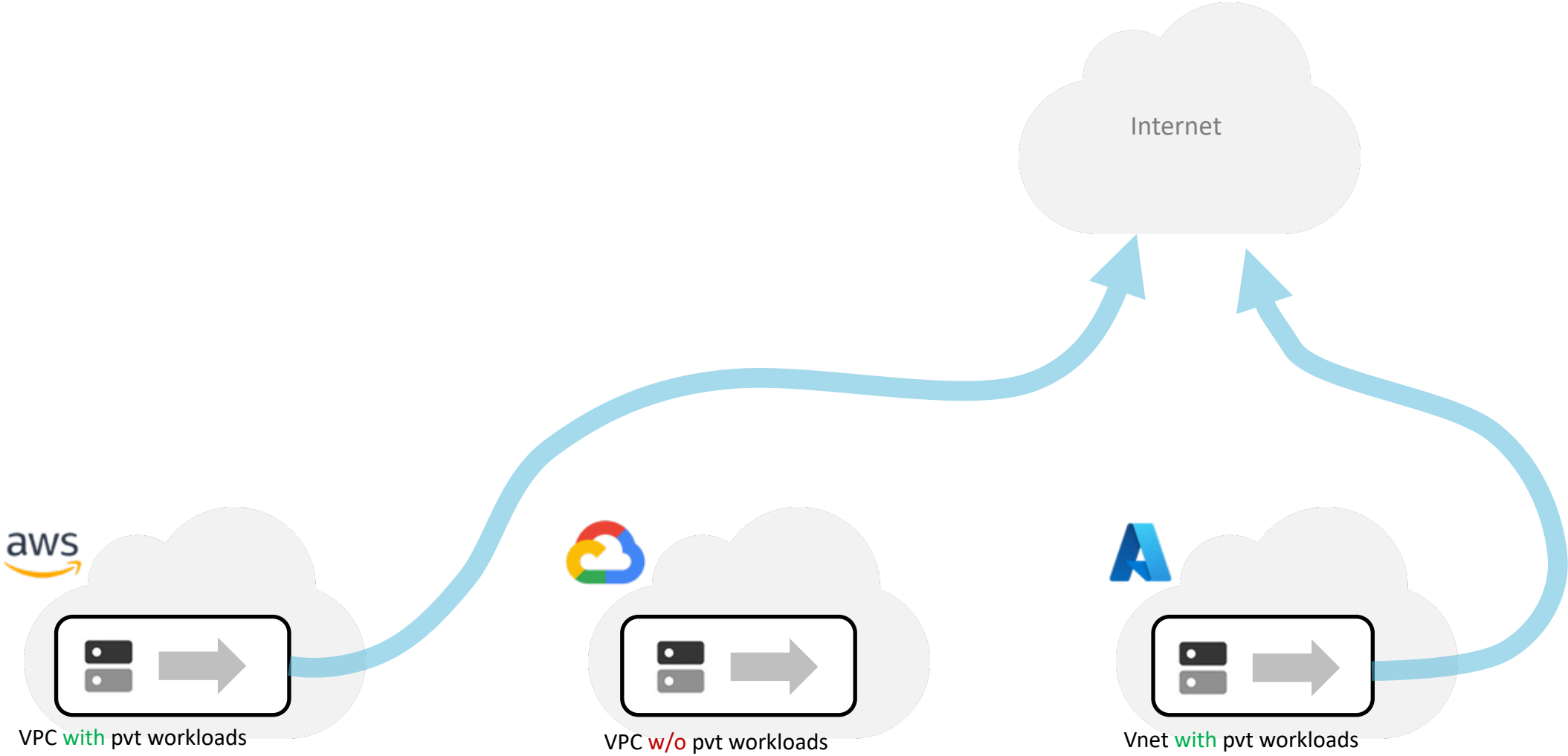


Layer-7 Firewall

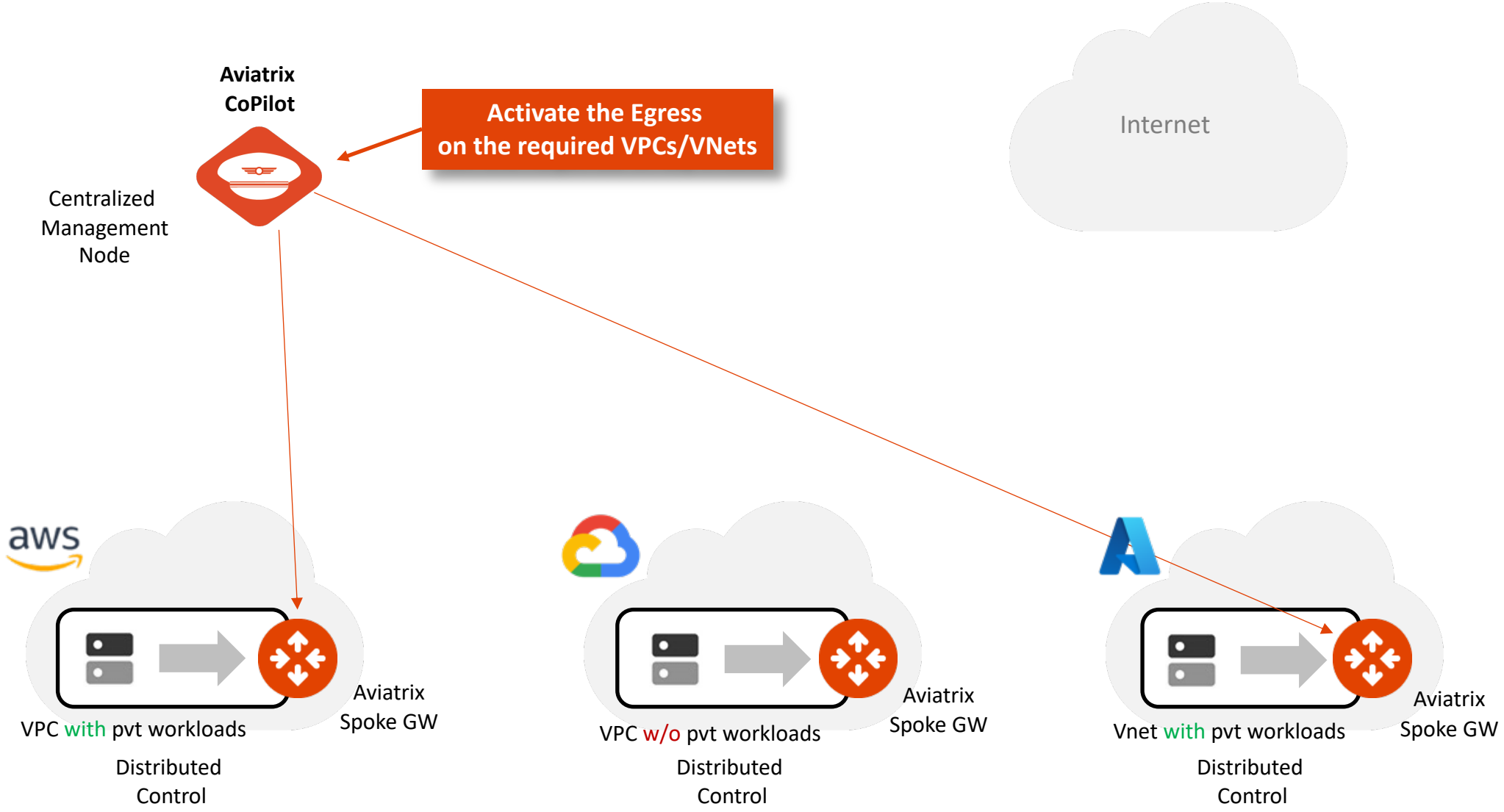
- Overkill
- Expensive



