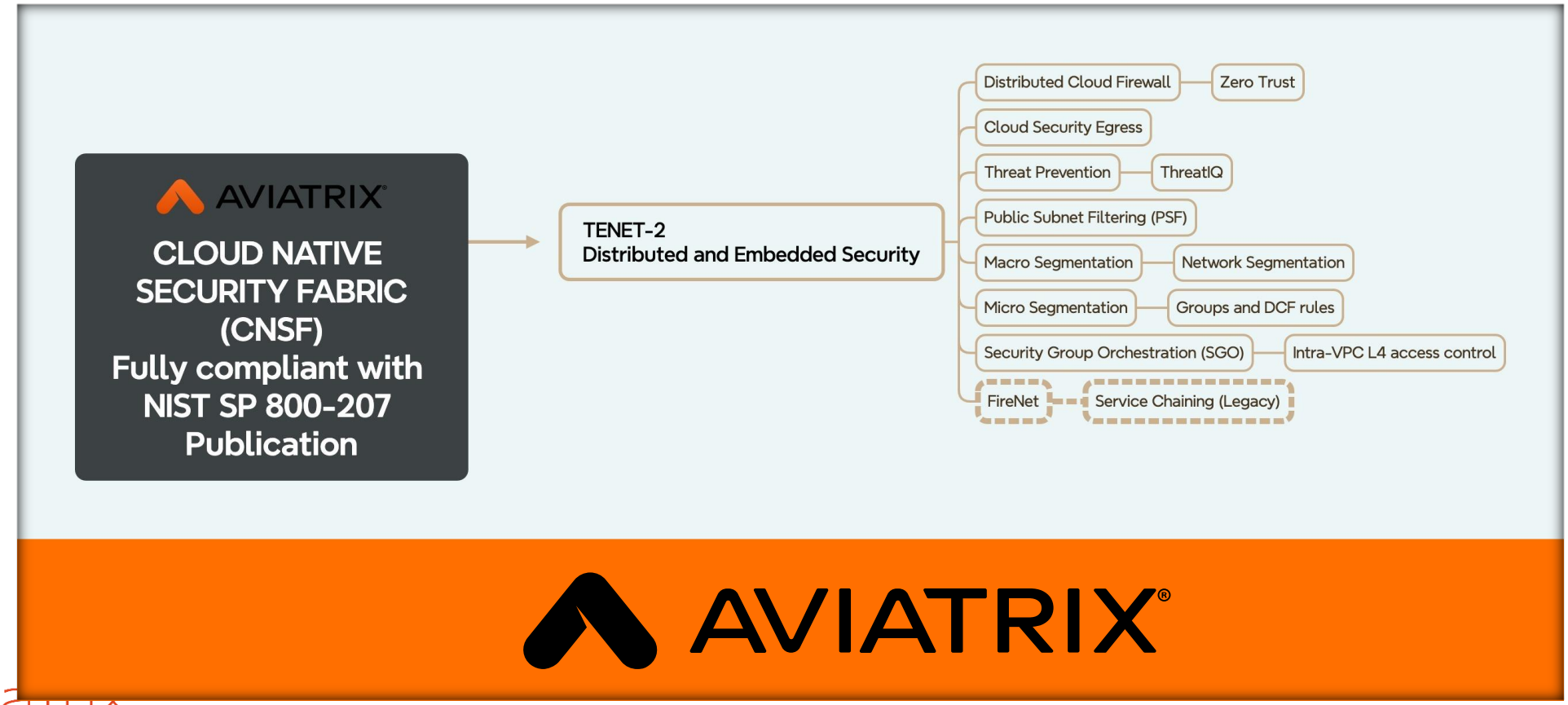
Tenet-2: Distributed and Embedded Security

ACE Solutions Architecture Team

Topics Covered

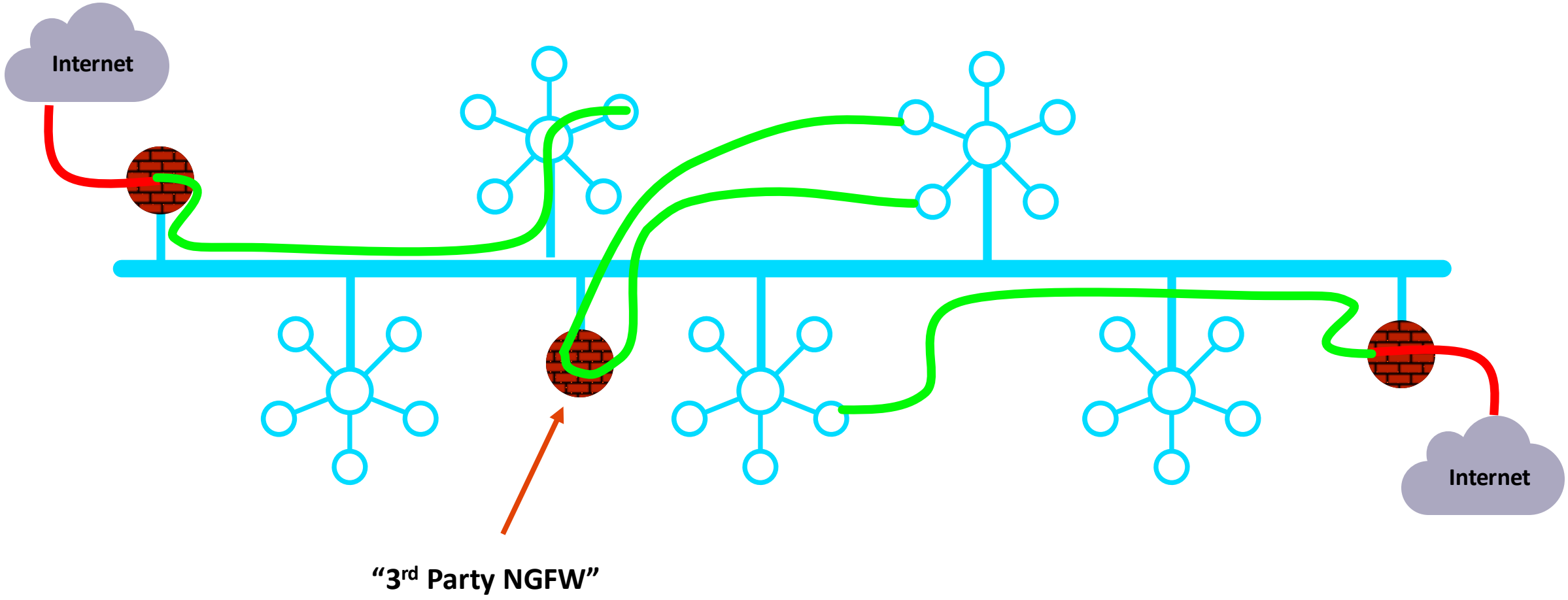
Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

Assets and traffic moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture. Workloads should retain their security posture when moving to or from enterprise-owned infrastructure. This includes devices that move from enterprise networks to non-enterprise networks. This also includes workloads migrating from on-premises data centers to non-enterprise cloud instances.

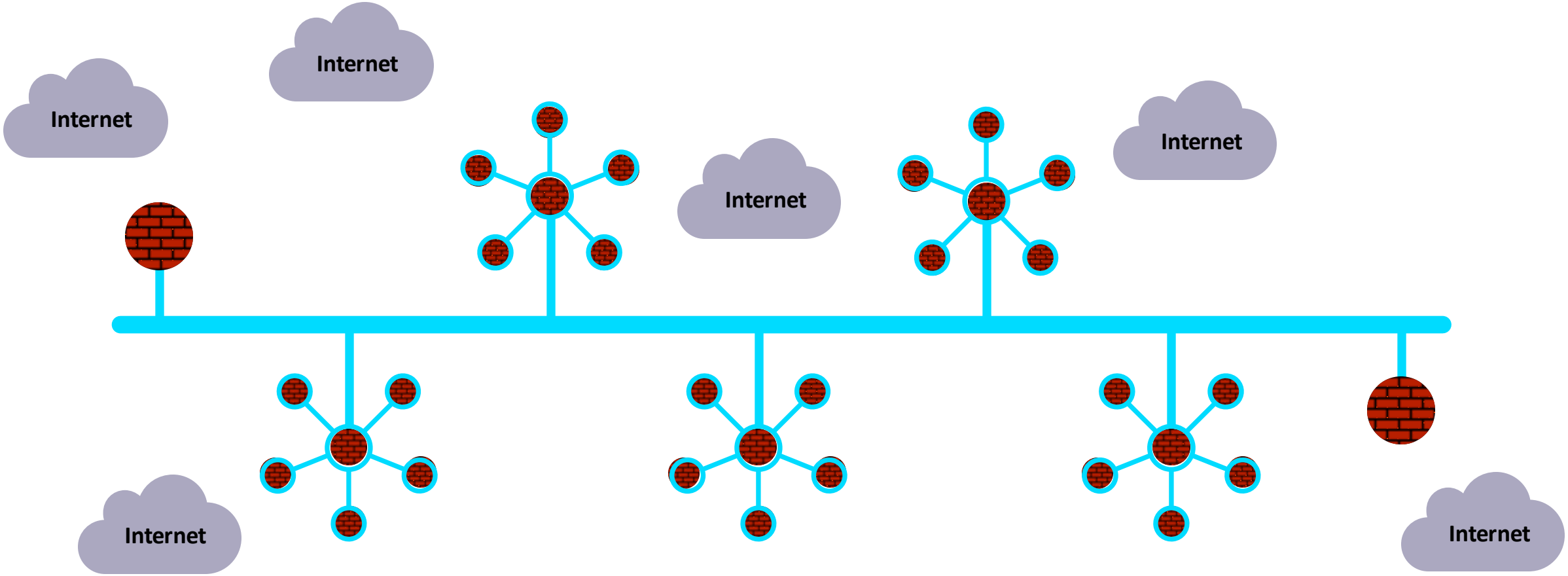


Distributed Cloud Firewall

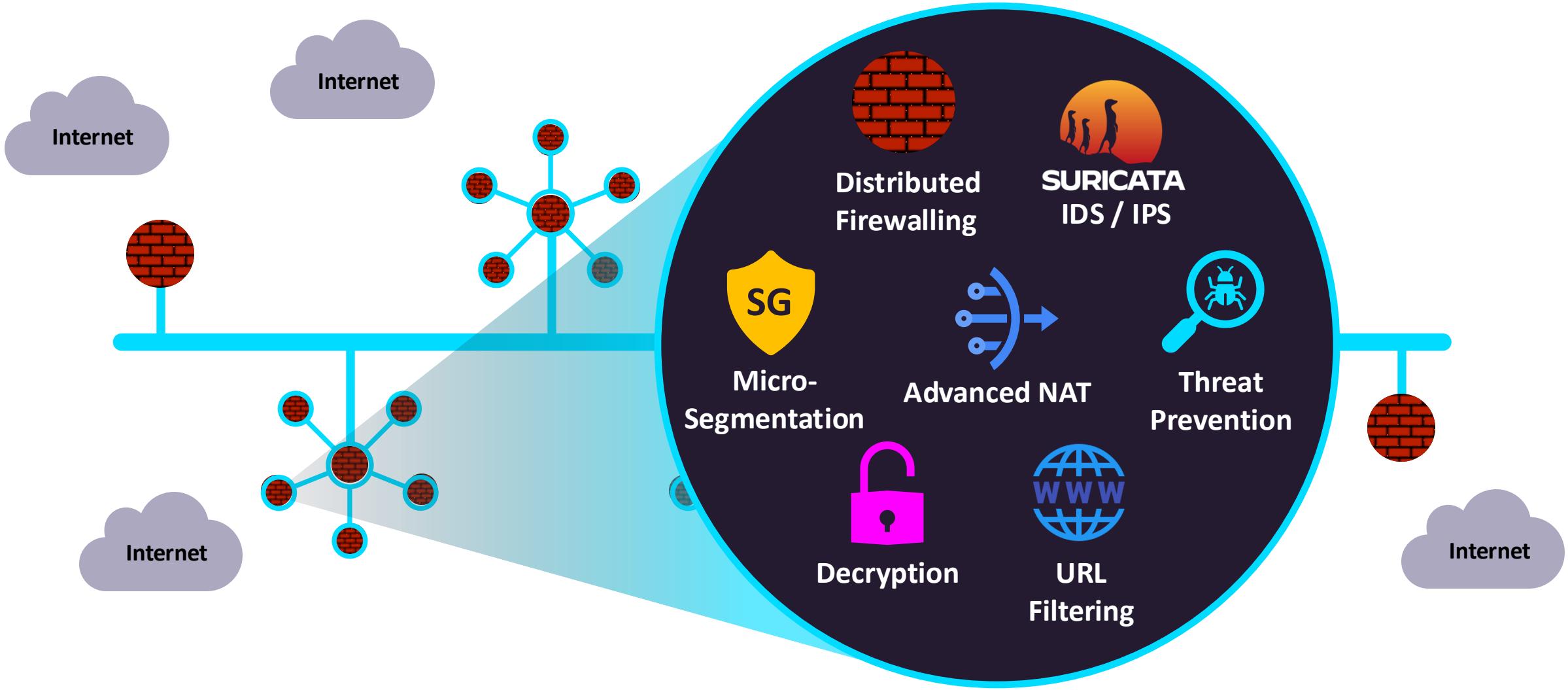
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products…



