Security

ACE Team

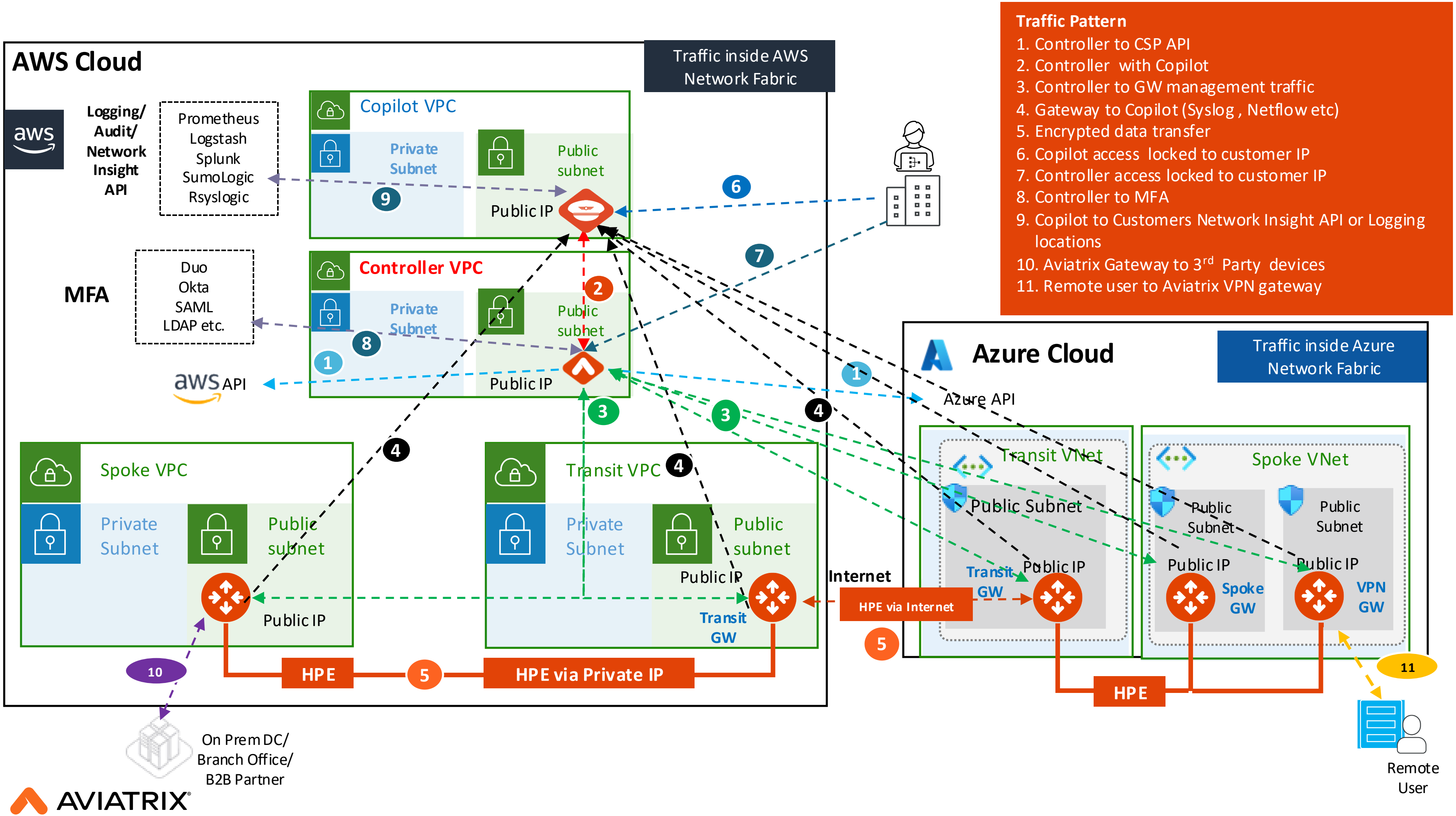
AVIATRIX

ACE

★★★★

PROFESSIONAL

Built-in Security of the Aviatrix Platform



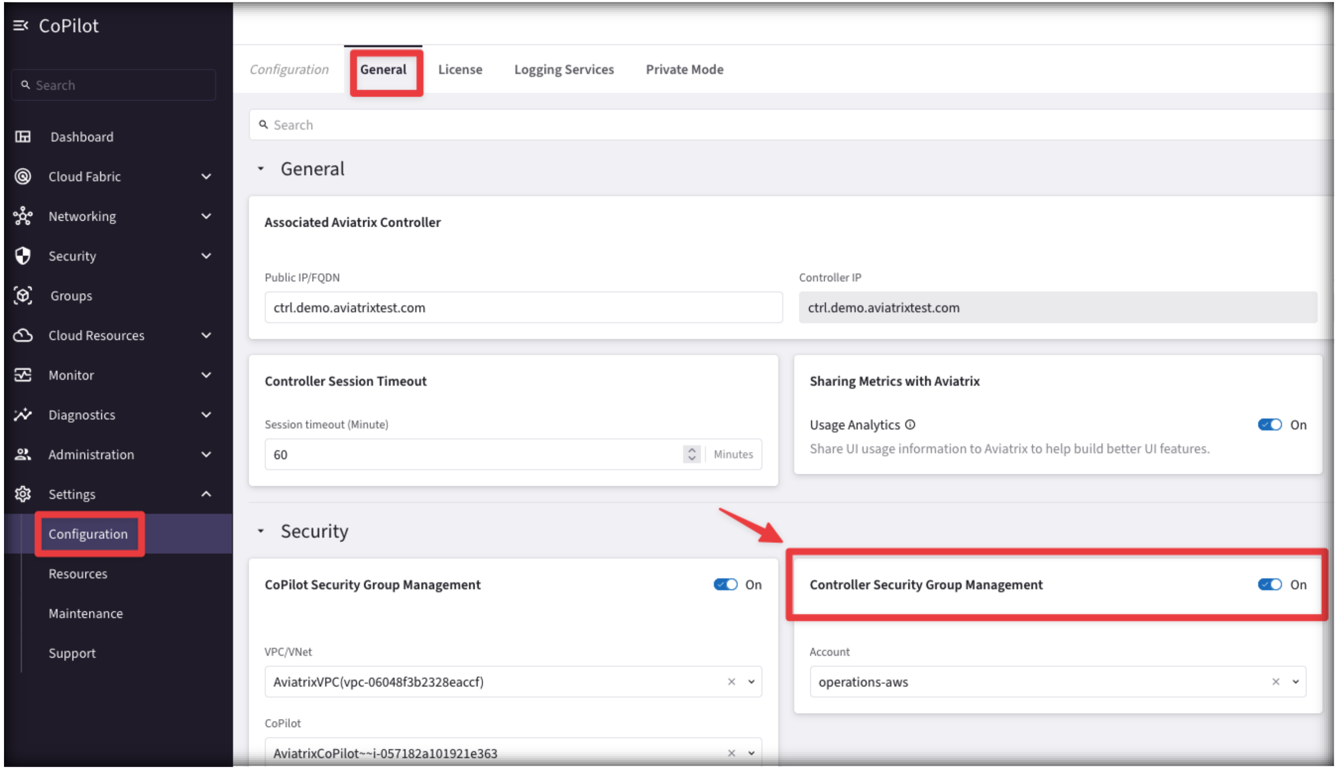
Traffic Pattern

1. Controller to CSP API
2. Controller with Copilot
3. Controller to GW management traffic
4. Gateway to Copilot (Syslog , Netflow etc)
5. Encrypted data transfer
6. Copilot access locked to customer IP
7. Controller access locked to customer IP
8. Controller to MFA
9. Copilot to Customers Network Insight API or Logging locations
10. Aviatrix Gateway to 3rd Party devices
11. Remote user to Aviatrix VPN gateway

Controller Security Group Management (part.1)

- You can use the **Controller Security Group Management** feature to automatically manage the Controller instance’s inbound rules from gateways.
- When enabled (**default**), each time you deploy an Aviatrix gateway, a rule will be automatically added to the Controller instance’s inbound rule to allow the gateway to reach the Controller. Only TCP port 443 needs to be opened for inbound traffic to the Controller. Gateways launched from the Controller use its public IP address to communicate back to the Controller.
- After the Controller Security Group Management feature is enabled, you can edit the security rules that are outside gateways public IP addresses to limit the source address range. When specifying the custom IP addresses to allow access, you must include your own public IP address.

Controller Security Group Management (part.2)



General

Associated Aviatrix Controller

Public IP/FQDN: ctrl.demo.aviatrixtest.com

Controller IP: ctrl.demo.aviatrixtest.com

Controller Session Timeout

Session timeout (Minute): 60 Minutes

Sharing Metrics with Aviatrix

Usage Analytics: On

Share UI usage information to Aviatrix to help build better UI features.

