



# Features Overview

## PART 1/2

ACE Solutions Architecture Team



aviatrix  
**ACE**

Aviatrix Certified  
Engineer

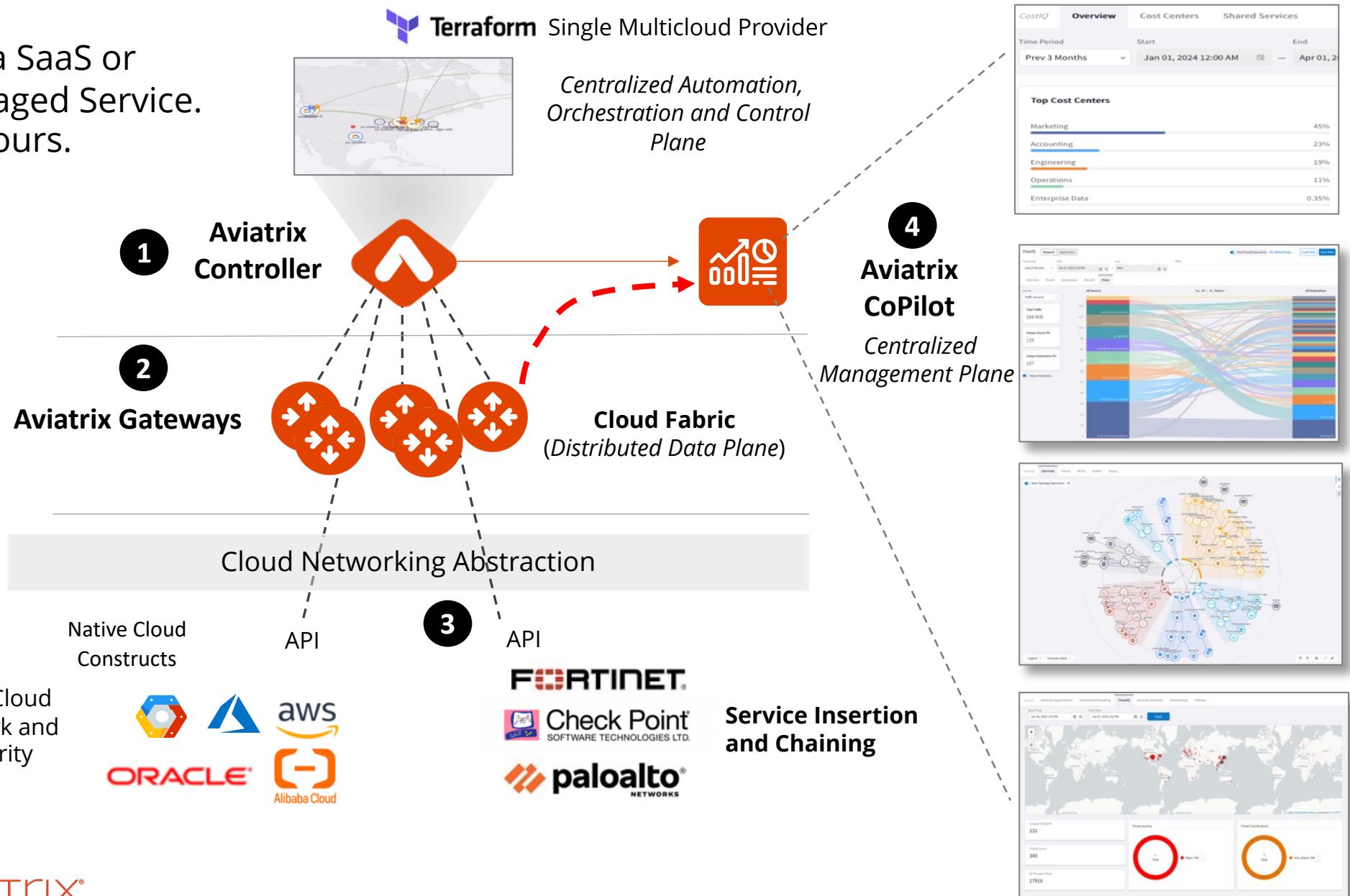
Overview  
Transit  
Network Segmentation  
Distributed Cloud Firewall  
Secure Egress  
High Performance Encryption



