



Tenet-2: Distributed and Embedded Security

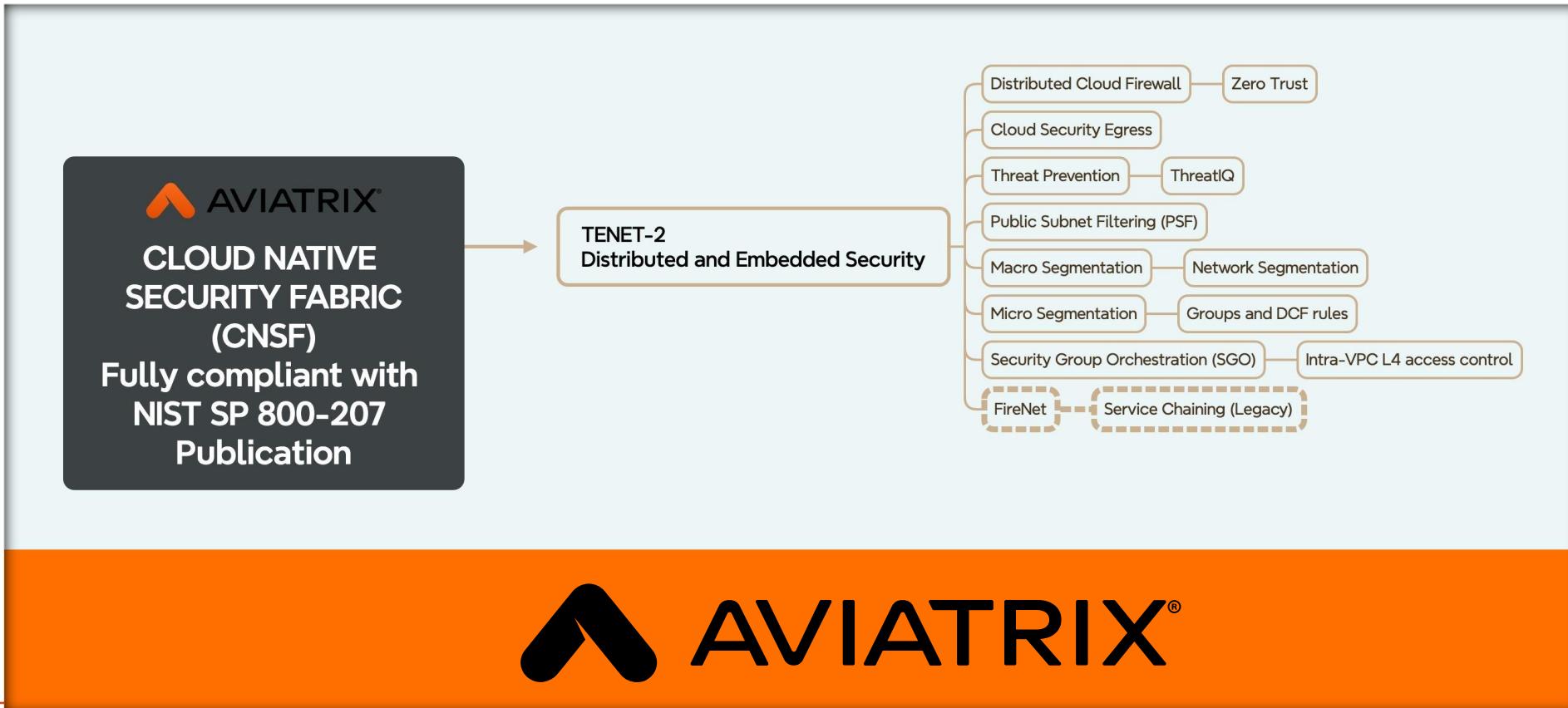
ACE Solutions Architecture Team



Topics Covered

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

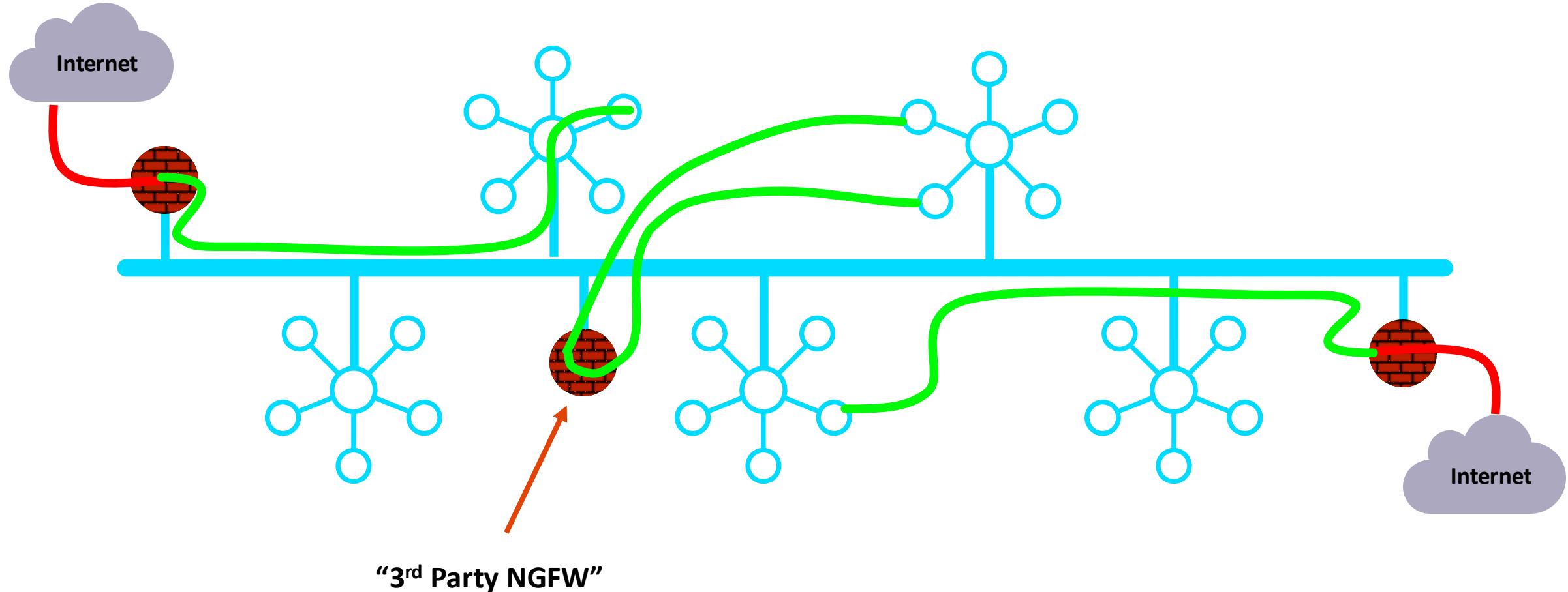
Assets and traffic moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture. Workloads should retain their security posture when moving to or from enterprise-owned infrastructure. This includes devices that move from enterprise networks to non-enterprise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



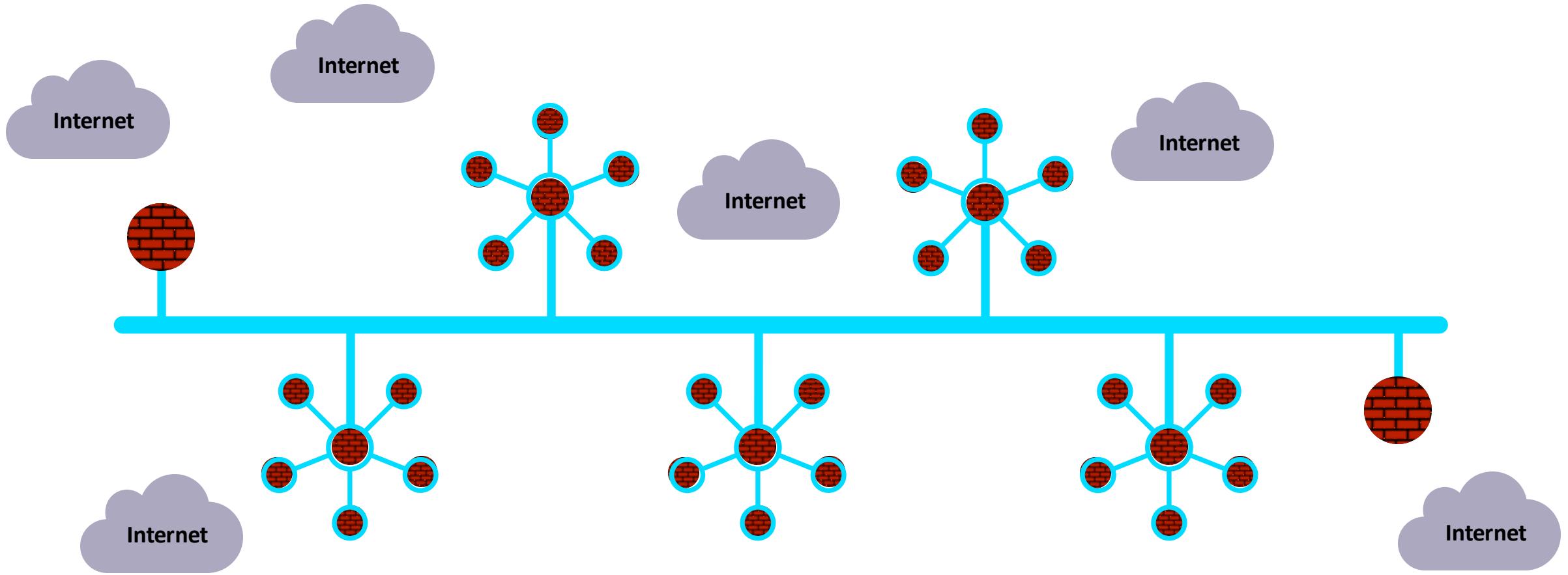


Distributed Cloud Firewall

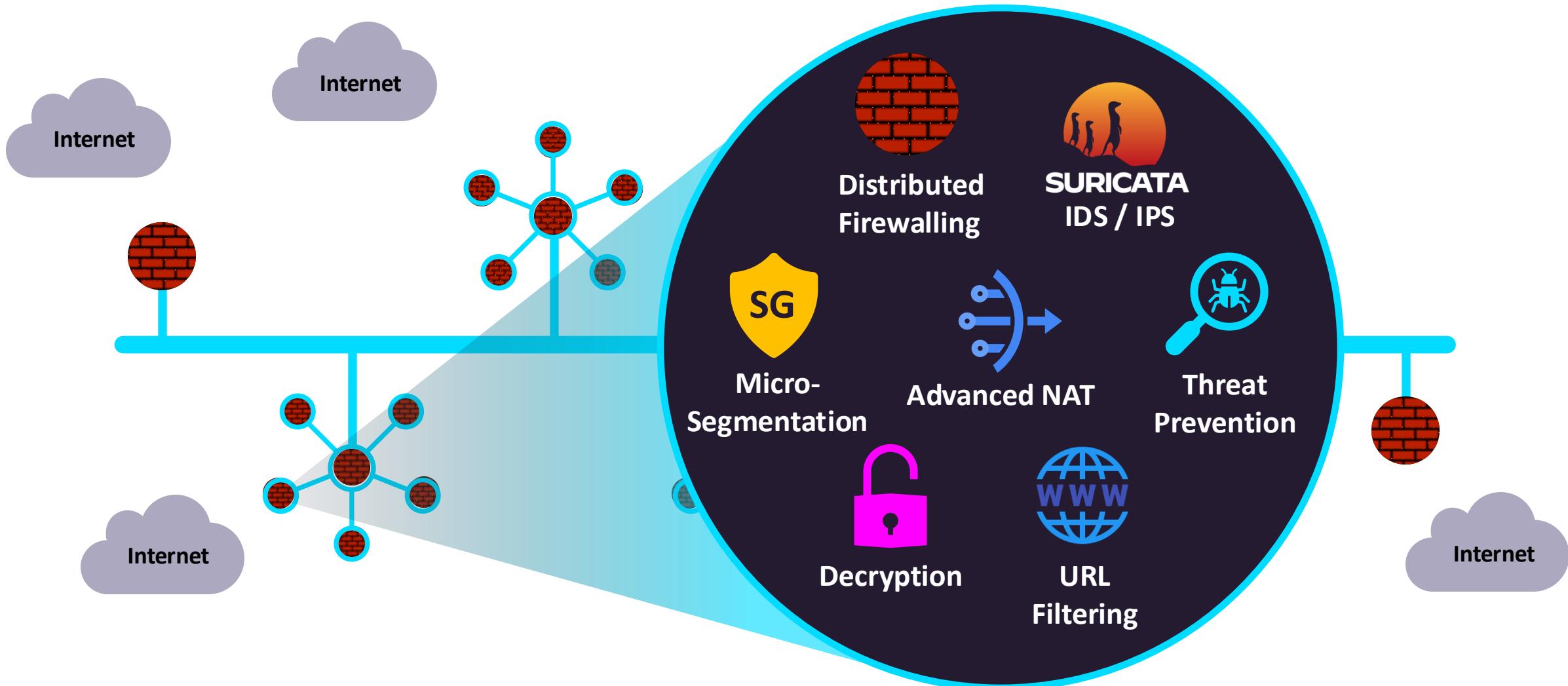
As Architected with Lift-and-Shift, Bolt-on, Data Center Era Products...



Firewalling Functions were Embedded in the Cloud Network Everywhere...



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

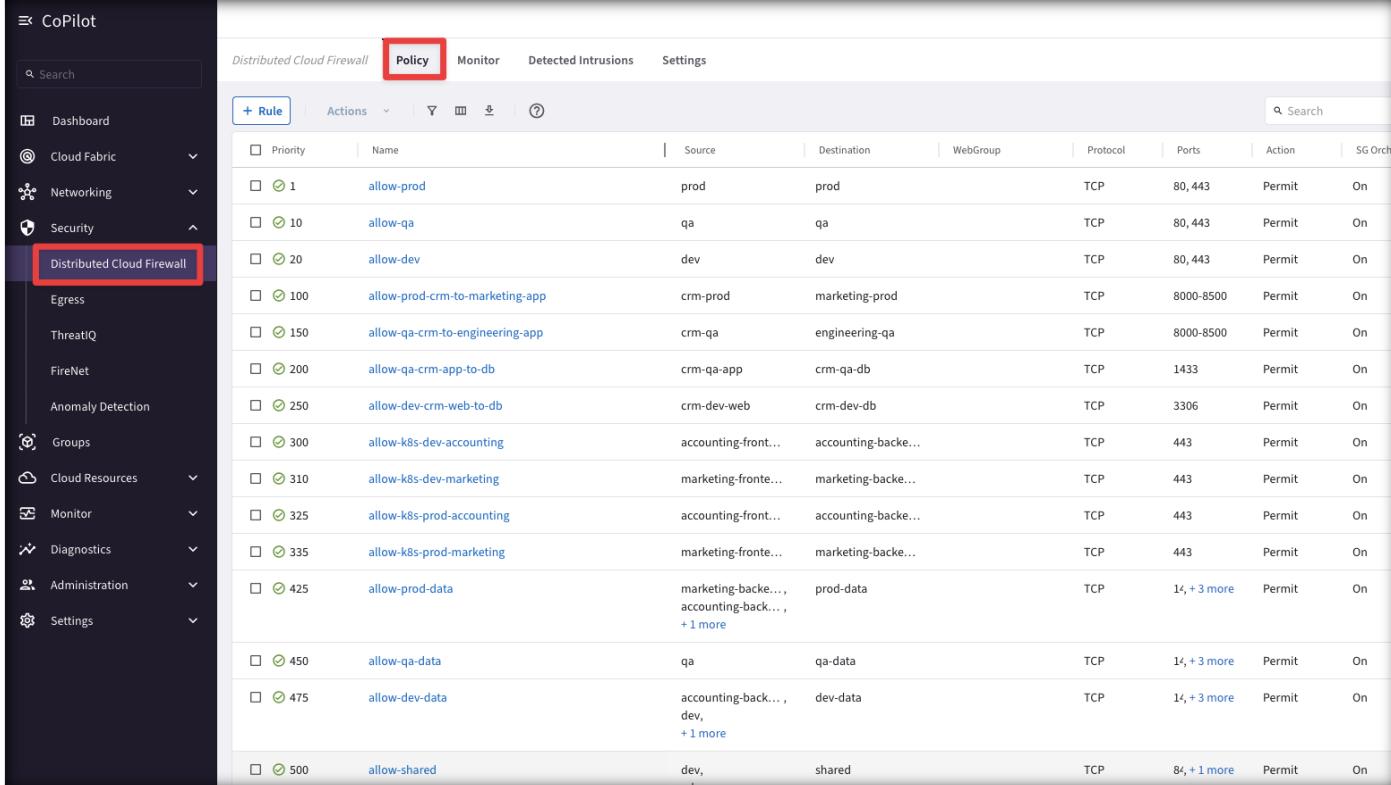


And, What If Policy Creation Looked Like One Big Firewall...