Security

CoPilot Security Group Management: On

VPC/VNet: AviatrixVPC(vpc-06048f3b2328eaccf)

CoPilot: AviatrixCoPilot~~i-057182a101921e363

Controller Security Group Management: On

Account: operations-aws

- You can enable Controller Security Group Management in CoPilot from **Settings > Configuration > General**

CoPilot Security Group Management (part.1)

- When **CoPilot Security Group Management** is enabled (**default**), the Controller creates a security group for the specified CoPilot virtual machine to manage its inbound security-group rules.

The feature adds gateway IP rules to customer-attached CoPilot security groups as well as CoPilot-created security groups. CoPilot comes with a base security group when it is first launched.

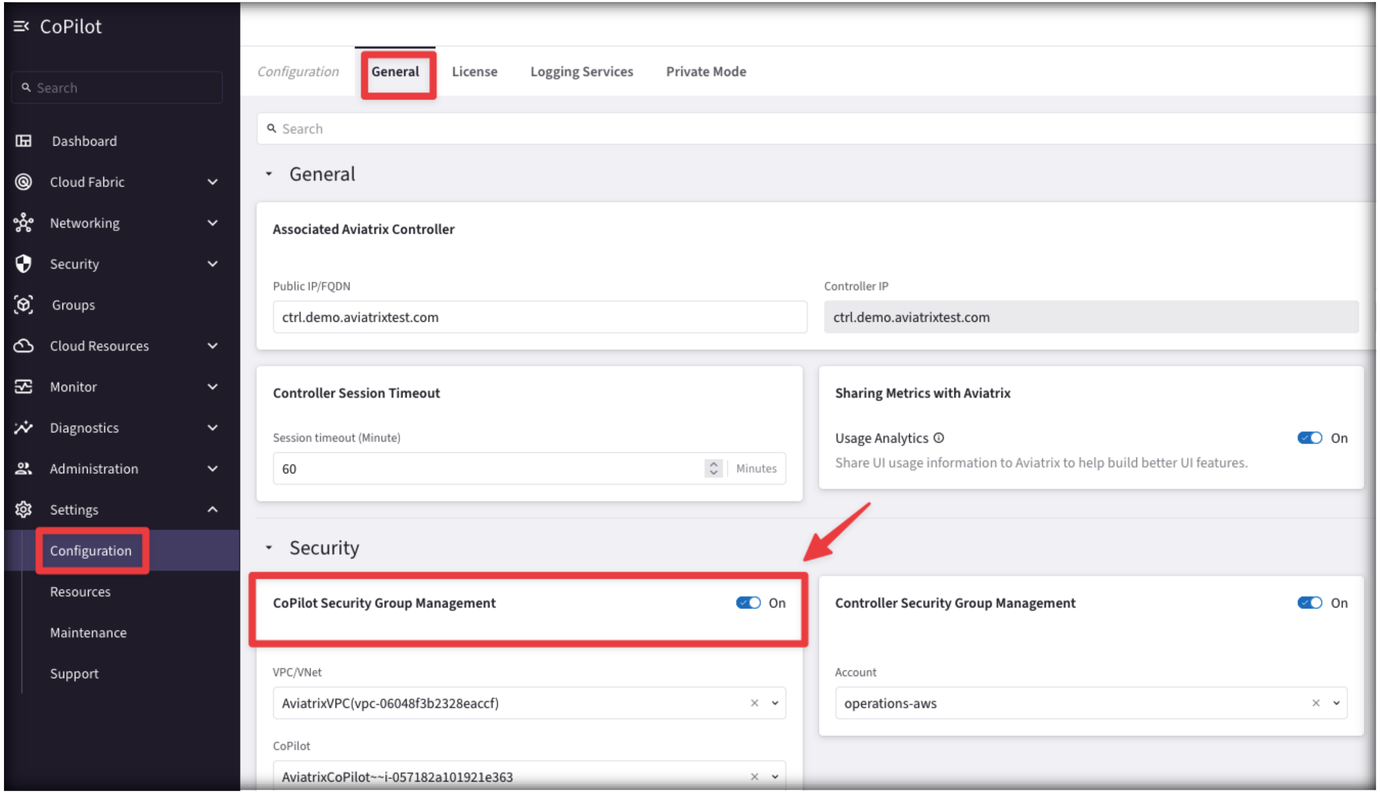
The Controller adds rules to the security group for each gateway IP for the following:

- ***UDP port 5000*** (default) — Enable Syslog for CoPilot Egress FQDN (Legacy) & Audit Data (from each gateway). Gateways send remote syslog data to CoPilot.
- **TCP port 5000** (default, if using Private Mode) — Enable Syslog for CoPilot Egress FQDN & Audit Data (from each gateway). Gateways send remote syslog data to CoPilot.
- **UDP port 31283** (default, port is configurable) — Enable NetFlow for CoPilot FlowIQ Data (from each gateway). Gateways send NetFlow to CoPilot.