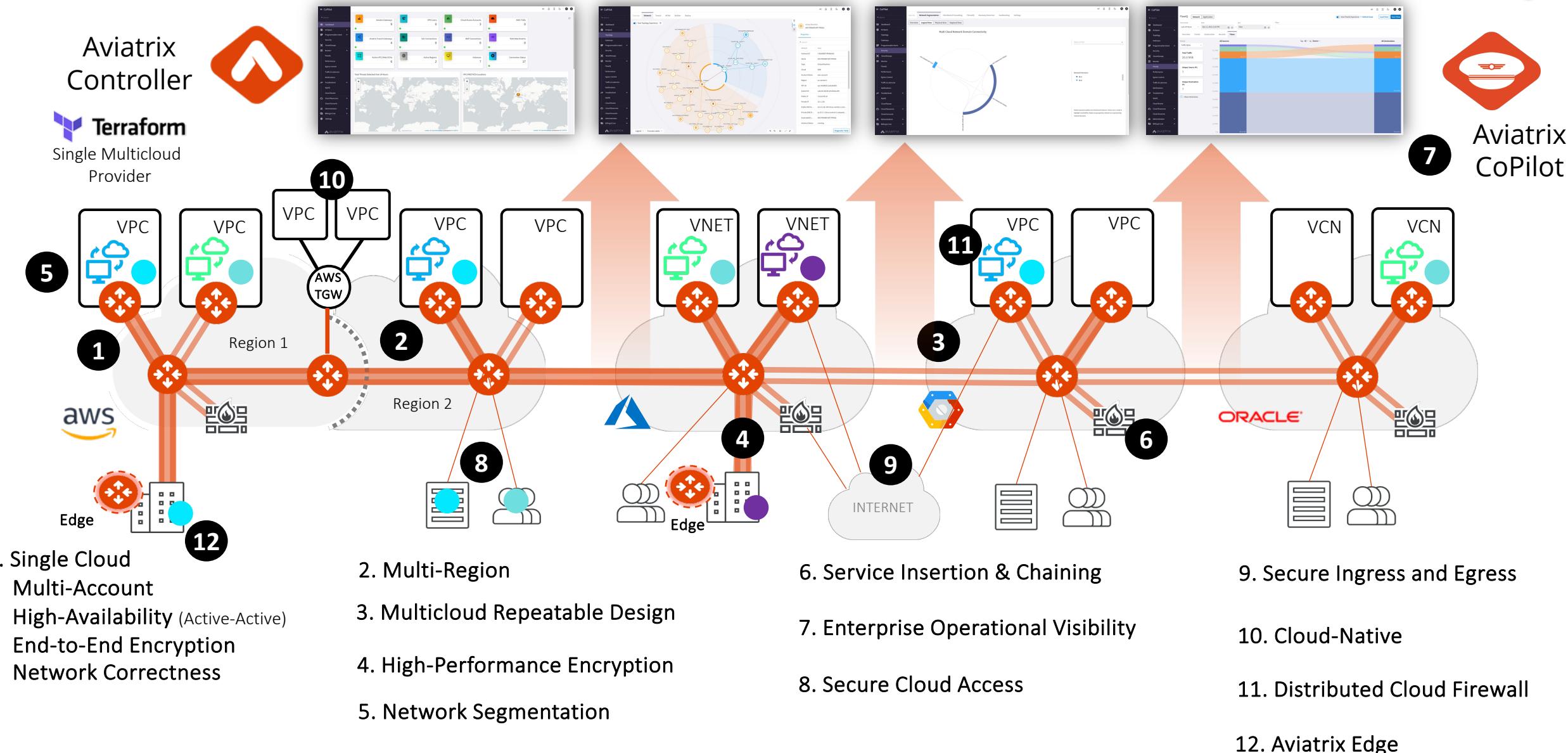
# Overview

# Aviatrix Cloud Network Platform Software

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



# Aviatrix – Foundation of Your Multicloud Networking and Security

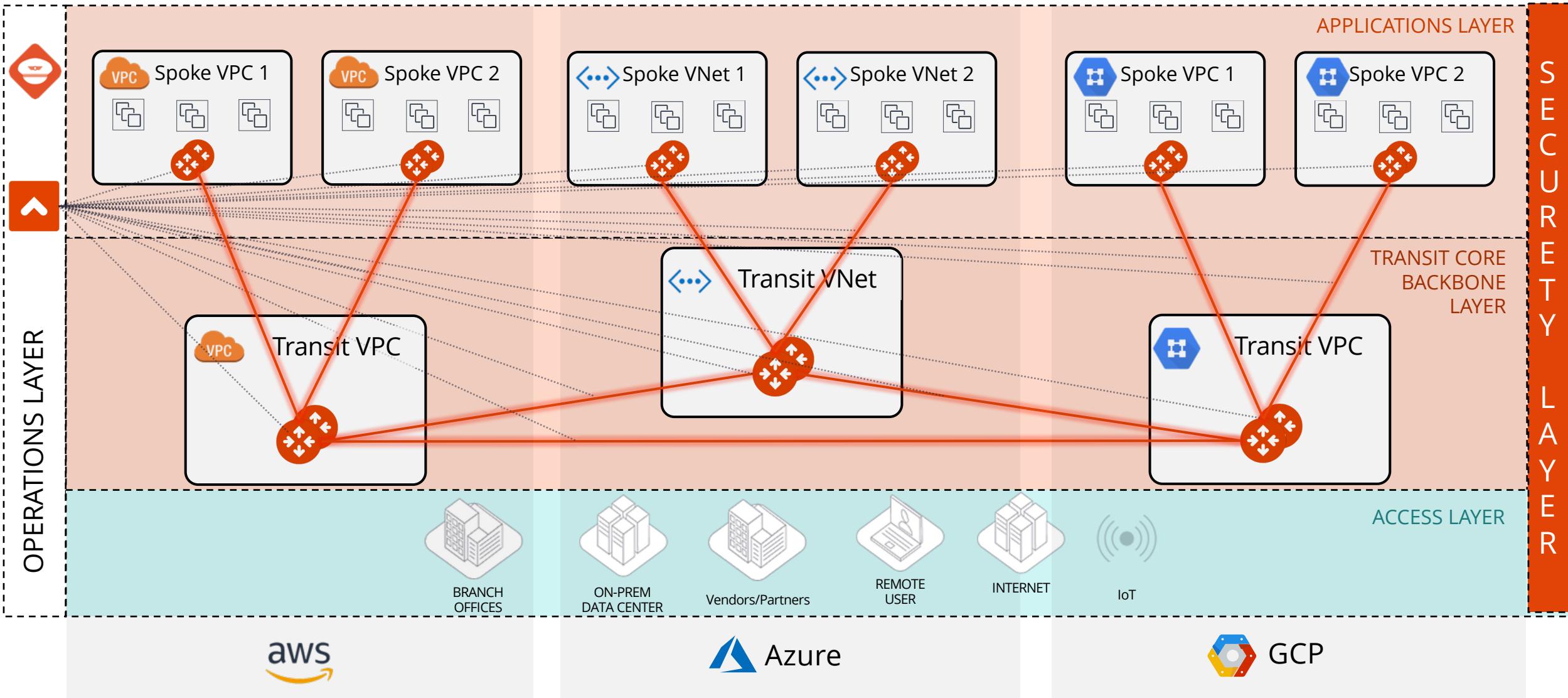




# Transit Networking

## With Dynamic Routing and Traffic Engineering

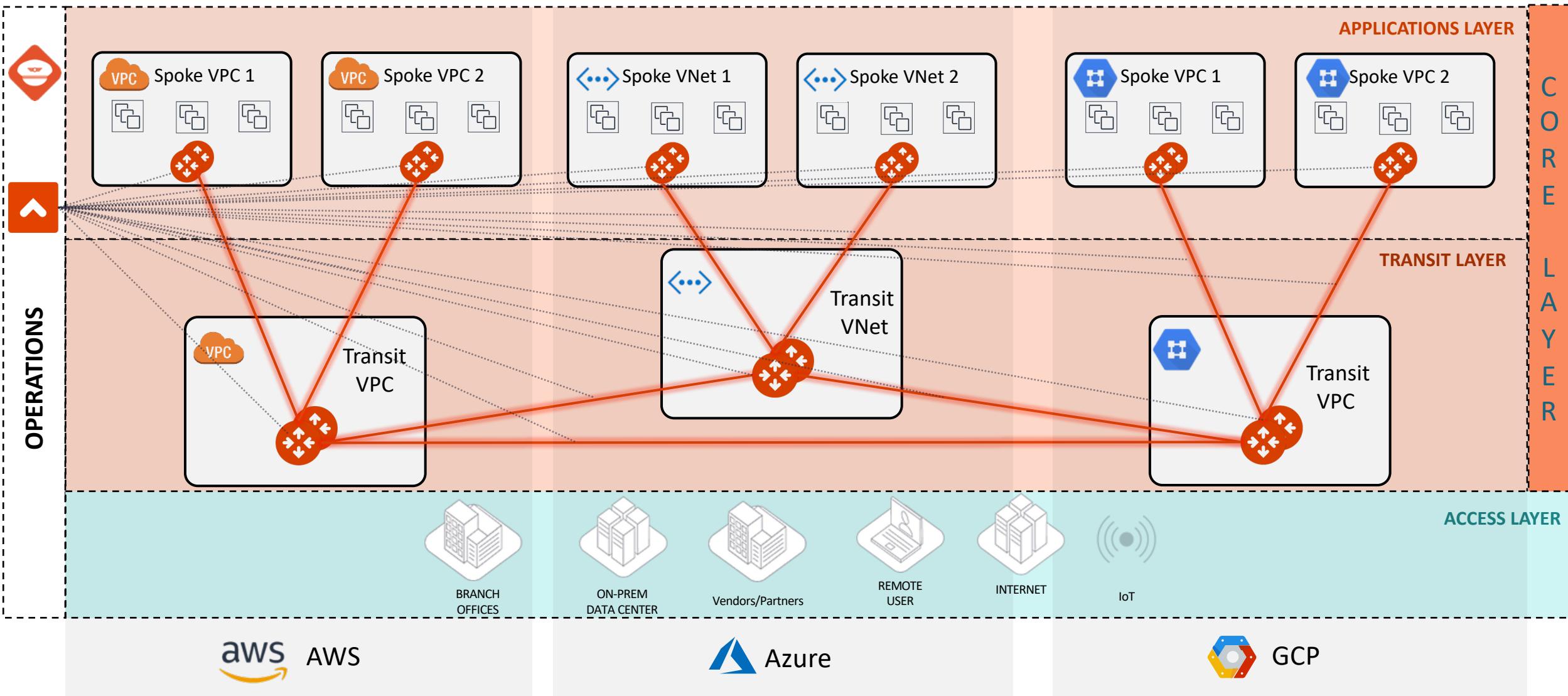
# Aviatrix Transit Network



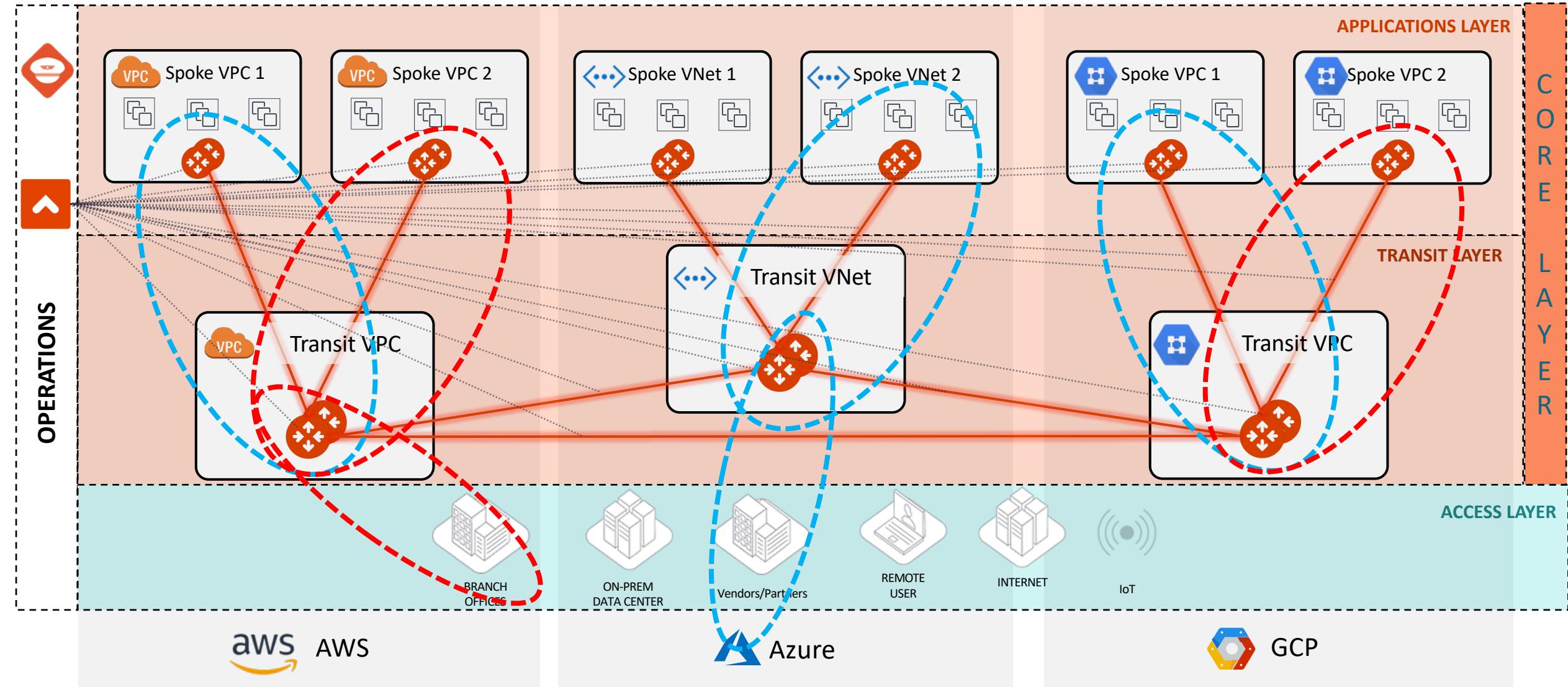


# Network Segmentation

# MCNA Deployment: the Foundations

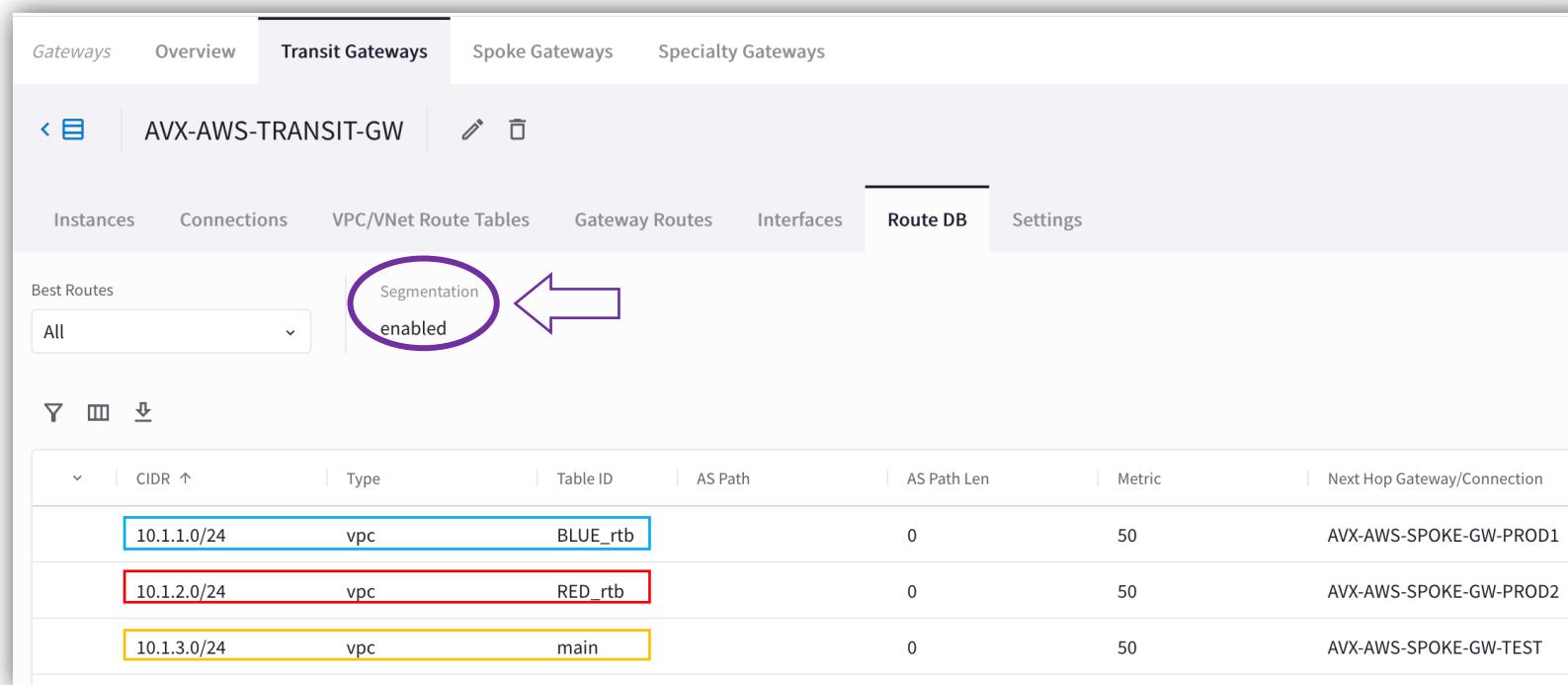


# Global Segmentation with Network Domains



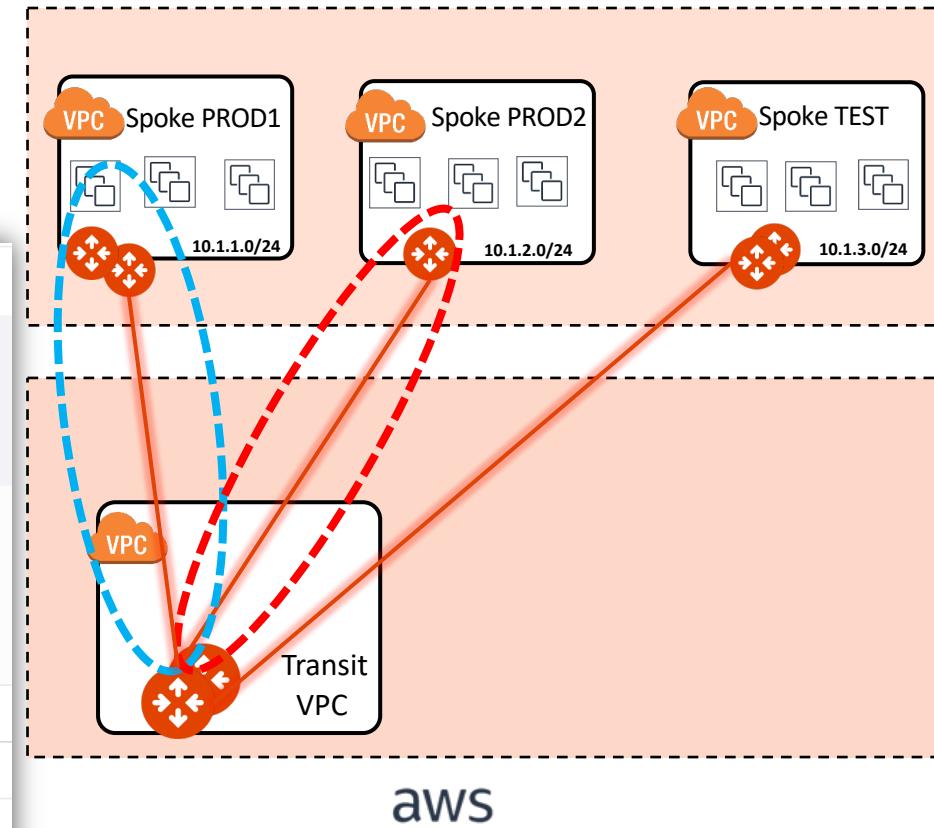
# Order of Operations for activating the Network Segmentation

- 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*)