Firewalling Functions were Embedded in the Cloud Network Everywhere…

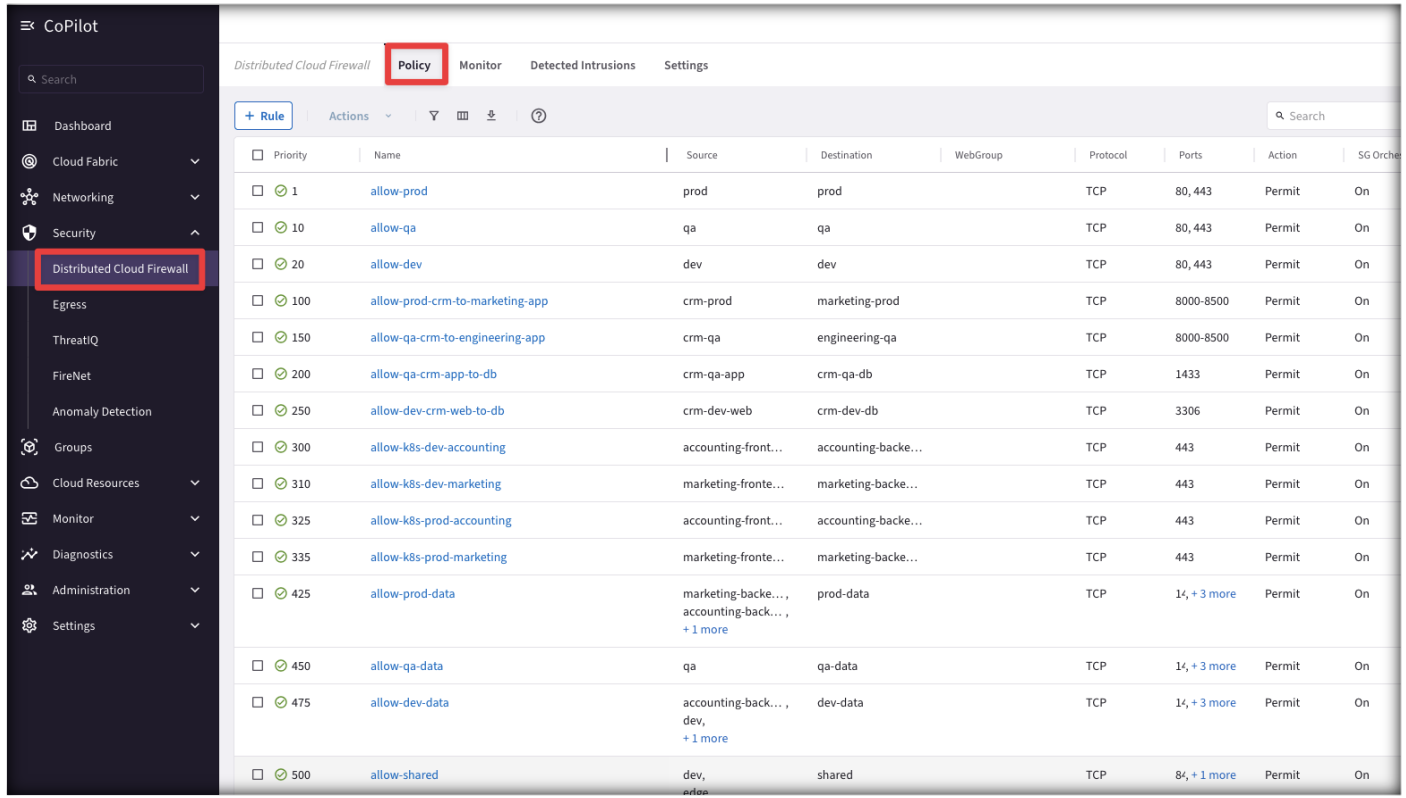


And, What If it was more than just firewalling…



And, What If Policy Creation Looked Like One Big Firewall…

Centralized Policy Creation → Distributed Enforcement



Aviatrix CoPilot

IDS / IPS

Micro-Segmentation

Threat Prevention

Distributed Firewalling

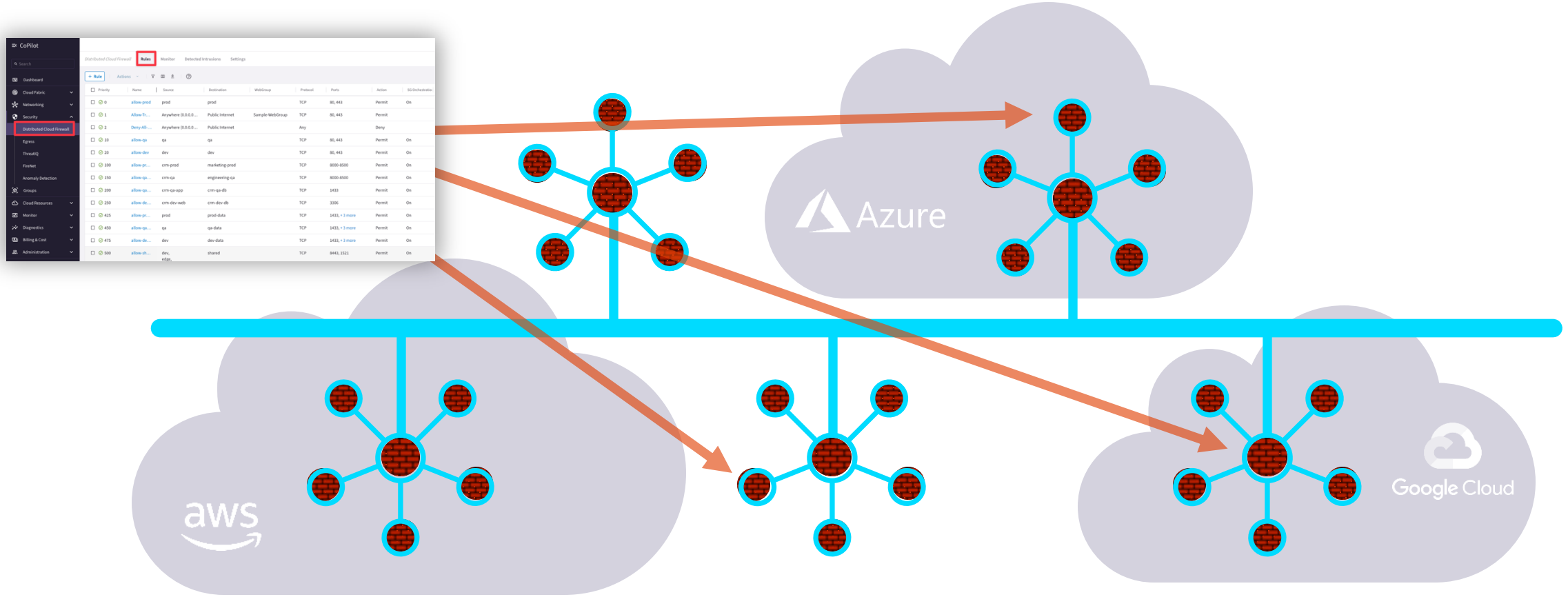
URL Filtering

Decryption

Advanced NAT

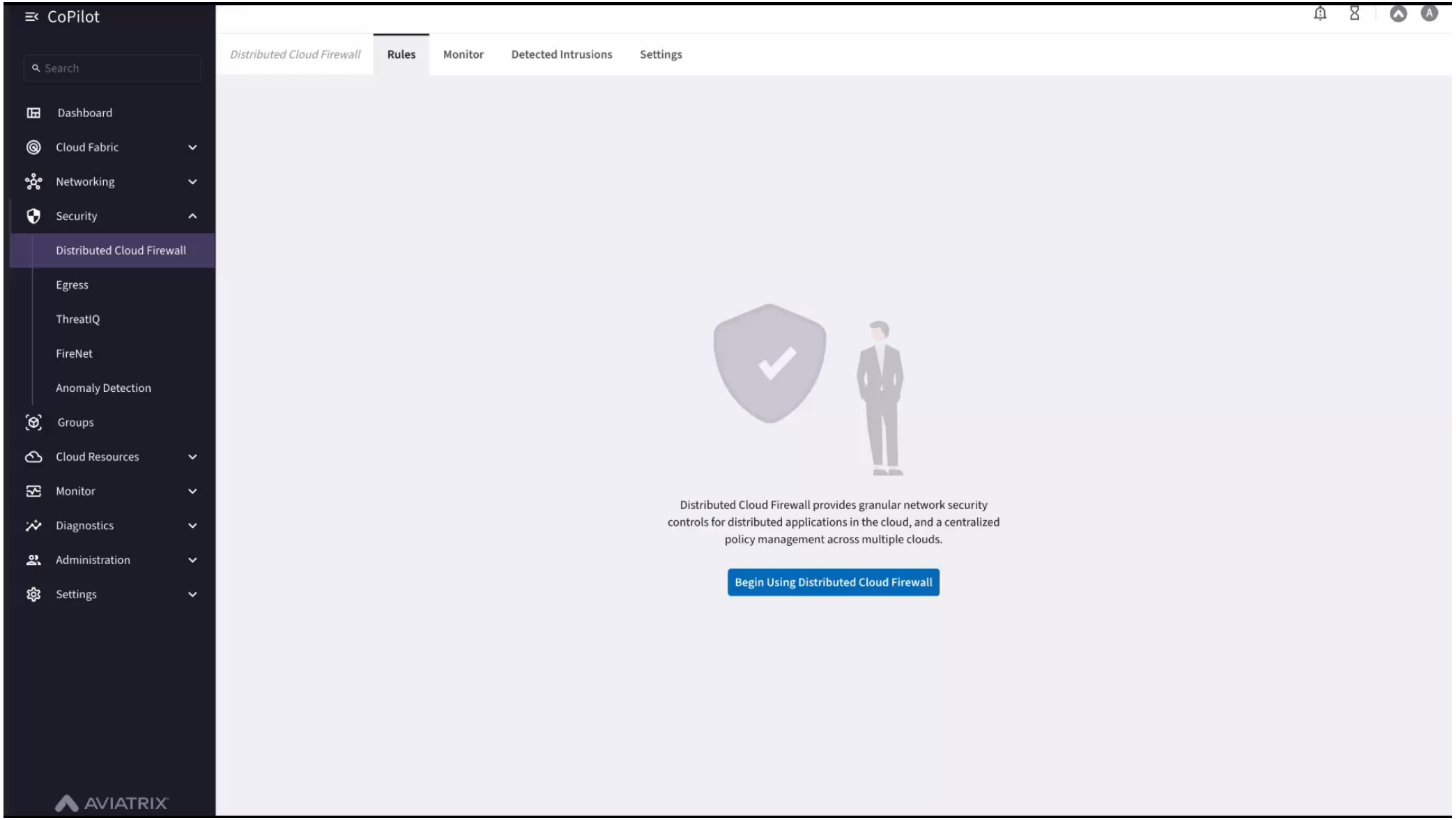
Aviatrix Spoke & Edge

A Distributed Cloud Firewall…

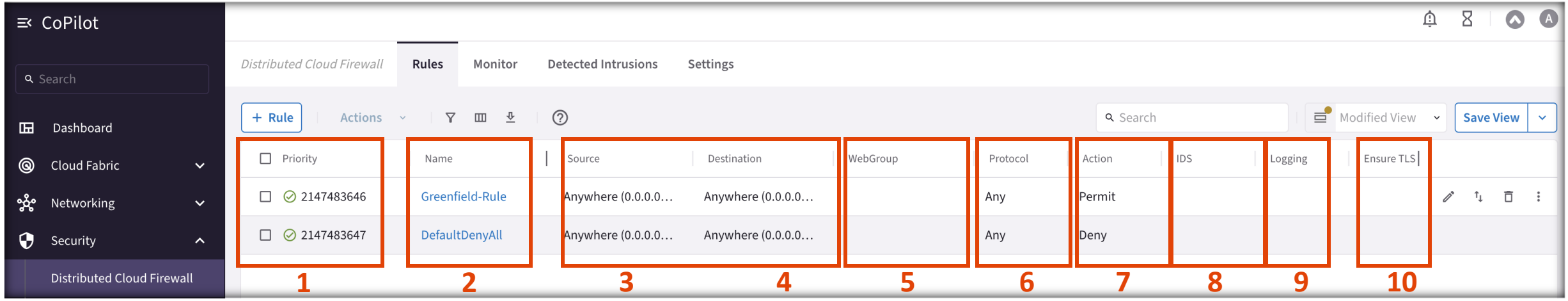


Where and How Policies Are Enforced Is Abstracted…

Distributed Cloud Firewall Activation



Distributed Cloud Firewall Rule: Field Position and their Meanings



1: Priority: the lowest priority wins

2: Distributed Cloud Firewall Rule Name

3-4: Source and Destination Groups

5: WebGroup: for filtering based on a specific Domain/URL

6: Protocol → TCP/UDP/ICMP

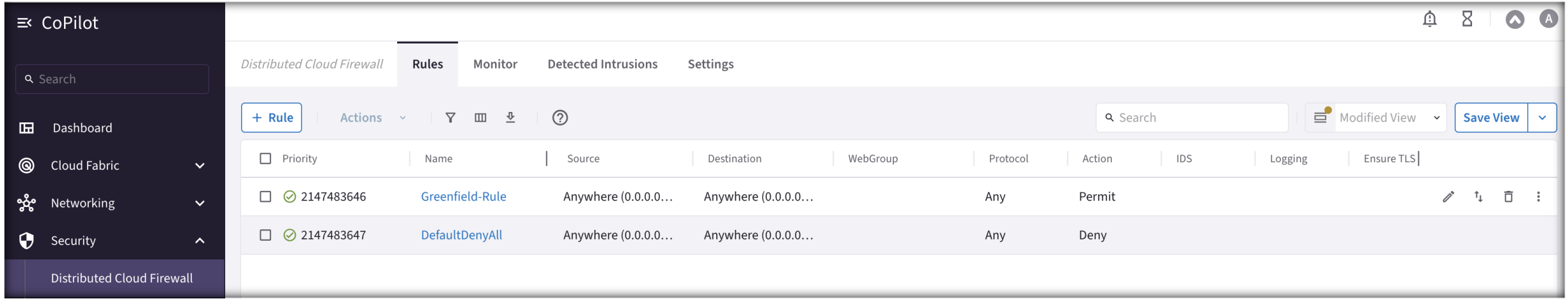
7: Action → Permit/Deny

8: Intrusion Detection System: Enabled/Disabled

9: Loggin → On/Off

10: Ensure TLS → On/Off

Distributed Cloud Firewall Rule: Initial configuration – Deny-List Model



In a deny-list (also called *blacklist*) firewall model, the default security posture is **permissive**:

Default Policy

All network traffic is allowed to pass through unless explicitly blocked by specific rules

Rule Processing

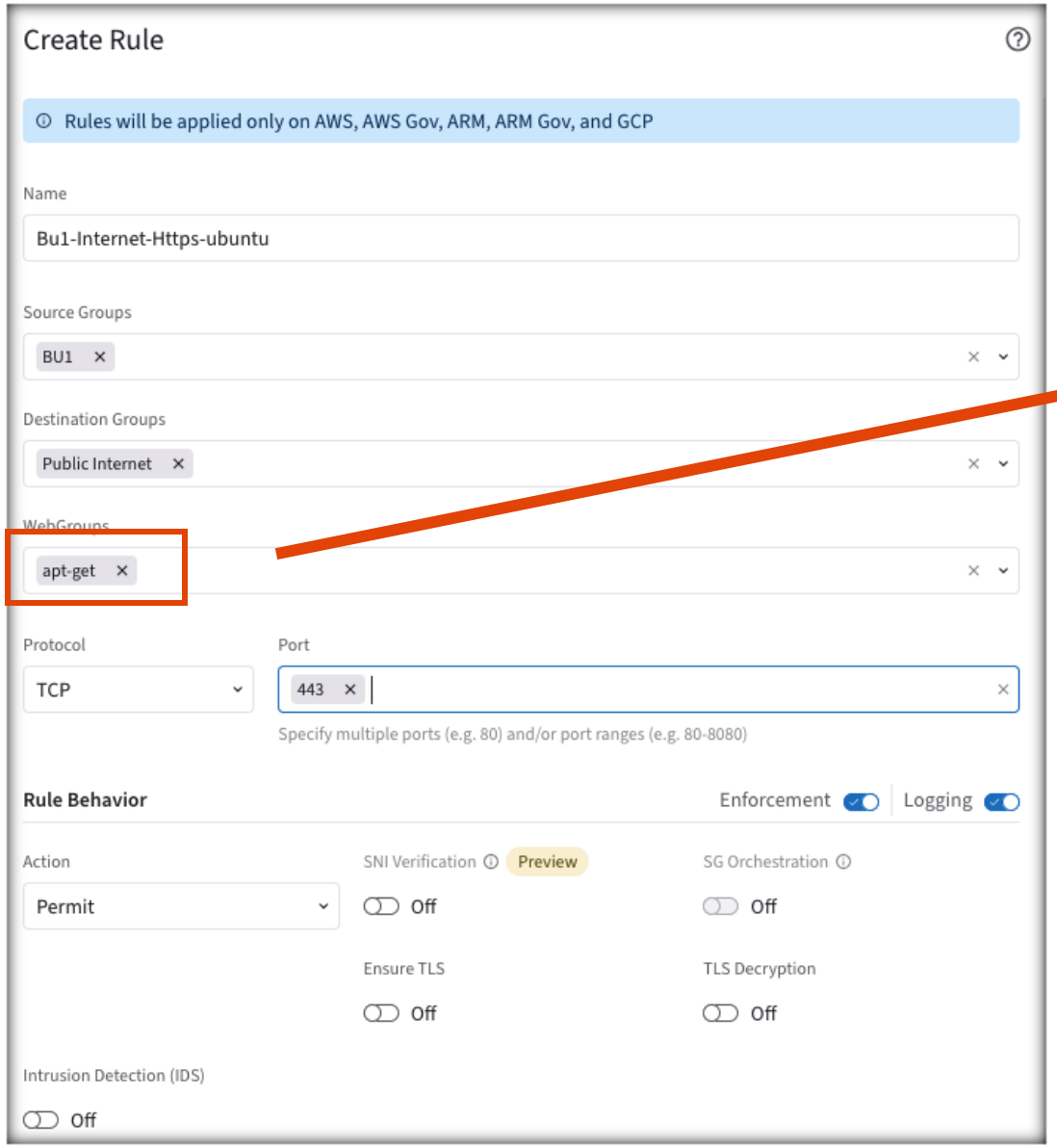
Firewall evaluates traffic against deny rules and only blocks what matches those explicit criteria

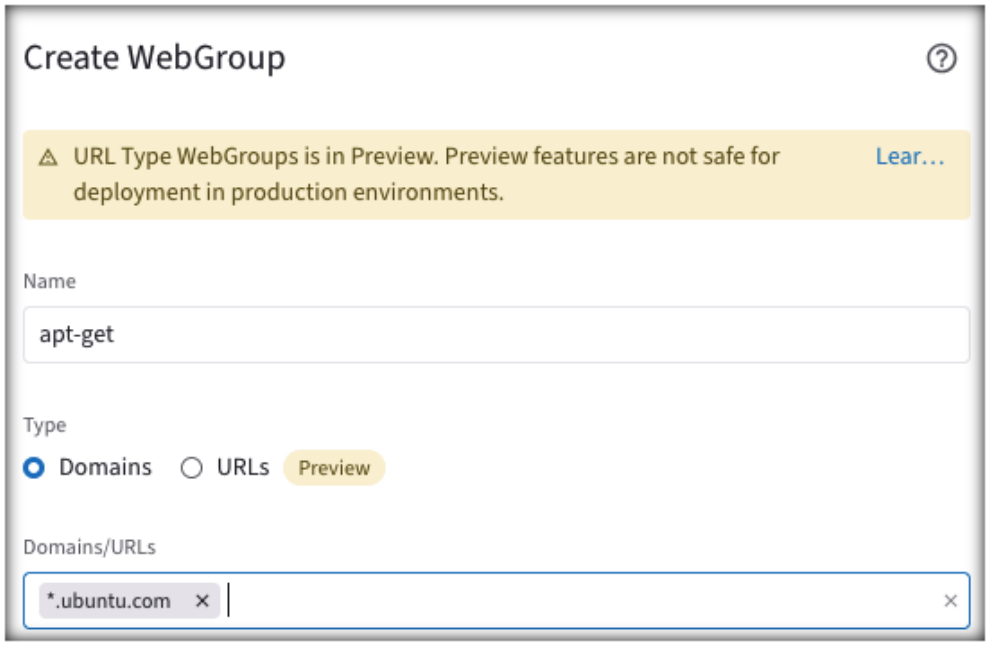
Security Risk: Since only known threats are blocked, new attack vectors can easily bypass deny-list firewalls, creating significant security vulnerabilities.

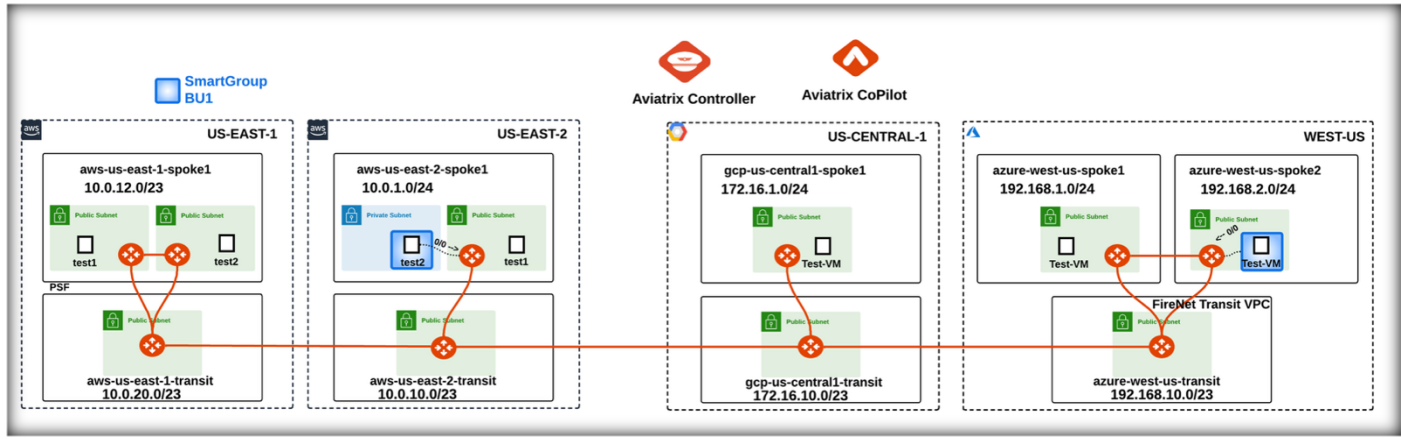
Security Implications

This approach has limitations because it relies on identifying and updating a list of threats. This leaves the network vulnerable to new, unknown, or evolving threats. Additionally, if the deny list is not carefully managed, legitimate traffic might be accidentally blocked, causing disruptions. Overall, deny-list models require constant maintenance

Distributed Cloud Firewall Rule: Creating Rules







Distributed Cloud Firewall Rule: Zero-Trust Approach

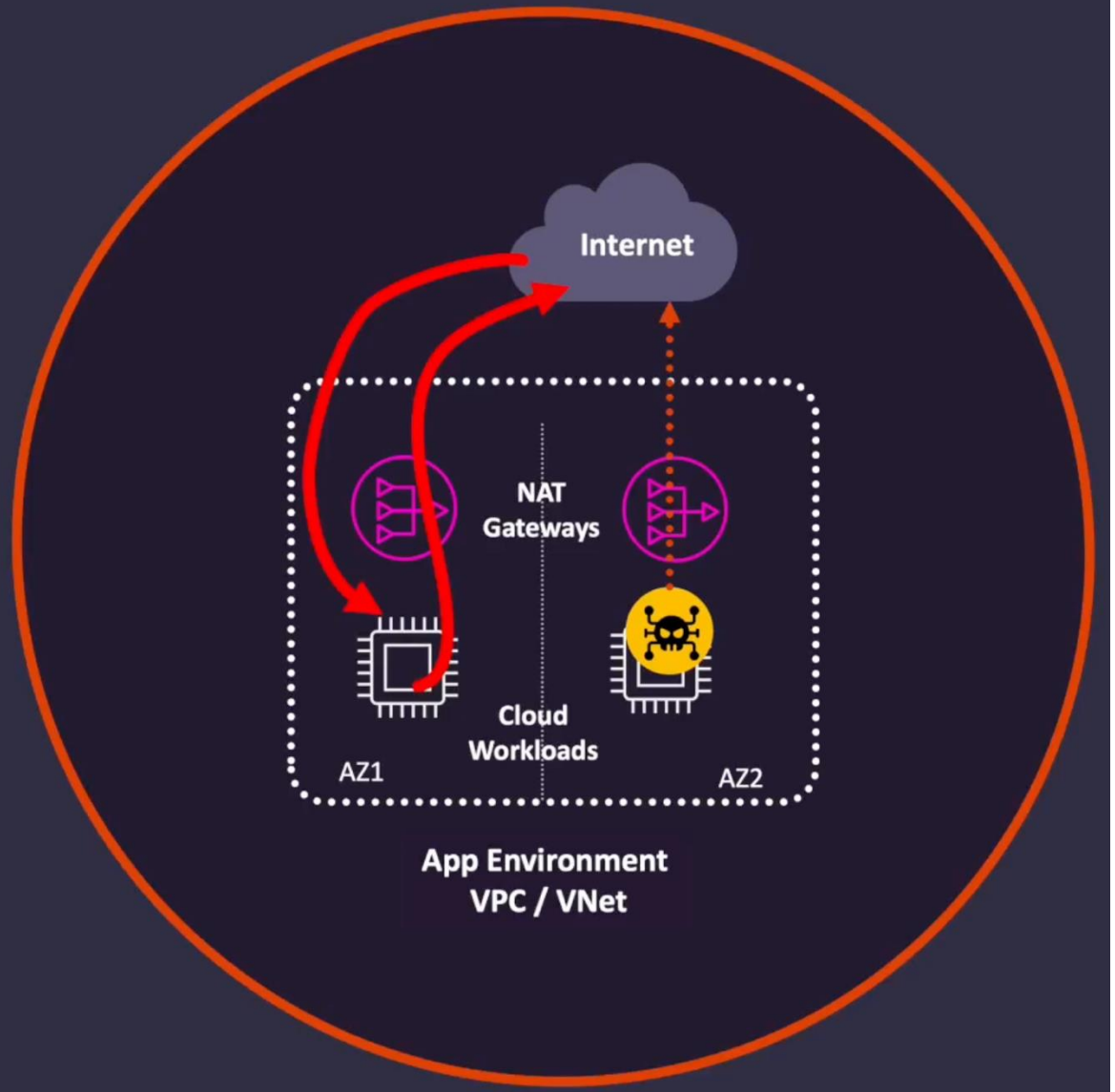
Distributed Cloud Firewall Rule: Zero-Trust Approach