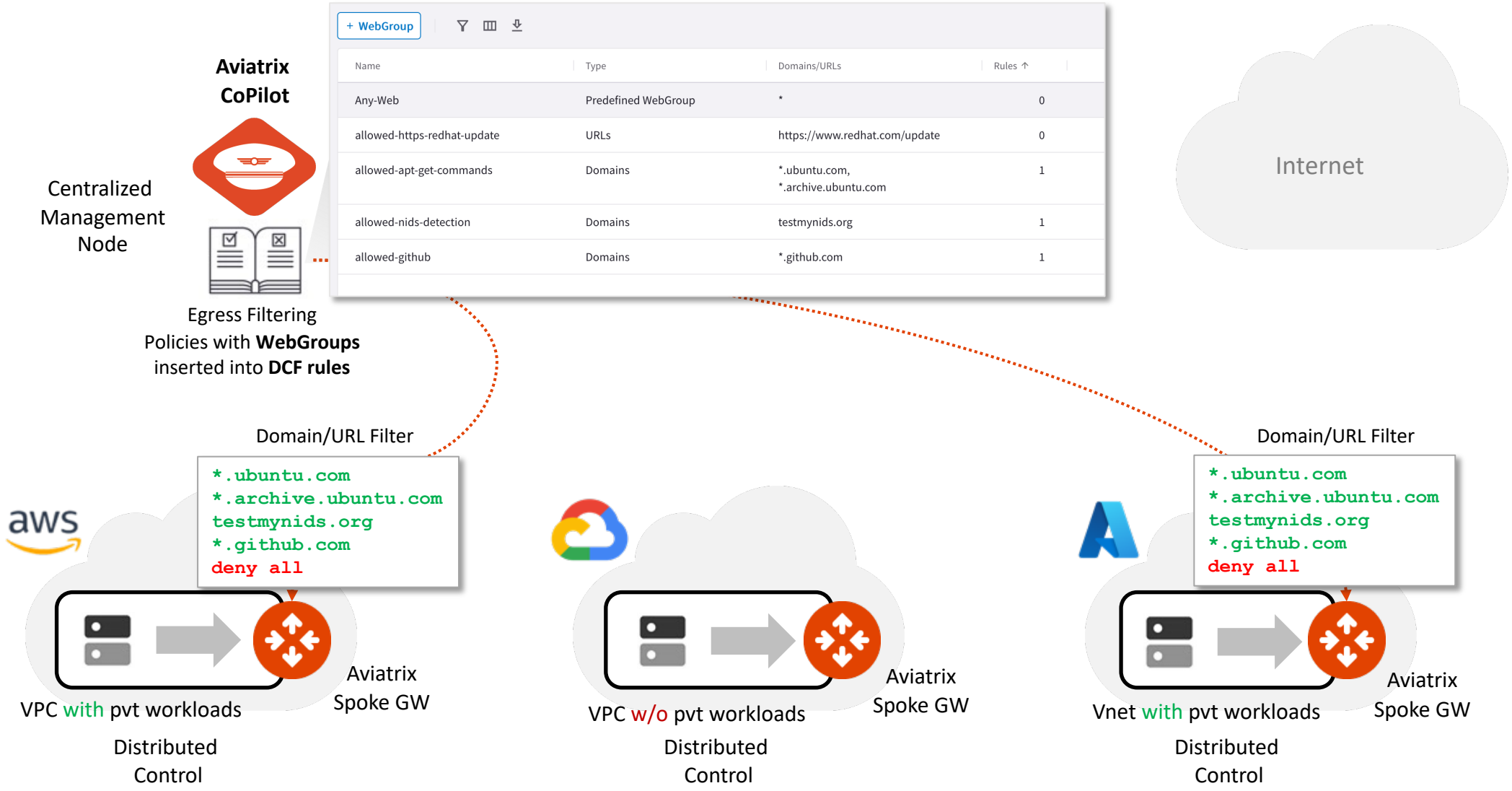
Aviatrix Secure Egress



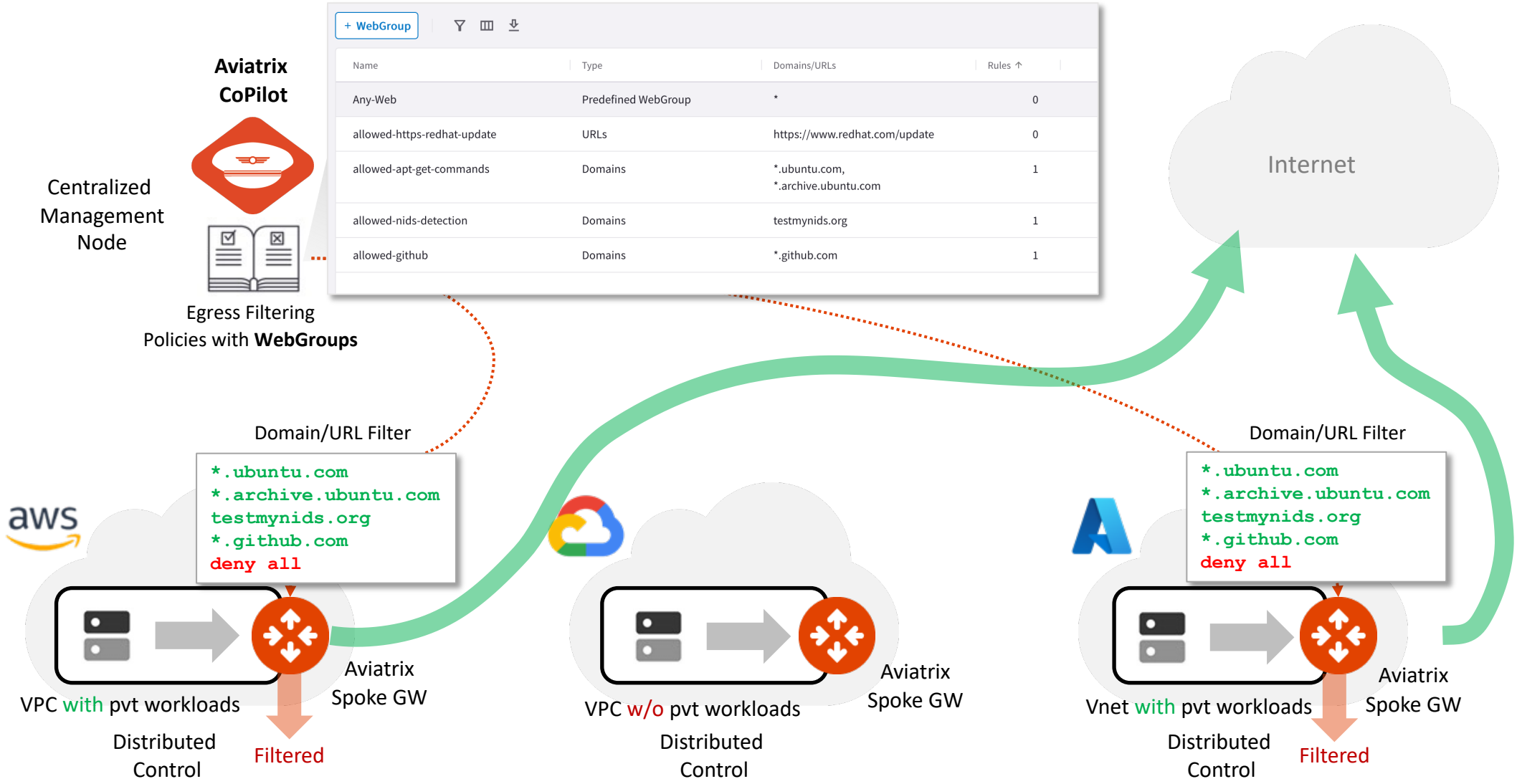
Aviatrix Secure Egress