Centralized Policy Creation



Distributed Enforcement



Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchestration
1	allow-prod	prod	prod		TCP	80, 443	Permit	On
10	allow-qa	qa	qa		TCP	80, 443	Permit	On
20	allow-dev	dev	dev		TCP	80, 443	Permit	On
100	allow-prod-crm-to-marketing-app	crm-prod	marketing-prod		TCP	8000-8500	Permit	On
150	allow-qa-crm-to-engineering-app	crm-qa	engineering-qa		TCP	8000-8500	Permit	On
200	allow-qa-crm-app-to-db	crm-qa-app	crm-qa-db		TCP	1433	Permit	On
250	allow-dev-crm-web-to-db	crm-dev-web	crm-dev-db		TCP	3306	Permit	On
300	allow-k8s-dev-accounting	accounting-front...	accounting-backe...		TCP	443	Permit	On
310	allow-k8s-dev-marketing	marketing-fronte...	marketing-backe...		TCP	443	Permit	On
325	allow-k8s-prod-accounting	accounting-front...	accounting-backe...		TCP	443	Permit	On
335	allow-k8s-prod-marketing	marketing-fronte...	marketing-backe...		TCP	443	Permit	On
425	allow-prod-data	marketing-backe..., accounting-backe..., + 1 more	prod-data		TCP	14, + 3 more	Permit	On
450	allow-qa-data	qa	qa-data		TCP	14, + 3 more	Permit	On
475	allow-dev-data	accounting-backe..., dev, + 1 more	dev-data		TCP	14, + 3 more	Permit	On
500	allow-shared	dev, qa	shared		TCP	84, + 1 more	Permit	On

Aviatrix CoPilot



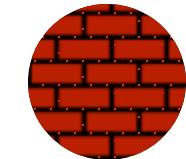
IDS / IPS



Micro-Segmentation



Threat Prevention



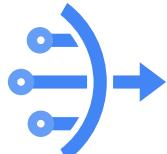
Distributed Firewalling



URL Filtering



Decryption

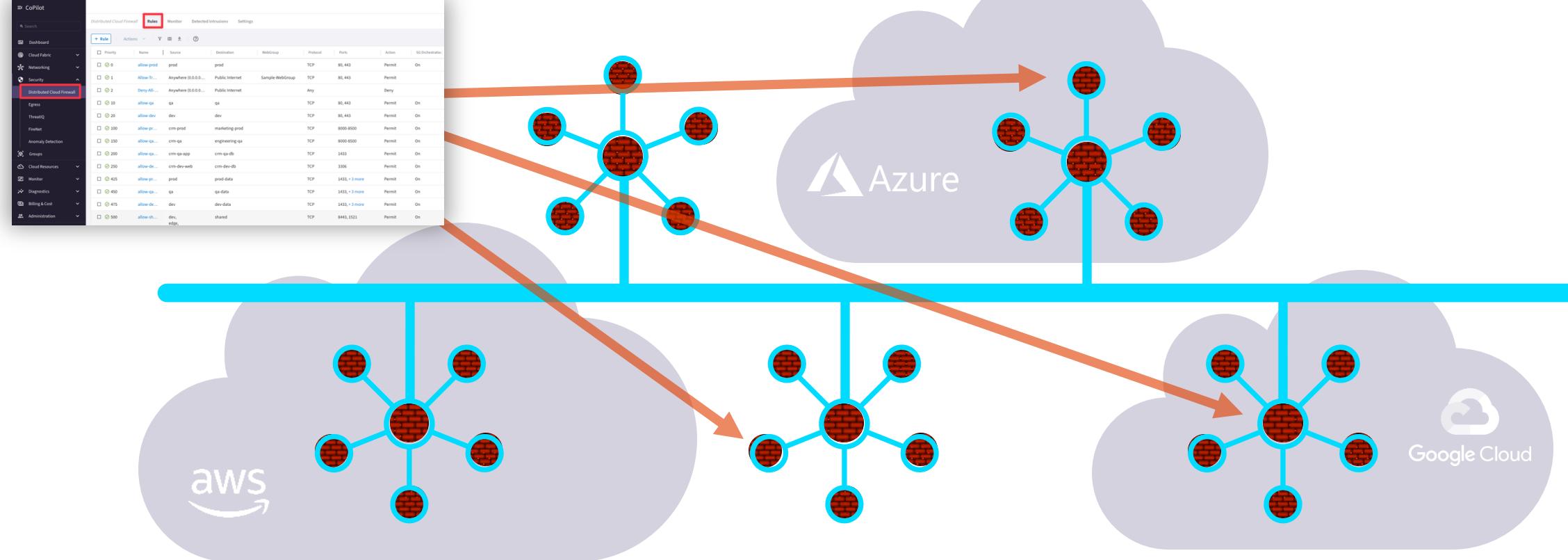


Advanced NAT

Aviatrix Spoke & Edge



A Distributed Cloud Firewall...



Where and How Policies Are Enforced Is Abstracted...

Distributed Cloud Firewall Activation

CoPilot

Search

- Dashboard
- Cloud Fabric
- Networking
- Security
 - Distributed Cloud Firewall
 - Egress
 - ThreatIQ
 - FireNet
 - Anomaly Detection
- Groups
- Cloud Resources
- Monitor
- Diagnostics
- Administration
- Settings

Distributed Cloud Firewall

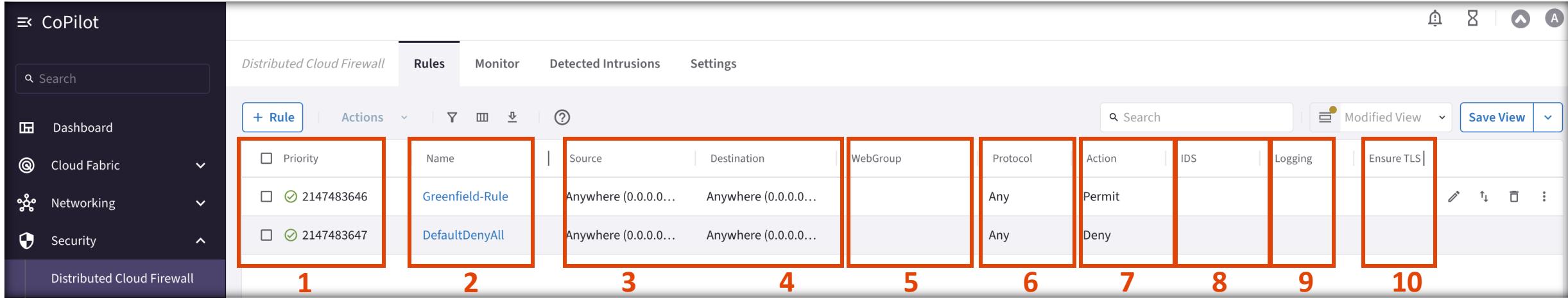
Rules Monitor Detected Intrusions Settings



Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, and a centralized policy management across multiple clouds.

[Begin Using Distributed Cloud Firewall](#)

Distributed Cloud Firewall Rule: Field Position and their Meanings



Priority	Name	Source	Destination	WebGroup	Protocol	Action	IDS	Logging	Ensure TLS
<input type="checkbox"/> 2147483646	Greenfield-Rule	Anywhere (0.0.0.0...)	Anywhere (0.0.0.0...)		Any	Permit			
<input type="checkbox"/> 2147483647	DefaultDenyAll	Anywhere (0.0.0.0...)	Anywhere (0.0.0.0...)		Any	Deny			

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

Priority	Name	Source	Destination	WebGroup	Protocol	Action	IDS	Logging	Ensure TLS
<input type="checkbox"/>	2147483646	Greenfield-Rule	Anywhere (0.0.0.0...)	Anywhere (0.0.0.0...)	Any	Permit			
<input type="checkbox"/>	2147483647	DefaultDenyAll	Anywhere (0.0.0.0...)	Anywhere (0.0.0.0...)	Any	Deny			

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

Create Rule

Rules will be applied only on AWS, AWS Gov, ARM, ARM Gov, and GCP

Name: Bu1-Internet-Https-ubuntu

Source Groups: BU1

Destination Groups: Public Internet

WebGroups: apt-get

Protocol: TCP Port: 443

Specify multiple ports (e.g. 80) and/or port ranges (e.g. 80-8080)

Rule Behavior:

- Action: Permit
- SNI Verification: Off
- SG Orchestration: Off
- Ensure TLS: Off
- TLS Decryption: Off
- Intrusion Detection (IDS): Off

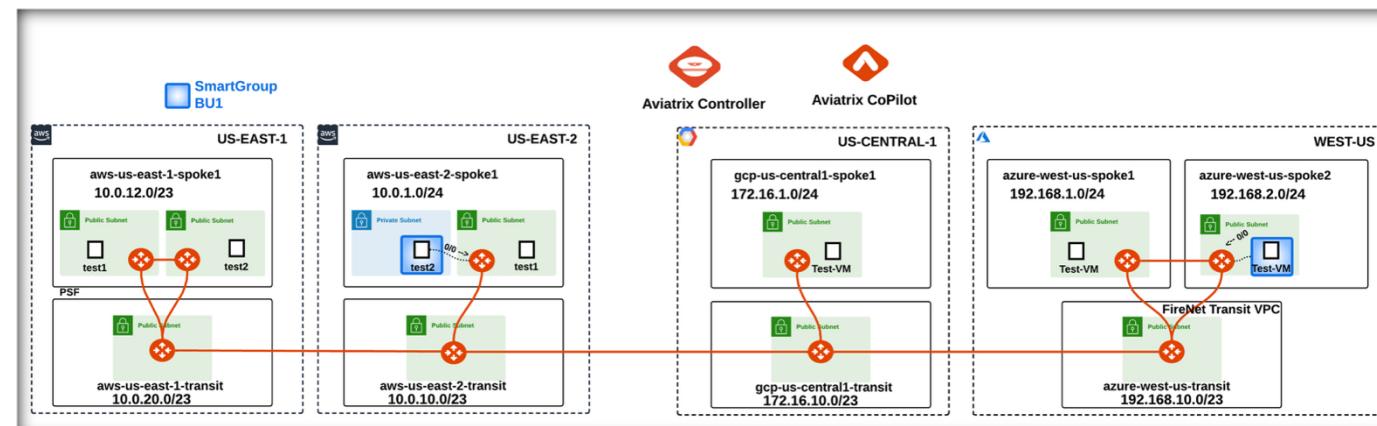
Create WebGroup

URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments.

Name: apt-get

Type: Domains URLs Preview

Domains/URLs: *.ubuntu.com





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**

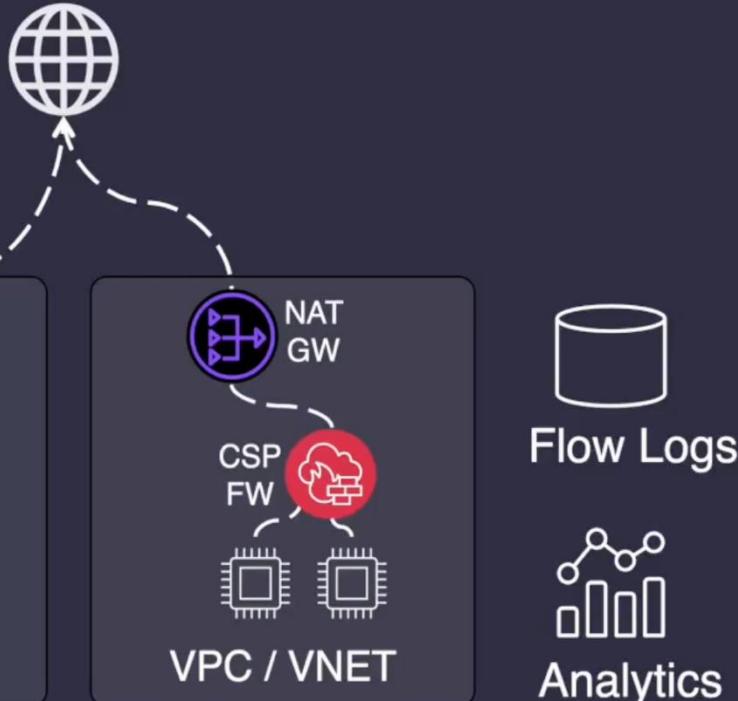
- Excessive Cloud Costs
- Lack of Compliance & Governance
- Risk to Business-Critical Workloads
- Regulatory Fines and Penalties
- Brand Health and Customer Trust

- **Technical Pain**

- No Policy Enforcement
- Slow Troubleshooting and Forensics
- Identifying Noisy Workloads
- Support Distributed Deployments
- Advanced Inspection Capabilities



Two Common Paths



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

DARK READING Secure your 2025 Marketing Dollars Today [LEARN MORE](#)

CLOUD SECURITY

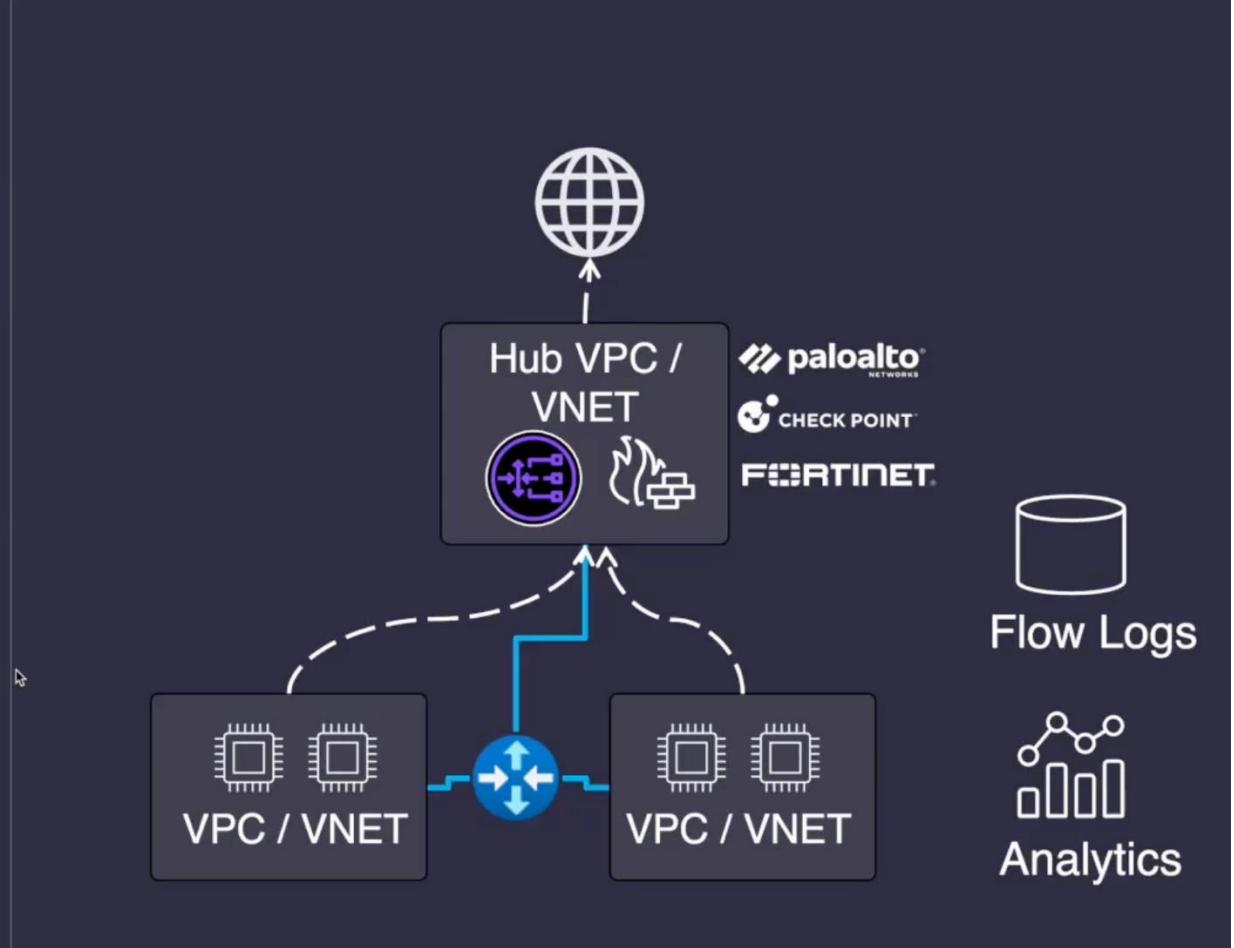
CyberRatings.org Announces Test Results for Cloud Service Provider Native Firewalls