The screenshot shows the Aviatrix Cloud Fabric interface with the 'Transit Gateways' tab selected. Under the 'Route DB' tab, the 'Segmentation enabled' status is highlighted with a purple oval and an arrow pointing to the network diagram on the right.

CIDR	Type	Table ID	AS Path	AS Path Len	Metric	Next Hop Gateway/Connection
10.1.1.0/24	vpc	BLUE_rtb		0	50	AVX-AWS-SPOKE-GW-PROD1
10.1.2.0/24	vpc	RED_rtb		0	50	AVX-AWS-SPOKE-GW-PROD2
10.1.3.0/24	vpc	main		0	50	AVX-AWS-SPOKE-GW-TEST



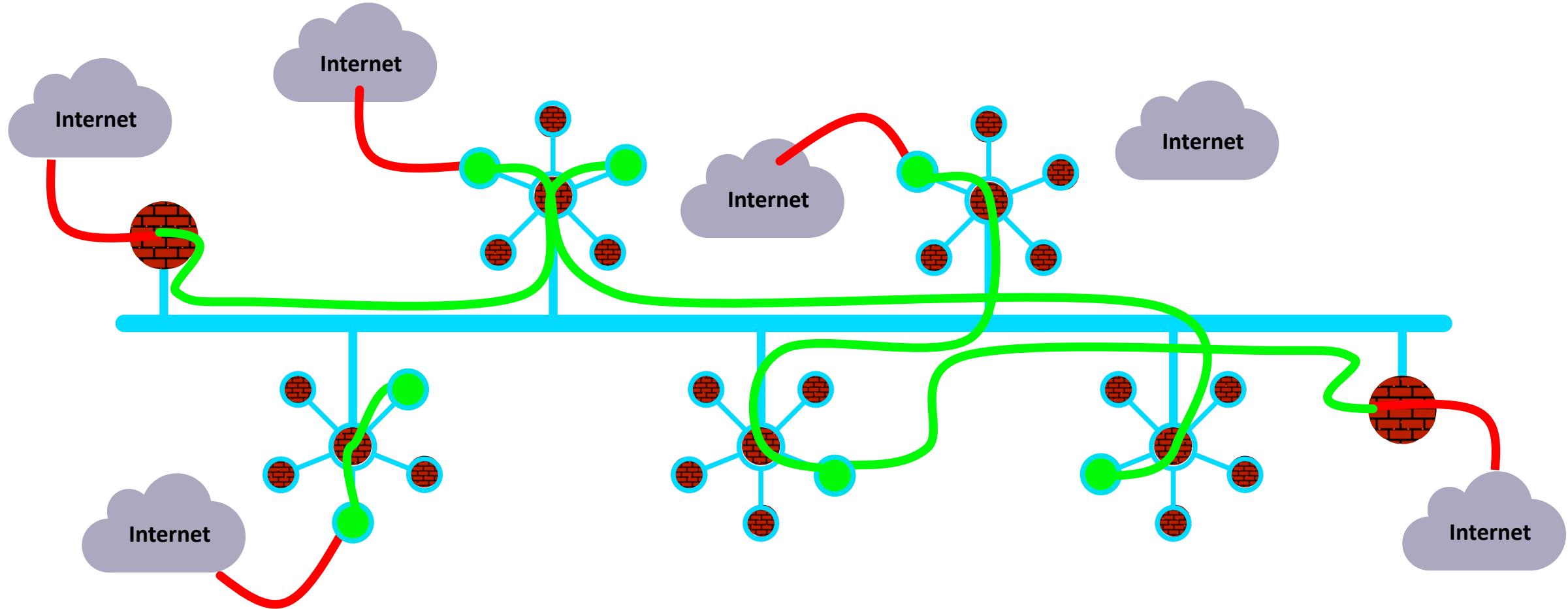
**PATH:** COPILOT > Cloud Fabric > Gateways > Transit Gateways > select the relevant GW > **Route DB** (equivalent of RIB)