Cloud Security Egress

Understanding the Pain

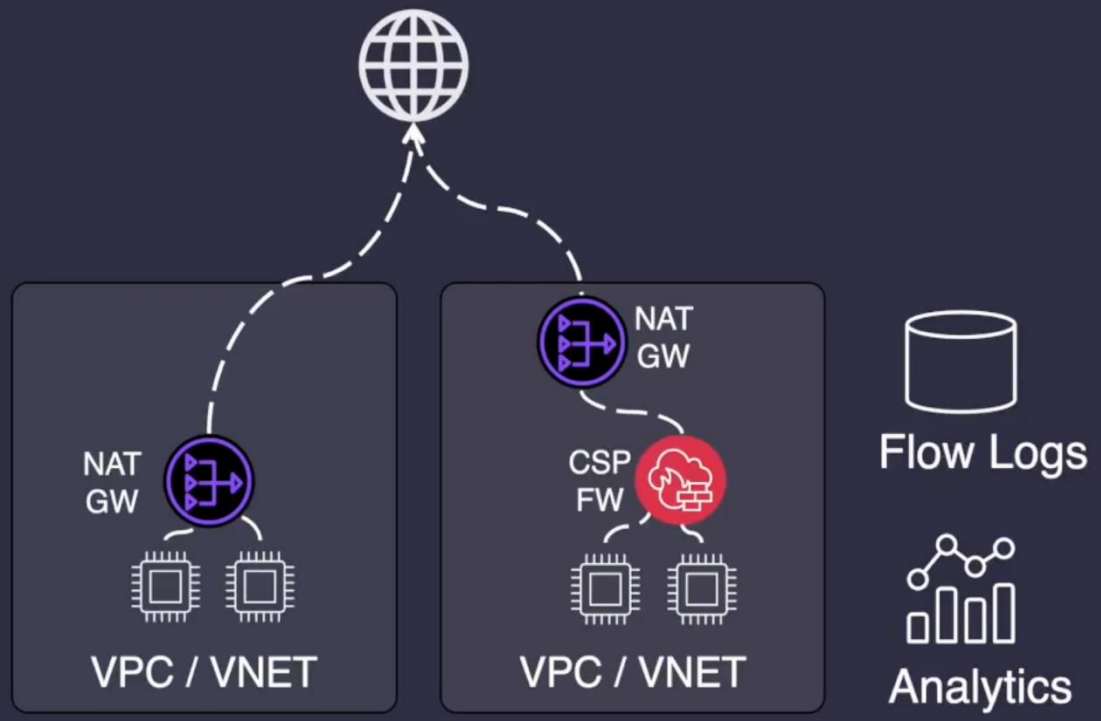
Improve Security and Lower Cloud Costs

- **Business Pain**
  - Excessive Cloud Costs
  - Lack of Compliance & Governance
  - Risk to Business-Critical Workloads
  - Regulatory Fines and Penalties
  - Brand Health and Customer Trust
- **Technical Pain**
  - No Policy Enforcement
  - Slow Troubleshooting and Forensics
  - Identifying Noisy Workloads
  - Support Distributed Deployments
  - Advanced Inspection Capabilities



aviatrix

Two Common Paths



Flow Logs

Analytics

1. Distributed Cloud Provider Services

- Expensive: High data-processing costs
- Zero / Weak Security
- Poor Visibility
  - Some visibility with a lot of tools
- Log storage and analytics costs
- No centralized intelligence
- Not multi-cloud capable

CLOUD SECURITY

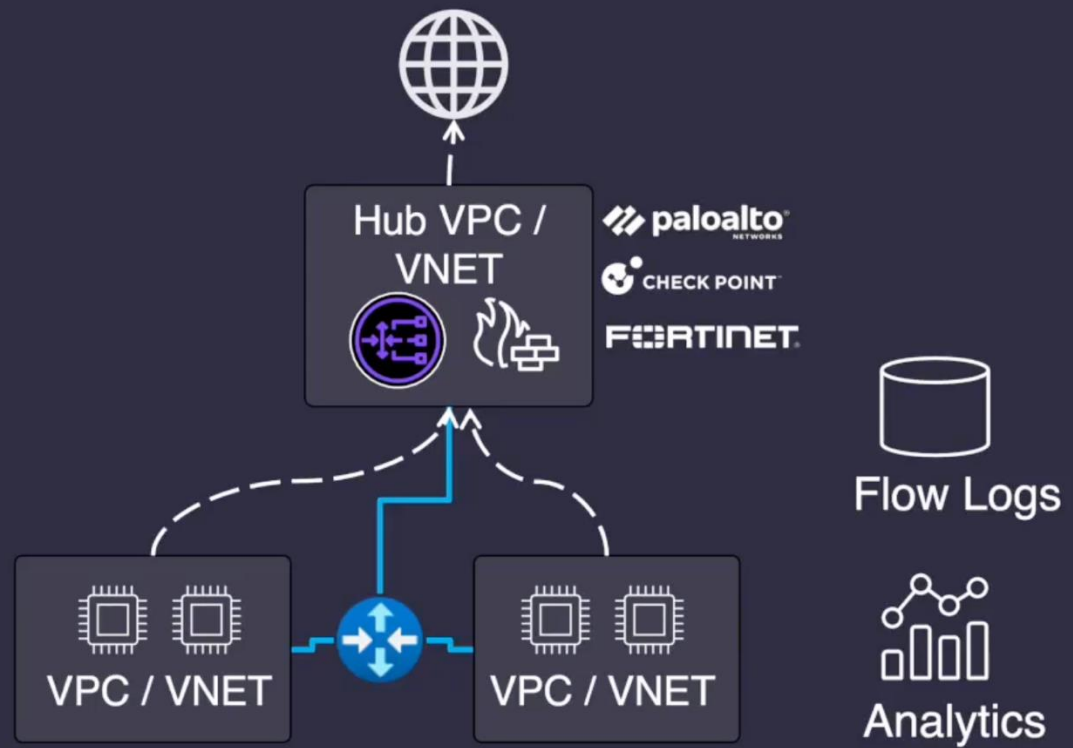
CyberRatings.org Announces Test Results for Cloud Service Provider Native Firewalls

Protection ranged from 0.38% to 50.57% for security effectiveness.

Two Common Paths

2. Central Virtualized Appliances

- Very Expensive
- Not built for cloud: operational complexity
- No support for Island VPCs / VNets
- Requires Overly Complex Routing Architecture
- Security Hub Connectivity dependent
- No centralized network and security intelligence
- Additional troubleshooting issues
- Not multi-cloud deployable



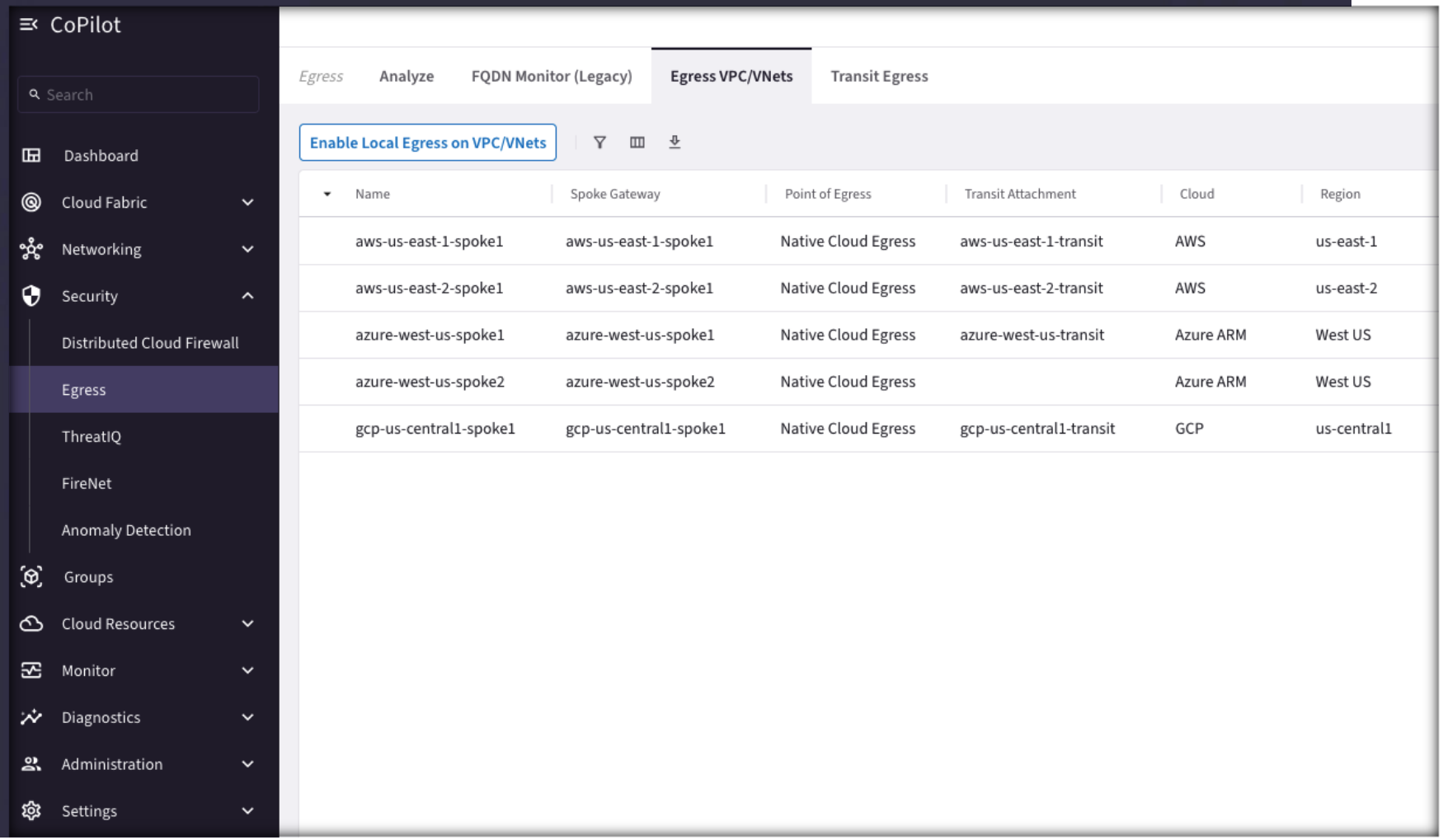
Aviatrix Cloud Firewall

What it is:

- Central Policy Management & Observability
- Distributed Enforcement: at the workload

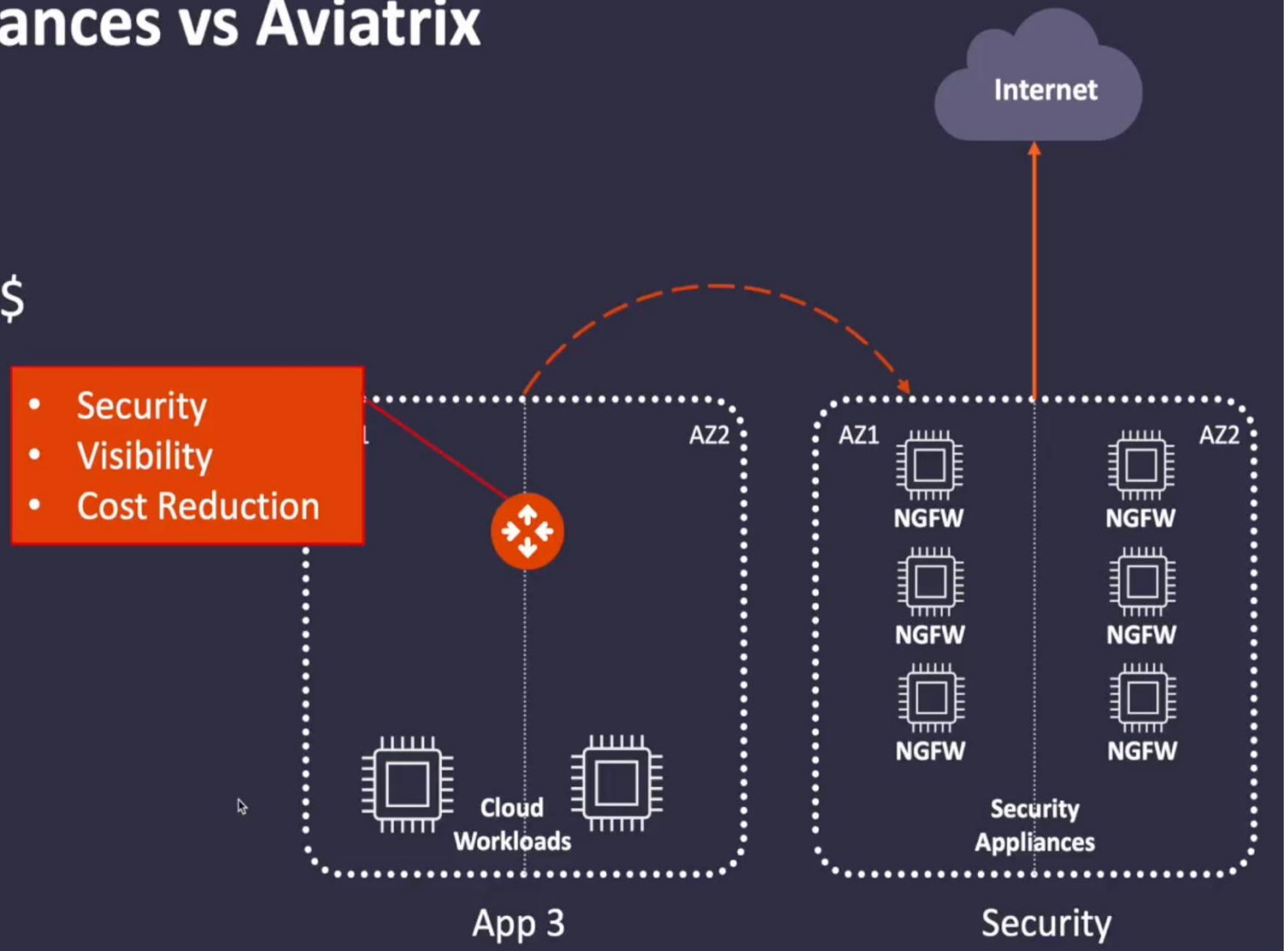
What you get:

- Secure Networking that's:
  - Agile,
  - Reduces Costs & Complexity
  - Increases Visibility



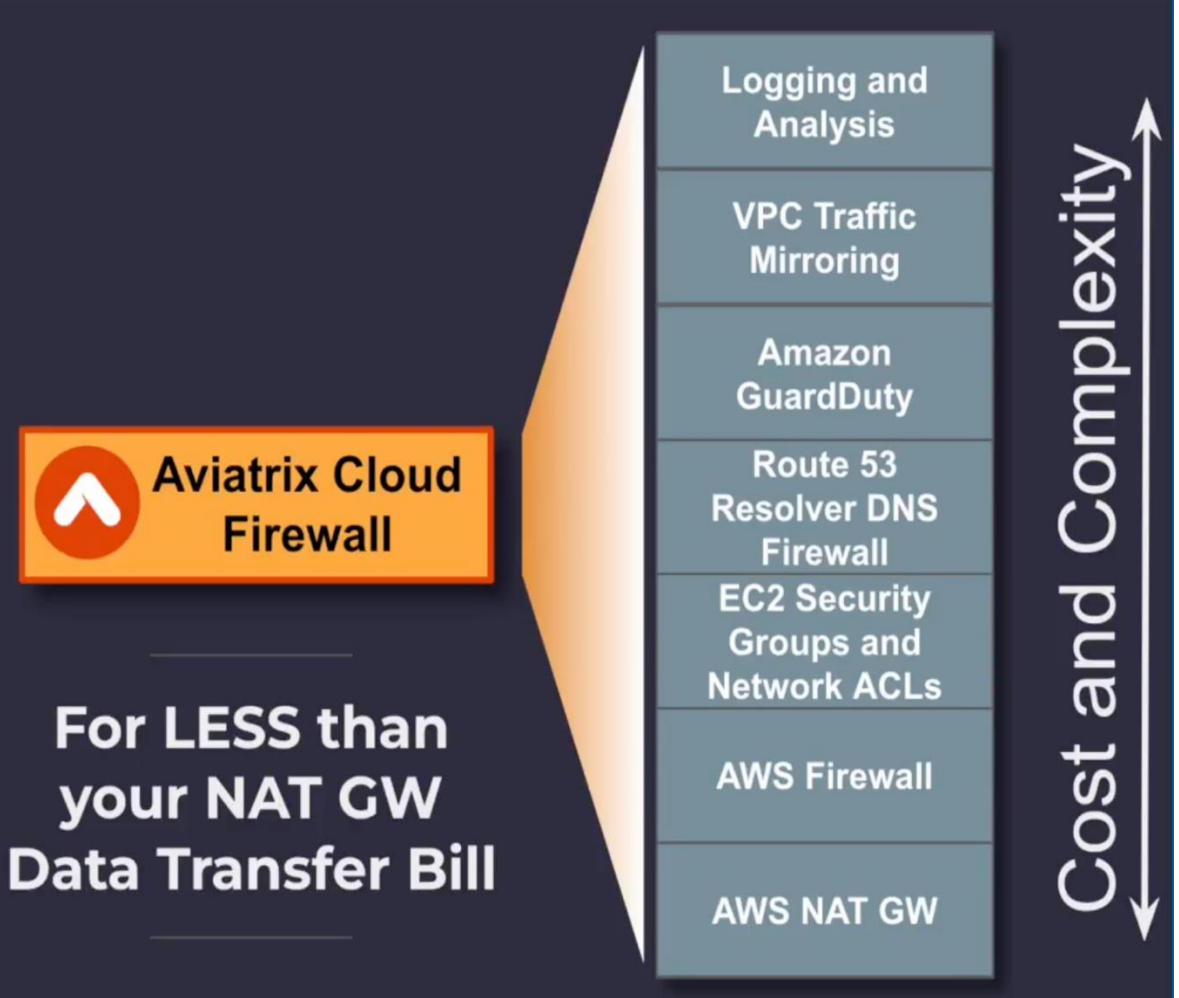
Central Virtualized Appliances vs Aviatrix

- Reduce Data Transfer Costs:
  - Enforcement at the Workload
- Reduced Data Transfer Costs $$$
- Reduced Route Complexity
- Reduced Operational Pain



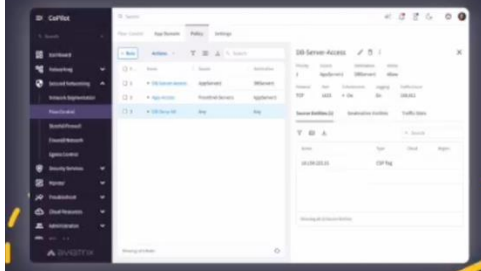
Distributed Cloud Provider Services vs Aviatrix

- Consolidation of Egress Security Stack
- Reduction in complexity
- Reduction in Data Transfer Costs $$$
- Reduction in Operational Pain