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



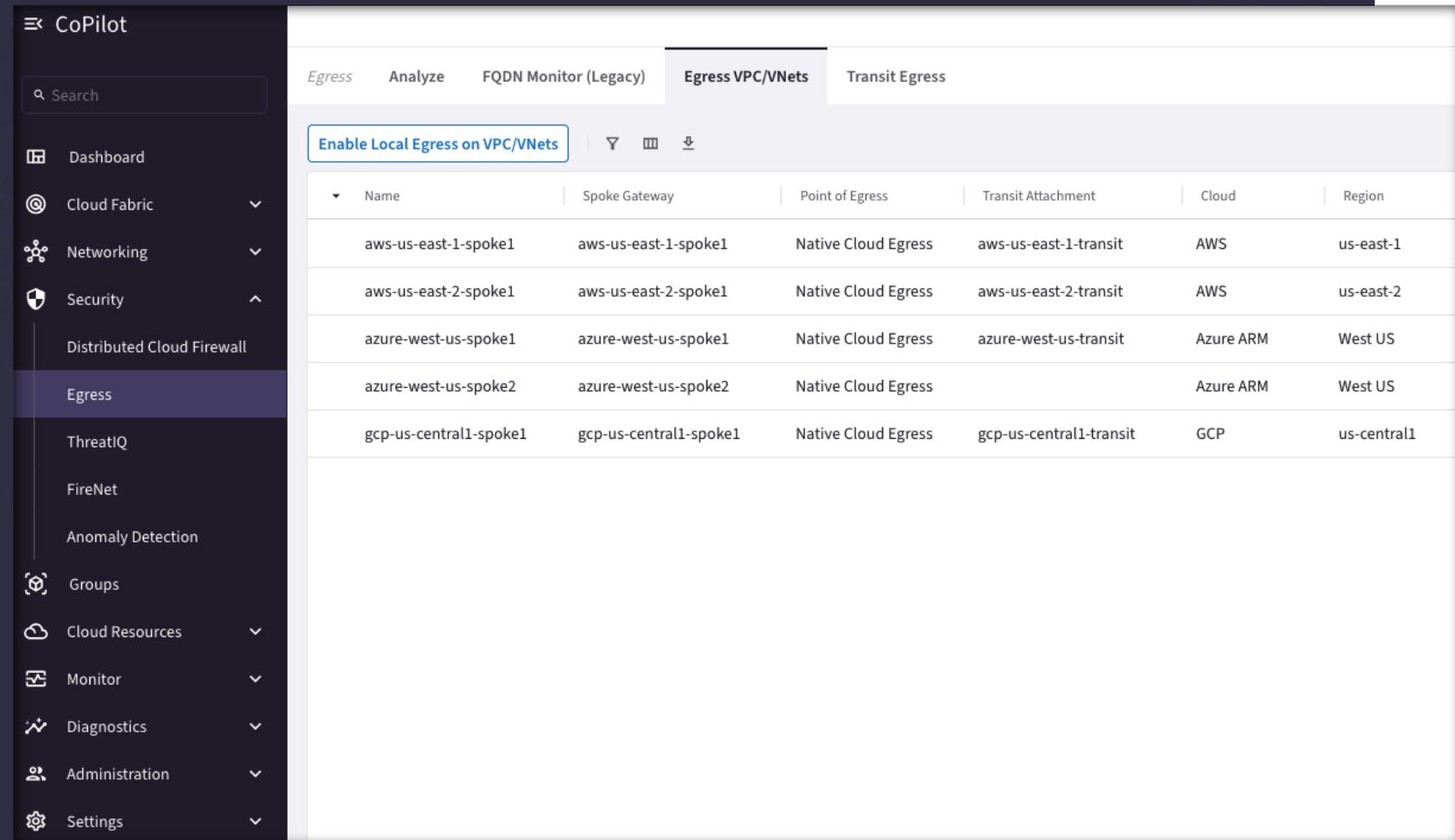
Aviatrix Cloud Firewall

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



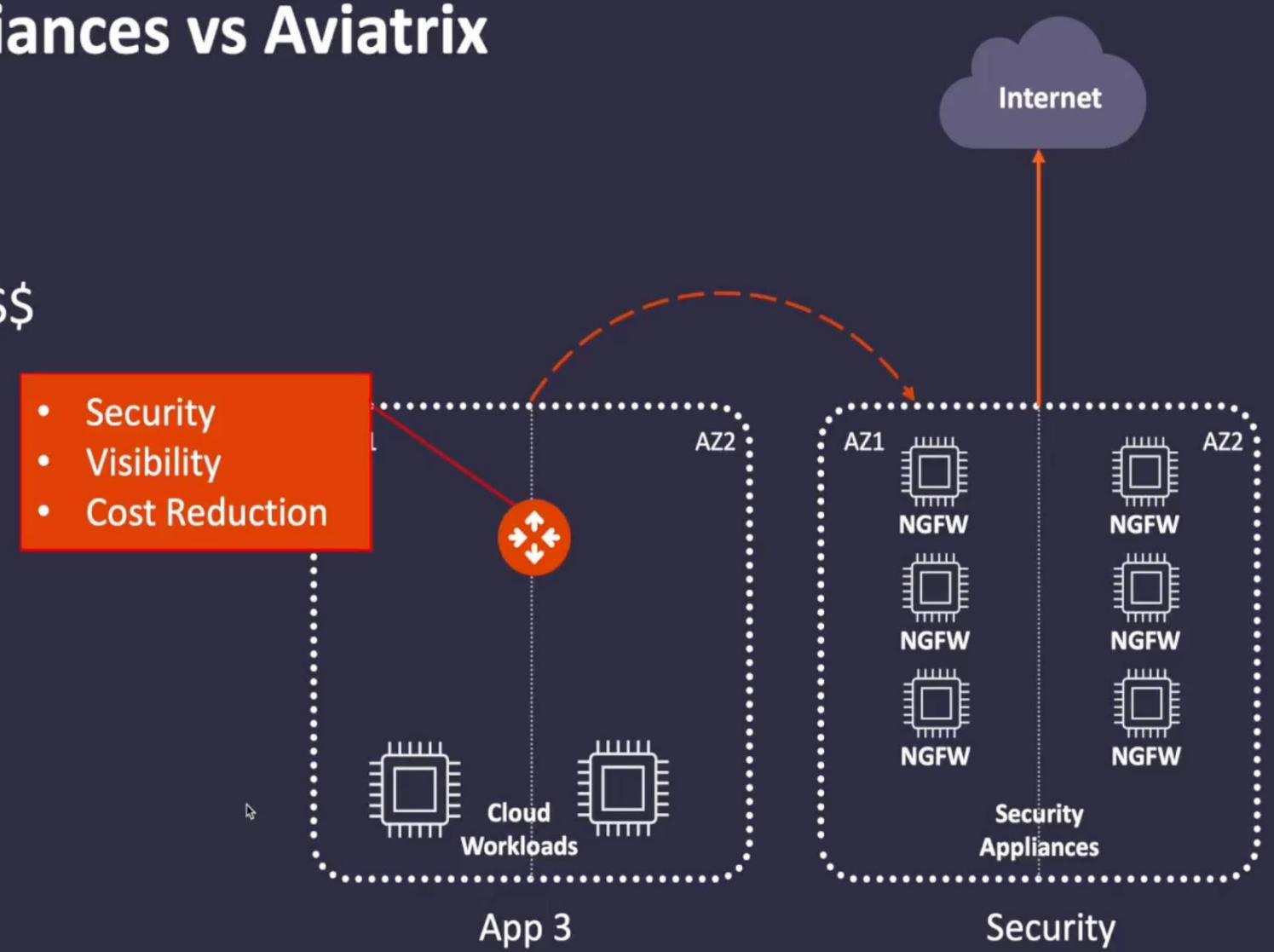
The screenshot shows the Aviatrix CoPilot web interface. On the left is a dark sidebar with various navigation options: Dashboard, Cloud Fabric (with Networking and Security sub-options), Distributed Cloud Firewall, Egress (which is highlighted in purple), ThreatIQ, FireNet, Anomaly Detection, Groups, Cloud Resources (with Monitor and Diagnostics sub-options), Administration, and Settings.

The main content area has a header with tabs: Egress, Analyze, FQDN Monitor (Legacy), Egress VPC/VNets (which is selected and highlighted in blue), and Transit Egress. Below the header is a sub-header "Enable Local Egress on VPC/VNets". The main content is a table with the following data:

Name	Spoke Gateway	Point of Egress	Transit Attachment	Cloud	Region
aws-us-east-1-spoke1	aws-us-east-1-spoke1	Native Cloud Egress	aws-us-east-1-transit	AWS	us-east-1
aws-us-east-2-spoke1	aws-us-east-2-spoke1	Native Cloud Egress	aws-us-east-2-transit	AWS	us-east-2
azure-west-us-spoke1	azure-west-us-spoke1	Native Cloud Egress	azure-west-us-transit	Azure ARM	West US
azure-west-us-spoke2	azure-west-us-spoke2	Native Cloud Egress		Azure ARM	West US
gcp-us-central1-spoke1	gcp-us-central1-spoke1	Native Cloud Egress	gcp-us-central1-transit	GCP	us-central1

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



For LESS than
your NAT GW
Data Transfer Bill

Logging and Analysis

VPC Traffic Mirroring

Amazon GuardDuty

Route 53 Resolver DNS Firewall

EC2 Security Groups and Network ACLs

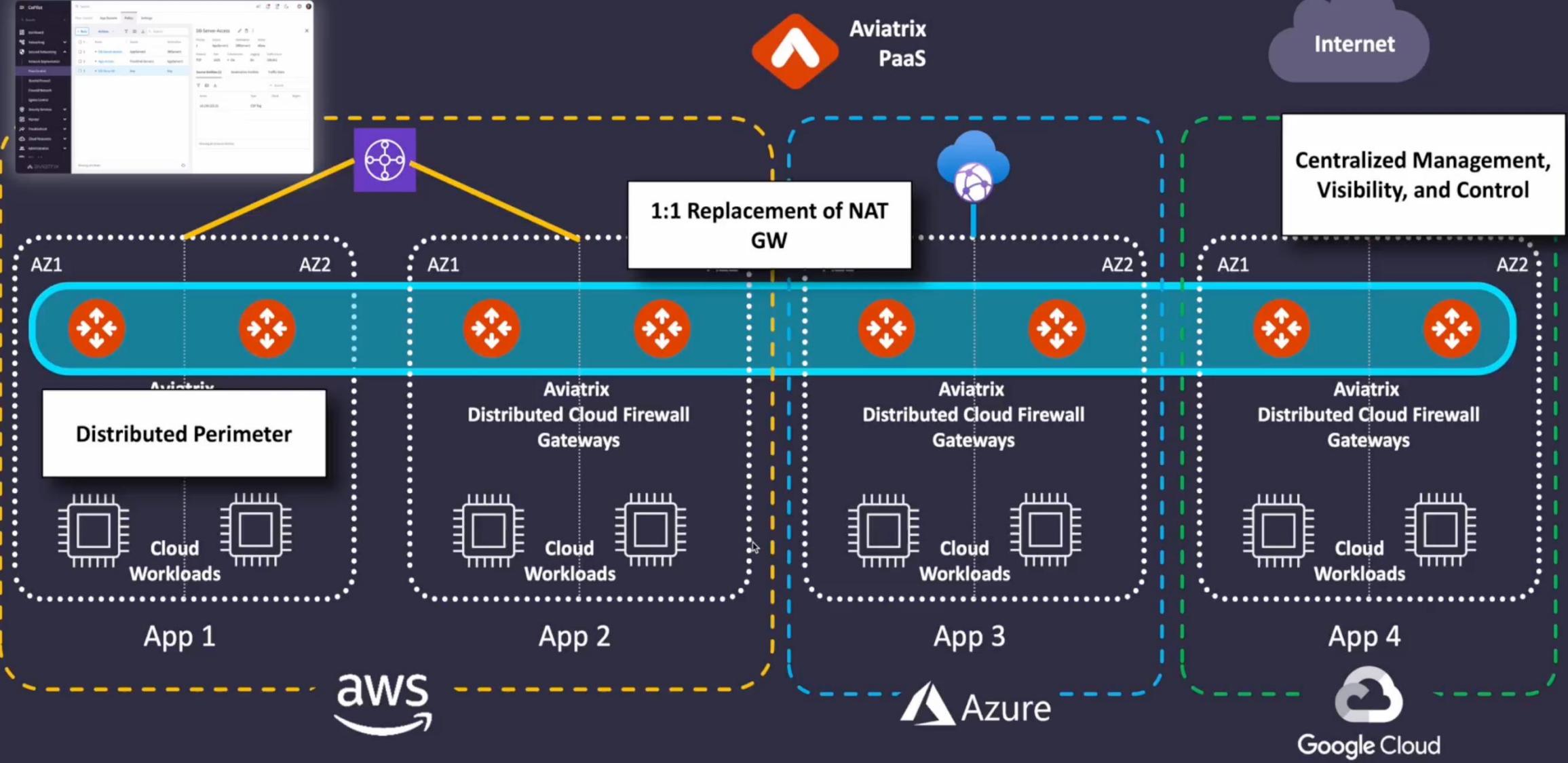
AWS Firewall

AWS NAT GW

Cost and Complexity ↑↓

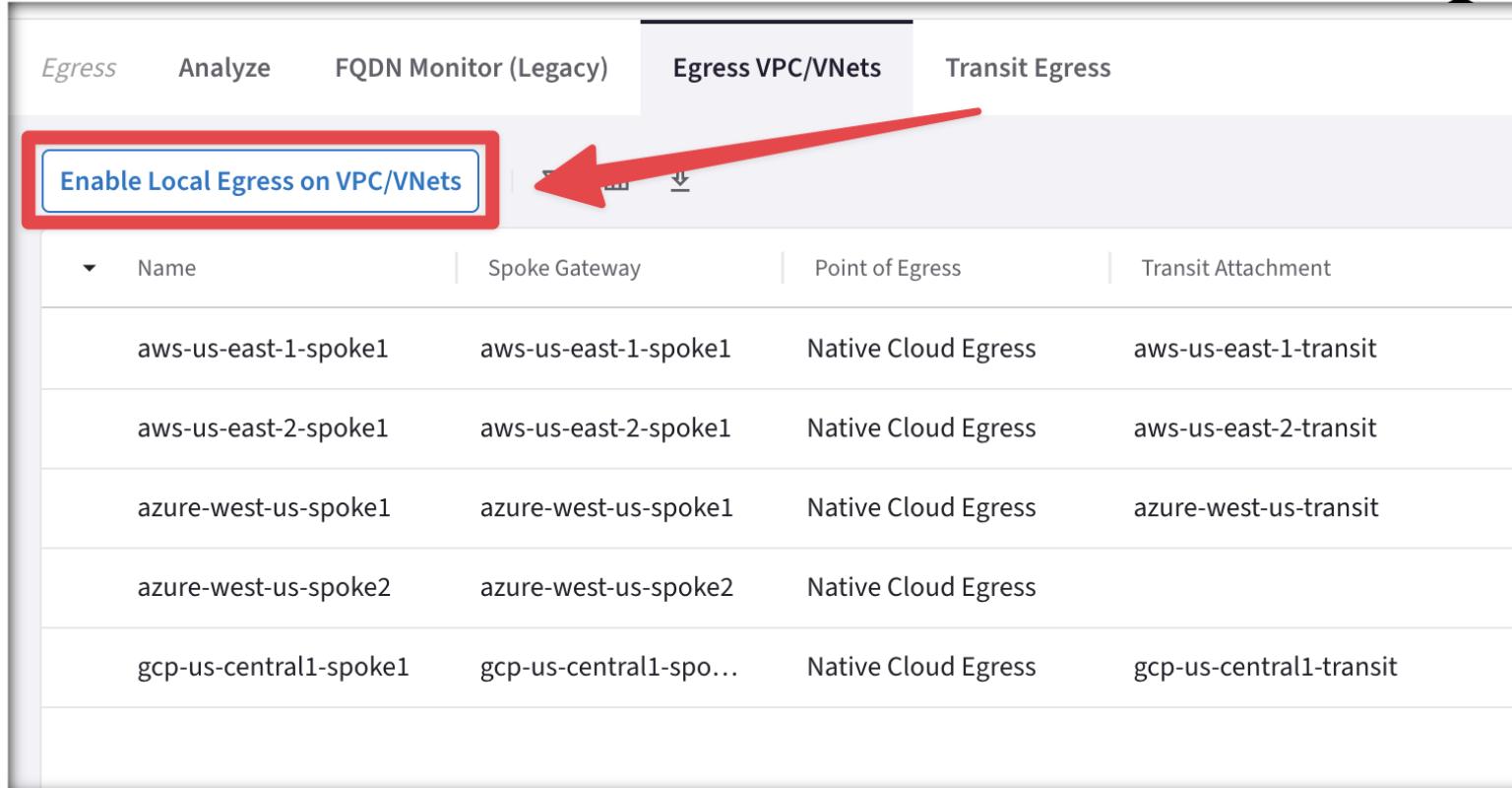
<https://aviatrix.com/aviatrix-paas>

Achieve 25% Cost Savings over 1st Party NAT GWs

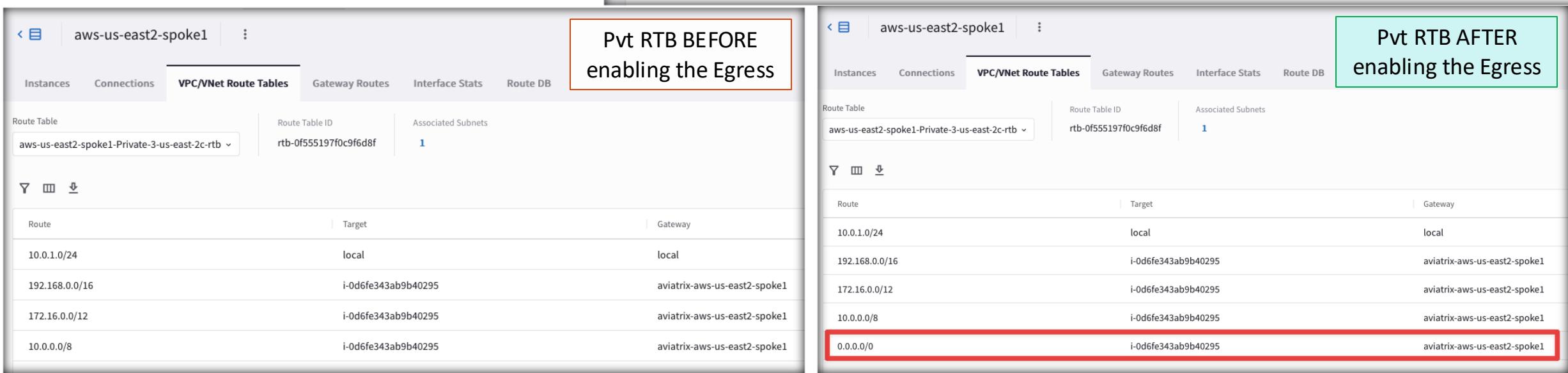


Enabling Cloud Security Egress

- 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 requires additional resources 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.