Aviatrix Secure Egress

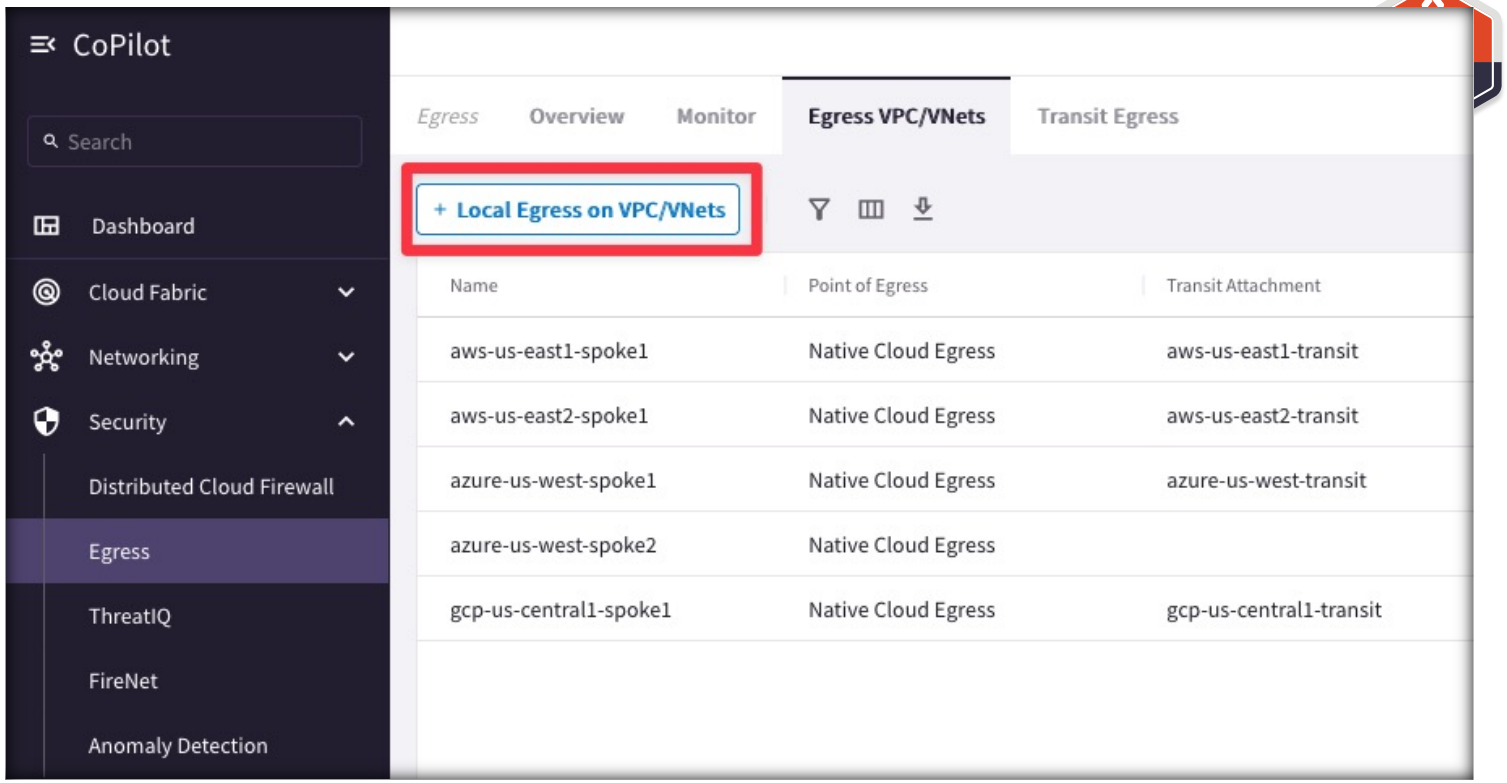


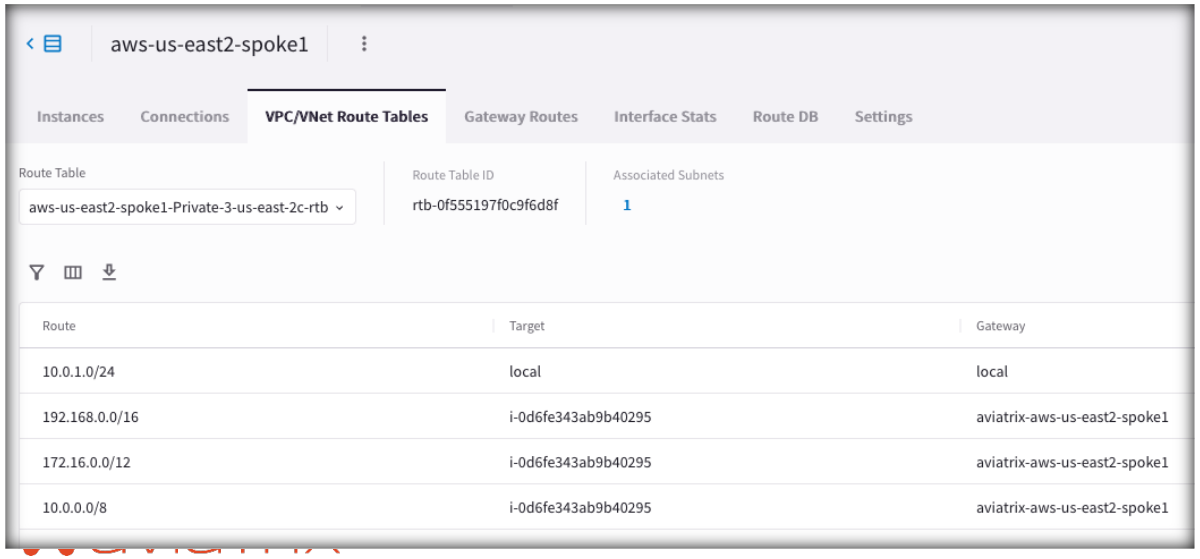
Aviatrix Secure Egress