The Controller adds the above rules for:

- New gateways launched from the Controller after the feature is enabled.
- Existing gateways launched from the Controller before the feature was enabled.

CoPilot Security Group Management (part.2)



General

Associated Aviatrix Controller

Public IP/FQDN
ctrl.demo.aviatrixtest.com

Controller IP
ctrl.demo.aviatrixtest.com

Controller Session Timeout

Session timeout (Minute)
60 Minutes

Sharing Metrics with Aviatrix

Usage Analytics ⓘ On
Share UI usage information to Aviatrix to help build better UI features.

Security

CoPilot Security Group Management On

VPC/VNet
AviatrixVPC(vpc-06048f3b2328eaccf)

CoPilot
AviatrixCoPilot~~i-057182a101921e363

Controller Security Group Management On

Account
operations-aws

- You can enable CoPilot Security Group Management in CoPilot from **Settings > Configuration > General**

Securing the Platform with Cloud Native Load Balancers

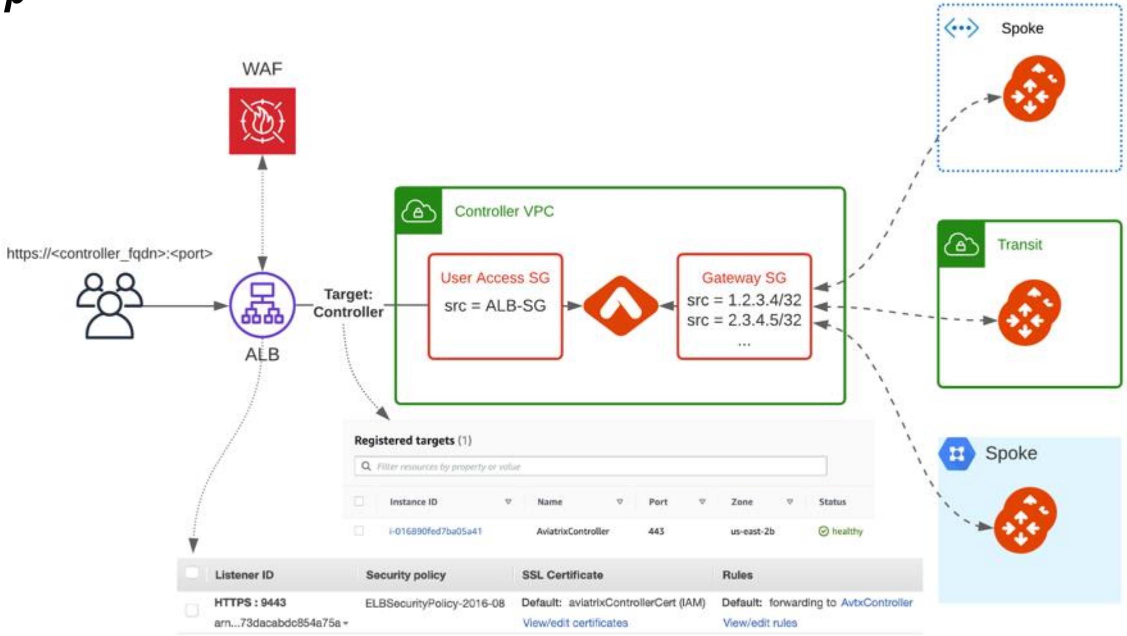
Problem Statement

- Enterprise concerns around putting Aviatrix Controller with a public IP in a Public subnet
- Enterprises need tighter security and availability
- What are the options?

1. Limit access using cloud native L4 stateful firewalls such as:
    - AWS Security Groups
    - Azure Network Security Groups
    - GCP Firewall Rules
2. Deploy a third-party Firewall in front of controller
3. Deploy an Application (L7) Load Balancer in front of Aviatrix Controller

AWS

- Verify that the ***Controller Security Group Management*** feature is NOT disabled. This feature allows access to the Controller EIP from Aviatrix Gateways, solely
- Create a new internet facing ALB
- Modify main Controller Security Group to only allow access from the ALB Security Group
- Enable WAF on the ALB with AWS Managed Rules
- Adjust ALB idle timeout, modify rulesets
- Modify ALB Security Group to only allow access from the admin user IP



Registered targets (1)

Filter resources by property or value

□	Instance ID	Name	Port	Zone	Status
□	i-016890fed7ba05a41	AviatrixController	443	us-east-2b	✓ healthy