https://aviatrix.com/aviatrix-paas

Achieve 25% Cost Savings over 1st Party NAT GWs



Aviatrix PaaS

Internet

Centralized Management, Visibility, and Control

1:1 Replacement of NAT GW

AZ1 AZ2 AZ1 AZ2 AZ1 AZ2

Distributed Perimeter

Aviatrix Distributed Cloud Firewall Gateways

Aviatrix Distributed Cloud Firewall Gateways

Aviatrix Distributed Cloud Firewall Gateways

Cloud Workloads

Cloud Workloads

Cloud Workloads

Cloud Workloads

App 1

App 2

App 3

App 4

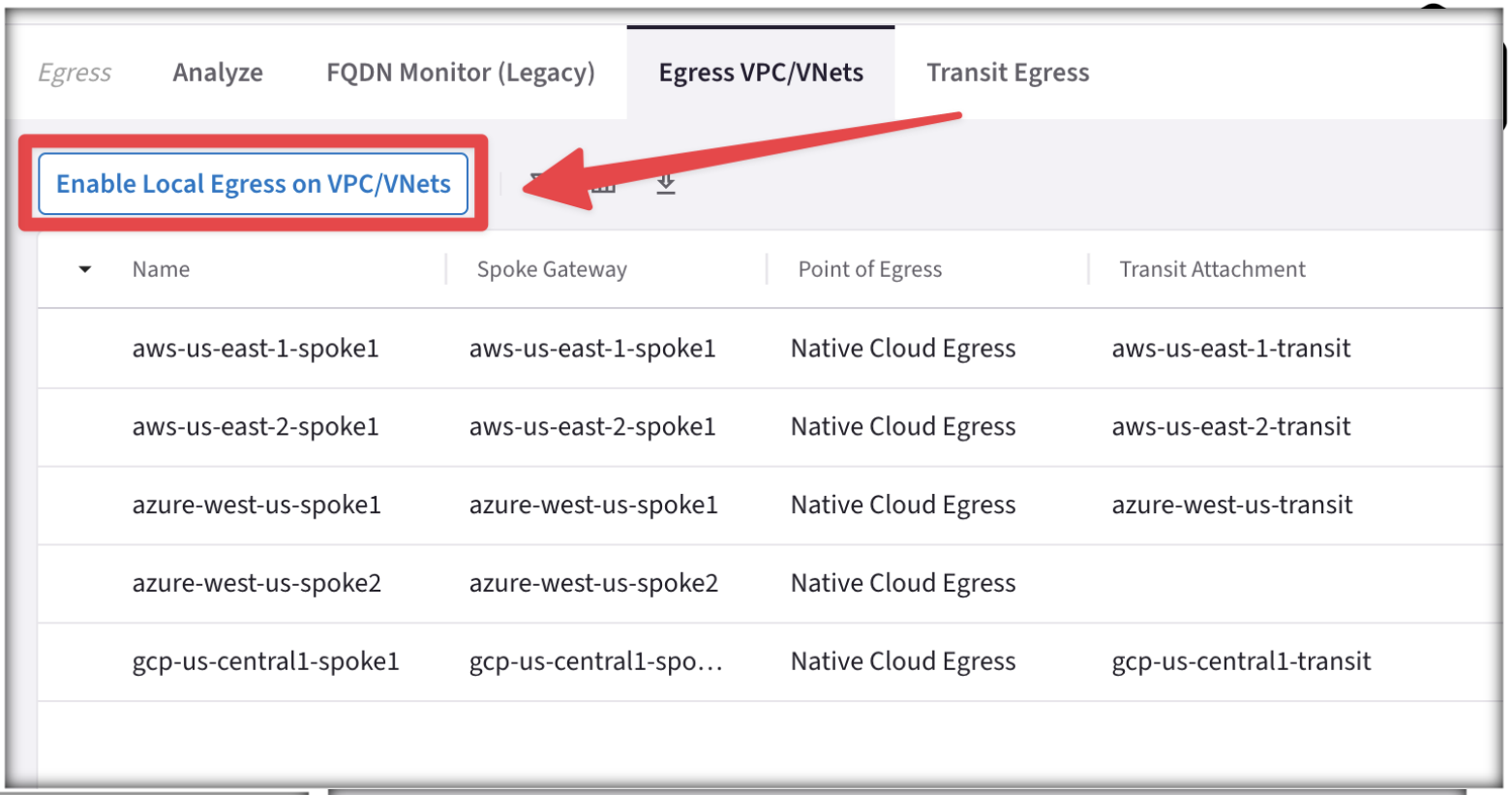
aws

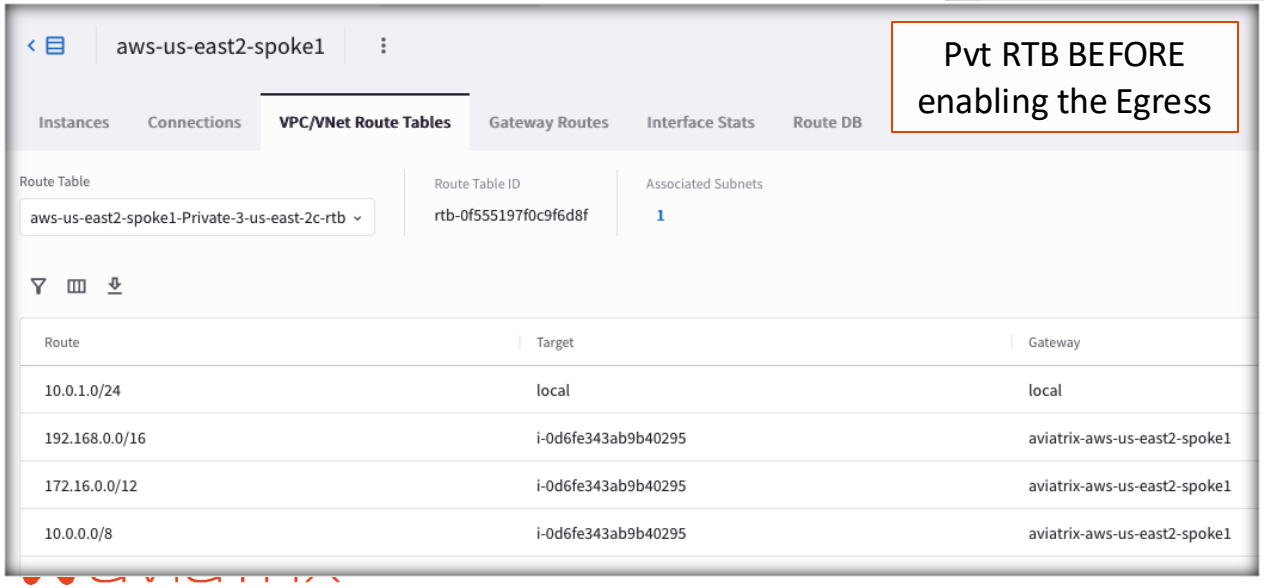
Azure

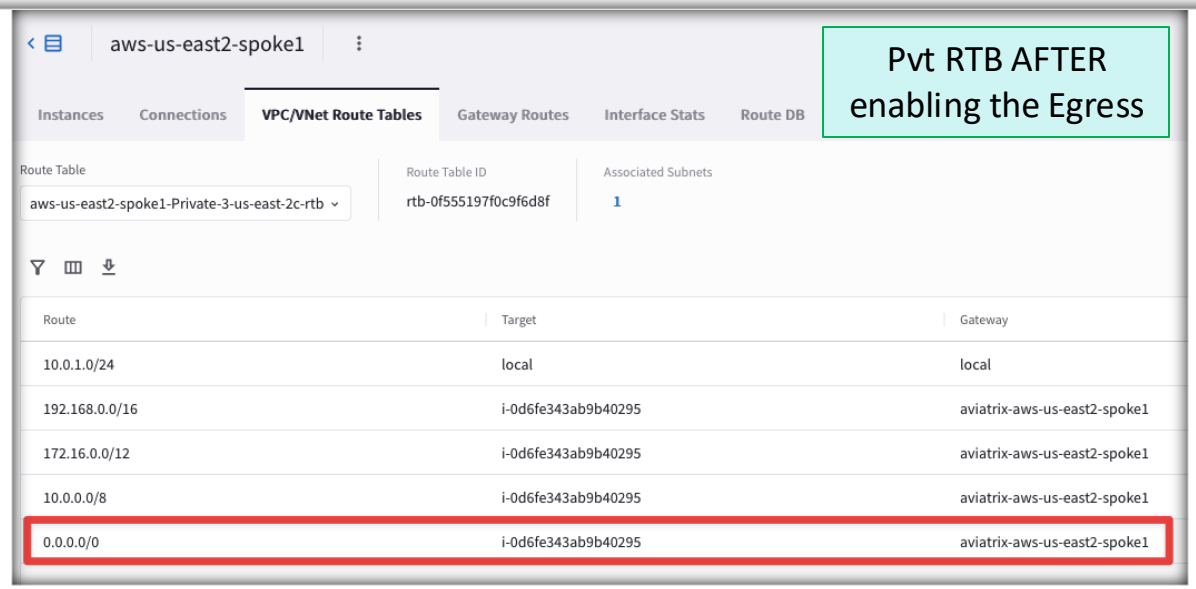
Google Cloud

Enabling Cloud Security Egress

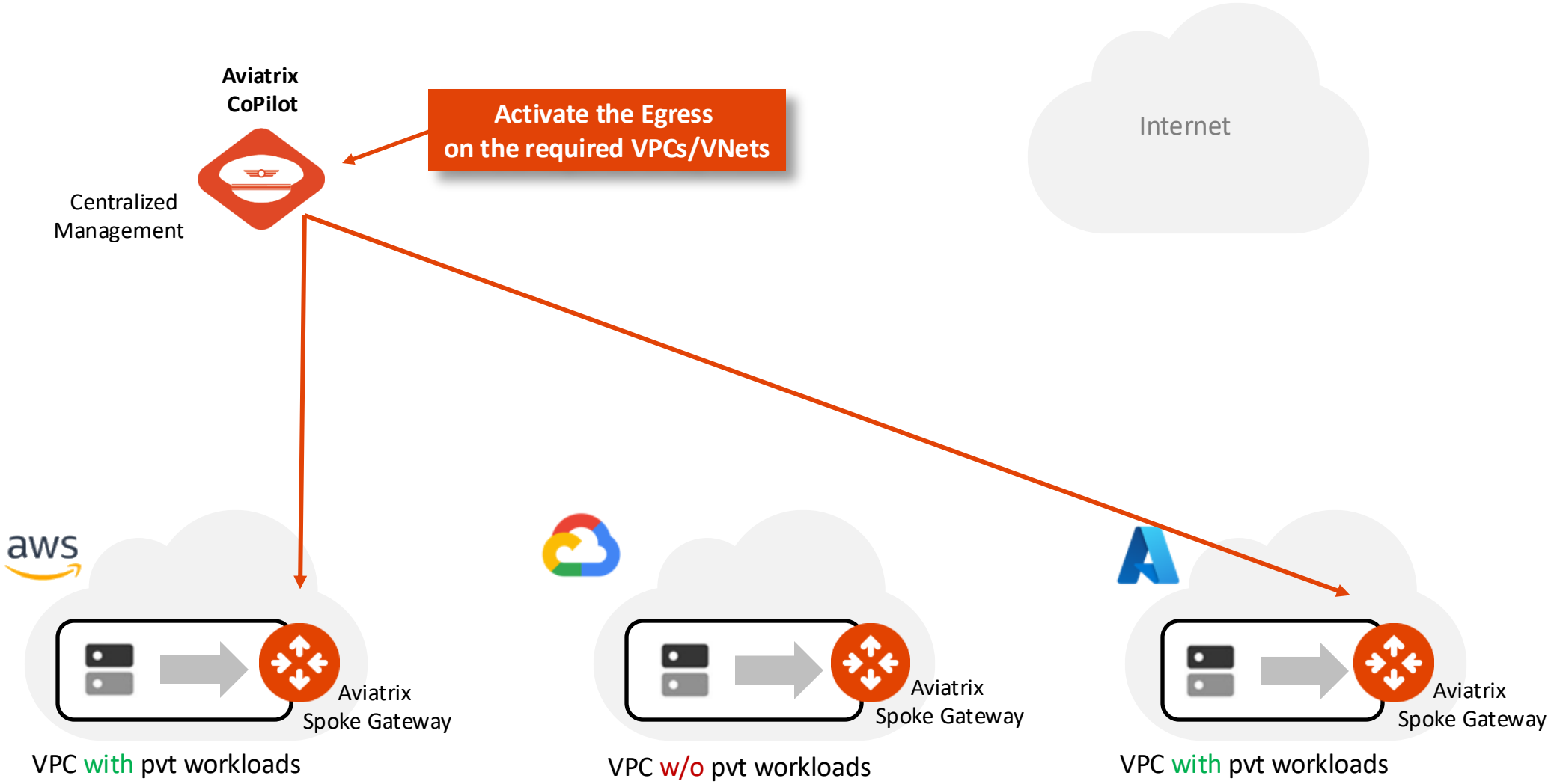
- Adding Egress Control on VPC/VNet changes the default route on VPC/VNet to point to the Spoke Gateway and enables **SNAT**.
- CAVEAT: Egress Control also <u>requires additional resources</u> on the Spoke Gateway (i.e. scale up the VM size). Before enabling Egress Control on Spoke Gateways, ensure that you have created the additional CPU resources on the Spoke Gateway required to support Egress Control.



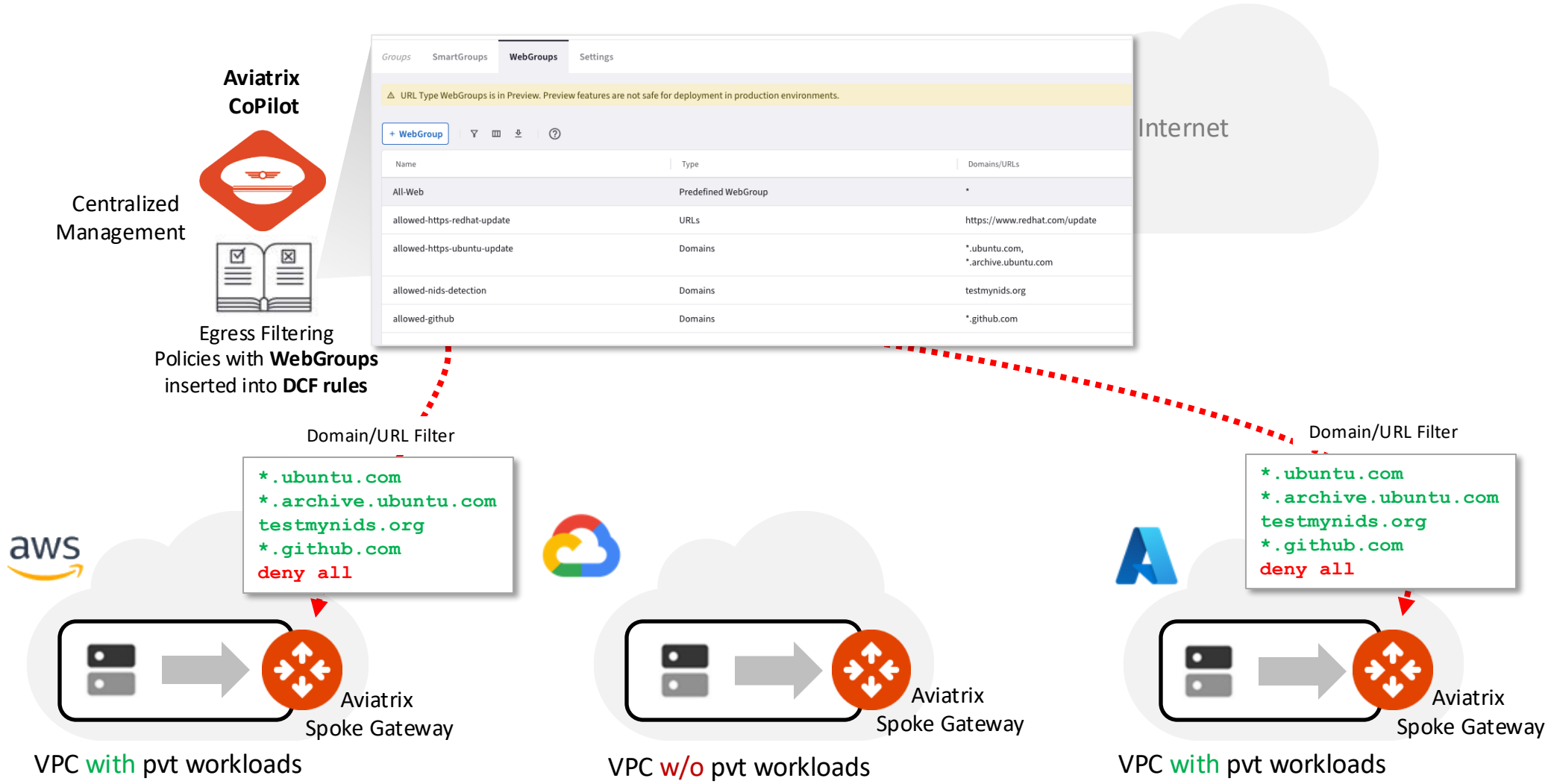




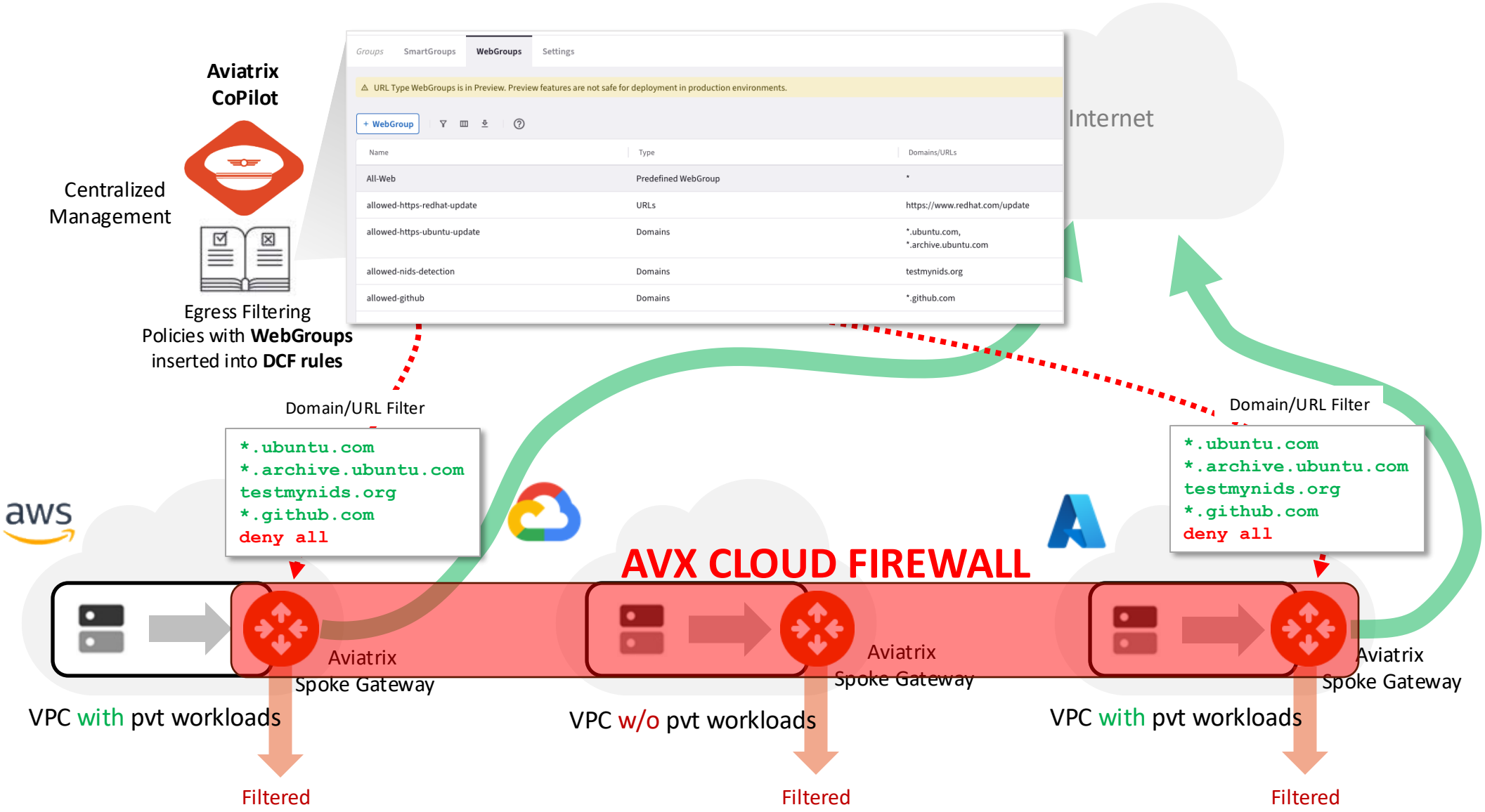
Aviatrix Cloud Firewall



Aviatrix Cloud Firewall



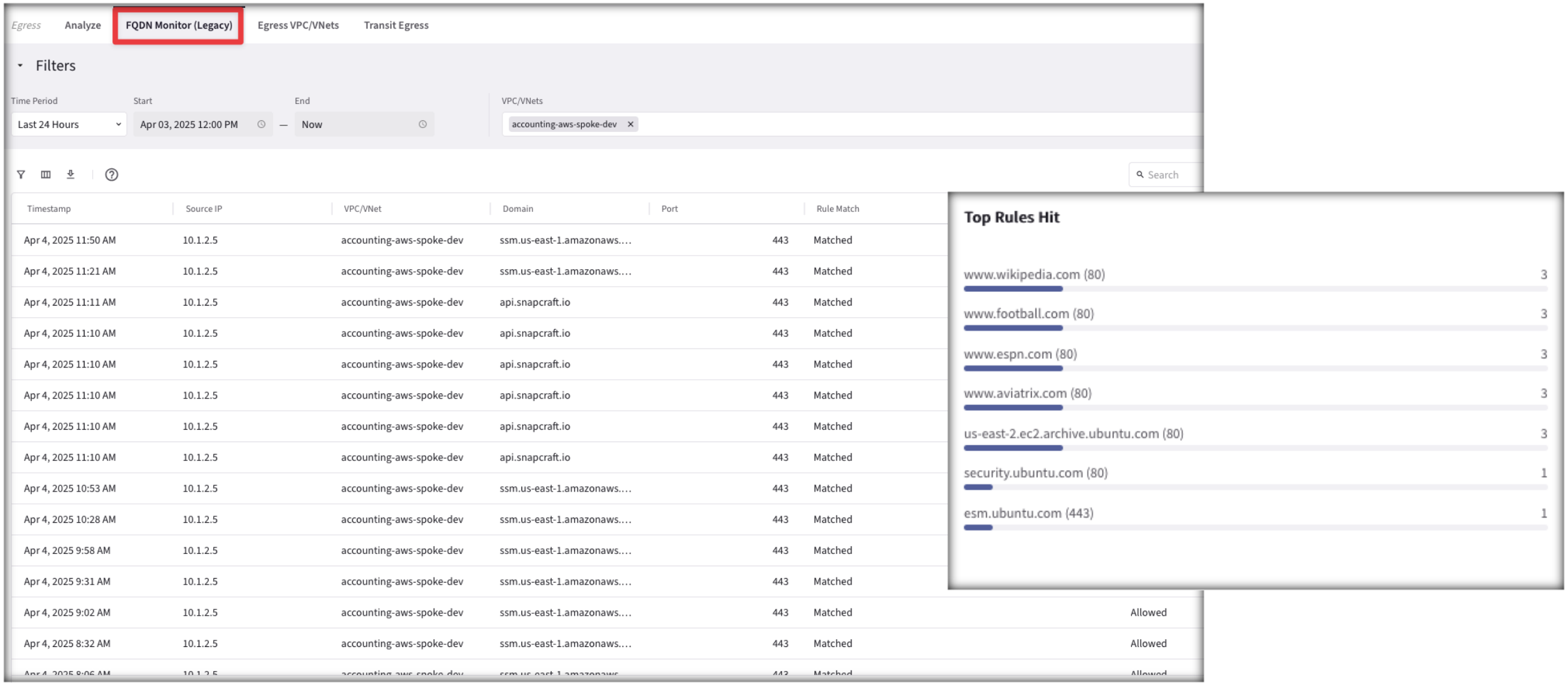
Aviatrix Cloud Firewall



- The Aviatrix Cloud Firewall can be extended also to the Edge

Monitor

- On the **FQDN Monitor (Legacy)** section you can retrieve all the logs and therefore distinguish the domains that should be permitted from those ones that should be denied.