Egress VPC/VNets			
Enable Local Egress on VPC/VNets			
Name	Spoke Gateway	Point of Egress	Transit Attachment
aws-us-east-1-spoke1	aws-us-east-1-spoke1	Native Cloud Egress	aws-us-east-1-transit
aws-us-east-2-spoke1	aws-us-east-2-spoke1	Native Cloud Egress	aws-us-east-2-transit
azure-west-us-spoke1	azure-west-us-spoke1	Native Cloud Egress	azure-west-us-transit
azure-west-us-spoke2	azure-west-us-spoke2	Native Cloud Egress	
gcp-us-central1-spoke1	gcp-us-central1-spo...	Native Cloud Egress	gcp-us-central1-transit



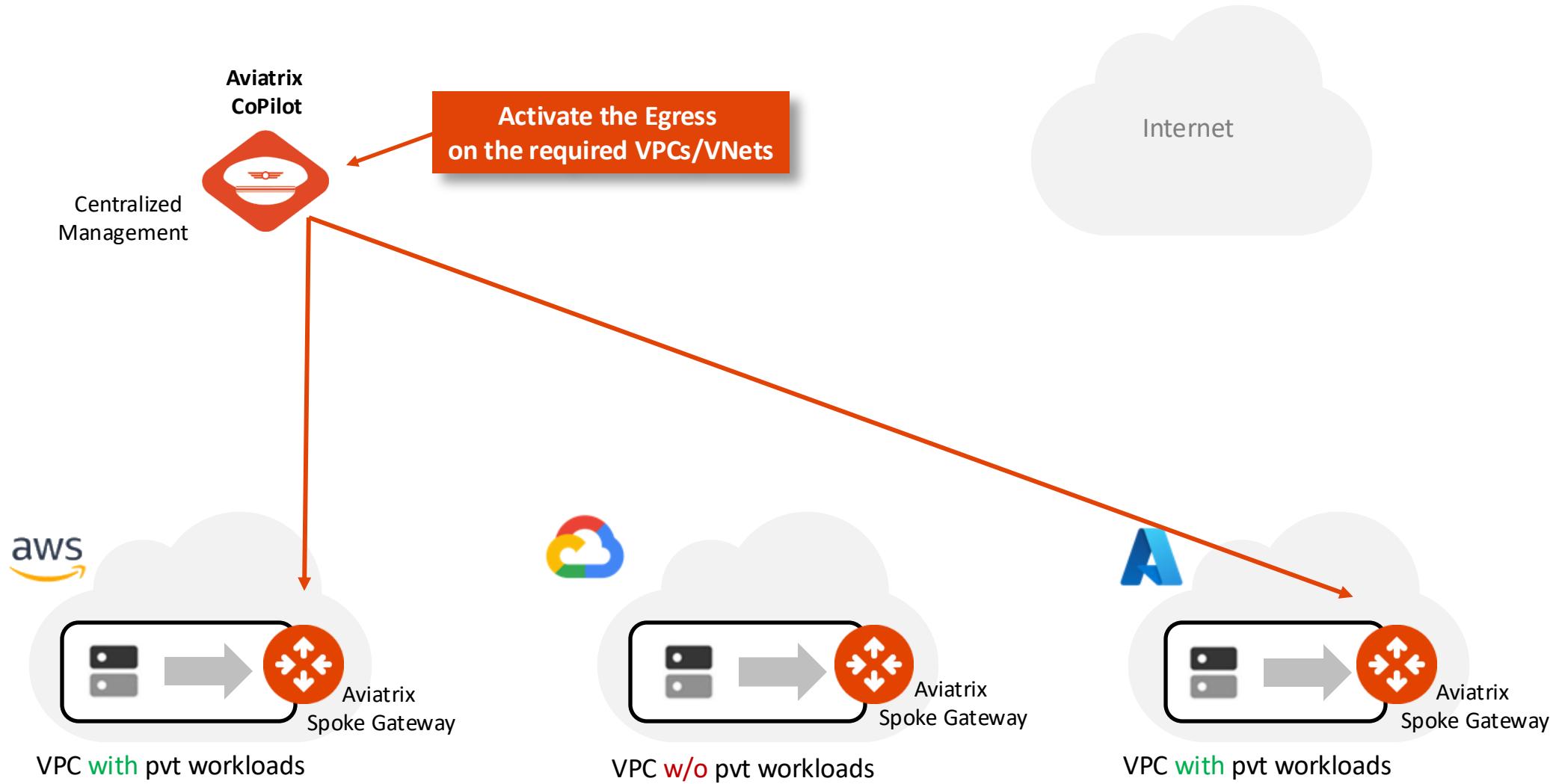
Pvt RTB BEFORE enabling the Egress

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

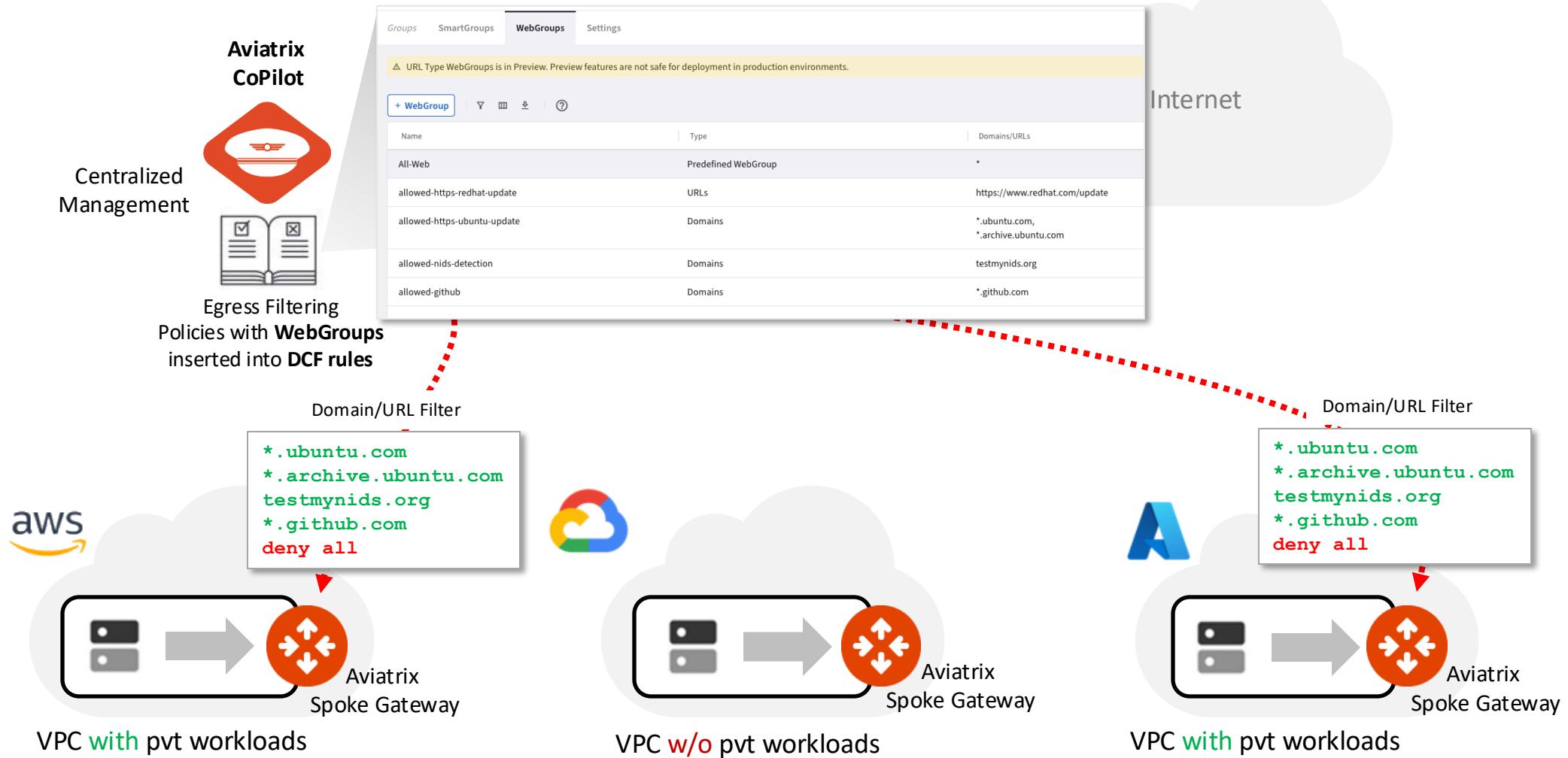
Pvt RTB AFTER enabling the Egress

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

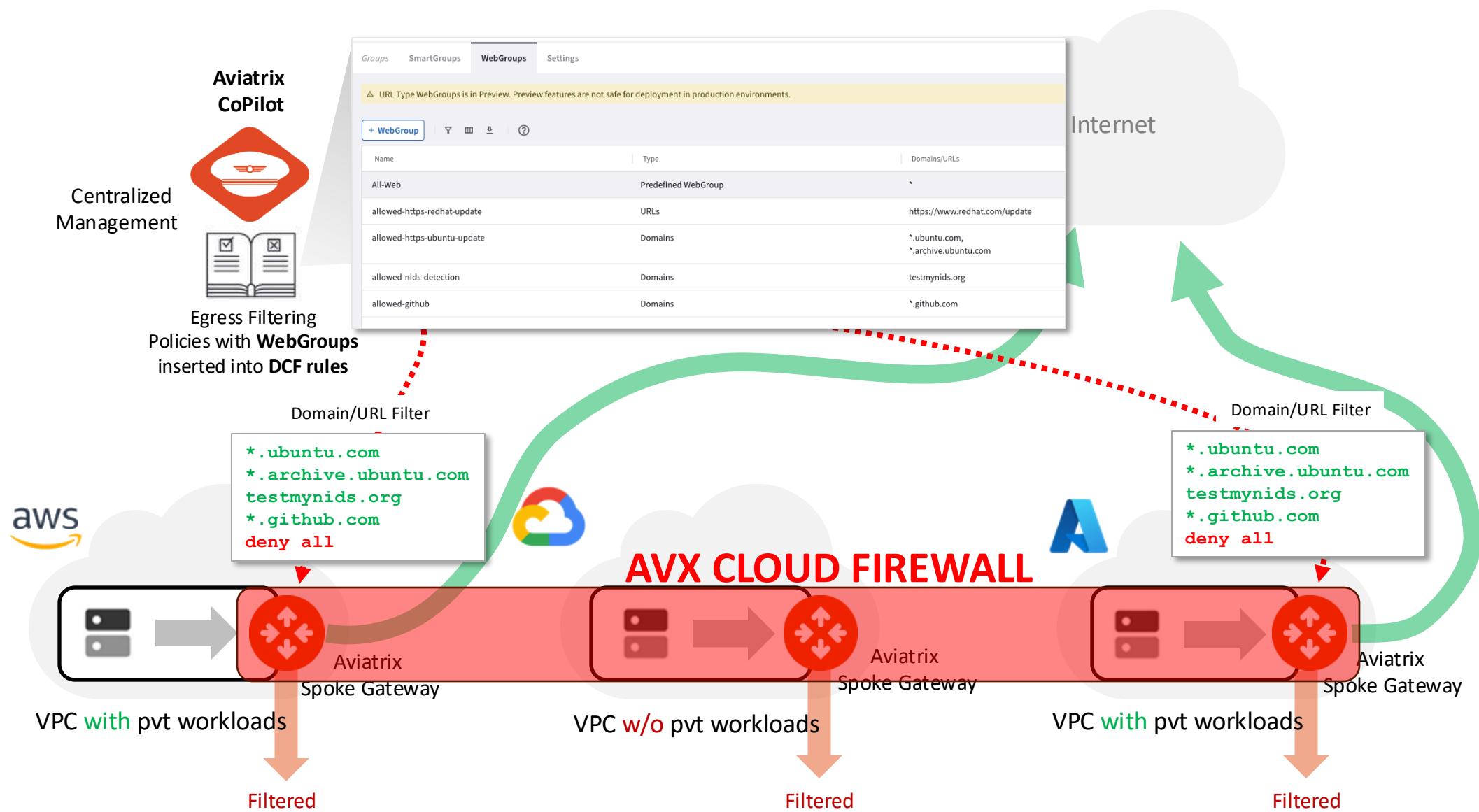
Aviatrix Cloud Firewall



Aviatrix Cloud Firewall



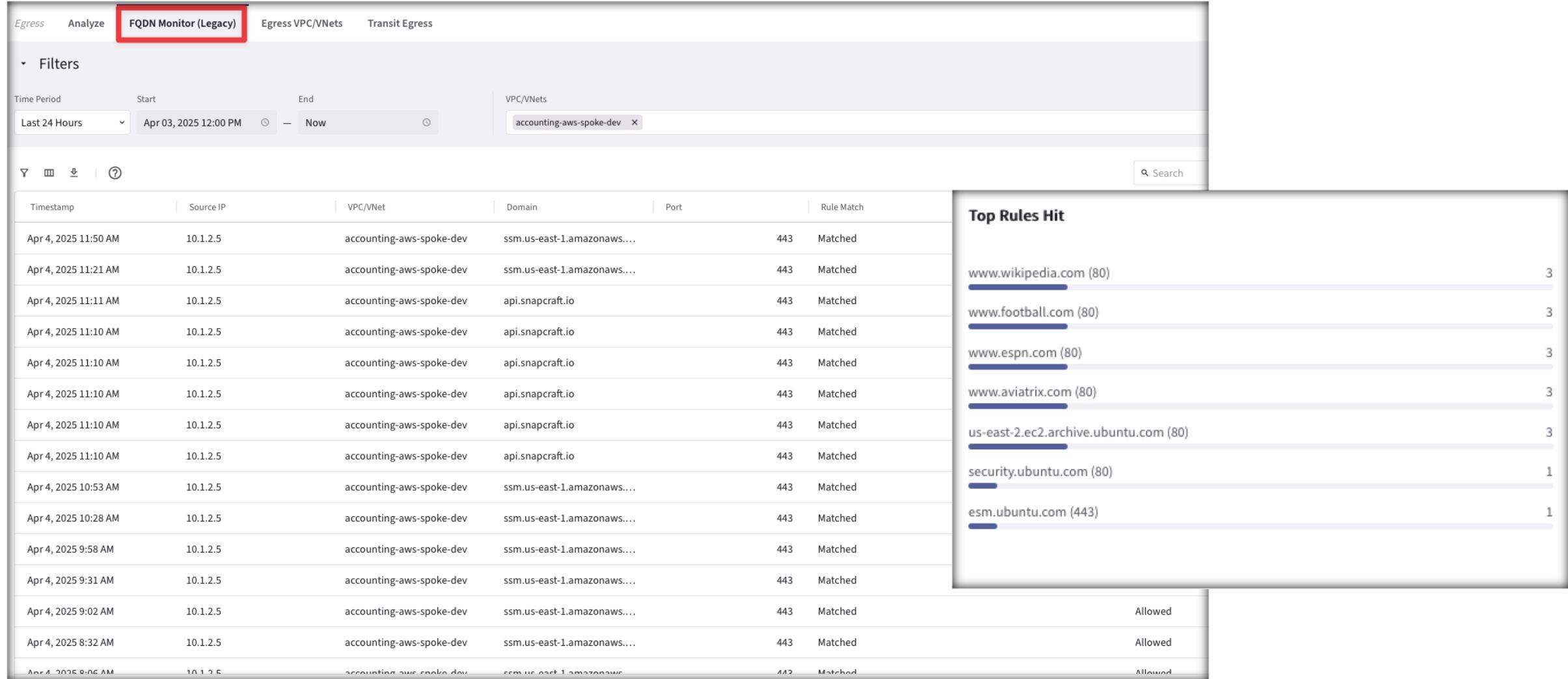
Aviatrix Cloud Firewall



- 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.



The screenshot shows the Aviatrix FQDN Monitor (Legacy) interface. At the top, there are tabs: Egress, Analyze, **FQDN Monitor (Legacy)**, Egress VPC/VNets, and Transit Egress. The **FQDN Monitor (Legacy)** tab is highlighted with a red border. Below the tabs, there are filters for Time Period (Last 24 Hours, Start: Apr 03, 2025 12:00 PM, End: Now), VPC/VNets (accounting-aws-spoke-dev), and a search bar. The main area displays a table of logs with columns: Timestamp, Source IP, VPC/VNet, Domain, Port, and Rule Match. The logs show multiple entries for the source IP 10.1.2.5 connecting to various domains (ssm.us-east-1.amazonaws.com, api.snapcraft.io, www.wikipedia.com, etc.) on port 443, with all rule matches being 'Matched'. To the right of the log table is a chart titled 'Top Rules Hit' showing the most frequent domains: www.wikipedia.com (80) with 3 hits, www.football.com (80) with 3 hits, www.espn.com (80) with 3 hits, www.aviatrix.com (80) with 3 hits, us-east-2.ec2.archive.ubuntu.com (80) with 3 hits, security.ubuntu.com (80) with 1 hit, and esm.ubuntu.com (443) with 1 hit.

Timestamp	Source IP	VPC/VNet	Domain	Port	Rule Match
Apr 4, 2025 11:50 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched
Apr 4, 2025 11:21 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched
Apr 4, 2025 11:11 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched
Apr 4, 2025 10:53 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched
Apr 4, 2025 10:28 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched
Apr 4, 2025 9:58 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched
Apr 4, 2025 9:31 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched
Apr 4, 2025 9:02 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched
Apr 4, 2025 8:32 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched
Apr 4, 2025 8:06 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched



Threat Prevention

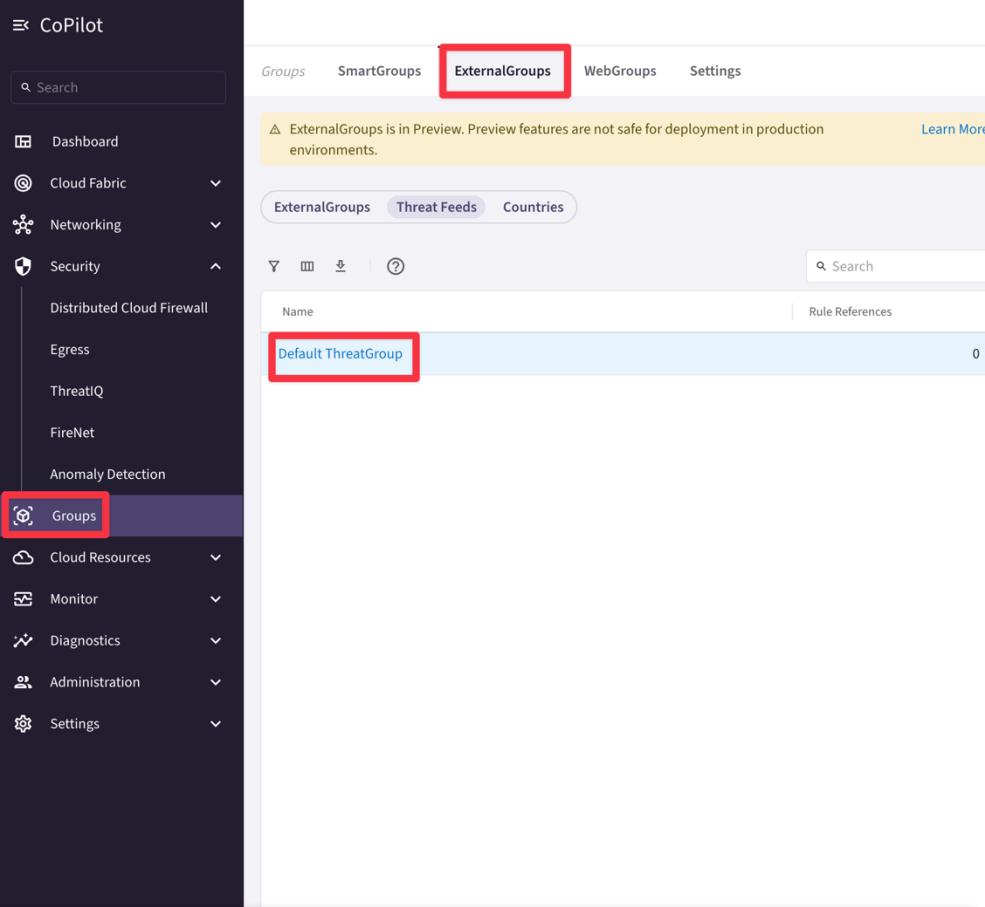
Default ThreatGroup

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

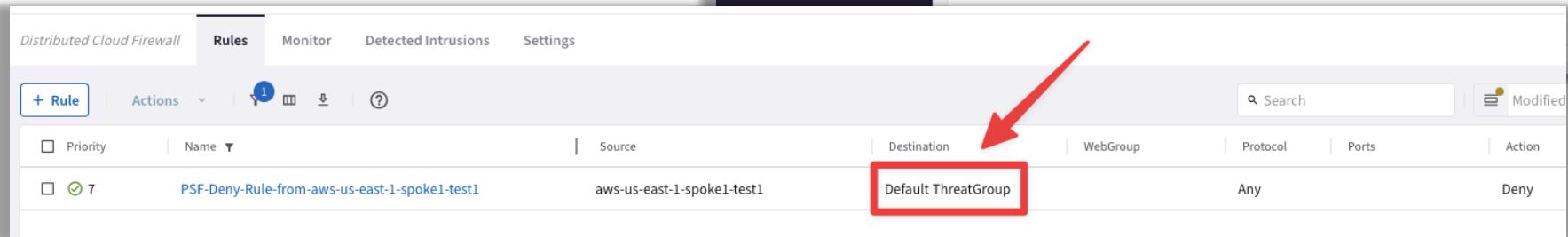


ExternalGroups

Default ThreatGroup

IP Address / CIDRs	Protocol	Threat Type	Severity
1.2.202.167/32		Threat Feed	Unknown
1.6.53.205/32		Threat Feed	Unknown
1.12.245.182/32		Threat Feed	Unknown
1.12.246.6/32		Threat Feed	Unknown
1.14.193.147/32		Threat Feed	Unknown
1.24.16.5/32		Threat Feed	Unknown
1.24.16.6/32		Threat Feed	Unknown
1.24.16.19/32		Threat Feed	Unknown
1.24.16.25/32		Threat Feed	Unknown
1.24.16.32/32		Threat Feed	Unknown
1.24.16.68/32		Threat Feed	Unknown
1.24.16.80/32		Threat Feed	Unknown
1.24.16.86/32		Threat Feed	Unknown
1.24.16.87/32		Threat Feed	Unknown

Total 11,707 IP Addresses



Rules

Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
7	PSF-Deny-Rule-from-aws-us-east-1-spoke1-test1	aws-us-east-1-spoke1-test1	Default ThreatGroup	Any			Deny

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).