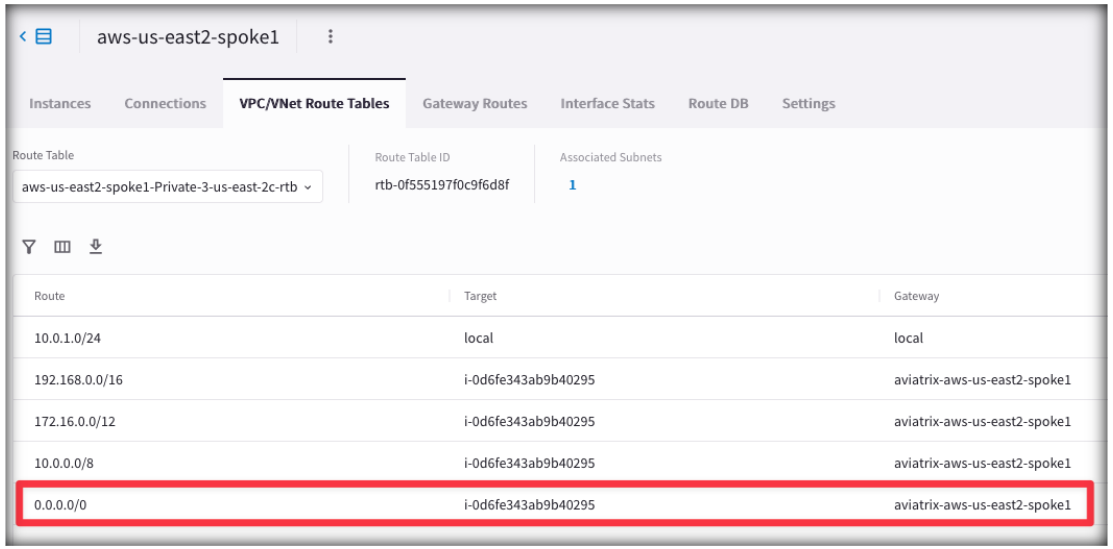


Enabling Egress

- Adding Egress Control on VPC/VNet changes the default route on VPC/VNet to point to the Spoke Gateway and enables **SNAT**.
- Egress Control also requires additional resources on the Spoke Gateway (i.e. scale up the VM size).
- In addition to the **Local route**, the **three RFC1918 routes**, also a **default route** will be injected.