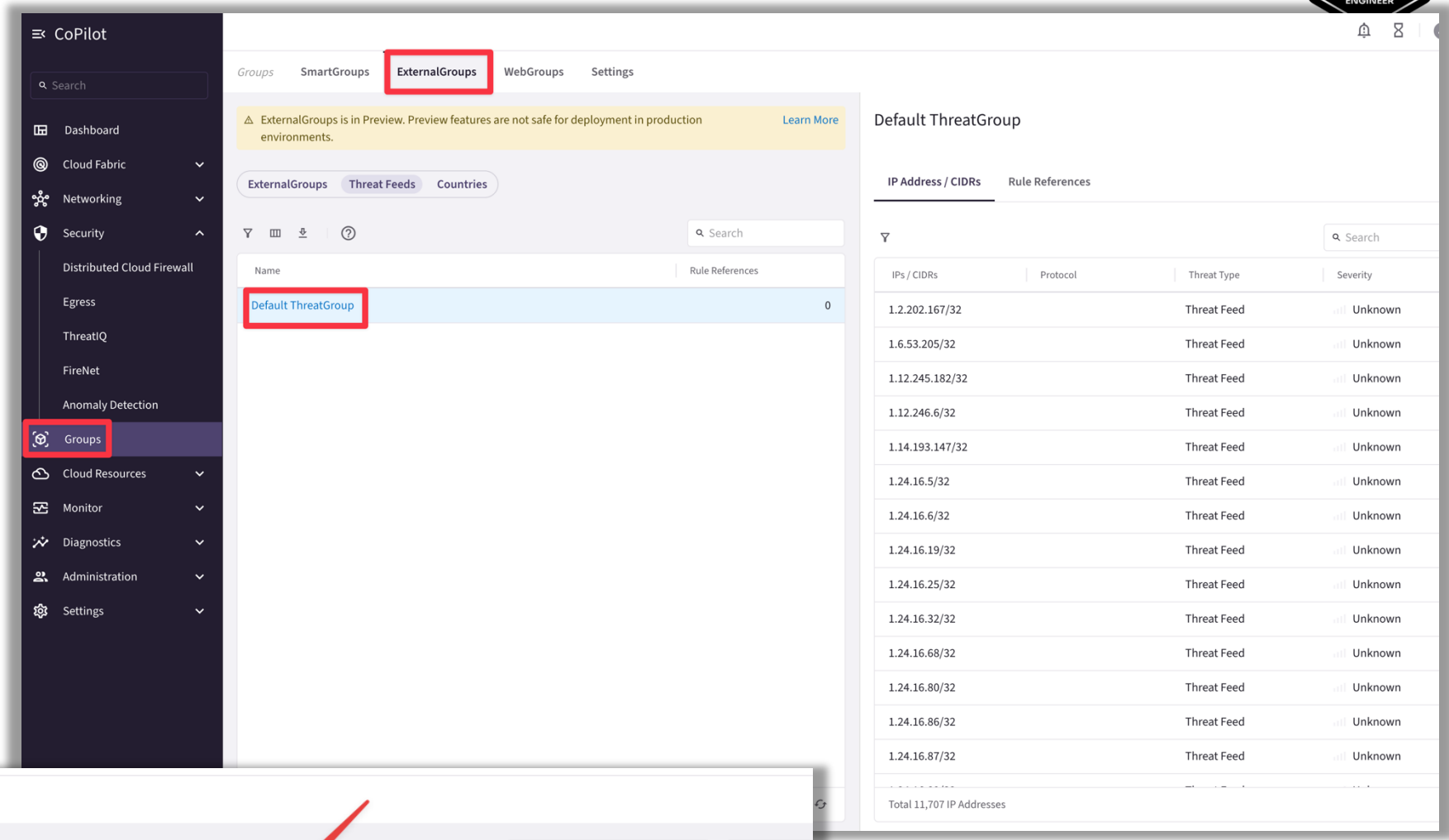
Threat Prevention

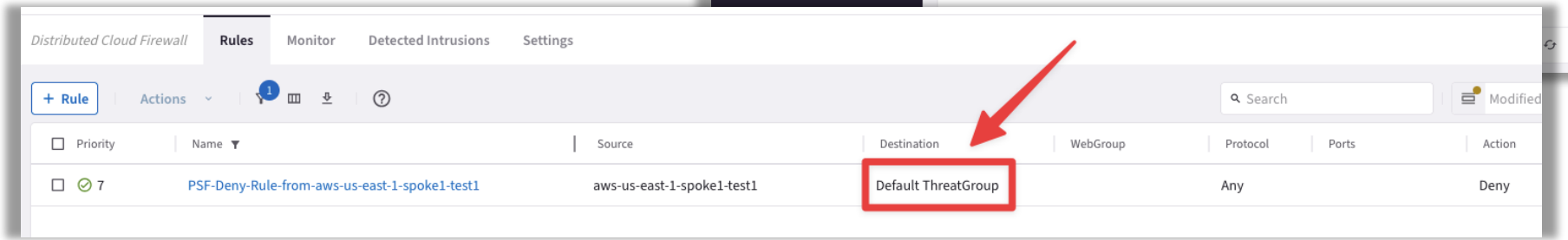
Default ThreatGroup

- **ProofPoint Database**
  - The **Default ThreatGroup** can be used to ensure that traffic meeting the ThreatGroup criteria is blocked
  - The **Default ThreatGroup** is regularly updated with data from *ProofPoint Global Threat Defense Database* (every 30 min)
  - The Default ThreatGroup references the complete list of all the Malicious IP addresses.

➢ **Note:**

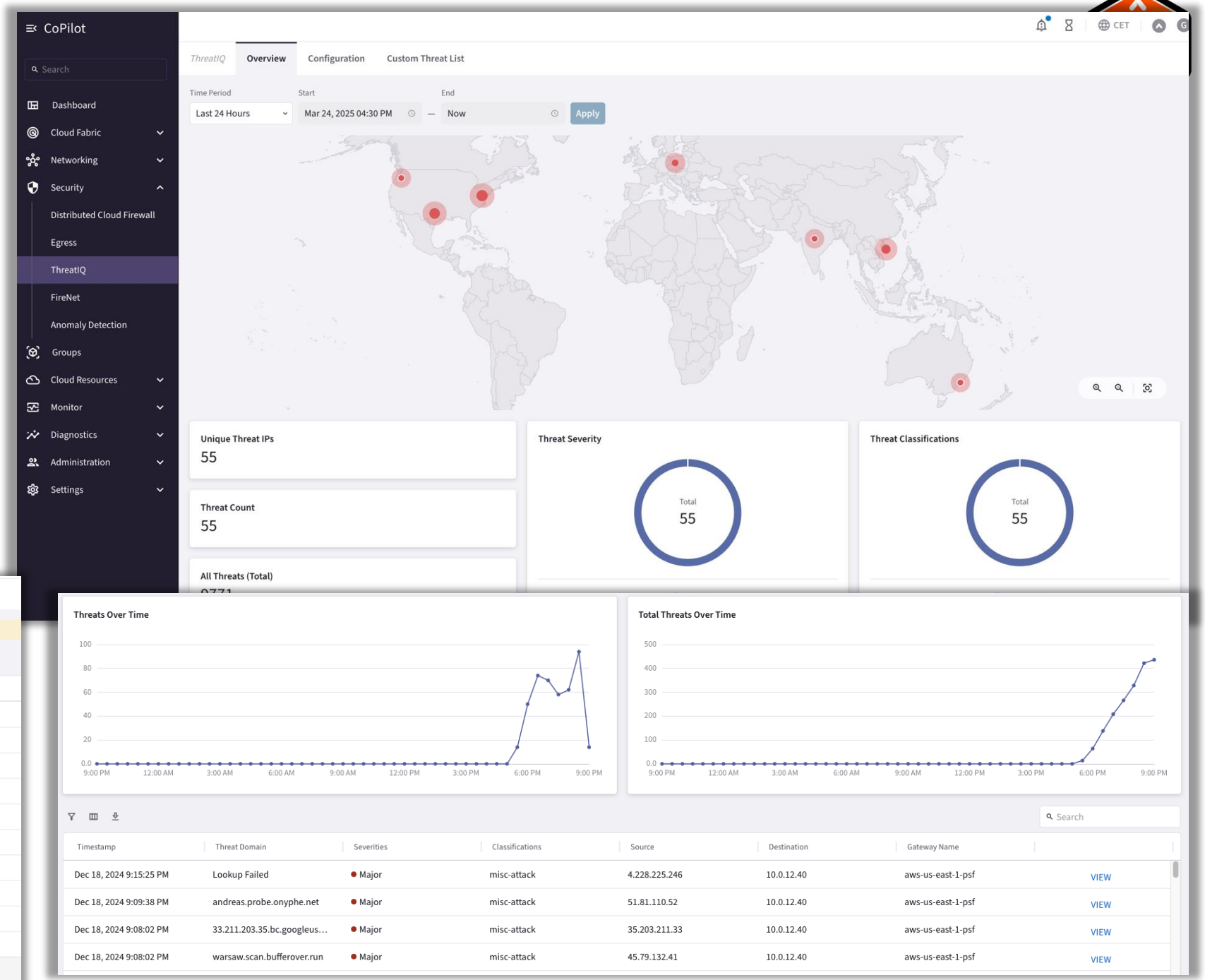
- You cannot have a ThreatGroup as both source and a destination in a DCF rule

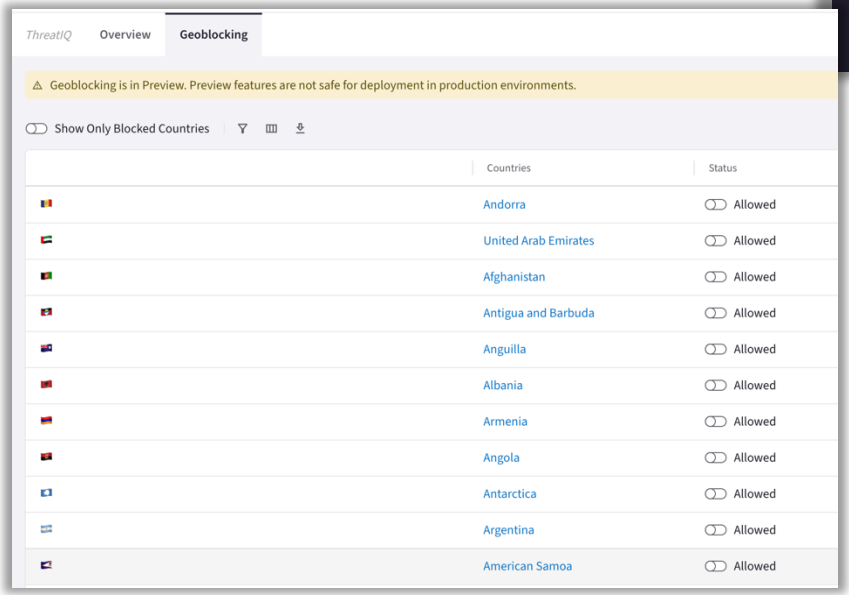




ThreatIQ

- **Overview Tab**
  - Shows a geographical map with the approximate locations of known malicious IPs that have communicated with your network within the specified time period selected.
  - You can view the severity level of detected threat IPs and their associated attack classifications (as categorized by the well-known threat IPs DB).
- **Geoblocking Tab**
  - Block traffic coming from other countries

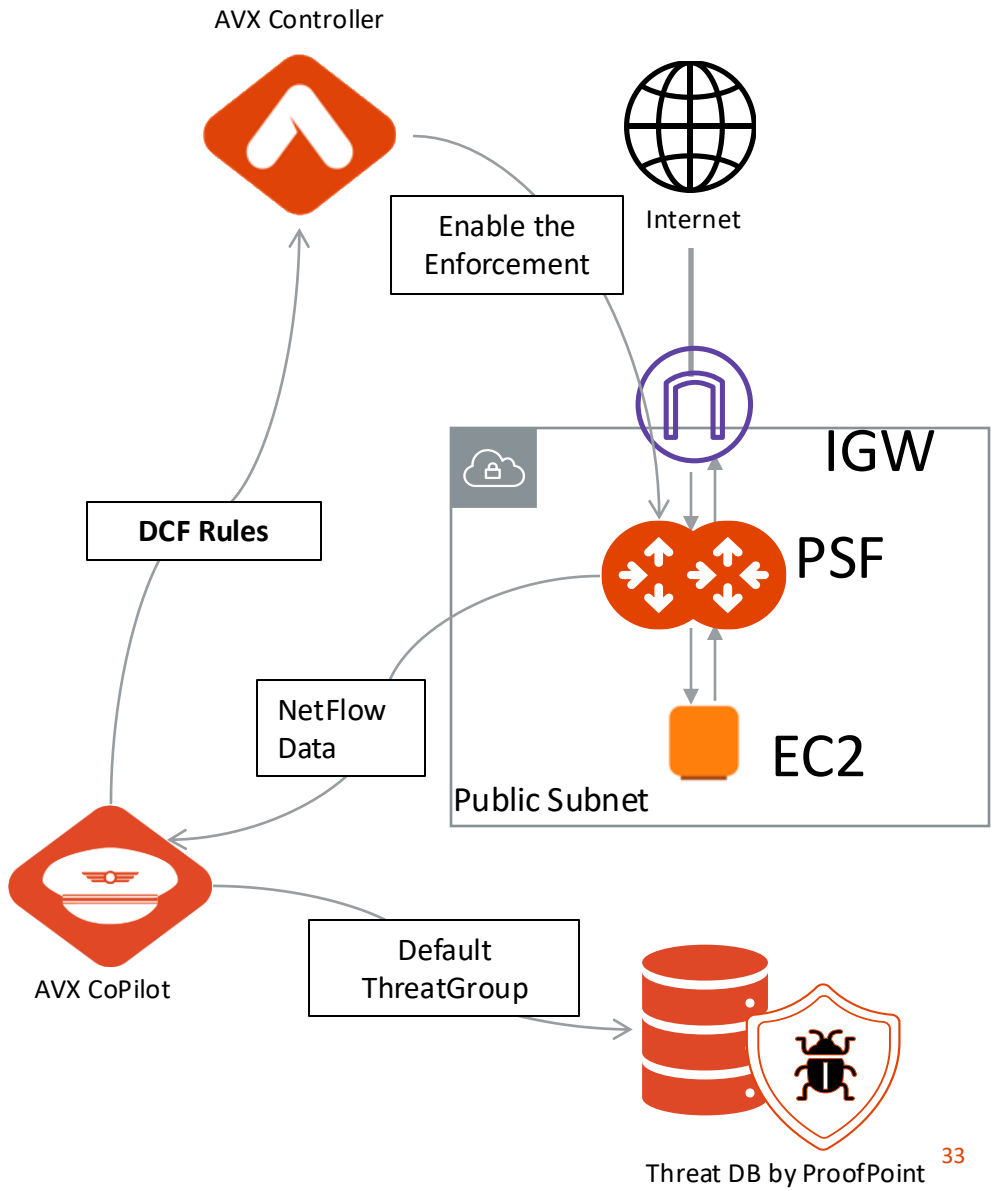




Public Subnet Filtering (PSF) Gateway

Aviatrix Public Subnet Filtering Gateways (PSF GWs)

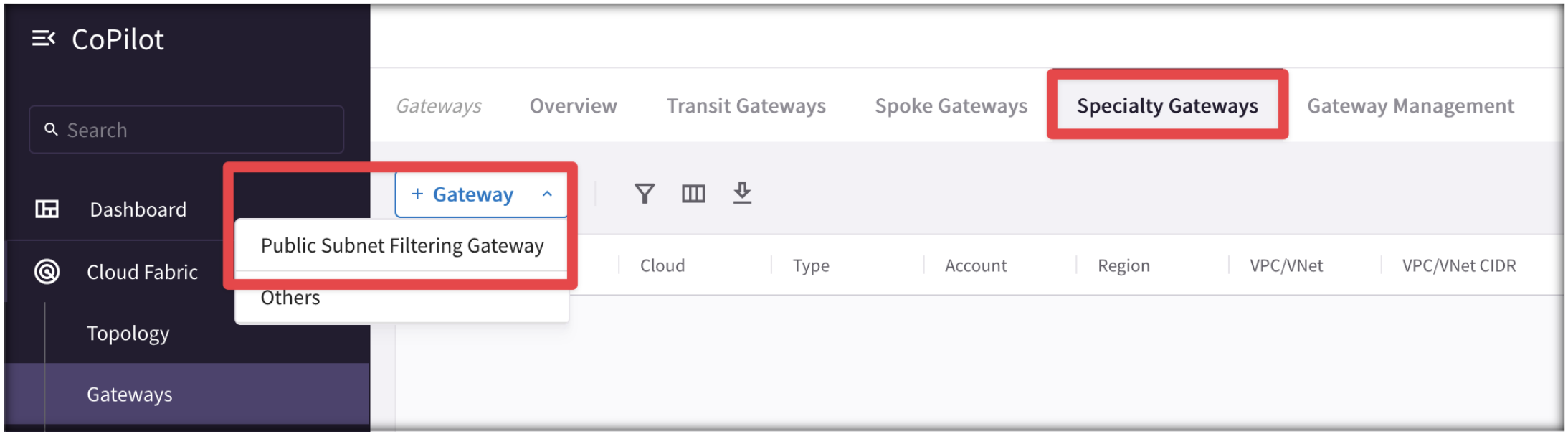
- **Public Subnet Filtering Gateways** (PSF gateways) provide ingress and egress security for **AWS** public subnets where instances have public IP addresses.
- After the Public Subnet Filtering (PSF) gateway is launched, you can apply also DCF (Distributed Cloud Firewall) rules – *enforcement must be enabled.*
- The PSF Gateway acts as a **standalone Gateway** (it's neither a Spoke nor a Transit).
- Leverage the **Default ThreatGroup** (i.e., a Malicious IP addresses DB supplied by ProofPoint) if you want to prevent attacks towards your public-facing workloads.



Aviatrix PSF Deployment Workflow (part.1)

To deploy a Public Subnet Filtering Gateway:

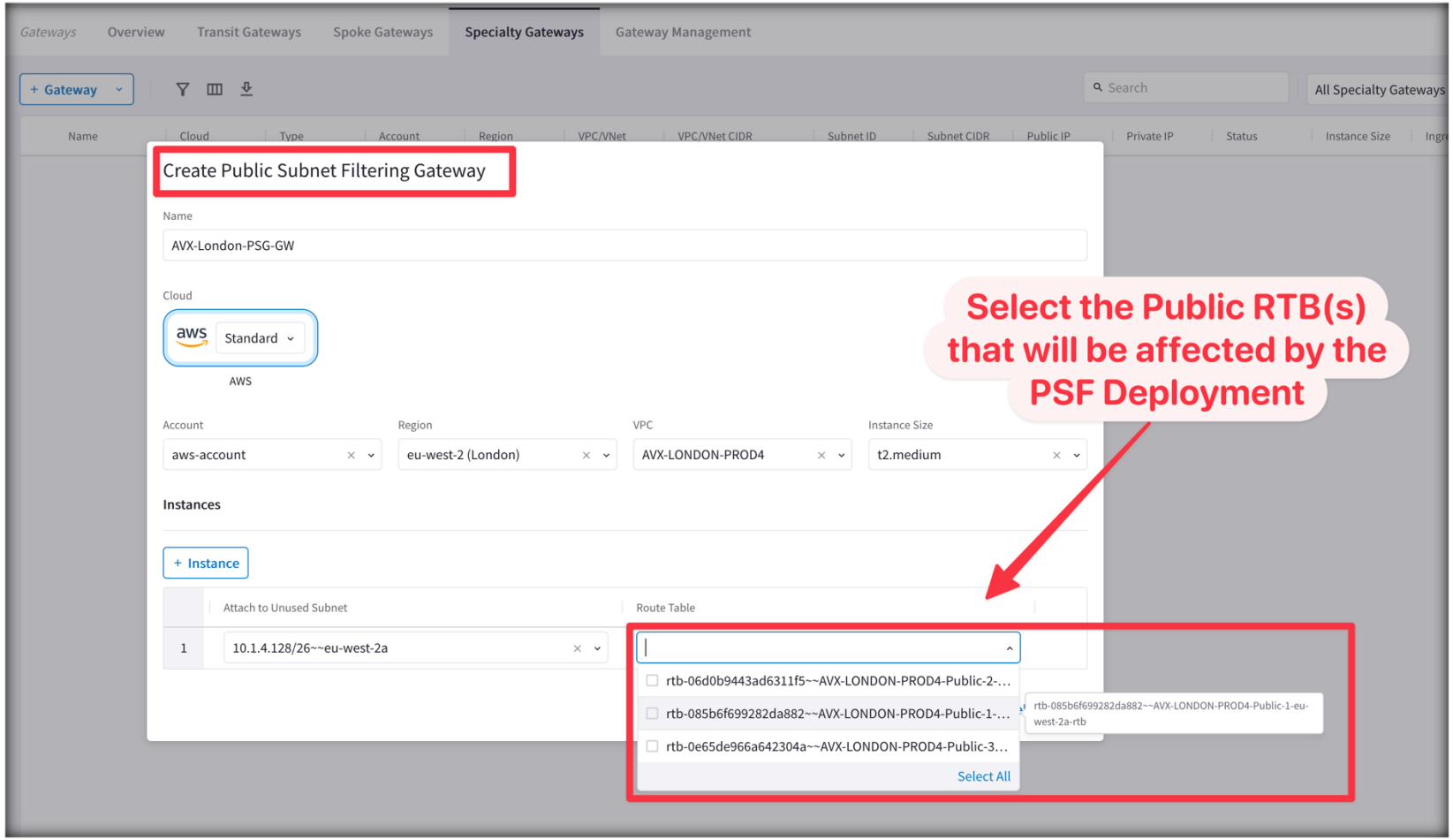
1. In CoPilot, navigate to **Cloud Fabric** > **Gateways** > **Speciality Gateways** tab.
2. Click **+Gateway** and select **Public Subnet Filtering Gateway**.