The screenshot displays the ThreatIQ CoPilot interface with the 'Overview' tab selected. The left sidebar contains a navigation menu with options like Dashboard, Cloud Fabric, Networking, Security, ThreatIQ, FireNet, Anomaly Detection, Groups, Cloud Resources, Monitor, Diagnostics, Administration, and Settings. The main area features a world map showing the locations of detected threats. Below the map are three circular dashboards: 'Unique Threat IPs' (55), 'Threat Severity' (Total 55), and 'Threat Classifications' (Total 55). At the bottom, there are two line charts: 'Threats Over Time' and 'Total Threats Over Time', both showing a sharp increase in activity around 6:00 PM. A table at the bottom lists specific threat events with columns for Timestamp, Threat Domain, Severity, Classification, Source, Destination, and Gateway Name, each with a 'VIEW' link.

ThreatIQ Overview Configuration Custom Threat List

Time Period Start End

Last 24 Hours Mar 24, 2025 04:30 PM — Now Apply

Unique Threat IPs
55

Threat Count
55

All Threats (Total)
0 771

Threat Severity
Total 55

Threat Classifications
Total 55

Threats Over Time

Total Threats Over Time

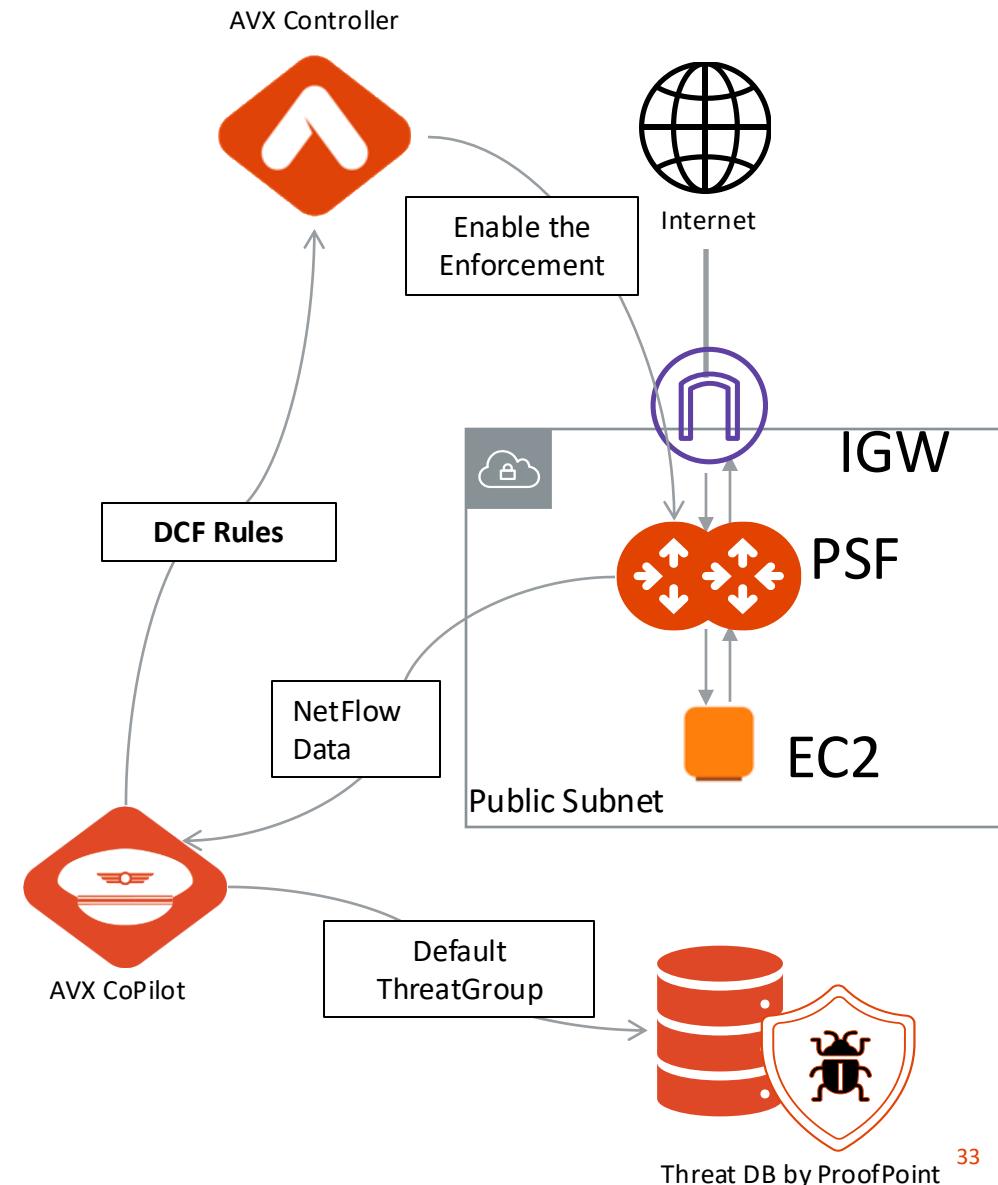
Timestamp	Threat Domain	Severities	Classifications	Source	Destination	Gateway Name	Action
Dec 18, 2024 9:15:25 PM	Lookup Failed	● Major	misc-attack	4.228.225.246	10.0.12.40	aws-us-east-1-psf	VIEW
Dec 18, 2024 9:09:38 PM	andreas.probe.onyphe.net	● Major	misc-attack	51.81.110.52	10.0.12.40	aws-us-east-1-psf	VIEW
Dec 18, 2024 9:08:02 PM	33.211.203.35.bc.googleus...	● Major	misc-attack	35.203.211.33	10.0.12.40	aws-us-east-1-psf	VIEW
Dec 18, 2024 9:08:02 PM	warsaw.scan.bufferover.run	● Major	misc-attack	45.79.132.41	10.0.12.40	aws-us-east-1-psf	VIEW



Public Subnet Filtering (PSF) Gateway

Aviatrix Public Subnet Filtering Gateways (PSF GWs)

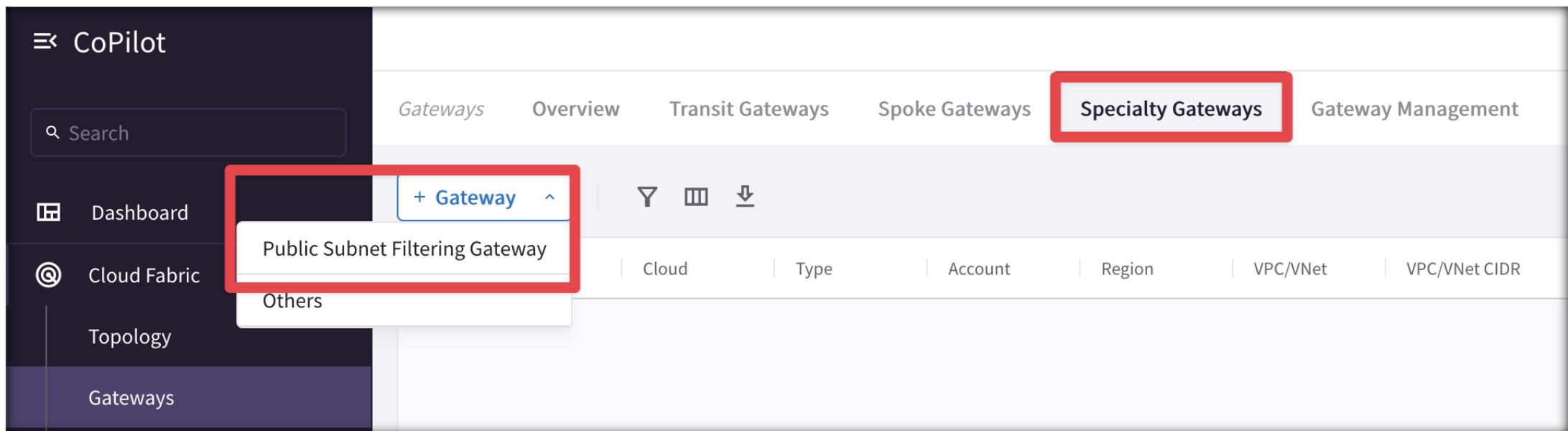
- **Public Subnet Filtering Gateways** (PSF gateways) provide ingress and egress security for **AWS** public subnets where instances have public IP addresses.
- After the Public Subnet Filtering (PSF) gateway is launched, you can apply also DCF (Distributed Cloud Firewall) rules – *enforcement must be 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:

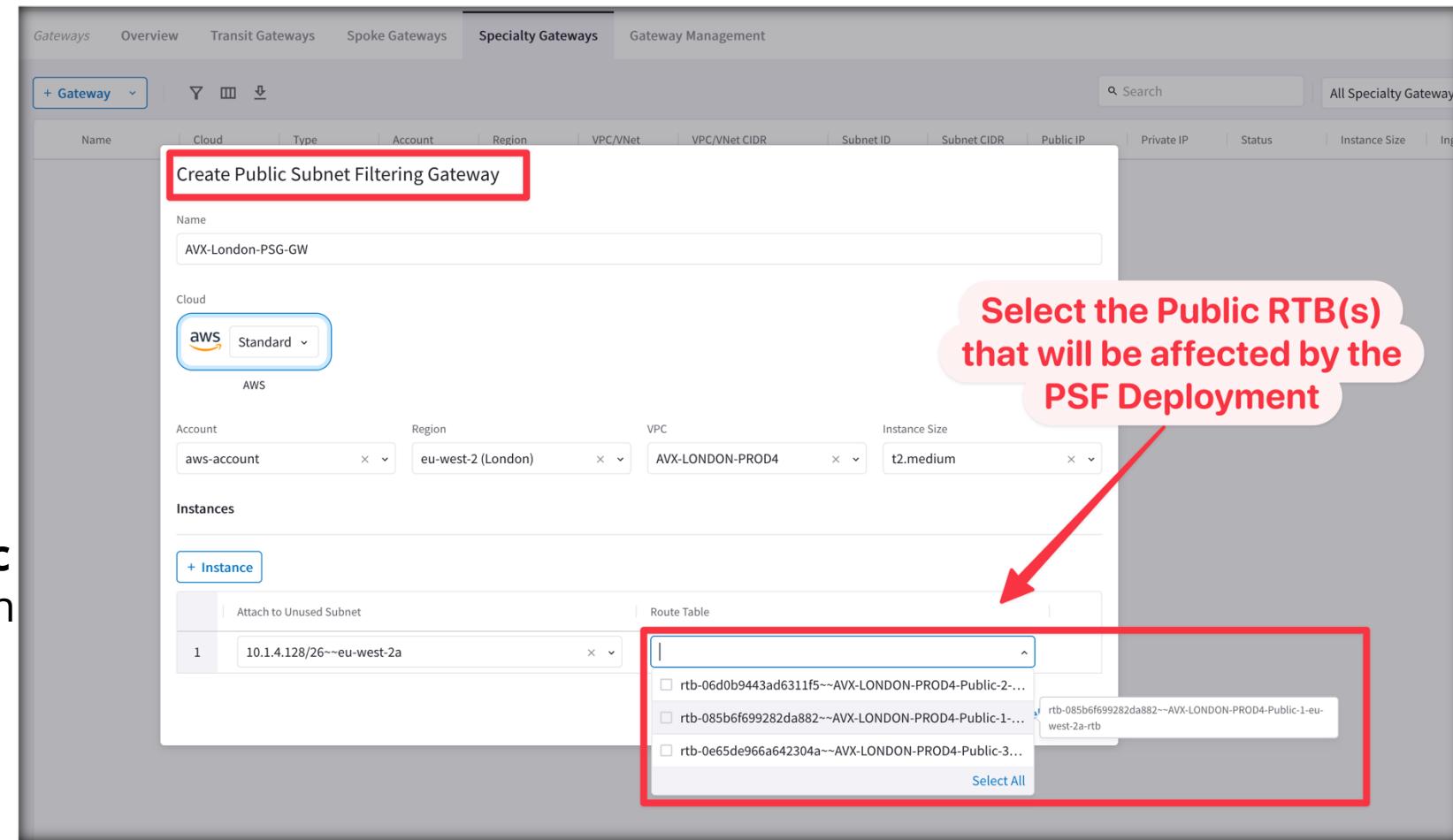
1. In CoPilot, navigate to **Cloud Fabric > Gateways > Specialty Gateways** tab.
2. Click **+Gateway** and select **Public Subnet Filtering Gateway**.



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.

Enforcement on PSF Gateways ⚠ Preview

Control the application of Distributed Cloud Firewall Policy on PSF Gateways.