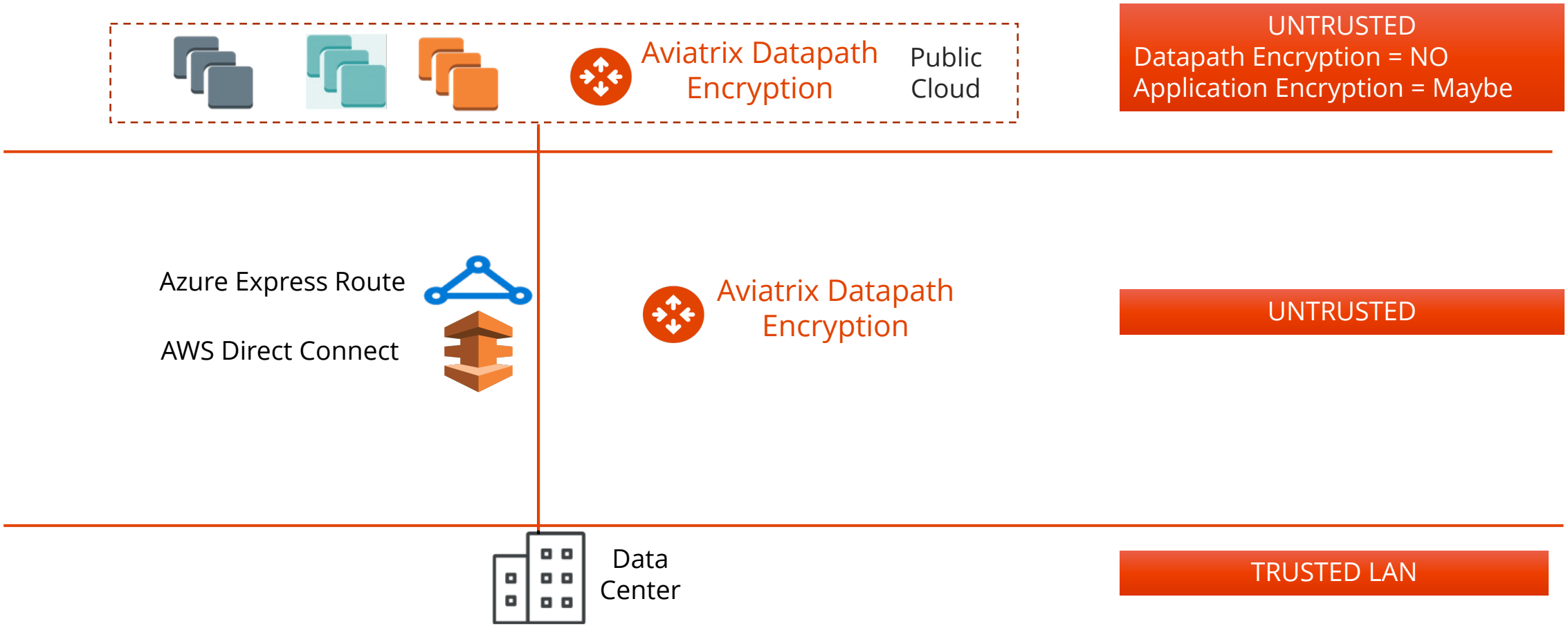




High Performance Encryption (HPE)