Aviatrix PSF Deployment Workflow (part.2)

3. Fill up the relevant fields with the required parameters.
4. Select the Public RTB that will get its default route affected (i.e. pointing to the PSF, instead of the IGW)

After the Public Subnet Filtering Gateway is deployed, **Ingress traffic** from IGW is routed to the gateway in a “pass through” manner. **Egress traffic** from instances in the protected public subnets is routed to the PSF gateway in a pass through manner.



Enforcement on PSF

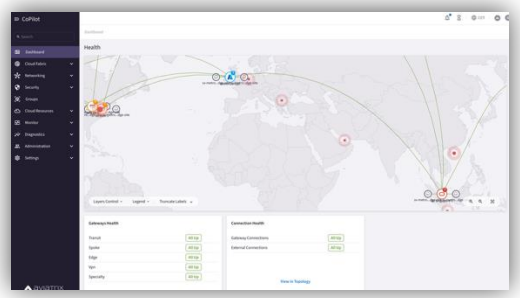
The Enforcement of DCF (Distributed Cloud Firewall) rules on the PSF Gateway is *disabled* by default.

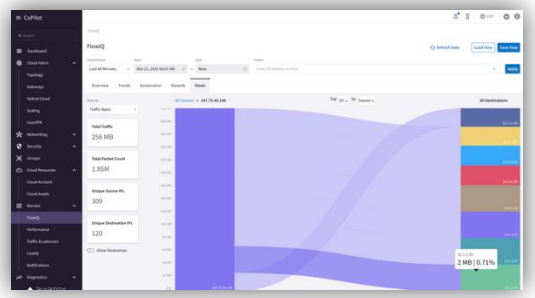
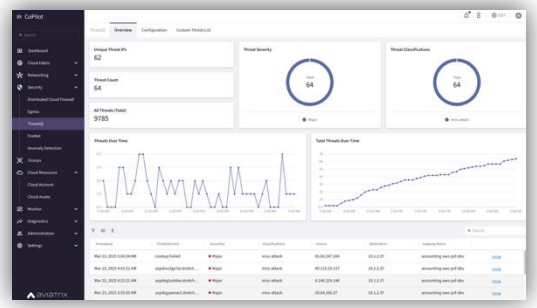
- CAVEAT: This feature must be enabled if you want the AVX Controller to push DCF Rules to this standalone Gateway as well.

Macro-Segmentation

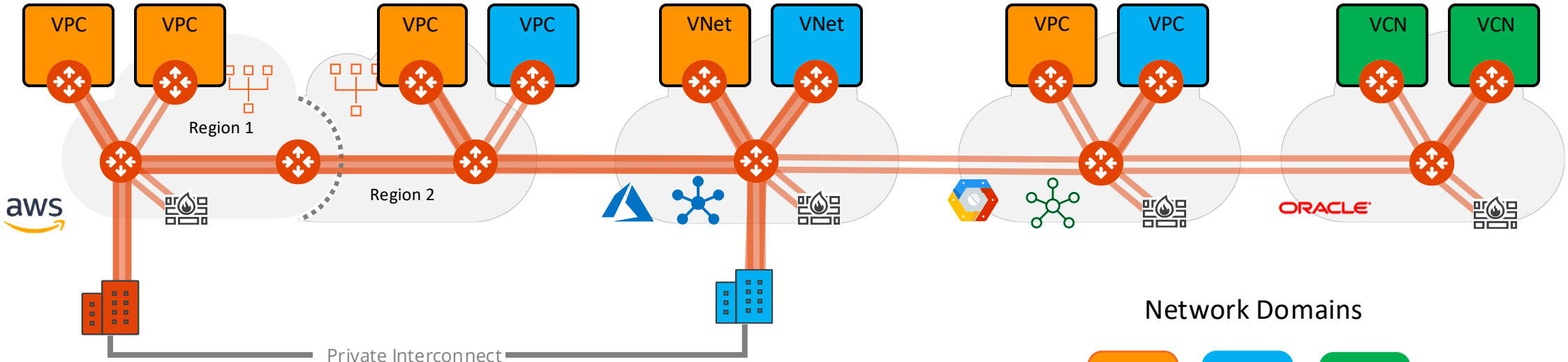
Network Segmentation

Aviatrix CoPilot



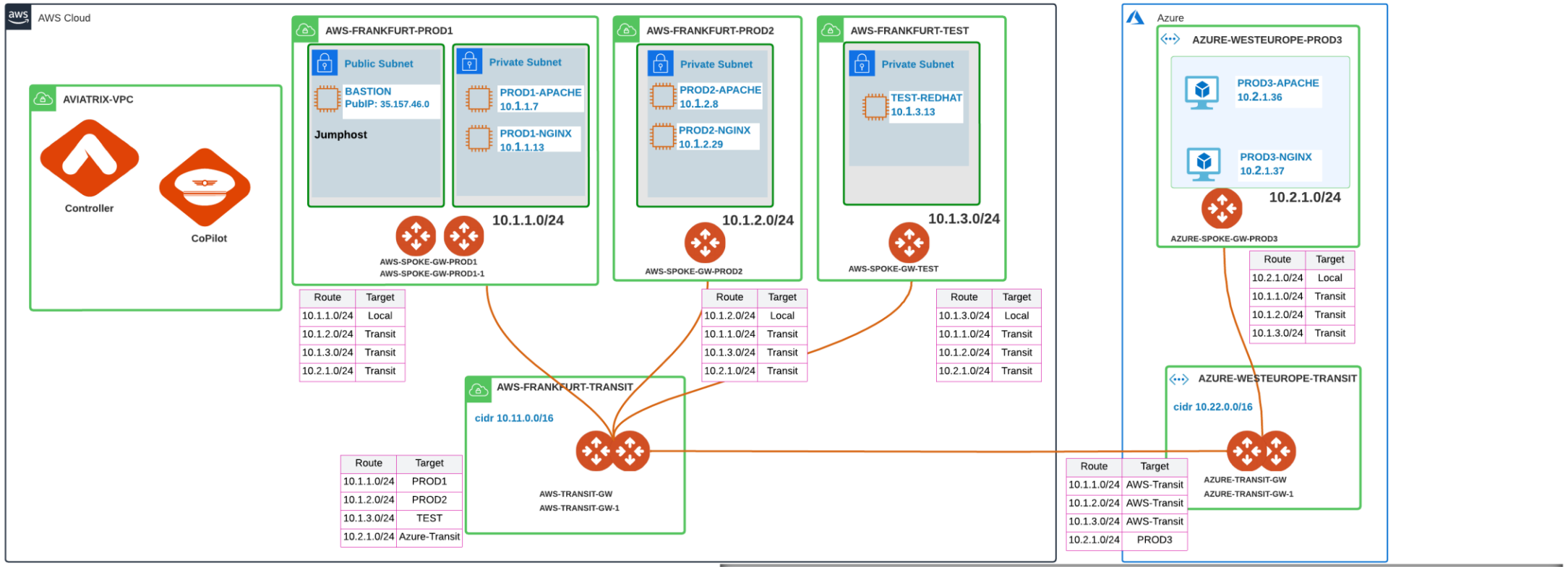
Network Granularity and Control



Network Domains

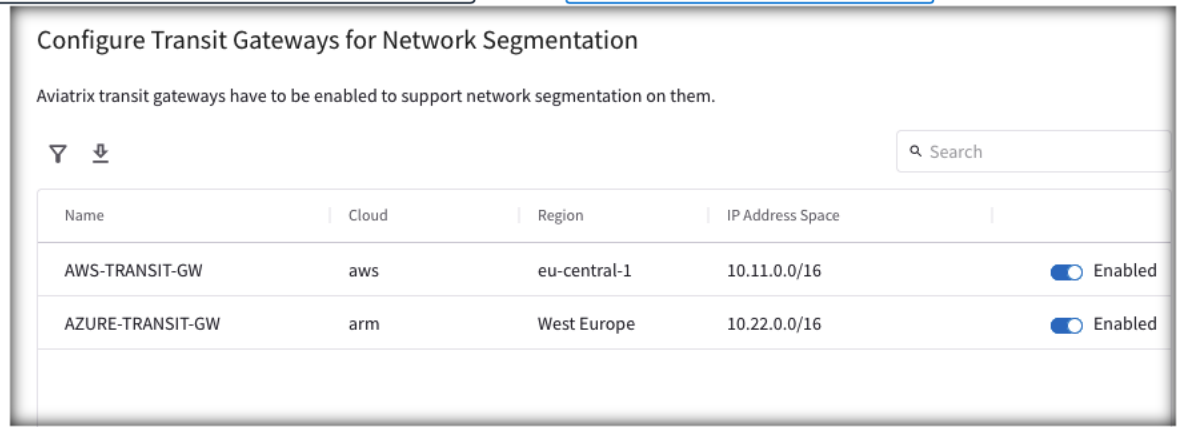
LOB1 LOB2 LOB3

1. Enable Transit Gateways for Network Segmentation

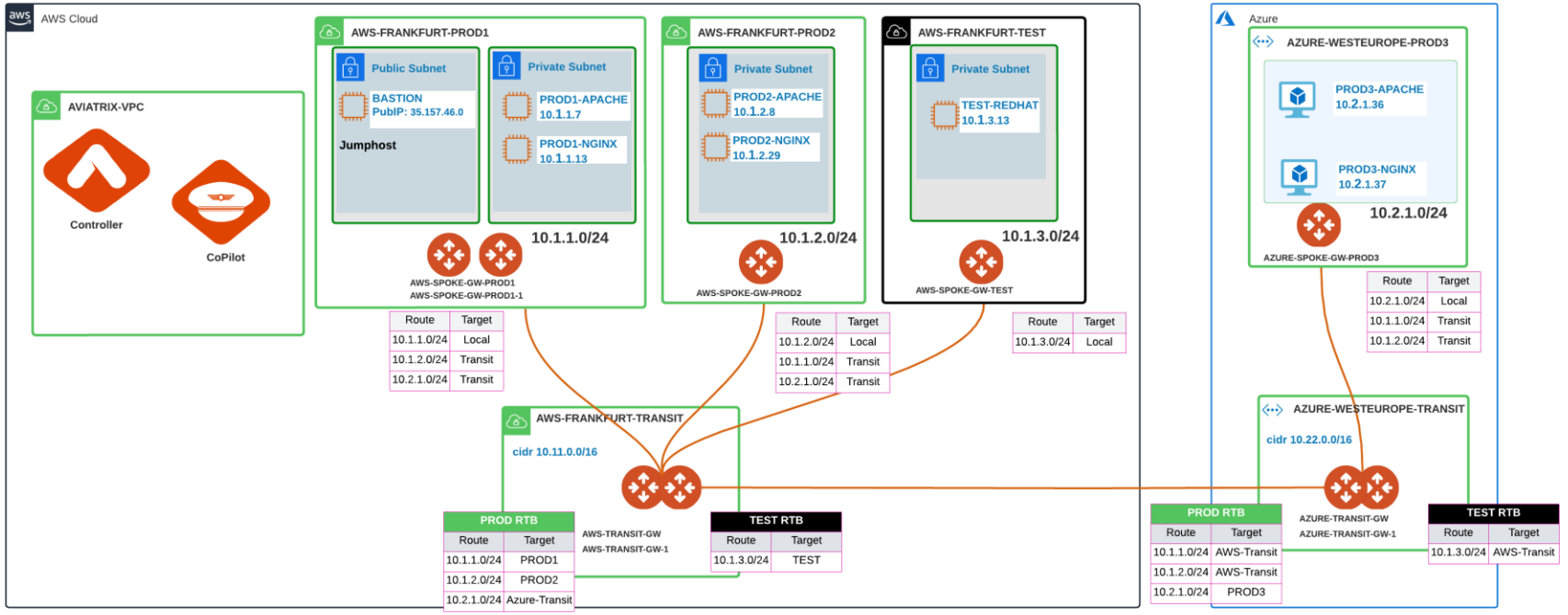


Enable the Network Segmentation:

- Choose the Transit Gateway(s) that will route traffic for its members.



2. Create and Associate a Network Domain



Transit Gateway

- Multiple RTBs (per each Network Domain)
- Main RTB:
  - The main RTB will host the Transit Routes (i.e. the routes of the *backbone layer*) and the routes that belong to *Unmanaged Network Domains* (i.e. VPCs/Vnets not assigned to any Network Domains yet).

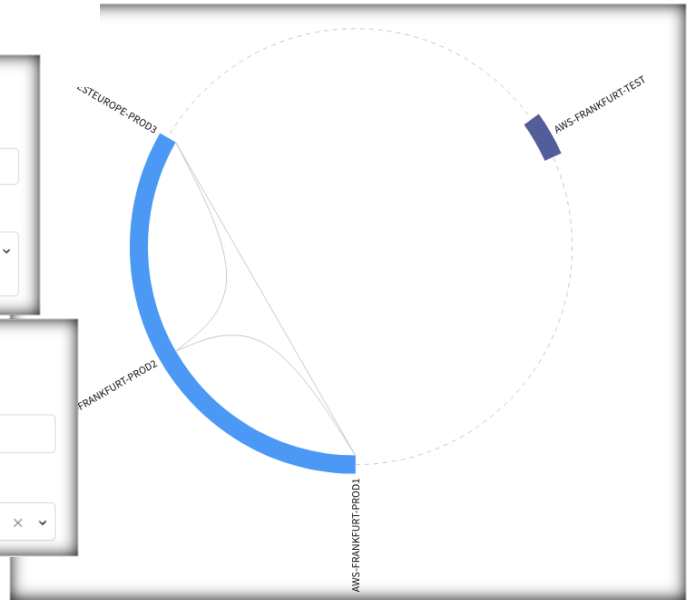
Spoke Gateway

- Single RTB (Main)

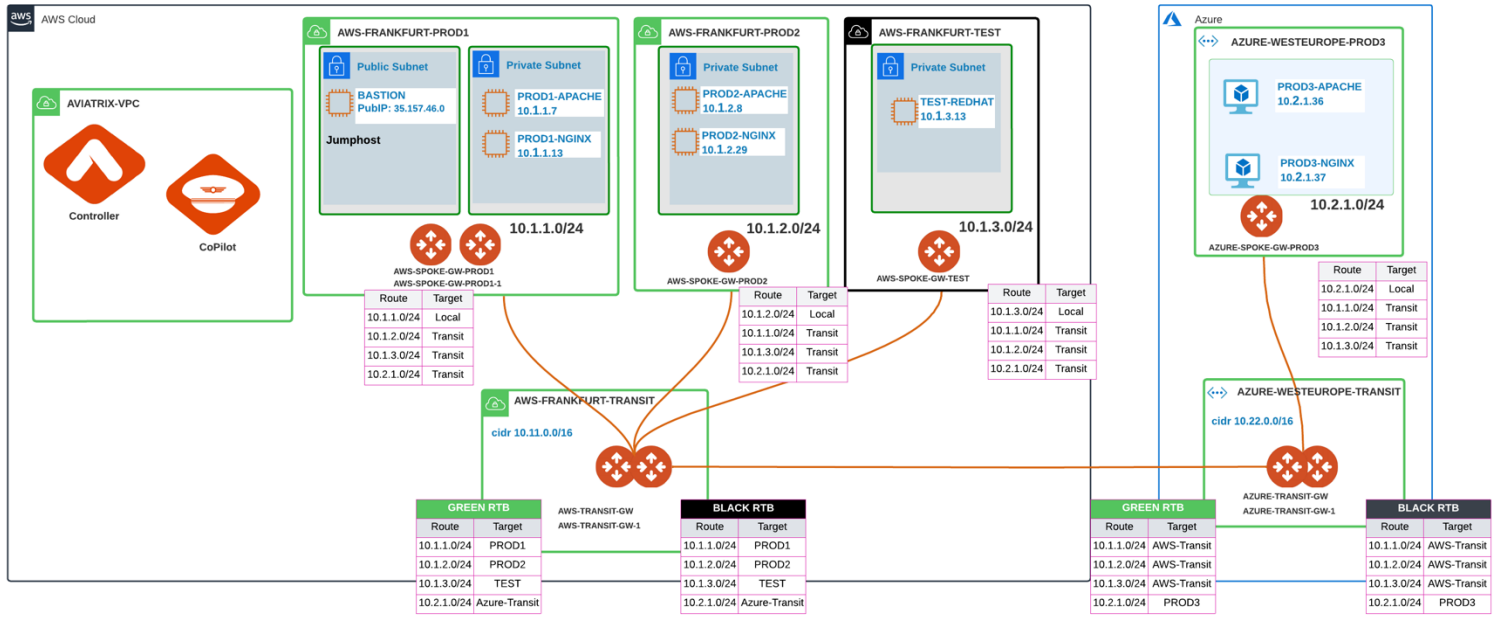
Create the Network Domains:

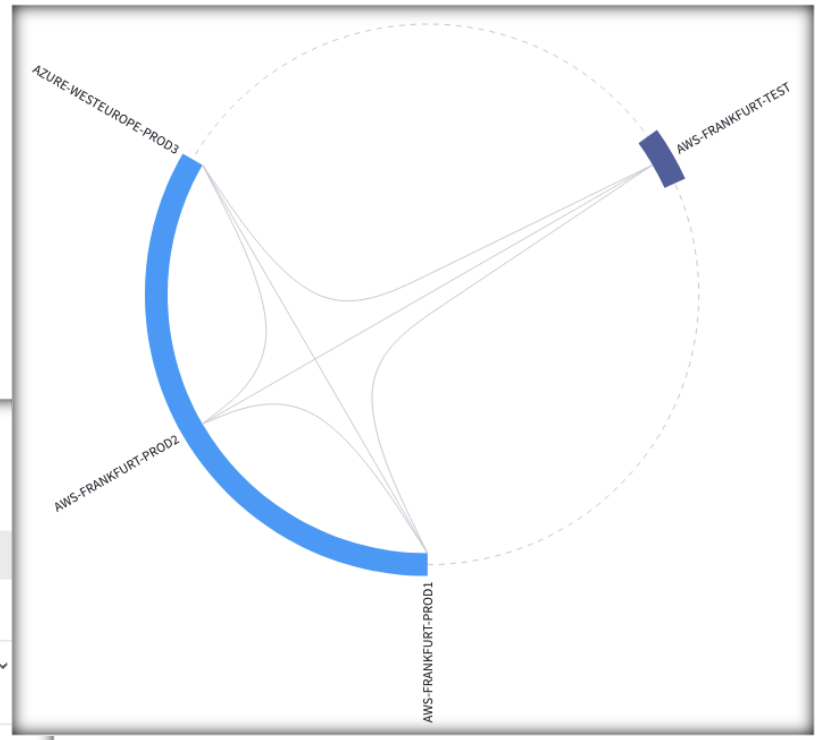
- Assign a Name to each Network Domain
- Associate the Spoke VPCs/Vnets and/or Site2Cloud Connections to the Network Domain