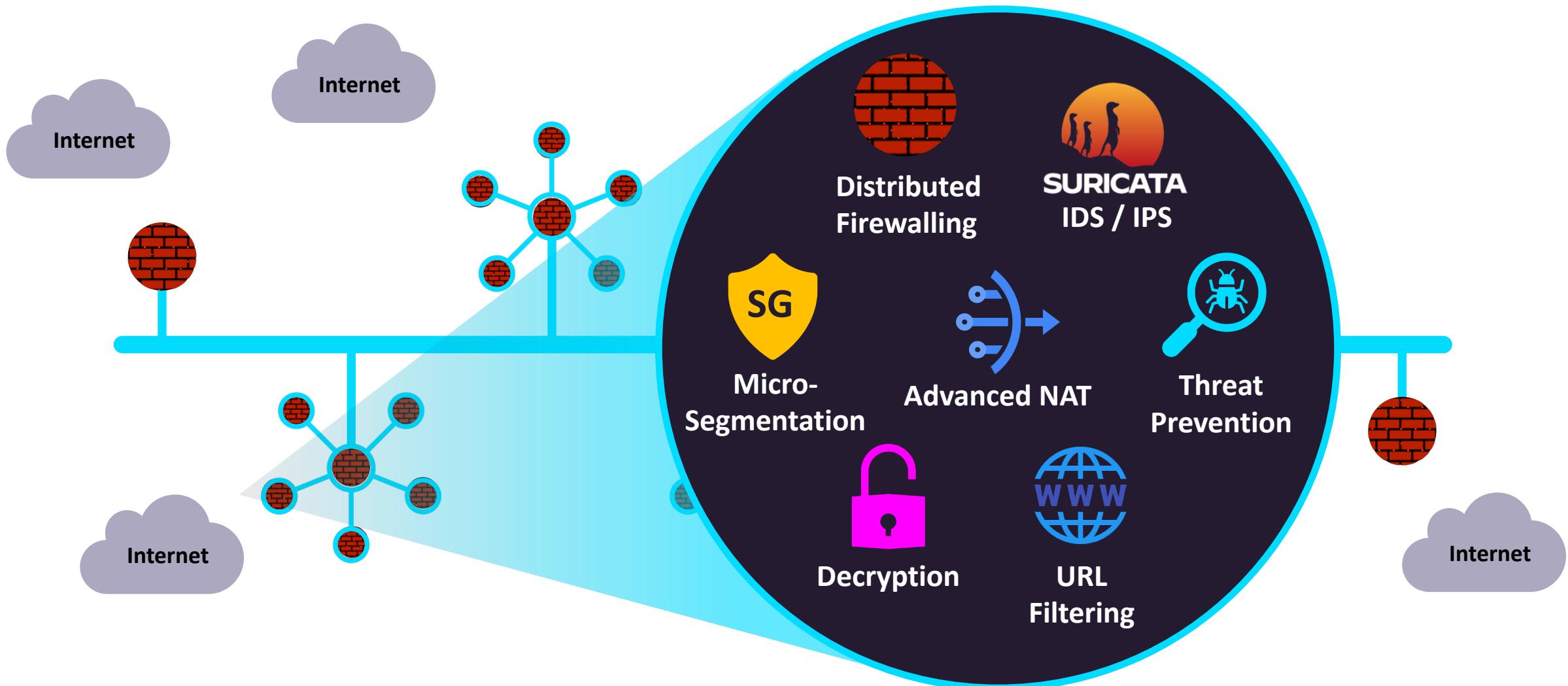
# Distributed Cloud Firewall

## Aviatrix DCF

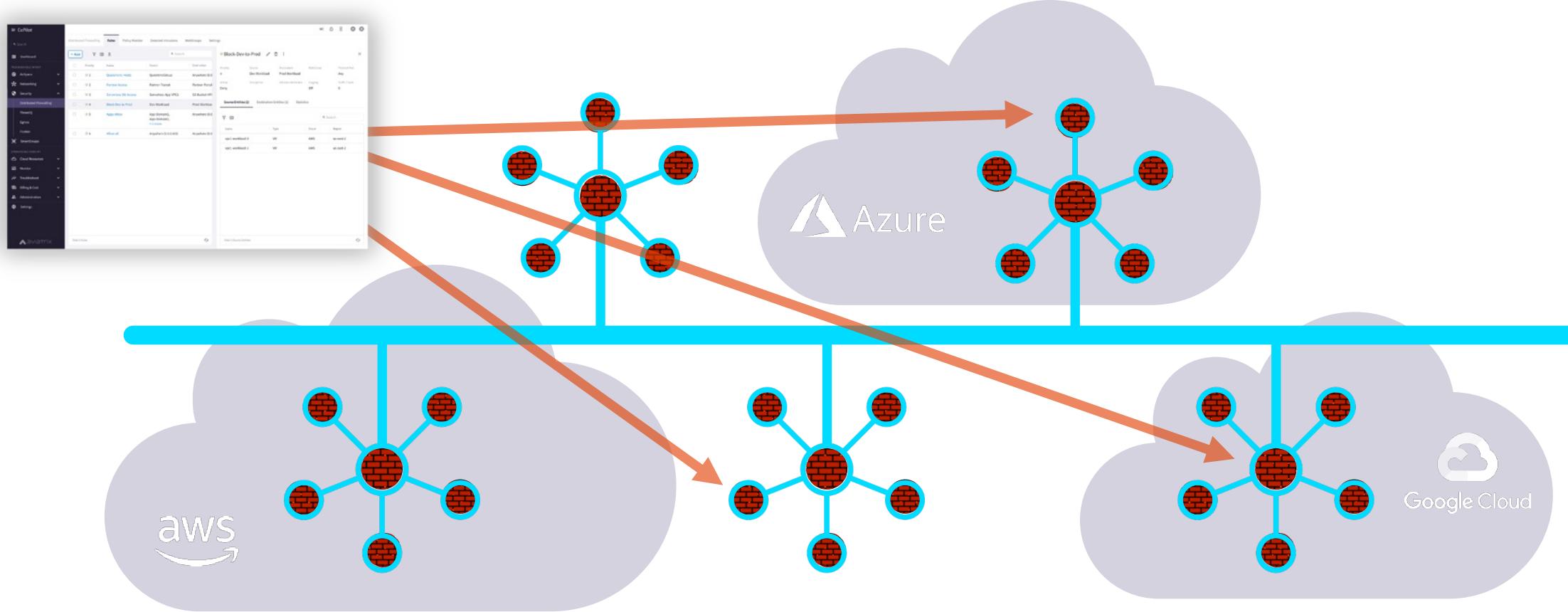
# Aviatrix DCF Centrally Managed, with Distributed Inspection & Enforcement...