□	Listener ID	Security policy	SSL Certificate	Rules
□	HTTPS : 9443 arn...73dacabdc854a75a ▾	ELBSecurityPolicy-2016-08	Default: aviatrixControllerCert (IAM) View/edit certificates	Default: forwarding to AvtxController View/edit rules

Aviatrix Cloud Firewall

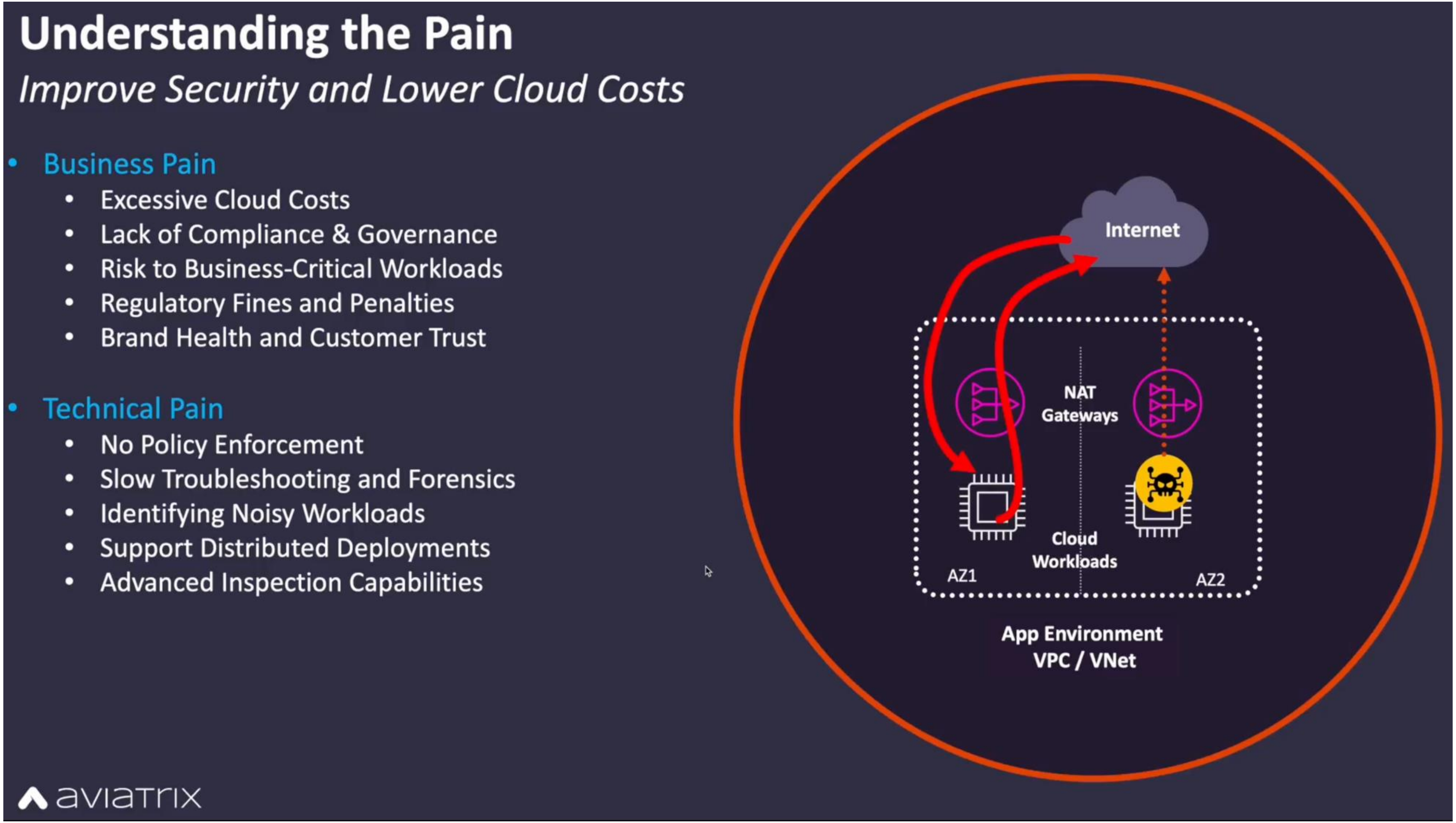
Problem Statement

Private workloads need internet access

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

SaaS

GitHub



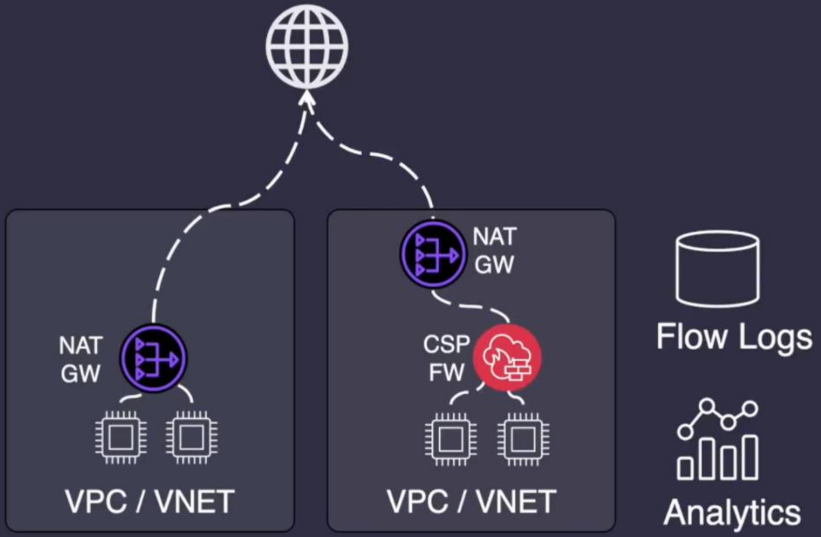