CAVEAT: You can create maximum **200** Network Domains per each Transit Gateway



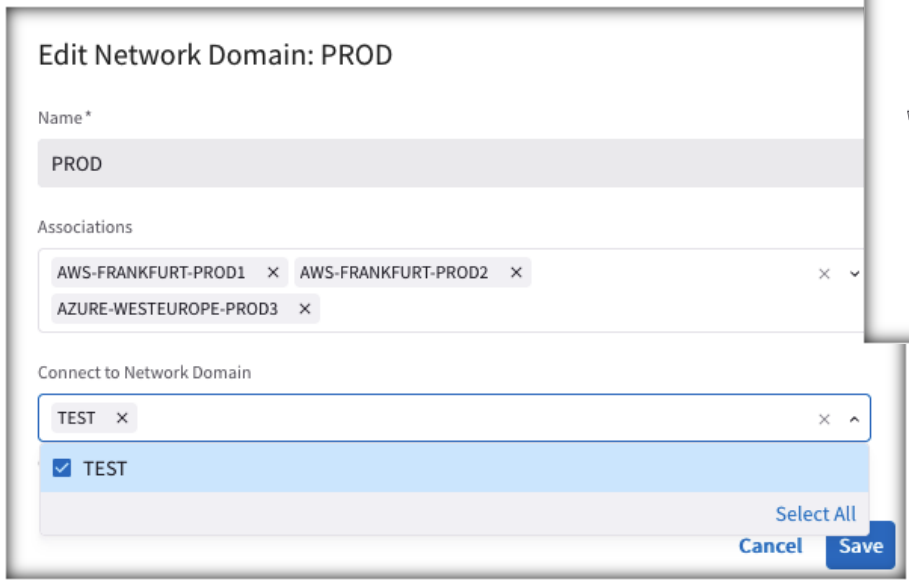
3. Apply the Connection Policy (optional)





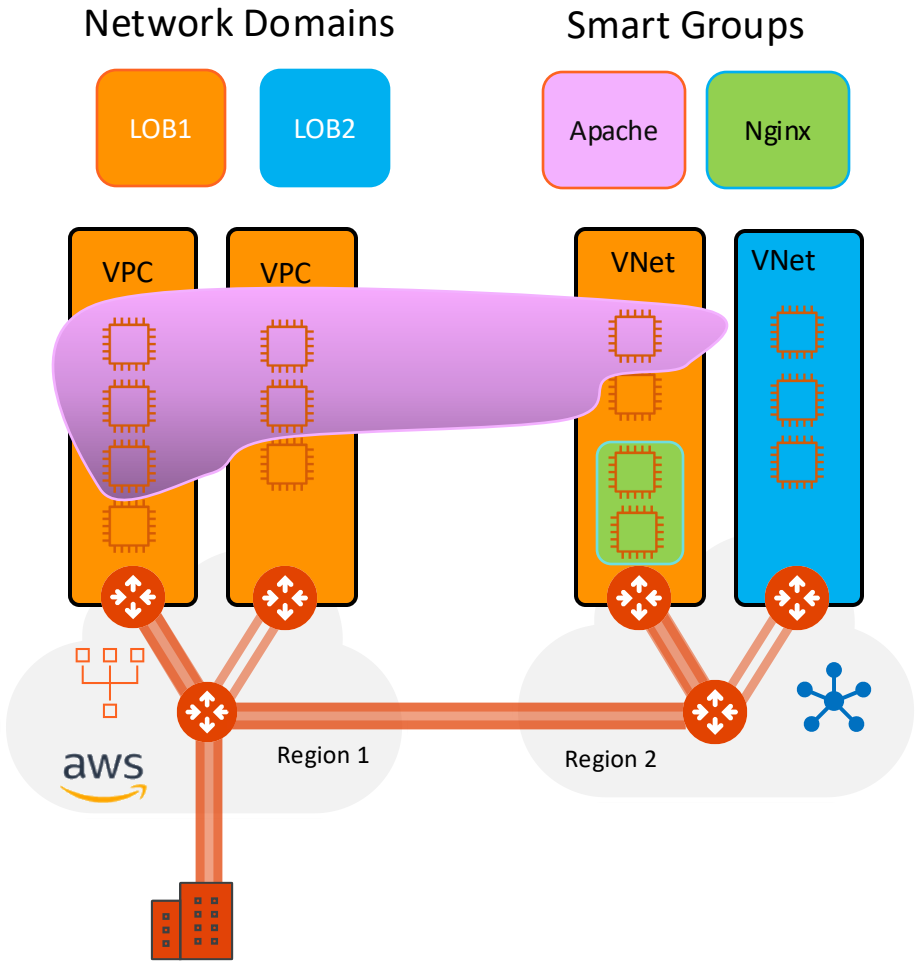
Optionally, enable the Connection Policy:

- Network Domains' routing tables are merged (i.e. *vrf leaking*).



Micro-Segmentation

Micro-Segmentation



Inter-rule

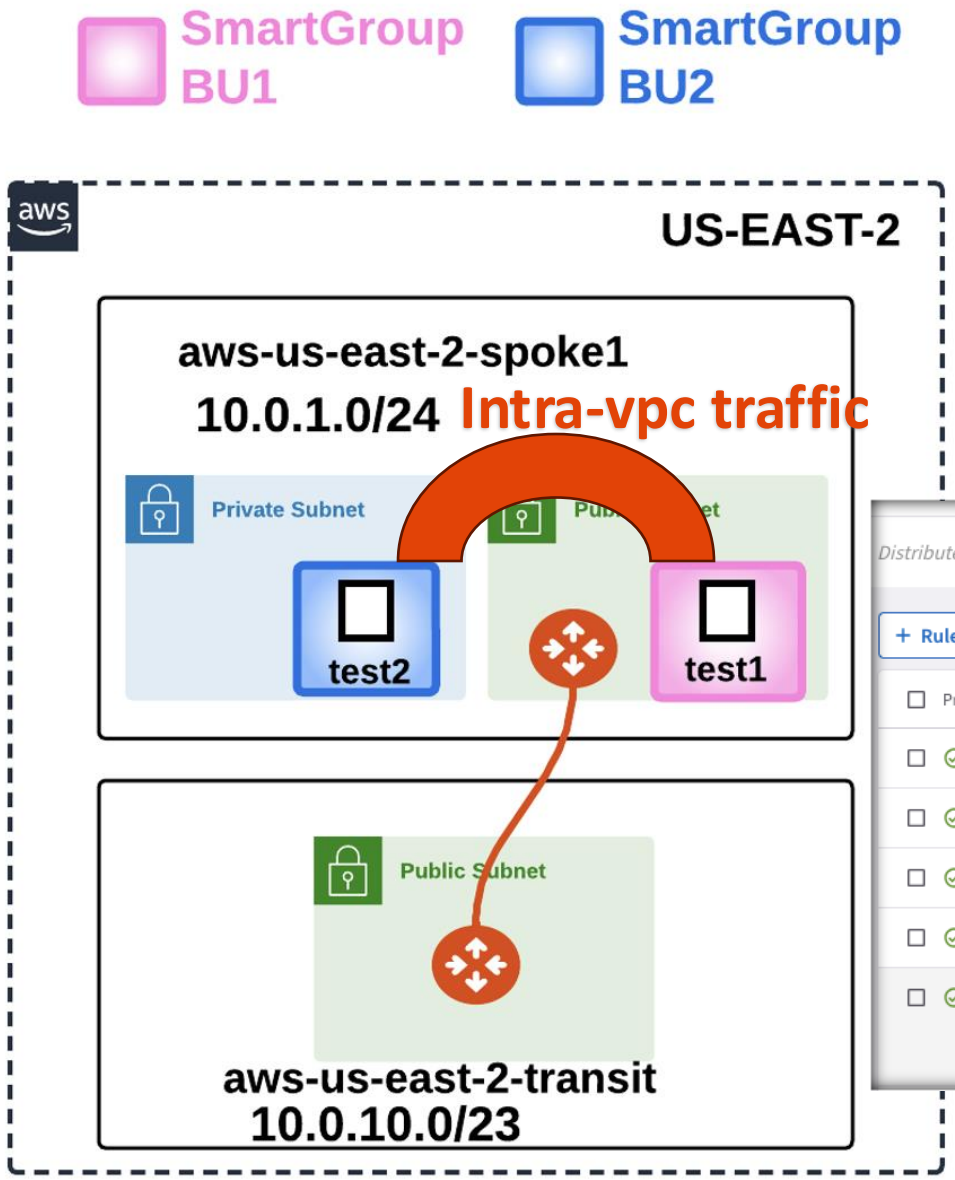
Source SmartGroup ≠ Destination SmartGroup

Intra-rule

Source SmartGroup = Destination SmartGroup

Security Group Orchestration

Security Group Orchestration: Intra-L4 Access Control (part.1)



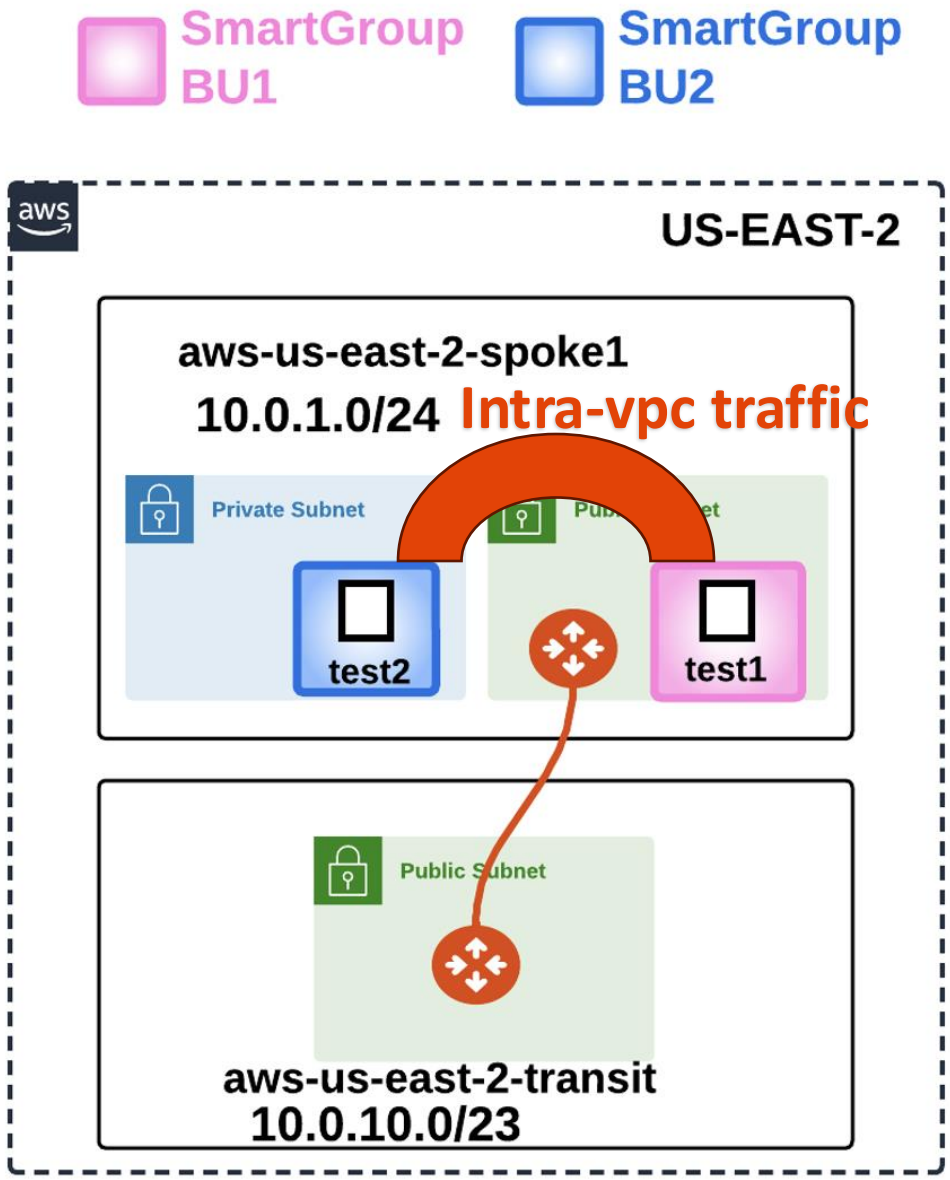
BU1 and BU2 are able to communicate with each other without any issues. The **ExplicitDenyAll** rule is never triggered or enforced in this scenario, allowing seamless communication between the two units.

Distributed Cloud Firewall | Rules | Monitor | Detected Intrusions | Settings

+ Rule | Actions

Priority	Name	Source	Destination	WebGroup	Protocol	Action
0	BU1-SSH	BU1	BU1		TCP	Permit
1	BU2-ICMP	BU2	BU2		ICMP	Permit
2	ExplicitDenyAll	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any	Deny
214748…	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any	Permit
214748…	DefaultDenyAll	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0), BU1, + 1 more		Any	Deny

Security Group Orchestration: Intra-L4 Access Control (part.2)



Enforcement Security Point

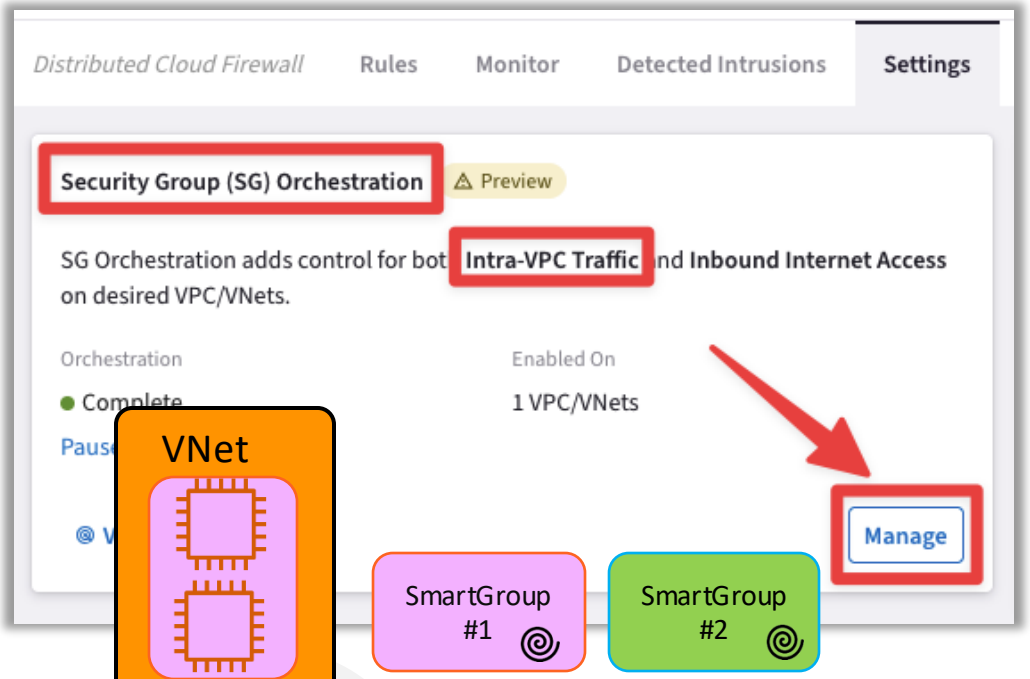
Aviatrix Spoke Gateway

- CAVEAT: Any rule you define to keep BU1 separate from BU2 will not prevent communication between the two instances, as the traffic is sent over the underlay network. It will never hit the Spoke Gateway.

  This is a typical example of intra-VPC traffic.

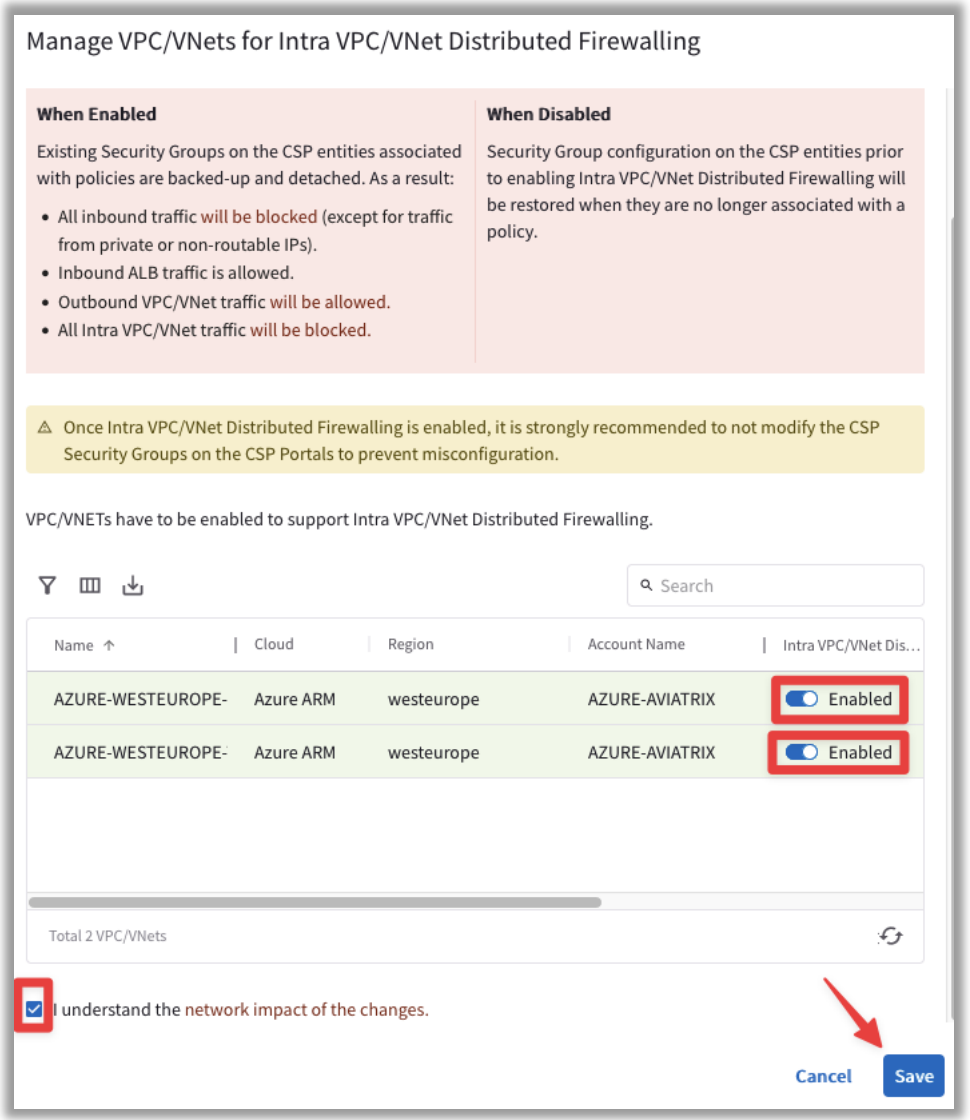
Security Group Orchestration: Intra-L4 Access Control (part.3)

❑ Enable the feature on the relevant VPC/VNet



- If you enable the **Security Group (SG) Orchestration** (*aka Intra-VPC Traffic Control*), the SmartGroups defined within the same VPC/VNet will not be able to communicate with each other, unless an inter rule is applied between them.
- This is pure L4 separation, leveraging the Native Cloud Constructs (such as SG, NSG and ASG). This is not L7 inspection.