Status

Disabled

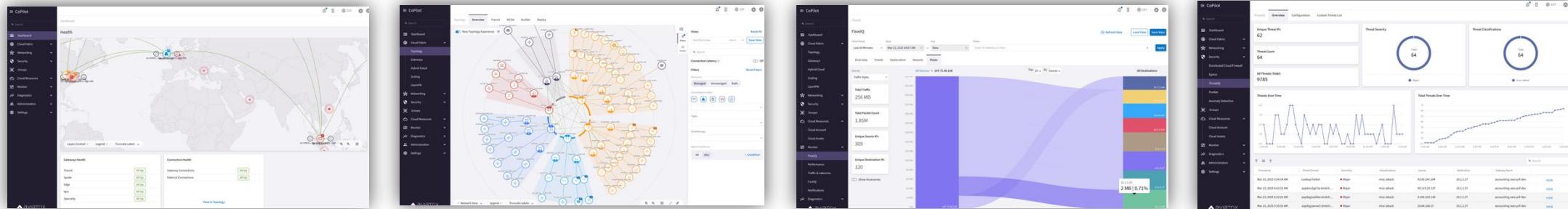
Enable



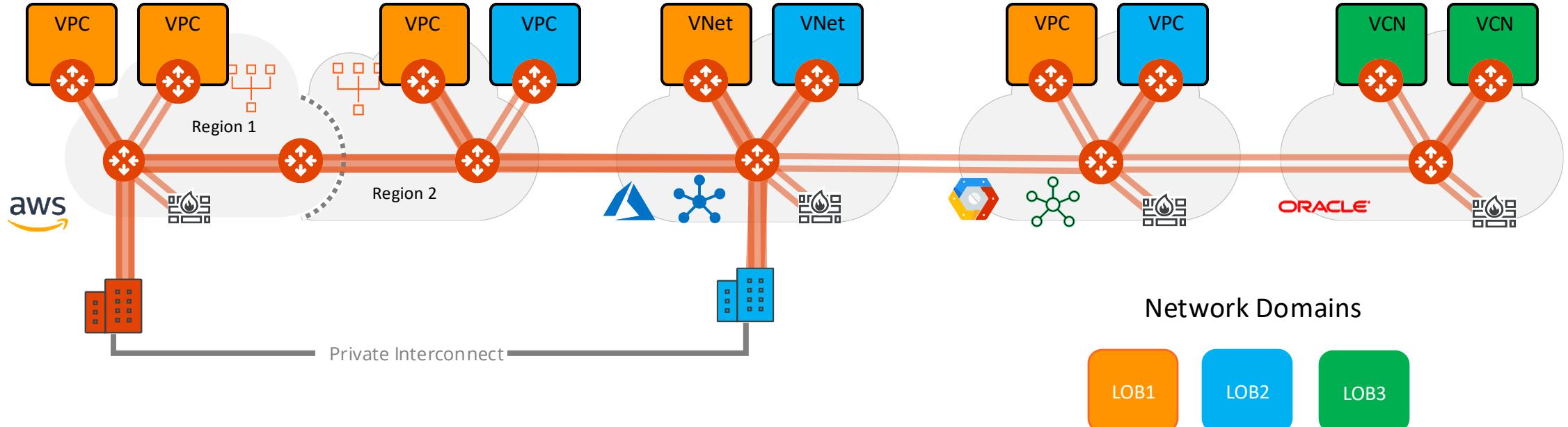
Macro-Segmentation

Network Segmentation

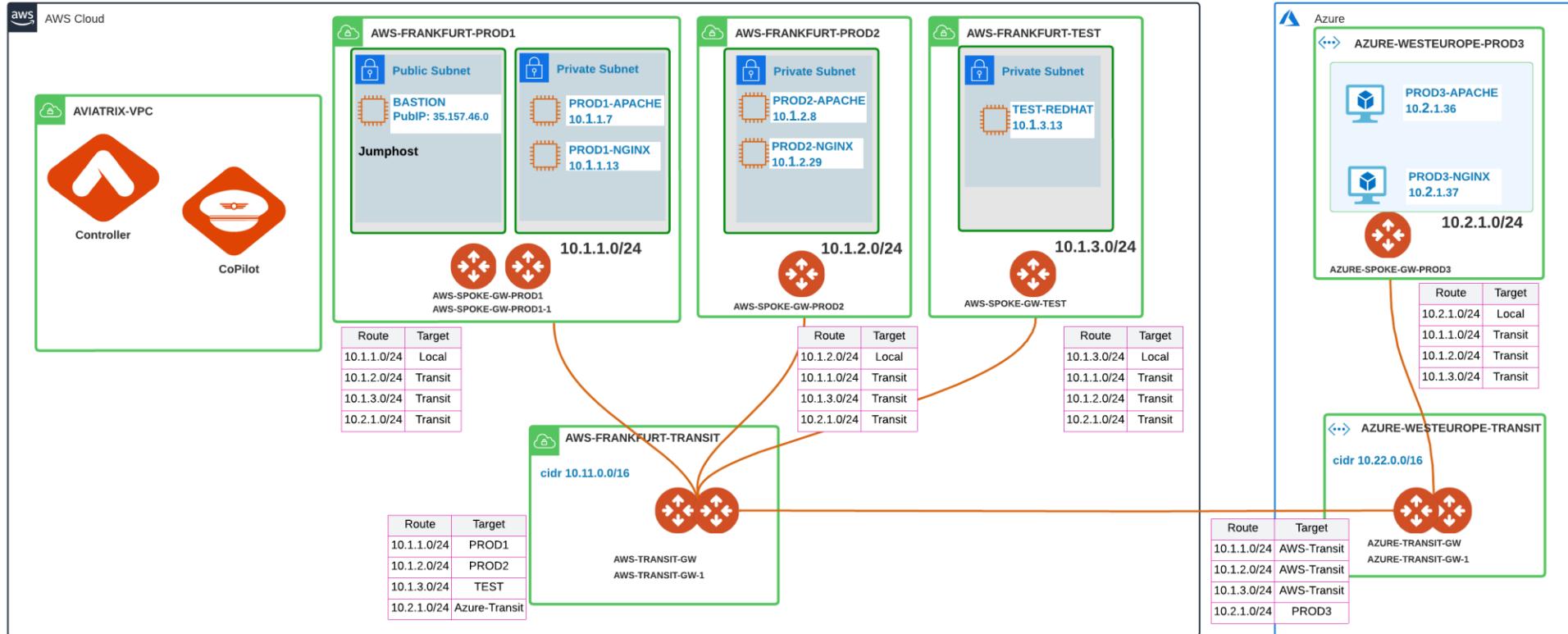
Aviatrix
CoPilot



← Network Granularity and Control →



1. Enable Transit Gateways for Network Segmentation



Enable the Network Segmentation:

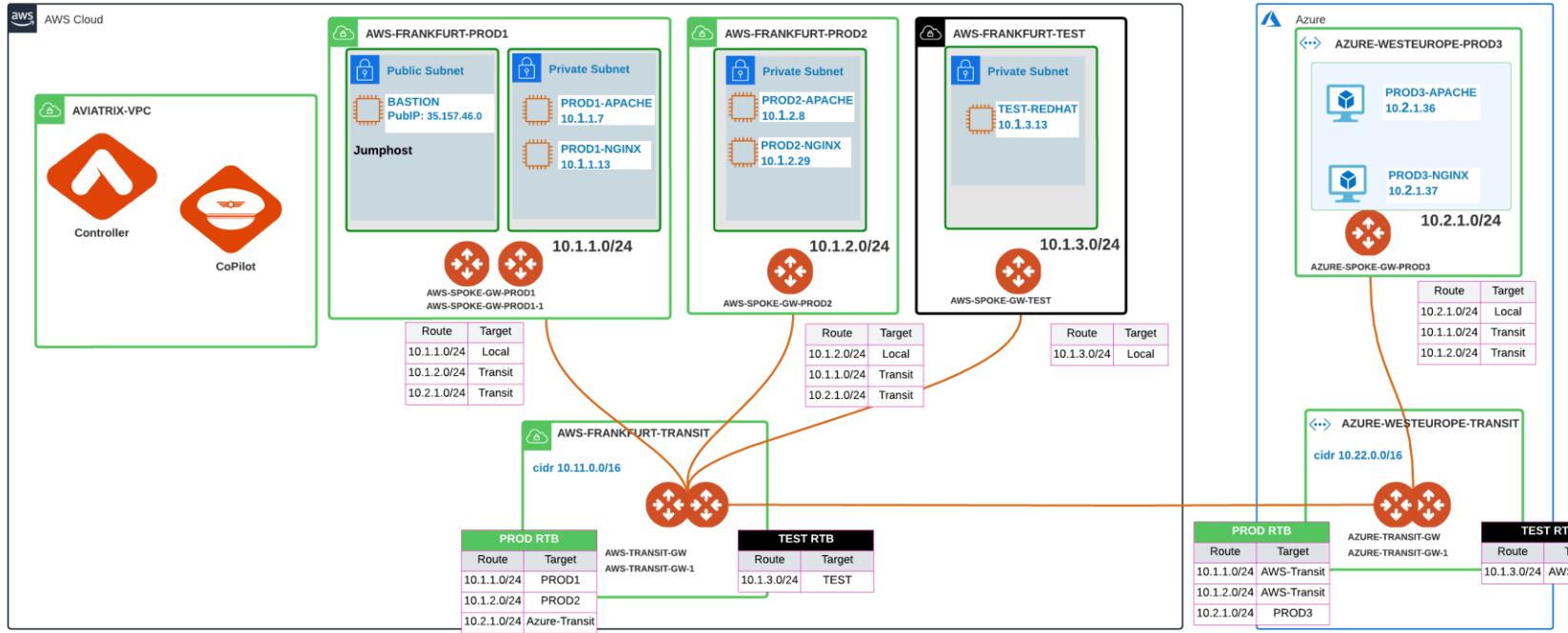
- Choose the Transit Gateway(s) that will route traffic for its members.

Configure Transit Gateways for Network Segmentation

Aviatrix transit gateways have to be enabled to support network segmentation on them.

Name	Cloud	Region	IP Address Space	
AWS-TRANSIT-GW	aws	eu-central-1	10.11.0.0/16	<input checked="" type="checkbox"/> Enabled
AZURE-TRANSIT-GW	arm	West Europe	10.22.0.0/16	<input checked="" type="checkbox"/> Enabled

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 Network Domain

Name *

Associations

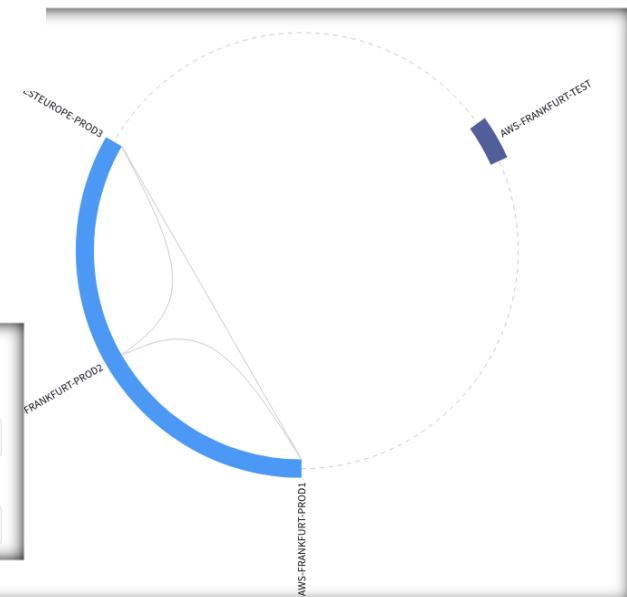
AWS-FRANKFURT-PROD1 X AWS-FRANKFURT-PROD2 X AZURE-WESTEUROPE-PROD3 X

Create Network Domain

Name *

Associations

AWS-FRANKFURT-TEST X

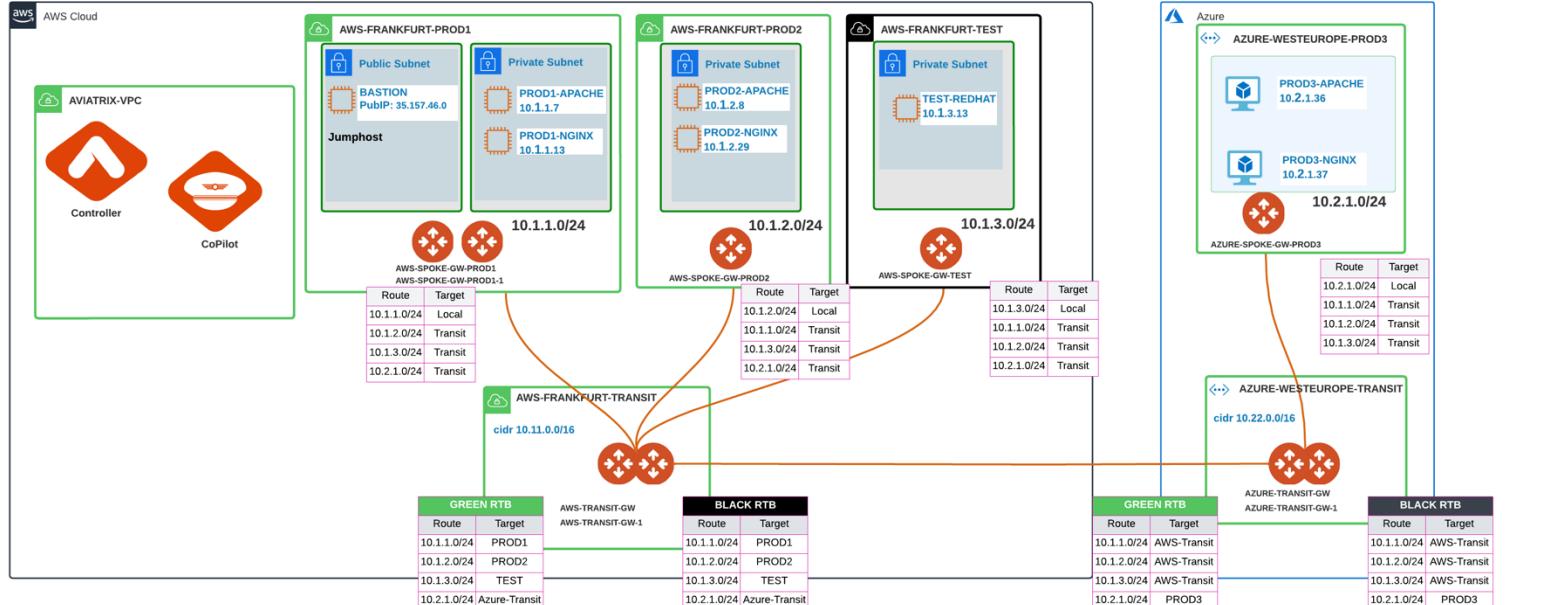


Create the Network Domains:

- 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)

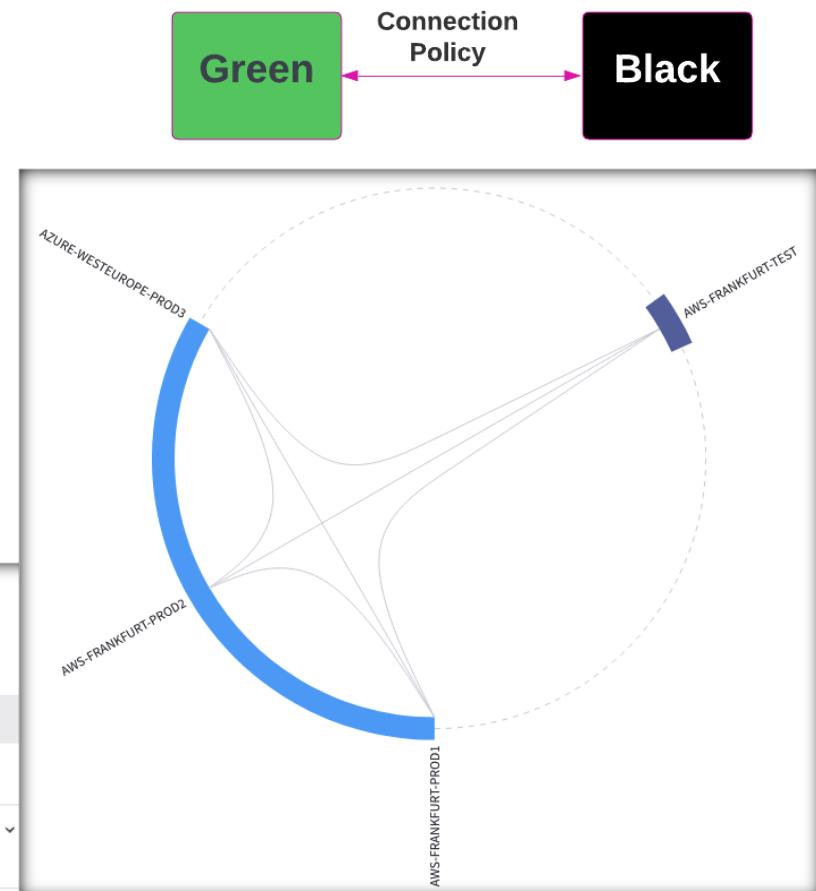


Optionally, enable the Connection Policy:

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

Edit Network Domain: PROD

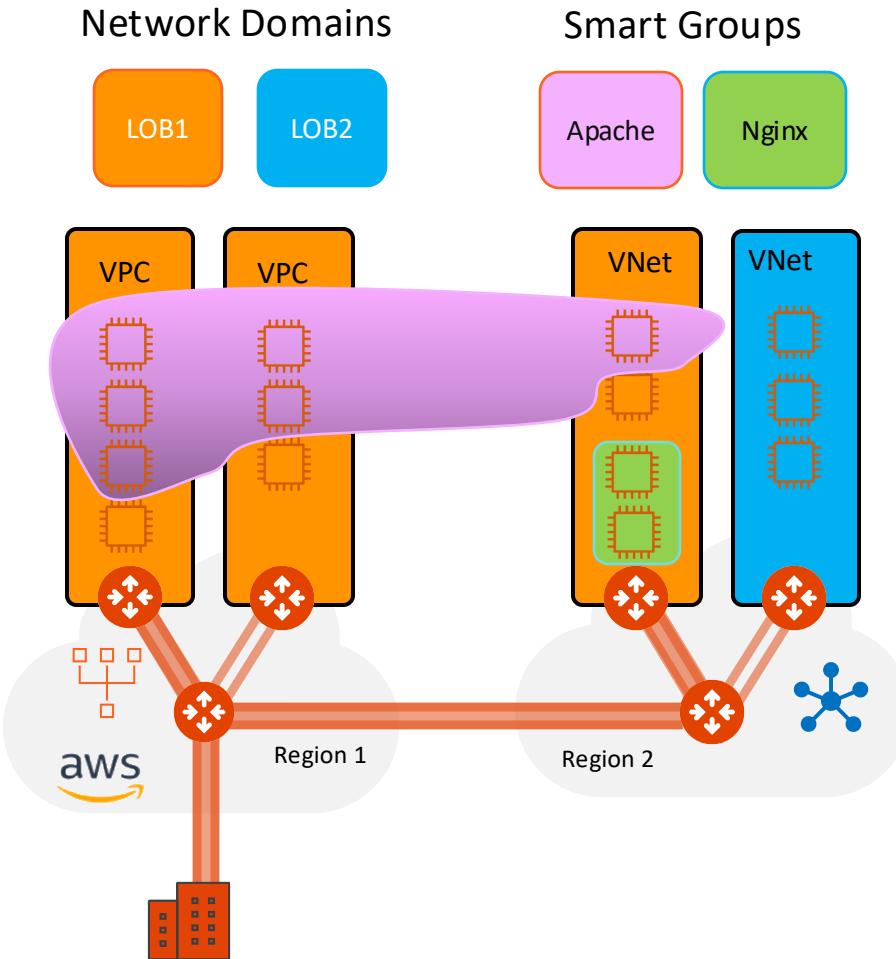
Name *	PROD
Associations	AWS-FRANKFURT-PROD1 X AWS-FRANKFURT-PROD2 X AZURE-WESTEUROPE-PROD3 X
Connect to Network Domain	TEST X <input checked="" type="checkbox"/> TEST Select All Cancel Save