Understanding the Pain

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

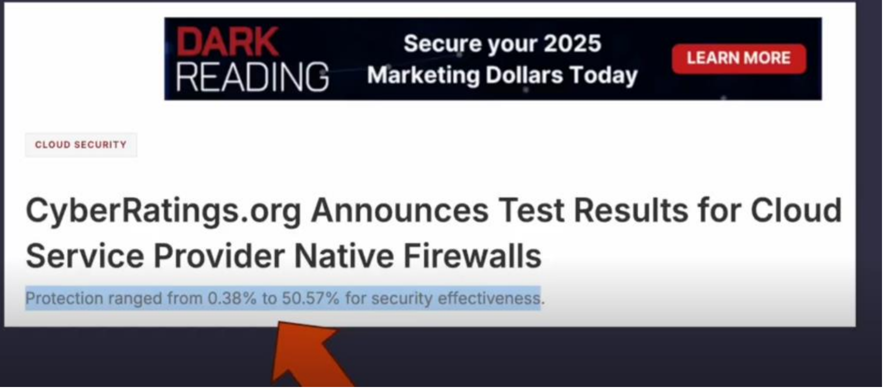
aviatrix

Two Common Paths



1. Distributed Cloud Provider Services

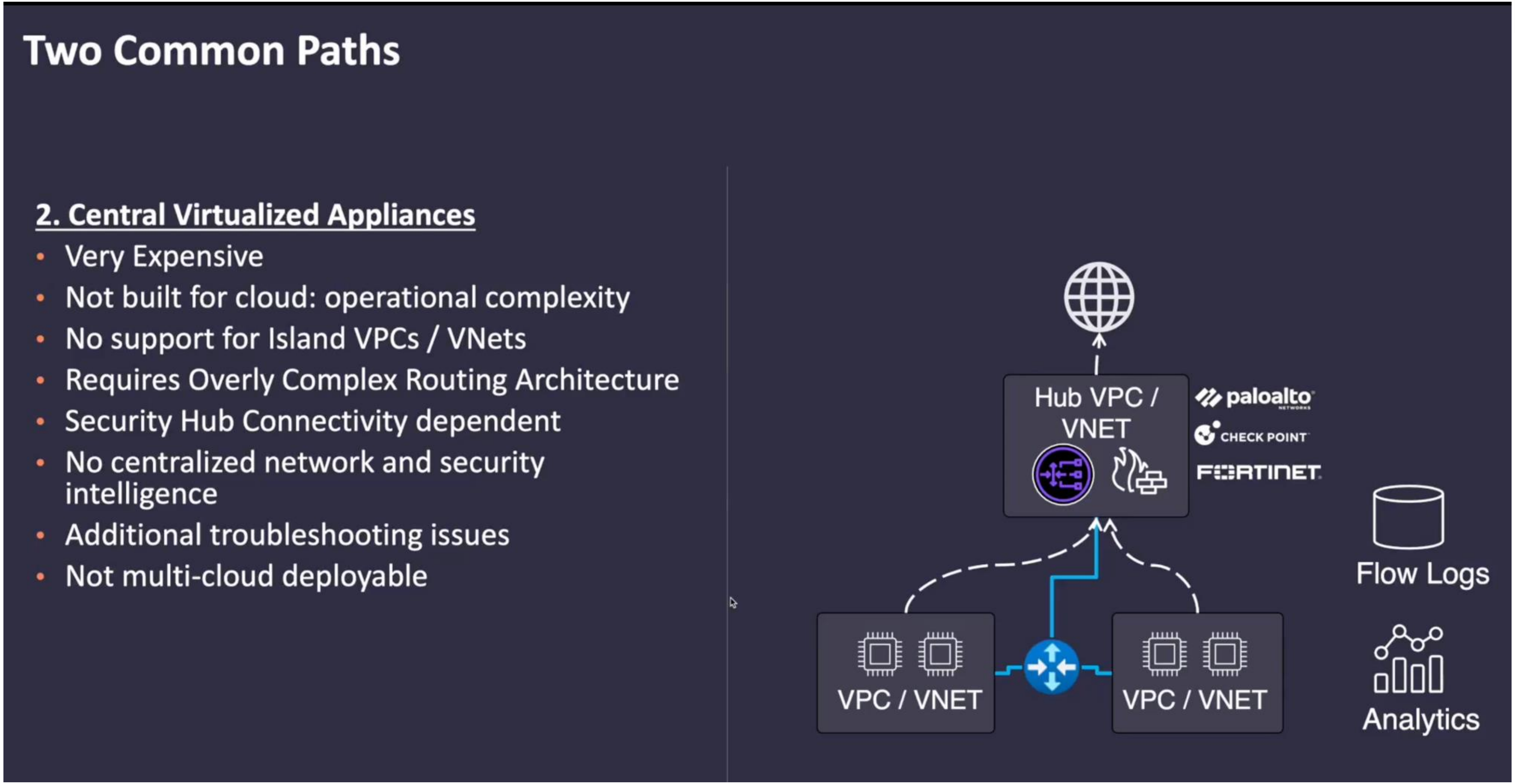
- Expensive: High data-processing costs
- Zero / Weak Security
- Poor Visibility
  - Some visibility with a lot of tools
- Log storage and analytics costs
- No centralized intelligence
- Not multi-cloud capable