# And, What If it was more than just firewalling...

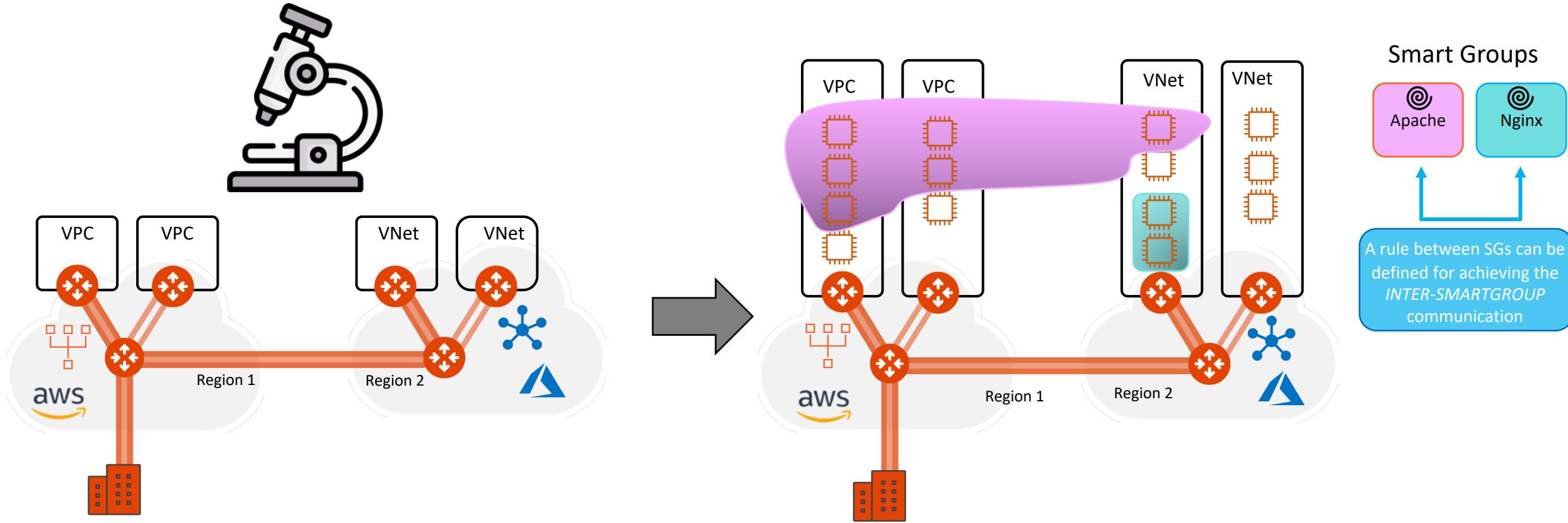


# A Distributed Cloud Firewall...



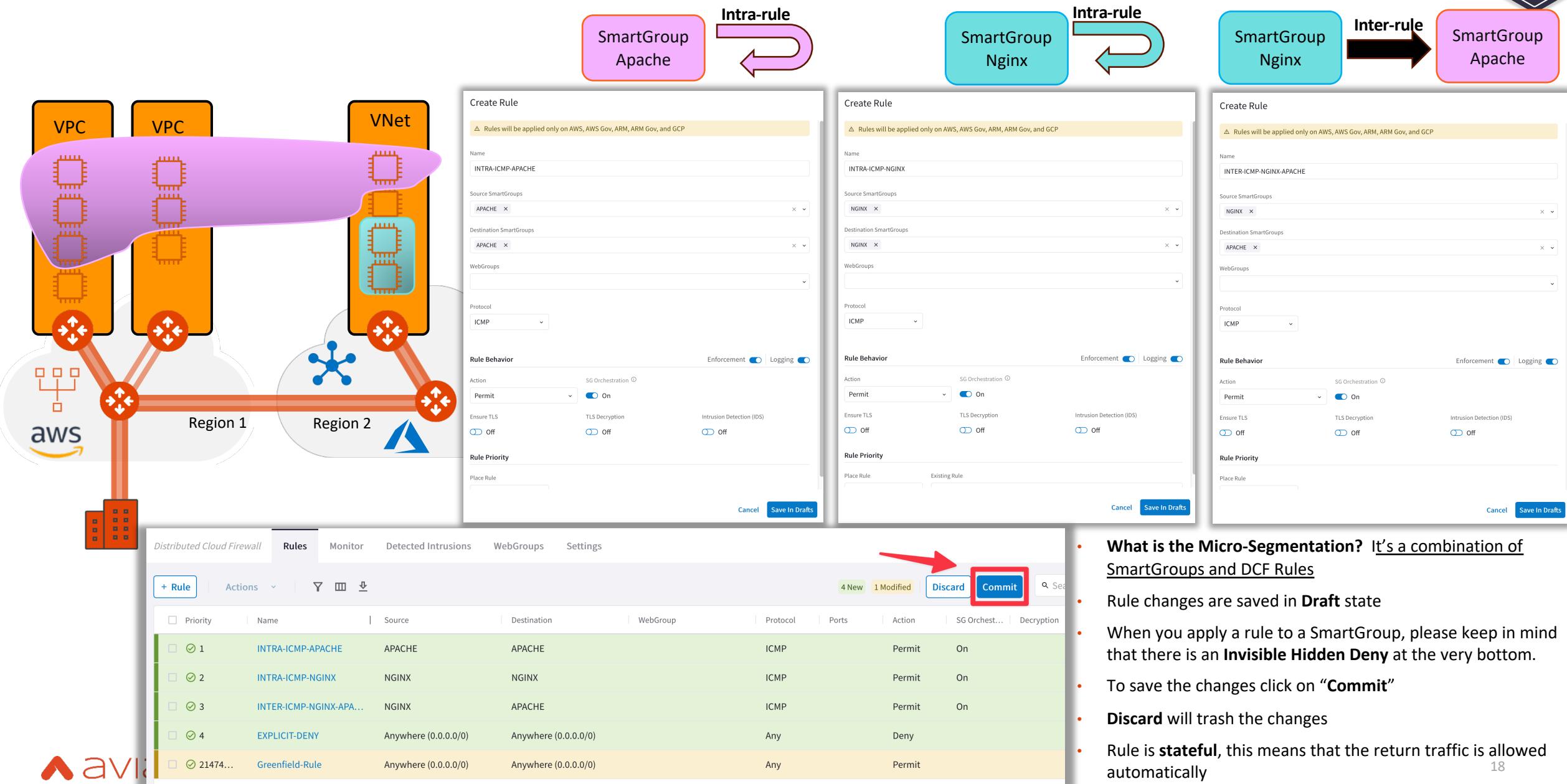
Where and How Policies Are Enforced Is Abstracted...

# 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-Segmentation: SmartGroups, Intra-Rules and Inter-Rules (5)



The diagram illustrates the Micro-Segmentation architecture and rule creation process across two regions:

- Region 1:** Contains two VPCs (represented by orange boxes) and a VNet (represented by a large orange box). A purple cloud highlights the VPCs and VNet.
- Region 2:** Contains a VNet (represented by a large orange box).
- SmartGroups:** Three SmartGroups are defined:
  - SmartGroup Apache:** Represented by a pink box. An arrow labeled "Intra-rule" points from this box to the first "Create Rule" dialog.
  - SmartGroup Nginx:** Represented by a blue box. An arrow labeled "Intra-rule" points from this box to the second "Create Rule" dialog.
  - SmartGroup Nginx:** Represented by a blue box. An arrow labeled "Inter-rule" points from this box to the third "Create Rule" dialog.
- Create Rule Dialogs:** Three "Create Rule" dialogs are shown, each for a different ICMP rule:
  - INTRA-ICMP-APACHE:** Source SmartGroups: APACHE; Destination SmartGroups: APACHE; Protocol: ICMP; Action: Permit; Ensure TLS: Off; SG Orchestration: On; Enforcement: Off; Logging: On.
  - INTRA-ICMP-NGINX:** Source SmartGroups: NGINX; Destination SmartGroups: NGINX; Protocol: ICMP; Action: Permit; Ensure TLS: Off; SG Orchestration: On; Enforcement: Off; Logging: On.
  - INTER-ICMP-NGINX-APACHE:** Source SmartGroups: NGINX; Destination SmartGroups: APACHE; Protocol: ICMP; Action: Permit; Ensure TLS: Off; SG Orchestration: On; Enforcement: On; Logging: On.
- Distributed Cloud Firewall UI:** Shows the Rules tab with a list of rules:
 

Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchestr...	Decryption
1	INTRA-ICMP-APACHE	APACHE	APACHE		ICMP		Permit	On	
2	INTRA-ICMP-NGINX	NGINX	NGINX		ICMP		Permit	On	
3	INTER-ICMP-NGINX-APA...	NGINX	APACHE		ICMP		Permit	On	
4	EXPLICIT-DENY	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Deny		
21474...	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit		
- Commit Process:** A red arrow points from the "Discard" button to the "Commit" button, which is highlighted with a red box.