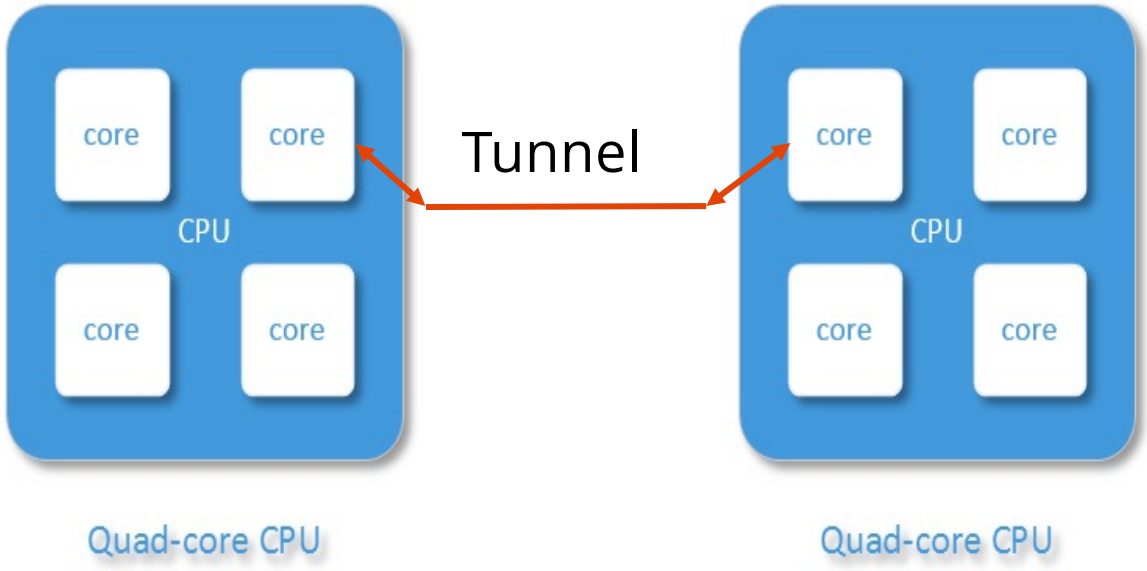
aka Insane Mode

Zero Trust – Datapath Encryption



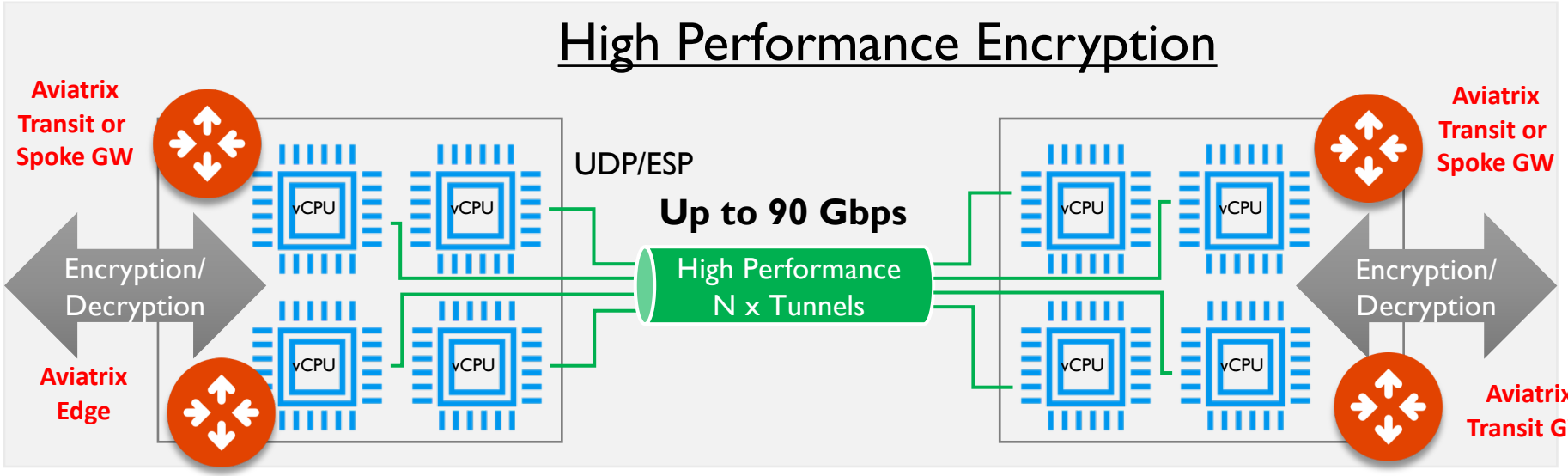
Problem Statement – Native Cloud IPsec Performance is Limited

- Native Cloud IPsec VPN solutions have a maximum encryption performance of 1.25Gbps per tunnel
  - VPC ←→ VPC
  - On-prem ←→ Cloud (including DX – but link could be 10G!)
  - Cloud ←→ Cloud
- That's because virtual routers utilize a single core, and they establish only one tunnel



Solution: Aviatrix High Performance Encryption (HPE)

- Aviatrix Controller automatically builds multiple tunnels between Aviatrix devices
- Uses all available CPU cores
- IPsec encryption performance can be up to 90 Gbps



Next: Platform Overview part.2