Micro-Segmentation

Micro-Segmentation



Inter-rule

Source SmartGroup ≠ Destination SmartGroup

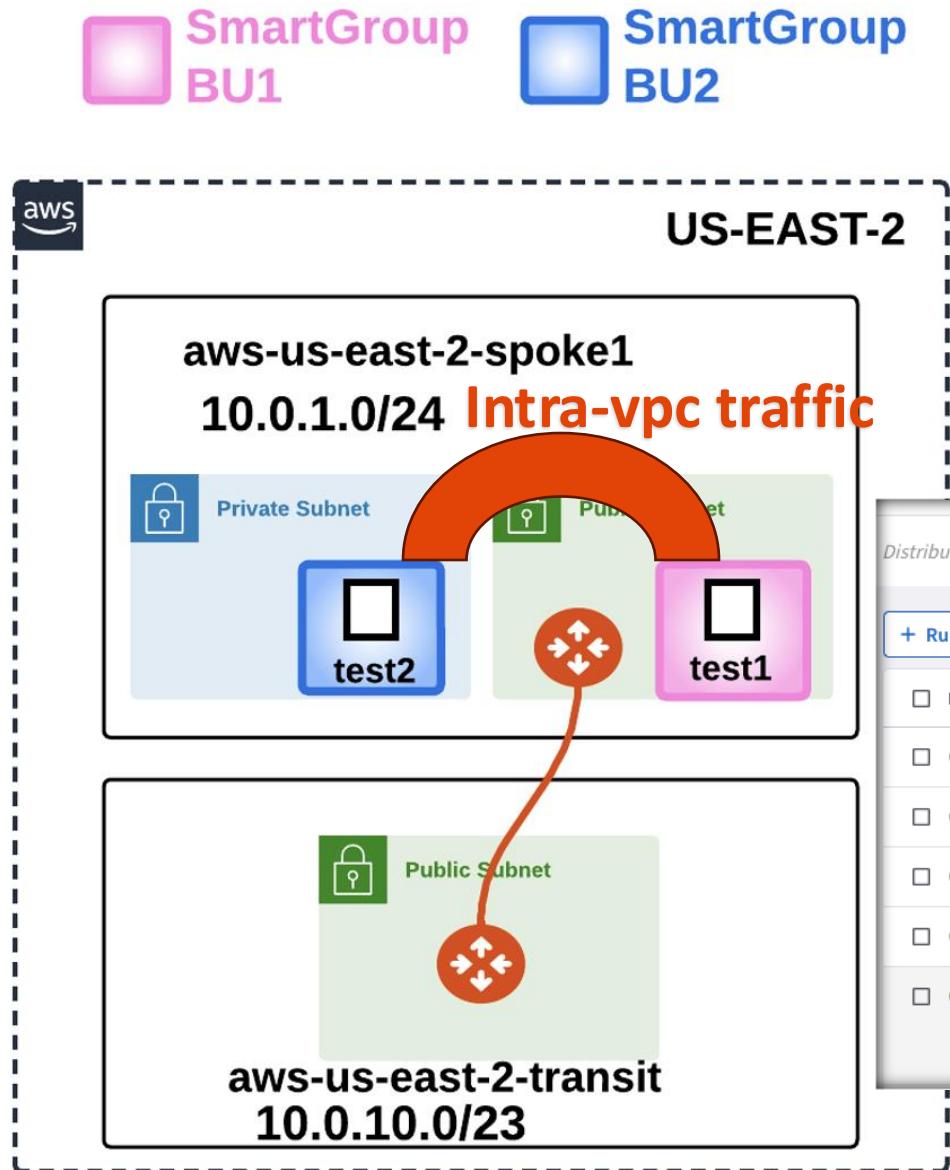
Intra-rule

Source SmartGroup = Destination SmartGroup



Security Group Orchestration

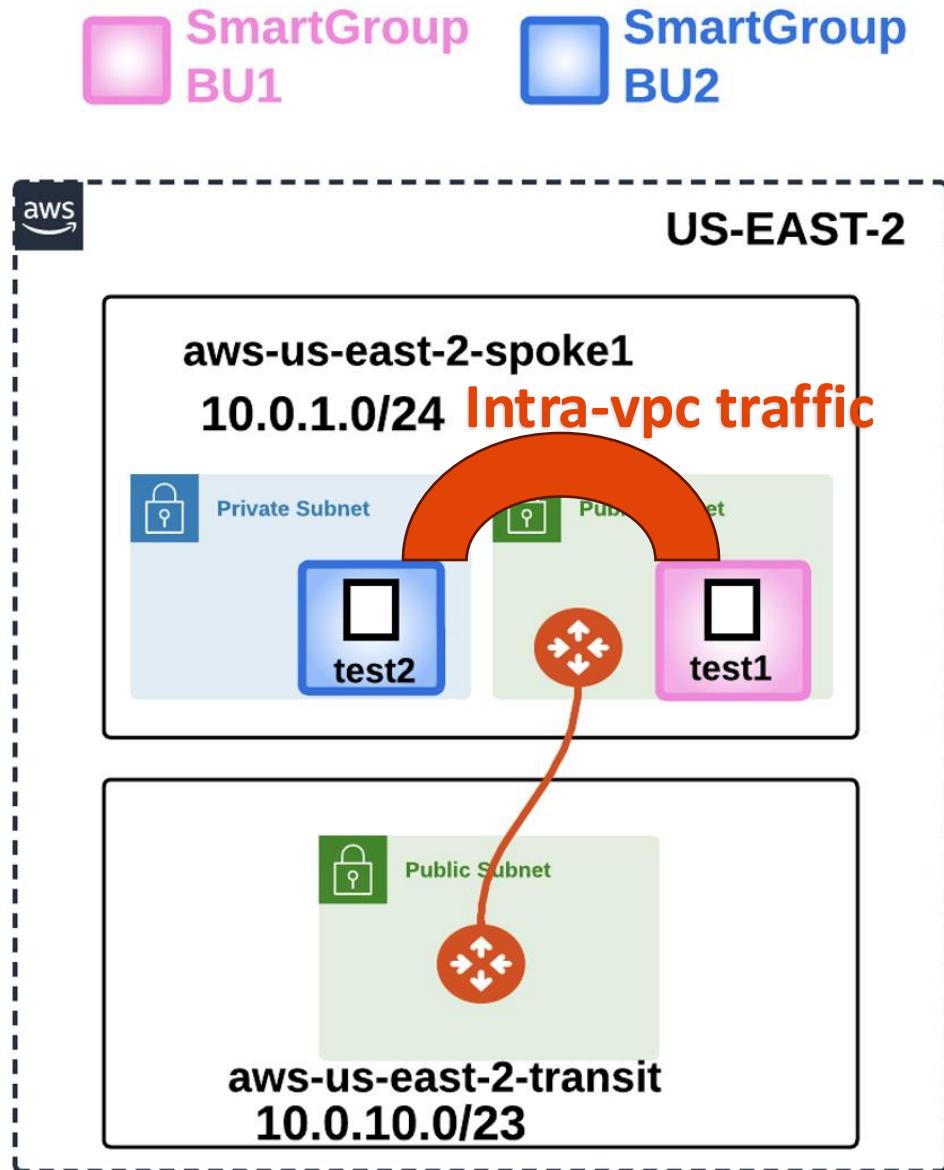
Security Group Orchestration: Intra-L4 Access Control (part.1)



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						
+ Rule		Actions	Rules	Monitor	Detected Intrusions	Settings
Priority	Name	Source	Destination	WebGroup	Protocol	Action
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 BU1-SSH	BU1	BU1		TCP	Permit
<input type="checkbox"/>	<input checked="" type="checkbox"/> 1 BU2-ICMP	BU2	BU2		ICMP	Permit
<input type="checkbox"/>	<input checked="" type="checkbox"/> 2 ExplicitDenyAll	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any	Deny
<input type="checkbox"/>	<input checked="" type="checkbox"/> 214748... Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any	Permit
<input type="checkbox"/>	<input checked="" type="checkbox"/> 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

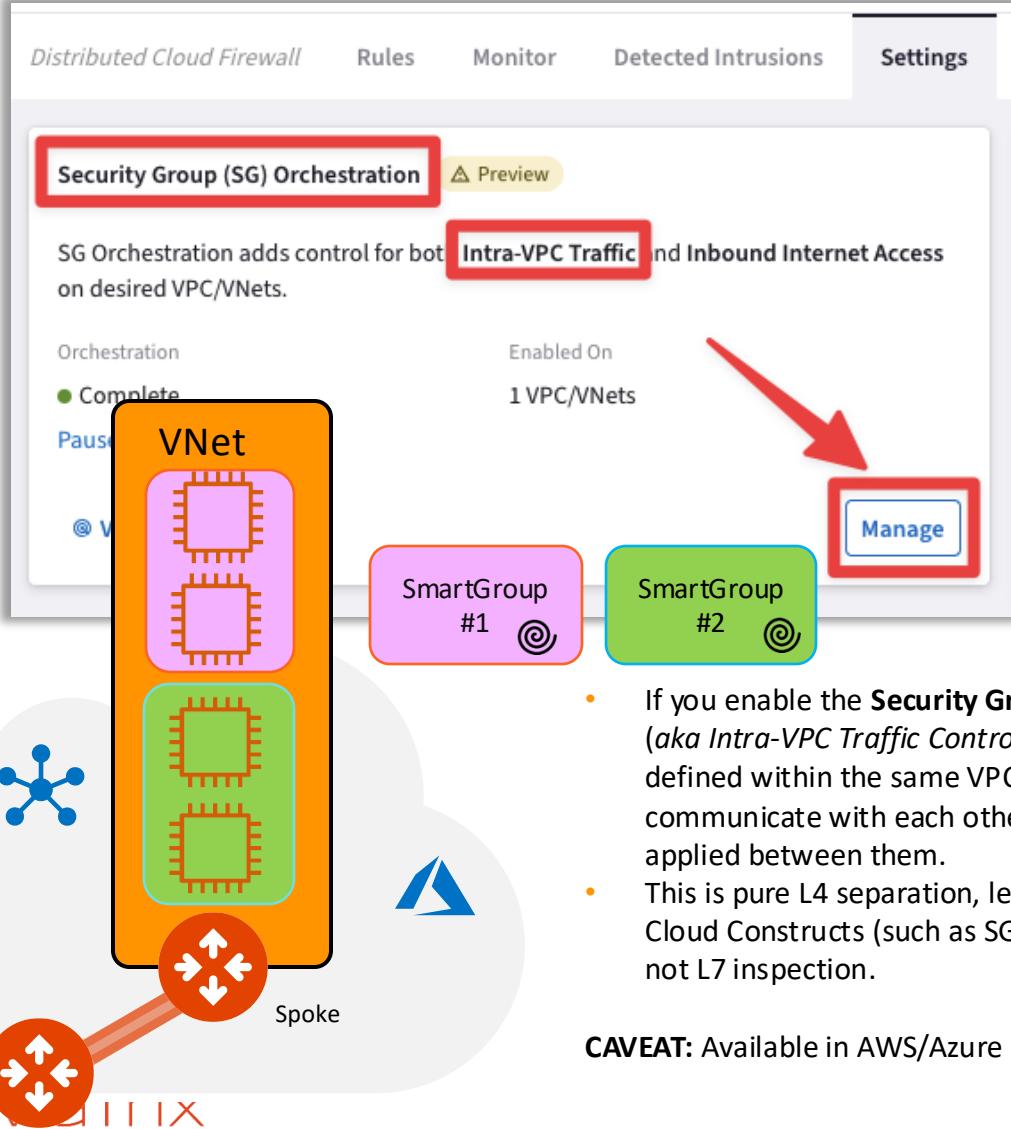
Aviatrix Spoke Gateway

- ❑ **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



Security Group (SG) Orchestration

SG Orchestration adds control for both **Intra-VPC Traffic** and **Inbound Internet Access** on desired VPC/VNets.

Orchestration
● Complete
Pause
@ VPC/VNet

Enabled On
1 VPC/VNets

VNet

SmartGroup #1

SmartGroup #2

Manage

Transit Spoke

CAVEAT: Available in AWS/Azure

- 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.

Manage VPC/VNets for Intra VPC/VNet Distributed Firewalling

When Enabled	When Disabled															
<p>Existing Security Groups on the CSP entities associated with policies are backed-up and detached. As a result:</p> <ul style="list-style-type: none"> All inbound traffic will be blocked (except for traffic from private or non-routable IPs). Inbound ALB traffic is allowed. Outbound VPC/VNet traffic will be allowed. All Intra VPC/VNet traffic will be blocked. 	<p>Security Group configuration on the CSP entities prior to enabling Intra VPC/VNet Distributed Firewalling will be restored when they are no longer associated with a policy.</p>															
<p>⚠ Once Intra VPC/VNet Distributed Firewalling is enabled, it is strongly recommended to not modify the CSP Security Groups on the CSP Portals to prevent misconfiguration.</p>																
<p>VPC/VNETs have to be enabled to support Intra VPC/VNet Distributed Firewalling.</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Cloud</th> <th>Region</th> <th>Account Name</th> <th>Intra VPC/VNet Dis...</th> </tr> </thead> <tbody> <tr> <td>AZURE-WESTEUROPE-</td> <td>Azure ARM</td> <td>westeuropa</td> <td>AZURE-AVIATRIX</td> <td><input checked="" type="checkbox"/> Enabled</td> </tr> <tr> <td>AZURE-WESTEUROPE-</td> <td>Azure ARM</td> <td>westeuropa</td> <td>AZURE-AVIATRIX</td> <td><input checked="" type="checkbox"/> Enabled</td> </tr> </tbody> </table> <p>Total 2 VPC/VNets</p> <p><input checked="" type="checkbox"/> I understand the network impact of the changes.</p> <p>Save</p>		Name	Cloud	Region	Account Name	Intra VPC/VNet Dis...	AZURE-WESTEUROPE-	Azure ARM	westeuropa	AZURE-AVIATRIX	<input checked="" type="checkbox"/> Enabled	AZURE-WESTEUROPE-	Azure ARM	westeuropa	AZURE-AVIATRIX	<input checked="" type="checkbox"/> Enabled
Name	Cloud	Region	Account Name	Intra VPC/VNet Dis...												
AZURE-WESTEUROPE-	Azure ARM	westeuropa	AZURE-AVIATRIX	<input checked="" type="checkbox"/> Enabled												
AZURE-WESTEUROPE-	Azure ARM	westeuropa	AZURE-AVIATRIX	<input checked="" type="checkbox"/> Enabled												



FireNet (Service Chaining)

Aviatrix Encrypted Transit Firewall Network



Scale out, multi-AZ FW deployments



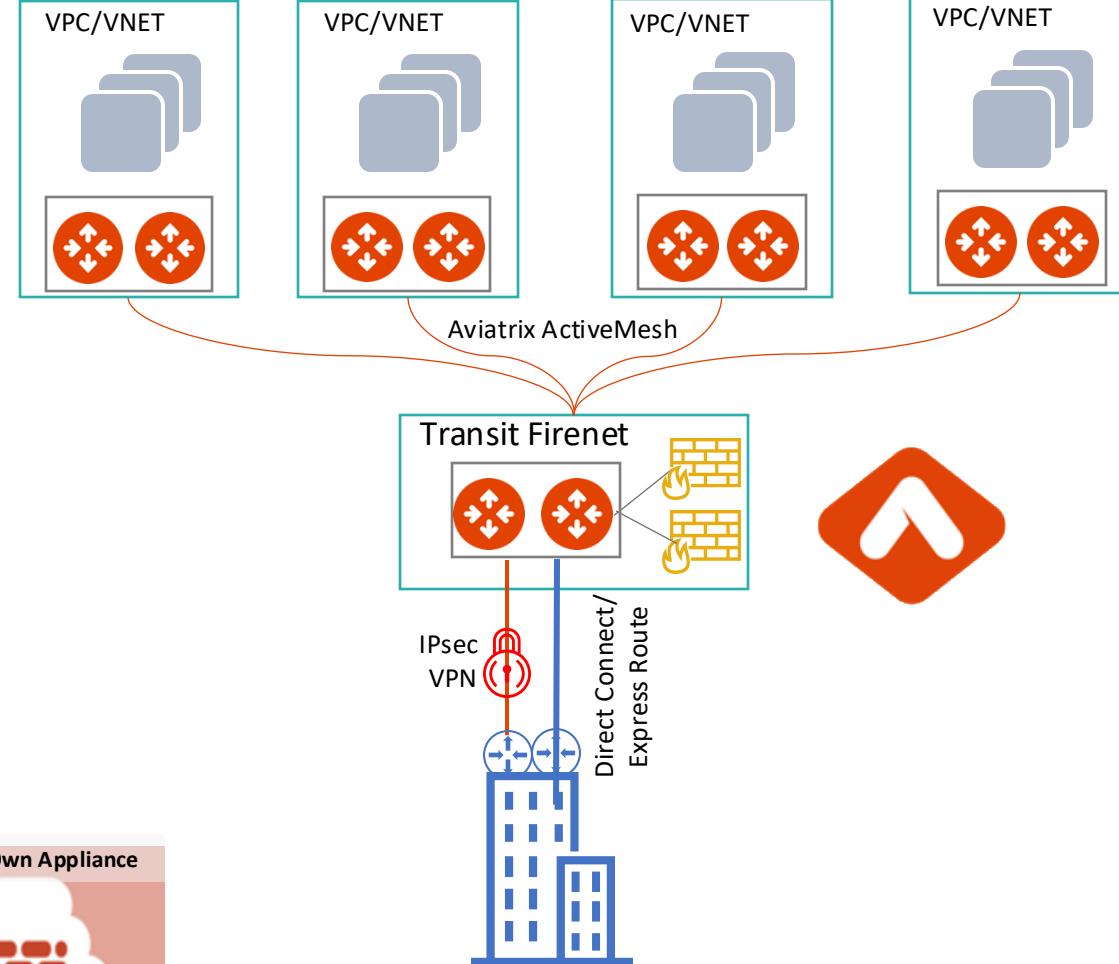
Automated route management
Segmentation and Connection Policies



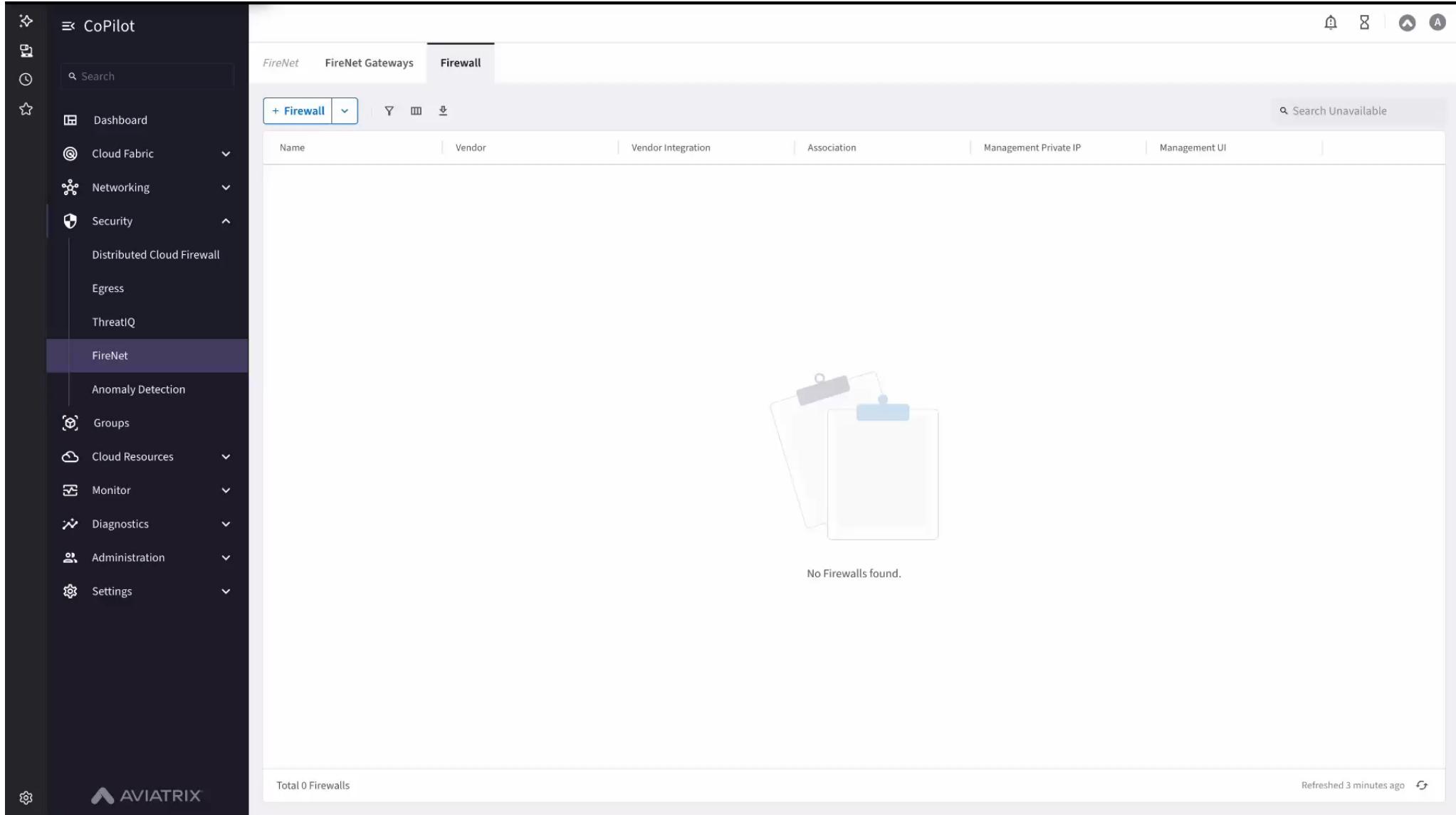
Deep visibility and operational capabilities