**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

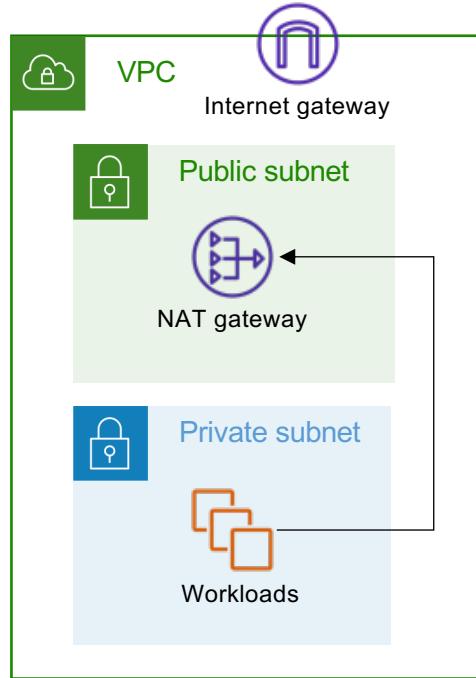


- Updates



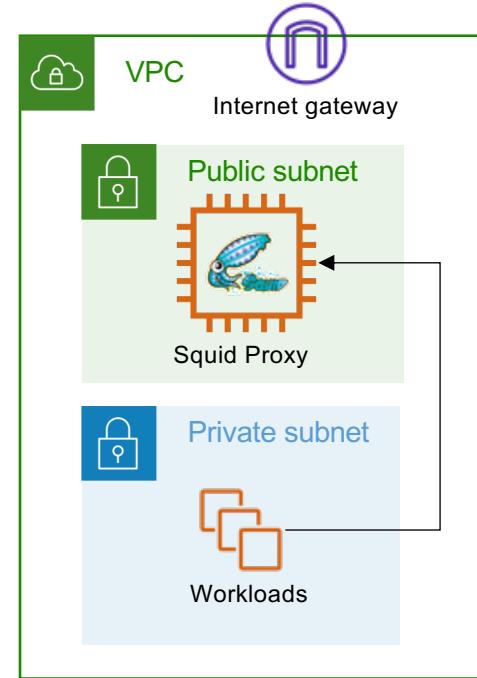
### NAT Gateway

- NACLs management
- Layer-4 only



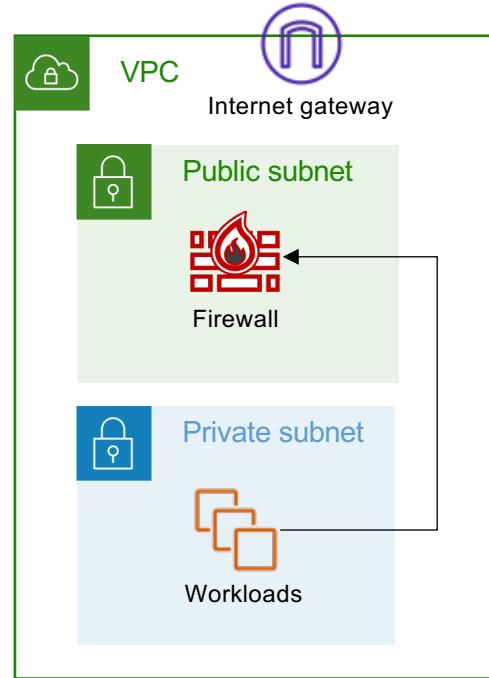
### Squid Proxy

- Hard to manage
- Scale and HA issues

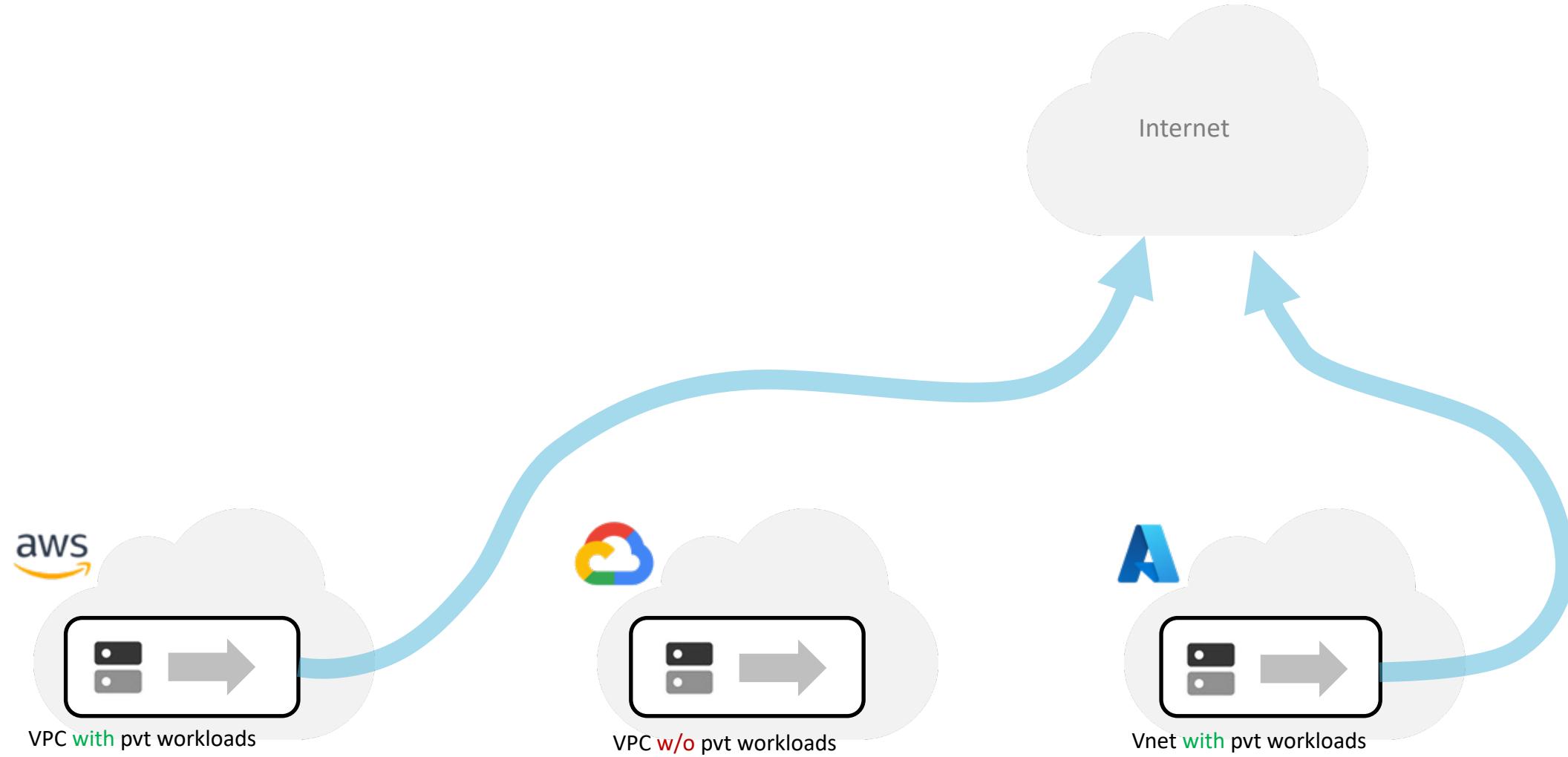


### Layer-7 Firewall

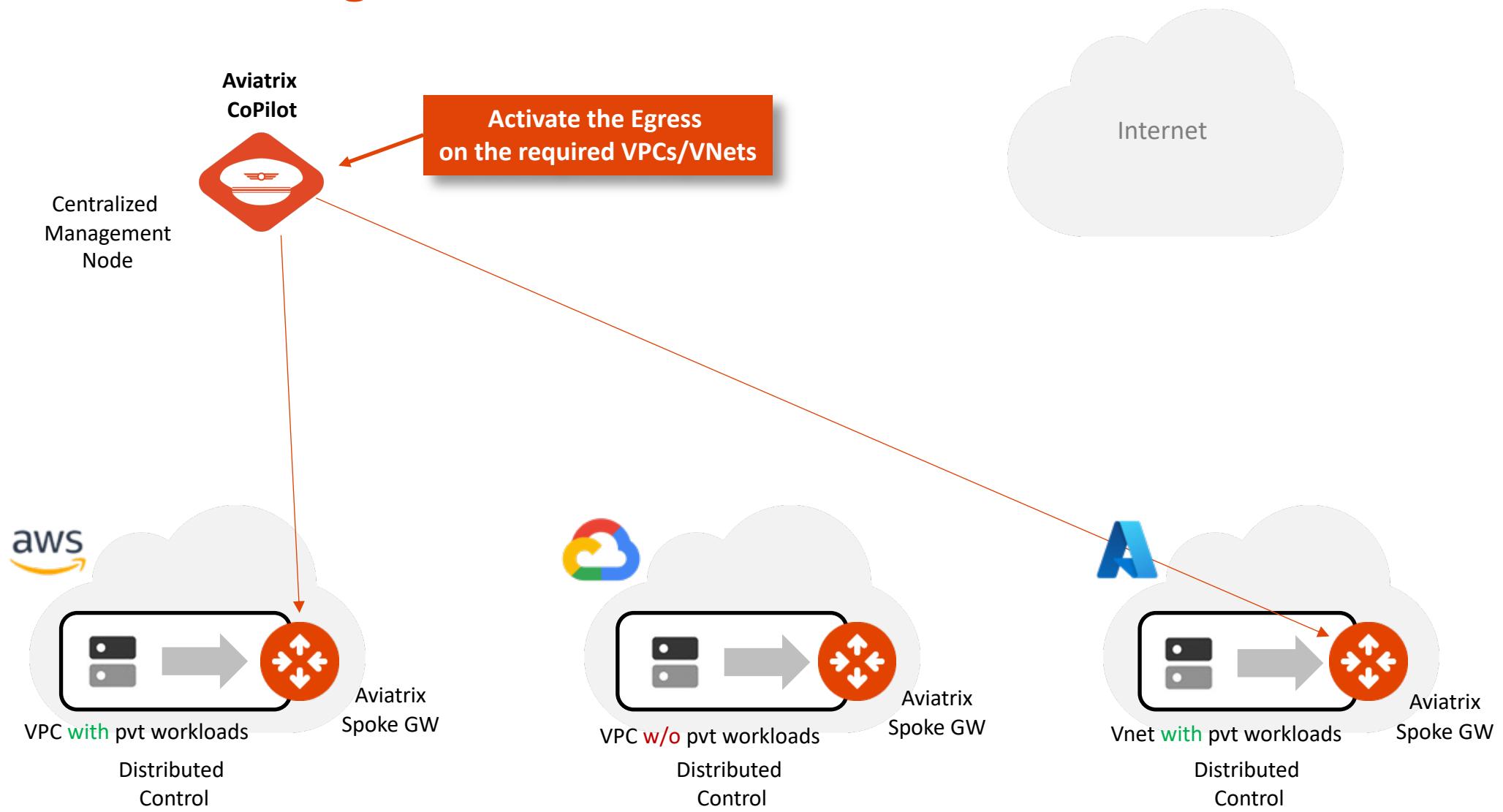
- Overkill
- Expensive



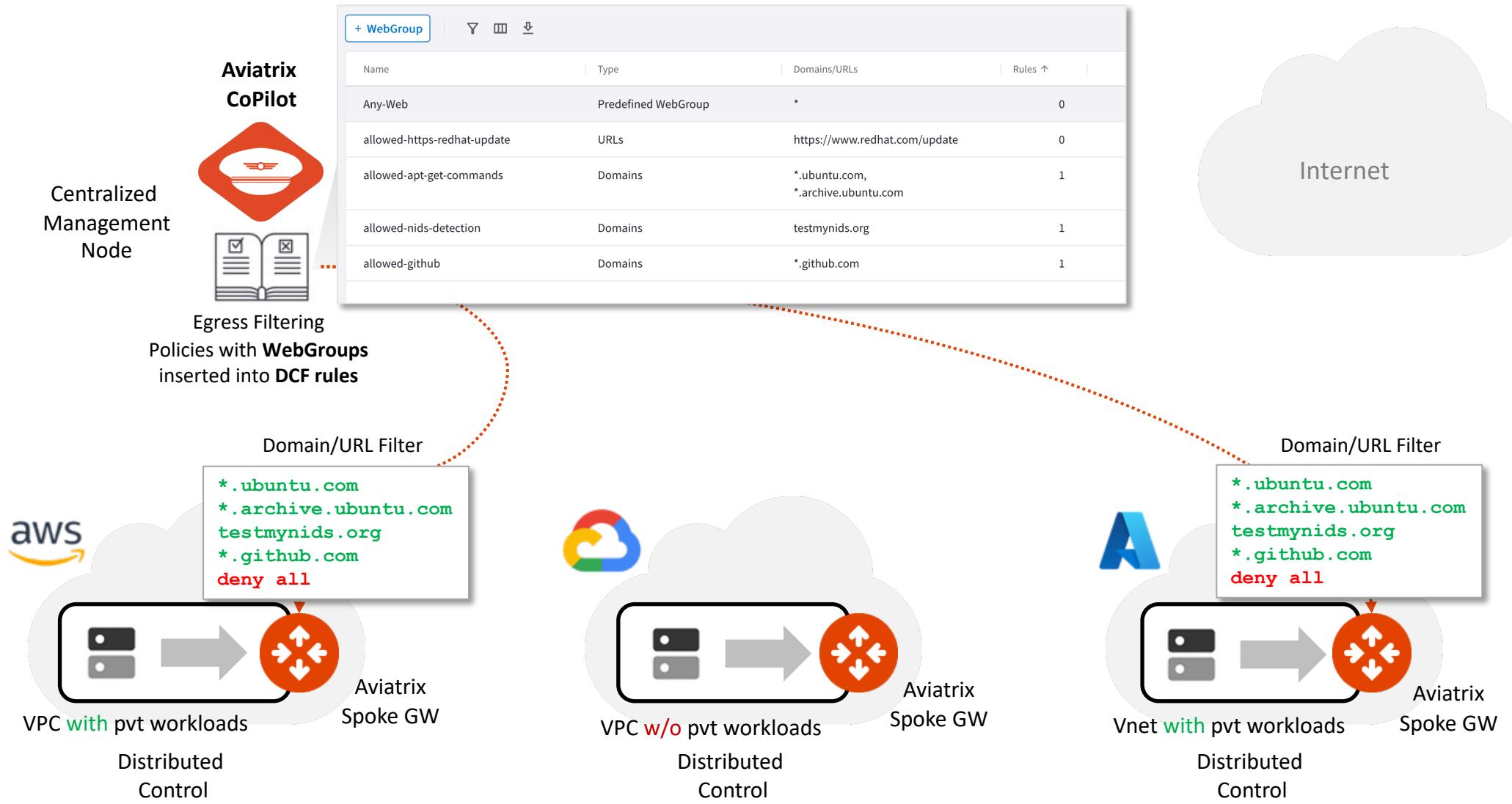
# Aviatrix Secure Egress



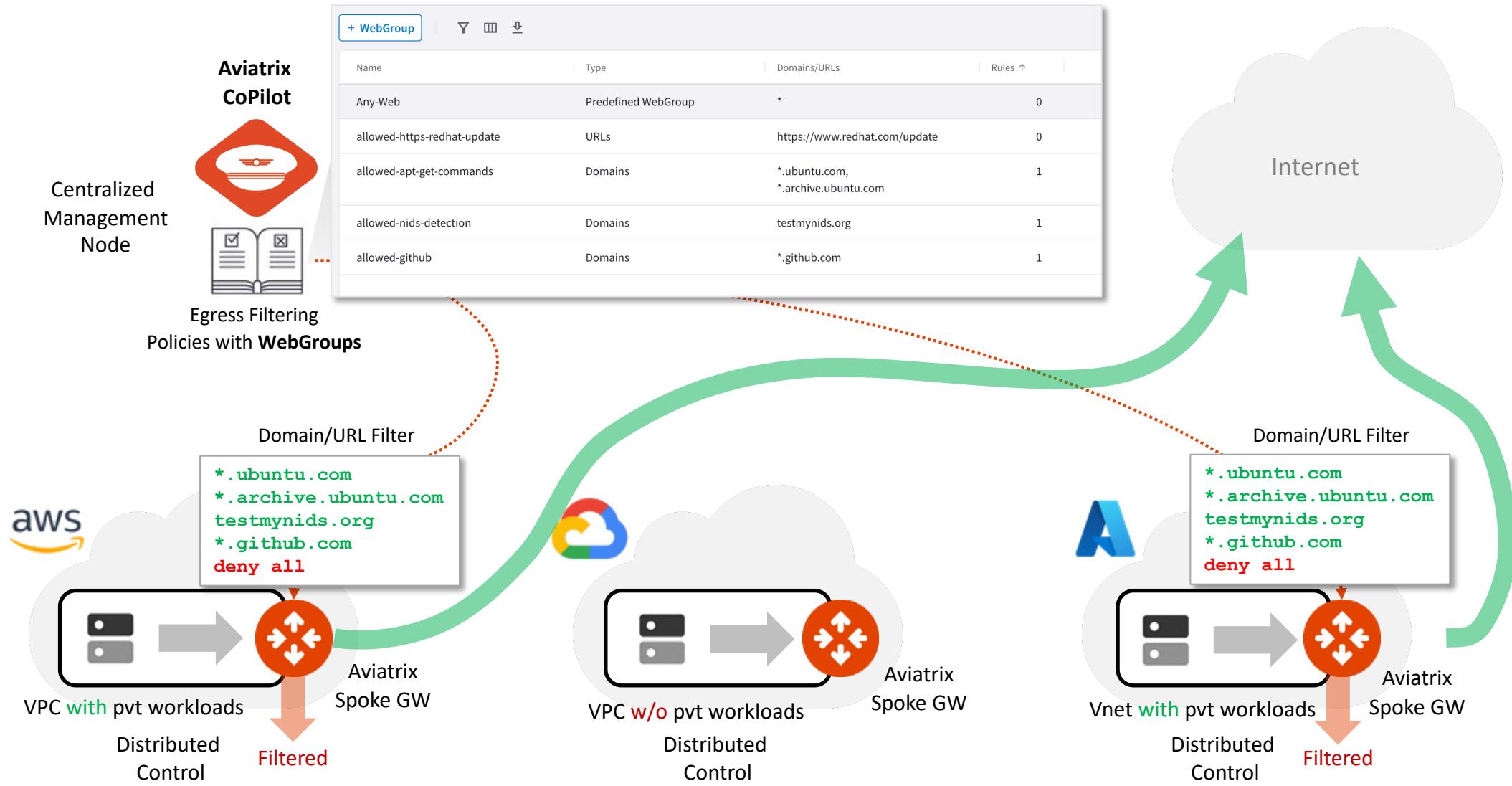
# Aviatrix Secure Egress



# 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.

The screenshot shows the CoPilot interface with the Egress VPC/VNets tab selected. A red box highlights the '+ Local Egress on VPC/VNets' button. The table lists six entries, each representing a spoke VPC with its name, point of egress, and transit attachment:

Name	Point of Egress	Transit Attachment
aws-us-east1-spoke1	Native Cloud Egress	aws-us-east1-transit
aws-us-east2-spoke1	Native Cloud Egress	aws-us-east2-transit
azure-us-west-spoke1	Native Cloud Egress	azure-us-west-transit
azure-us-west-spoke2	Native Cloud Egress	
gcp-us-central1-spoke1	Native Cloud Egress	gcp-us-central1-transit