CAVEAT: Available in AWS/Azure



FireNet (Service Chaining)

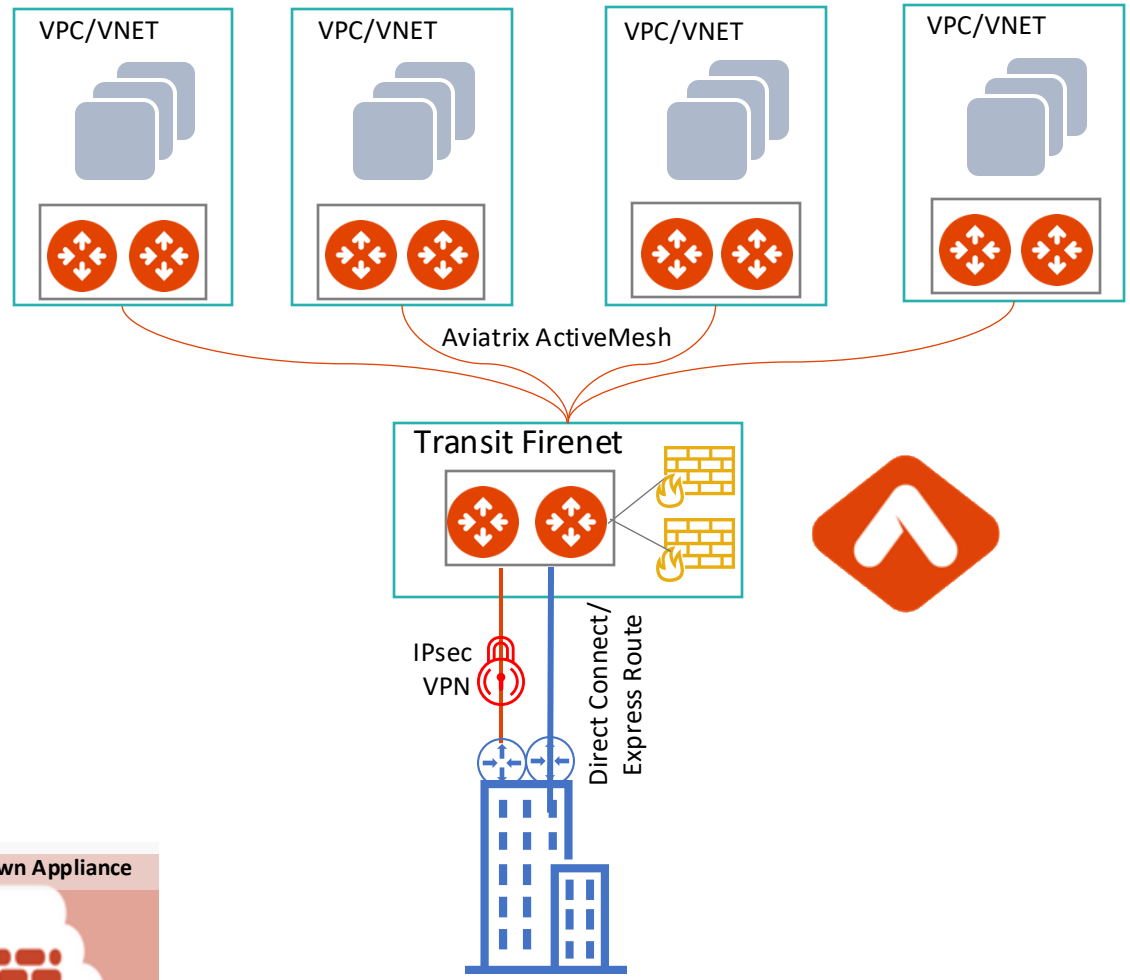
Aviatrix Encrypted Transit Firewall Network

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

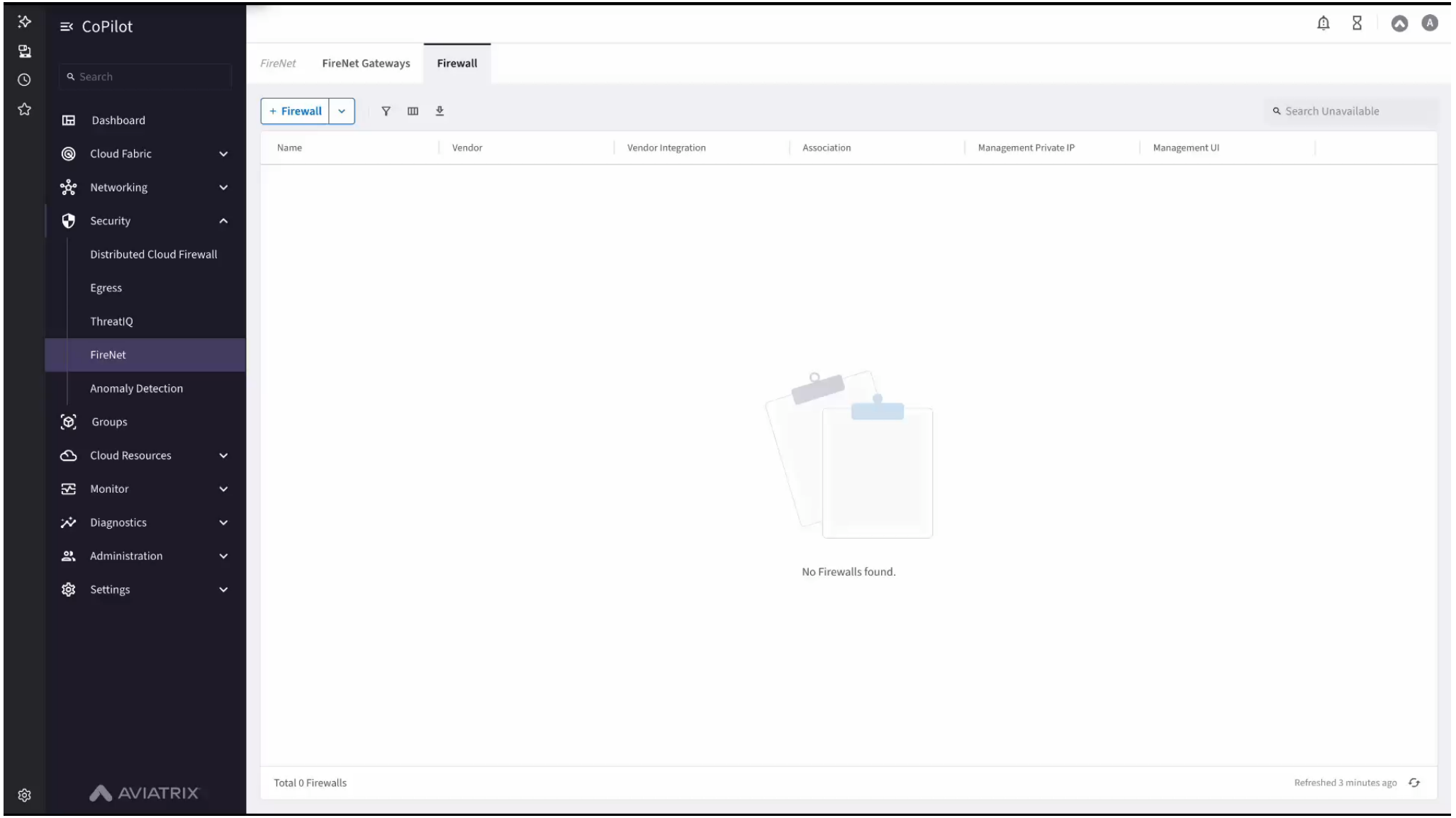
Check Point SOFTWARE TECHNOLOGIES LTD

f5

FORTINET

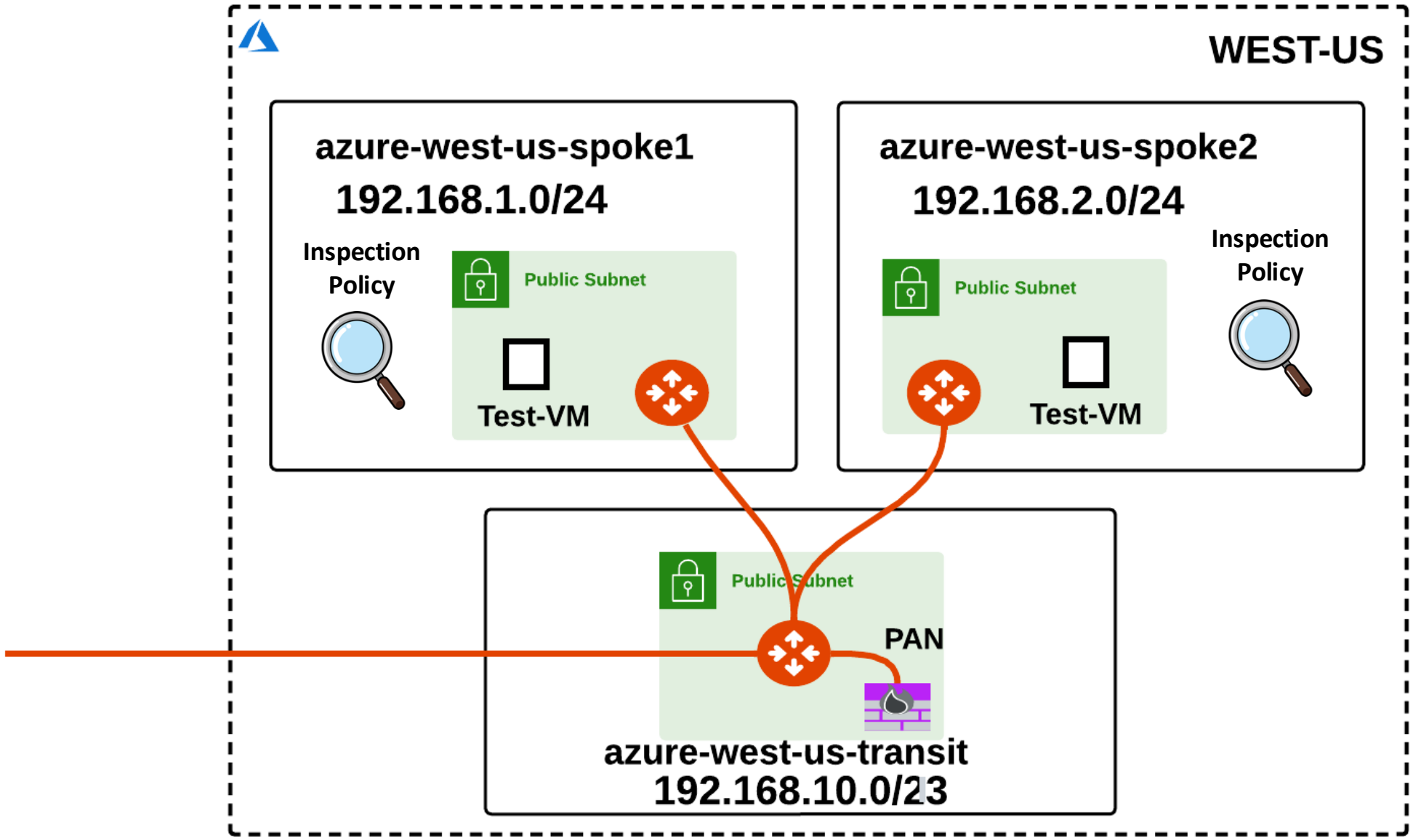
Bring Your Own Appliance

FireNet: Firewall Deployment, Bootstrapping & Vendor Integration

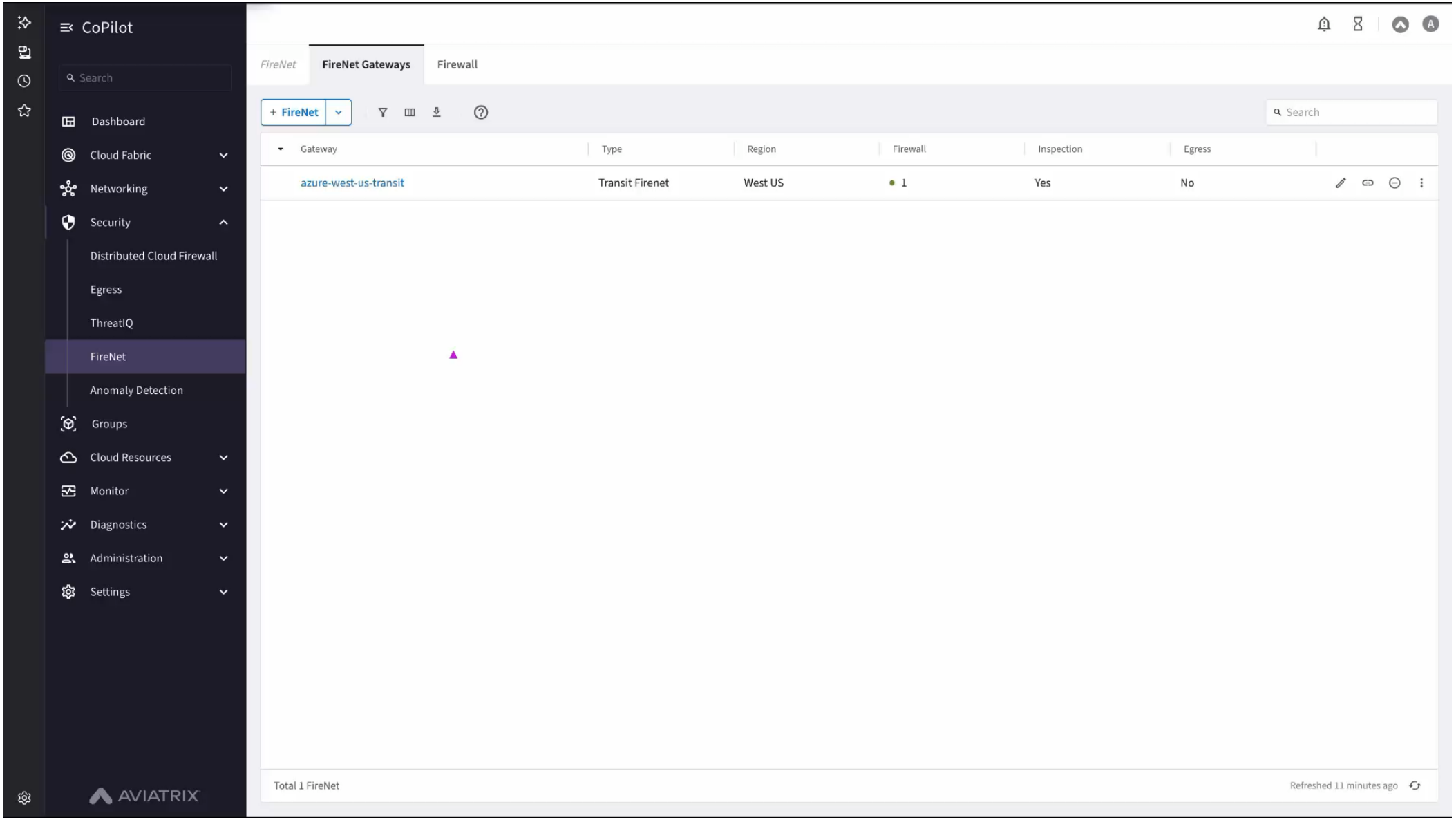


aviatrix

FireNet: Inspection Policy (part.1)

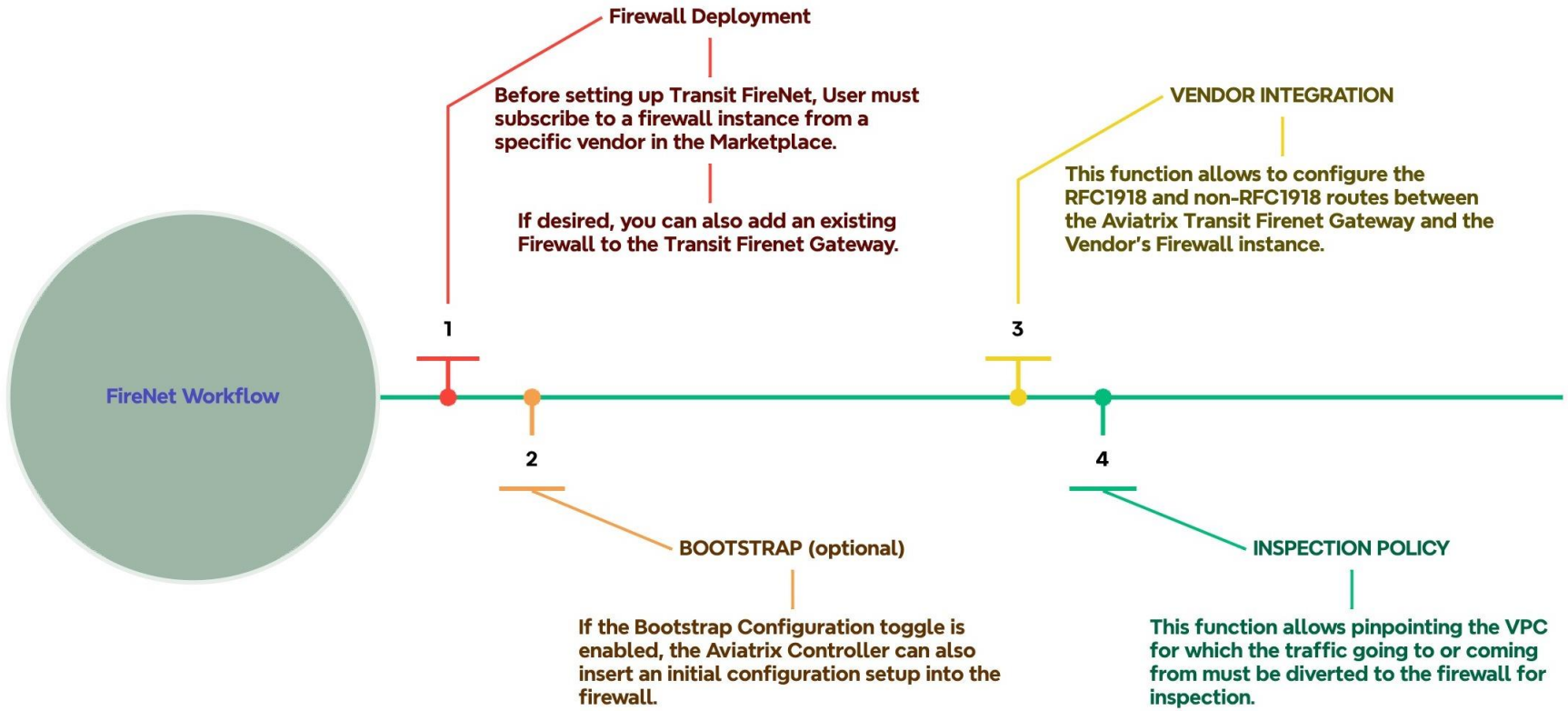


FireNet: Inspection Policy (part.2)



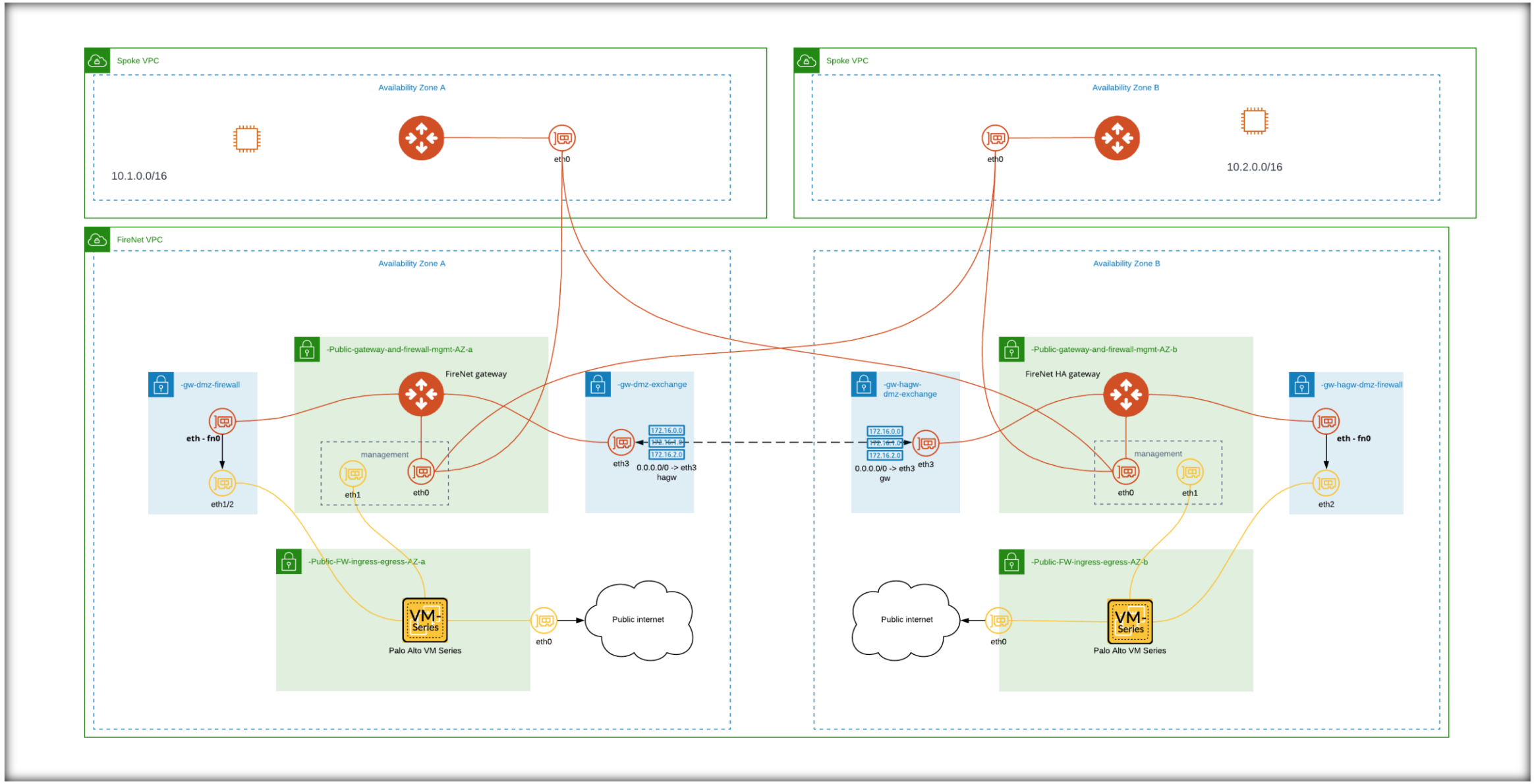
aviatrix

FireNet: Deployment Workflow



AVIATRIX®

FireNet – Under the hood



Next: Tenet-3 Global, Dynamic and Centralized Policy (CoPilot Tour)