Repeatable architecture, across regions
and clouds



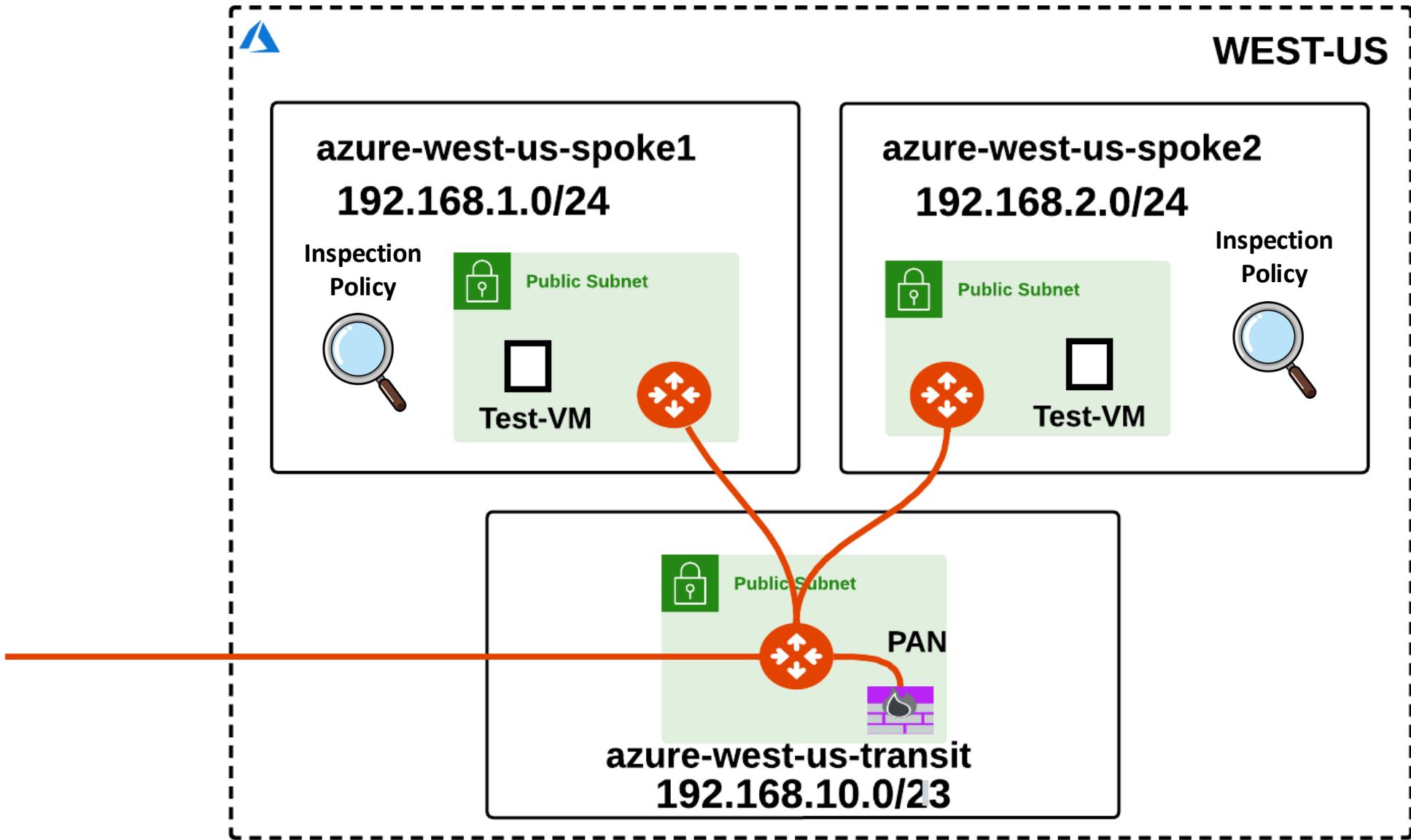
FireNet: Firewall Deployment, Bootstrapping & Vendor Integration



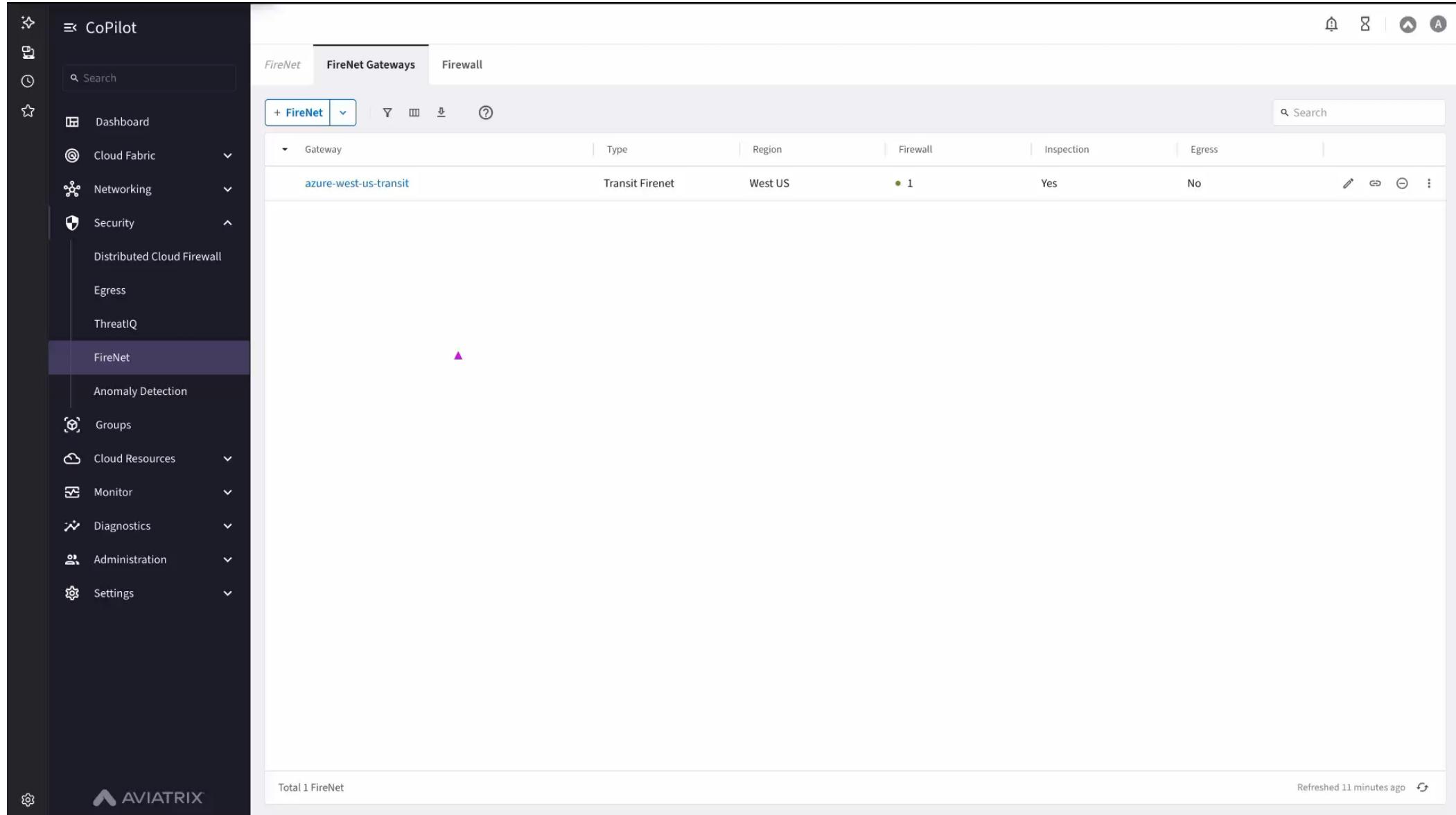
The screenshot shows the Aviatrix CoPilot interface with the following details:

- Left Sidebar (CoPilot):** Includes icons for Home, Search, Dashboard, Cloud Fabric, Networking, Security (with sub-options: Distributed Cloud Firewall, Egress, ThreatIQ), FireNet (selected), Anomaly Detection, Groups, Cloud Resources, Monitor, Diagnostics, Administration, and Settings.
- Top Navigation:** FireNet, FireNet Gateways, Firewall (selected).
- Toolbar:** + Firewall, search bar, refresh, and other UI controls.
- Table Headers:** Name, Vendor, Vendor Integration, Association, Management Private IP, Management UI.
- Content Area:** Displays a clipboard icon with a blue paperclip and the text "No Firewalls found."
- Bottom Status:** Total 0 Firewalls, Refreshed 3 minutes ago.

FireNet: Inspection Policy (part.1)



FireNet: Inspection Policy (part.2)

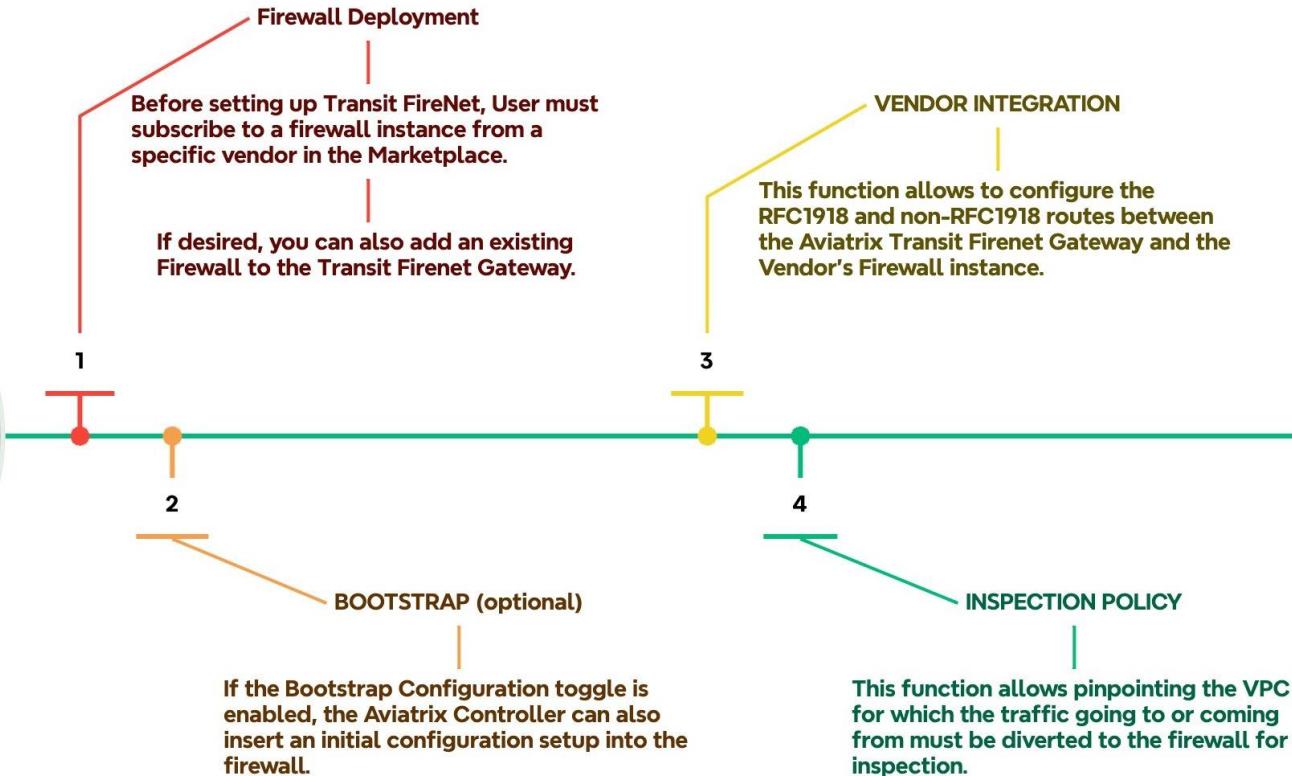
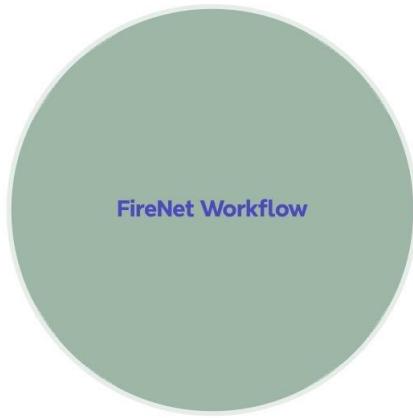


The screenshot shows the Aviatrix CoPilot interface with the 'FireNet' section selected. The main table displays a single gateway configuration:

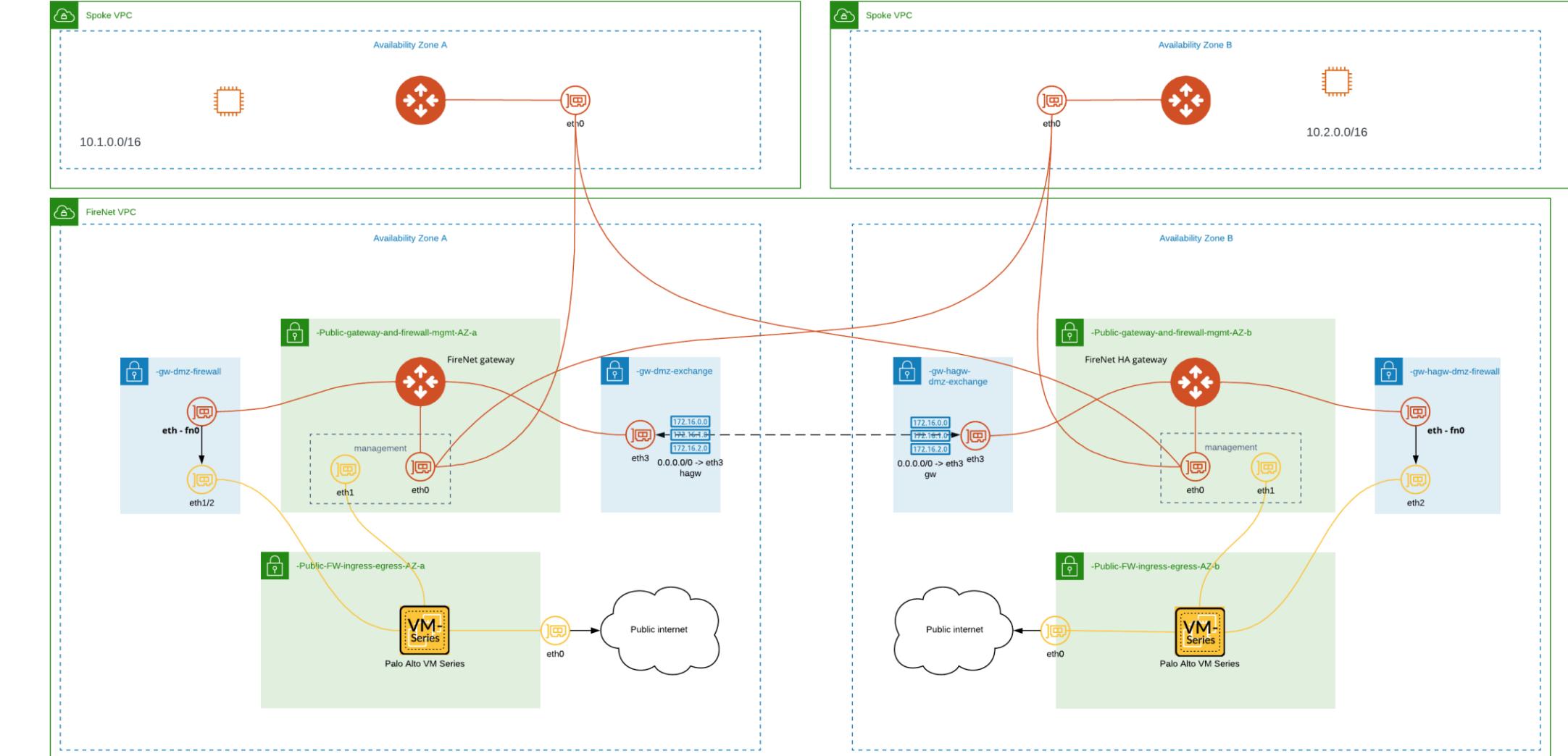
Gateway	Type	Region	Firewall	Inspection	Egress
azure-west-us-transit	Transit Firenet	West US	• 1	Yes	No

Total 1 FireNet

FireNet: Deployment Workflow



FireNet – Under the hood





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