The screenshot shows the AWS CloudWatch Metrics interface for the VPC/VNet Route Tables tab of the aws-us-east2-spoke1 resource. It displays the Route Table ID (rtb-0f555197f0c9f6d8f) and Associated Subnets (1). The main table lists the route table structure:

Route	Target	Gateway
10.0.1.0/24	local	local
192.168.0.0/16	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
172.16.0.0/12	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
10.0.0.0/8	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1

The screenshot shows the AWS CloudWatch Metrics interface for the VPC/VNet Route Tables tab of the aws-us-east2-spoke1 resource. It displays the Route Table ID (rtb-0f555197f0c9f6d8f) and Associated Subnets (1). The main table lists the route table structure, including a red box around the 0.0.0.0/0 route:

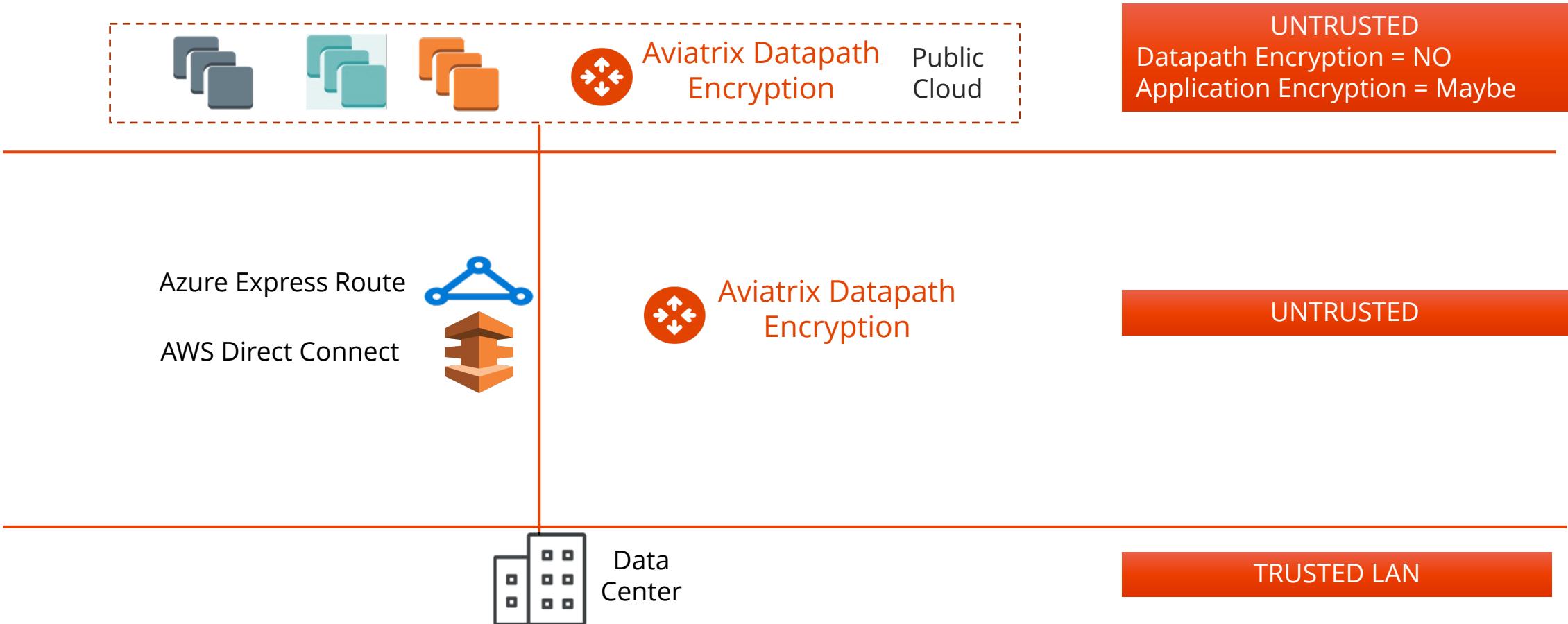
Route	Target	Gateway
10.0.1.0/24	local	local
192.168.0.0/16	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
172.16.0.0/12	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
10.0.0.0/8	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
0.0.0.0/0	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1



# High Performance Encryption (HPE)

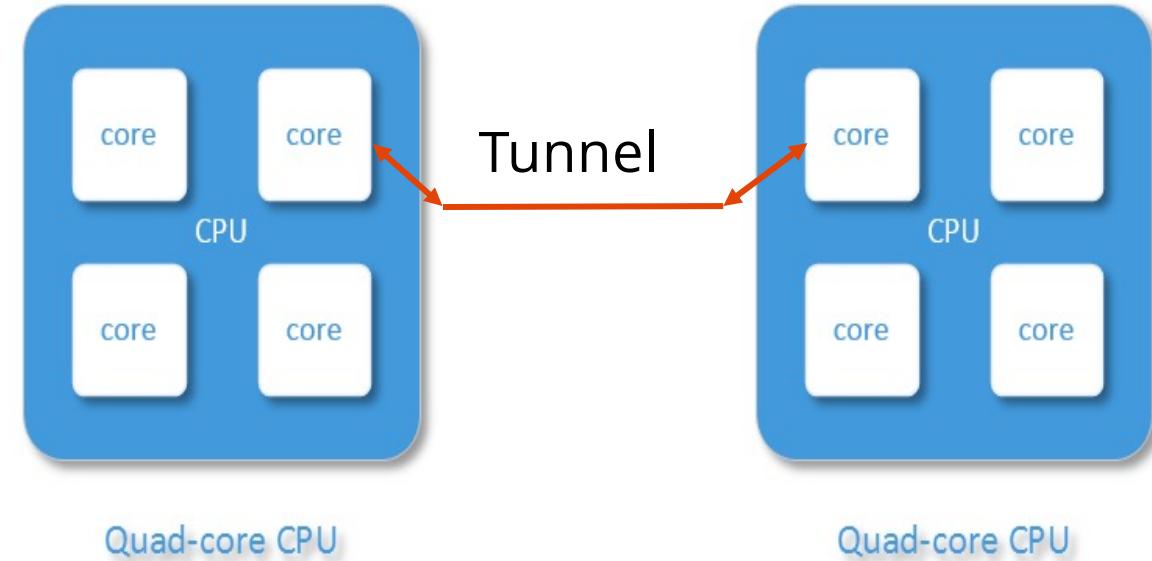
aka Insane Mode

# Zero Trust – Datapath Encryption



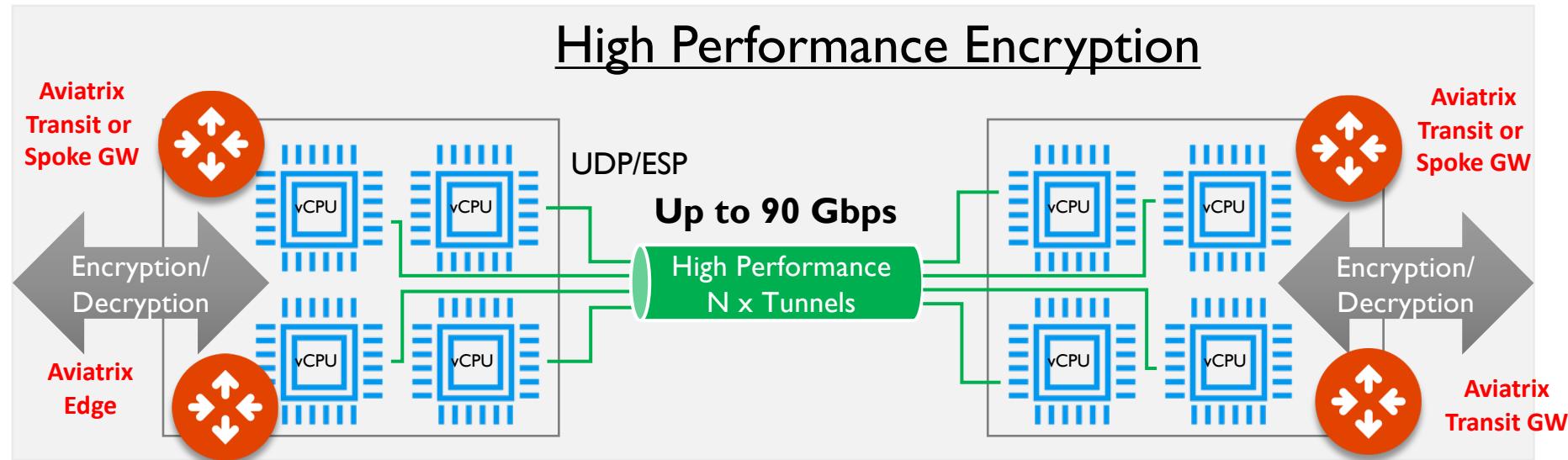
# Problem Statement – Native Cloud IPsec Performance is Limited

- Native Cloud IPsec VPN solutions have a maximum encryption performance of **1.25Gbps per tunnel**
  - VPC  $\leftrightarrow$  VPC
  - On-prem  $\leftrightarrow$  Cloud (including DX – but link could be 10G!)
  - Cloud  $\leftrightarrow$  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