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

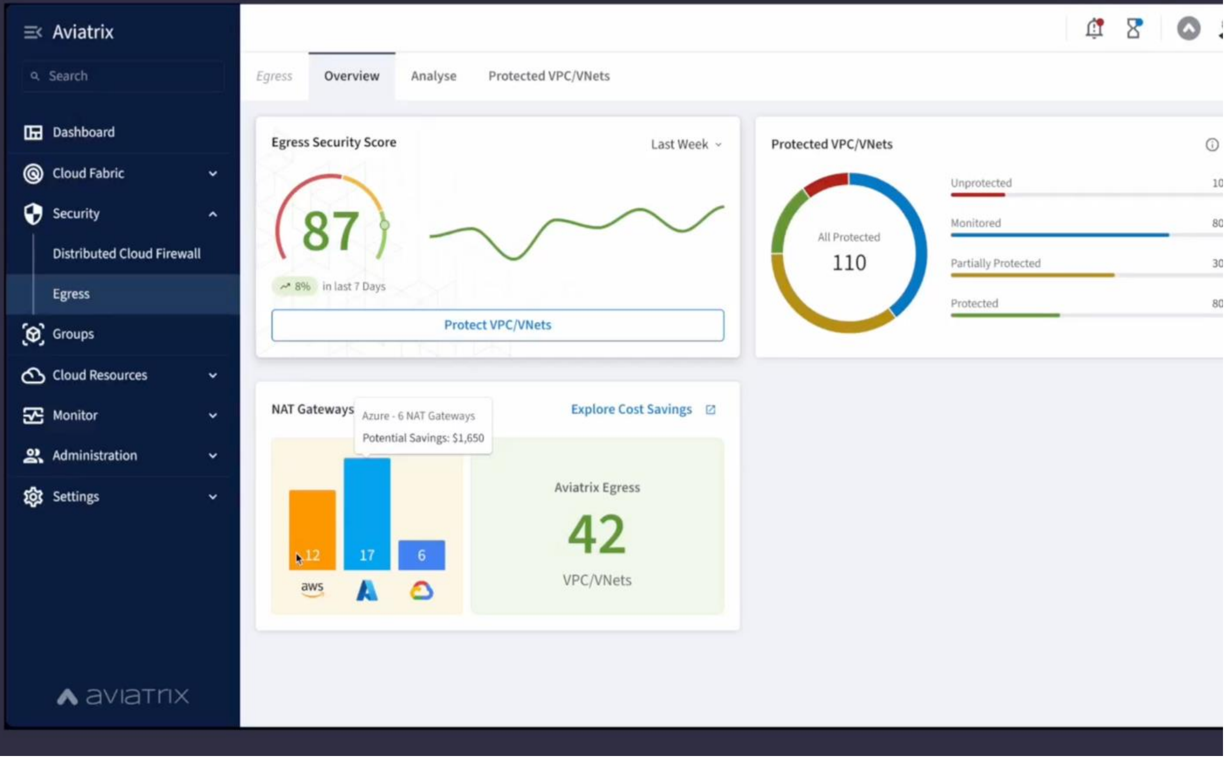
Aviatrix Cloud Firewall

What it is:

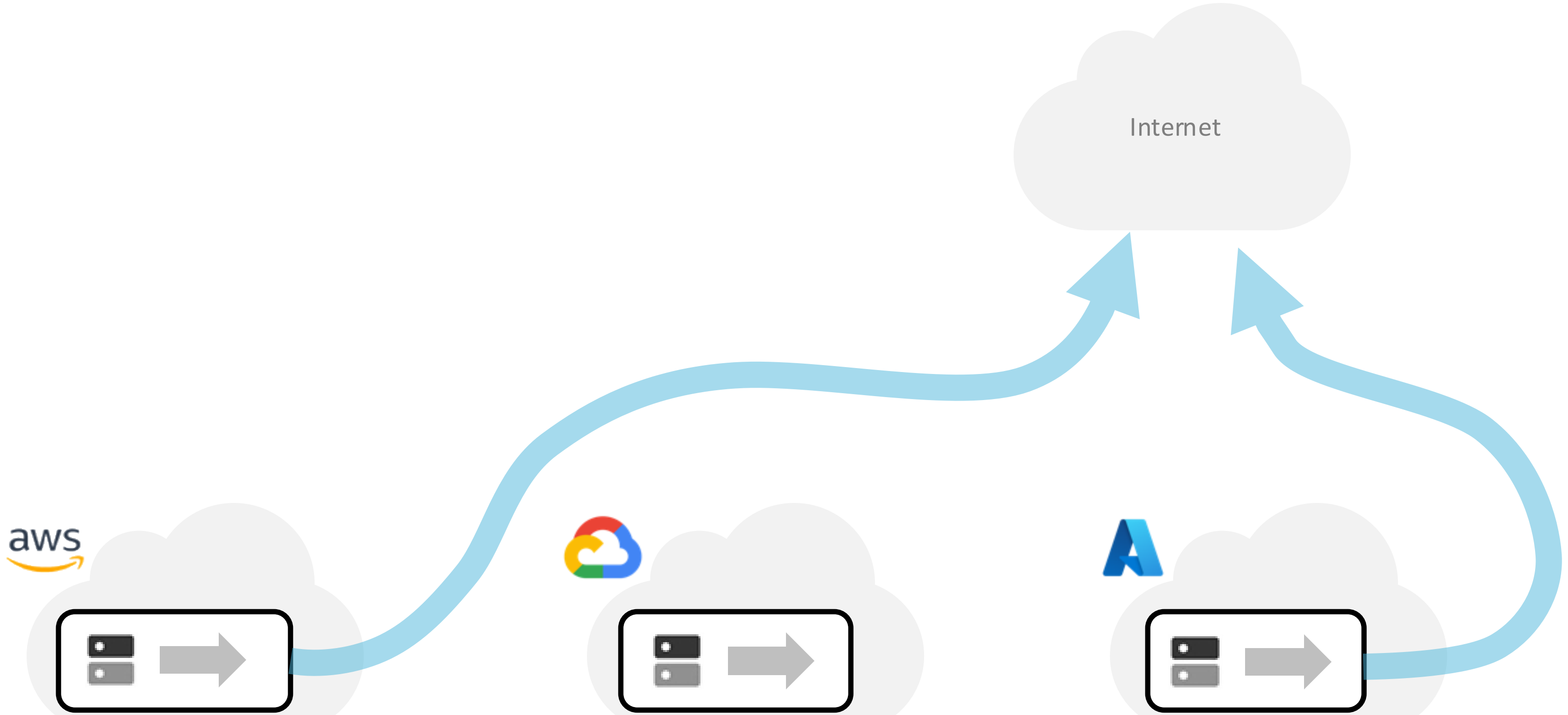
- Central Policy Management & Observability
- Distributed Enforcement: at the workload

What you get:

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



Aviatrix Cloud Firewall

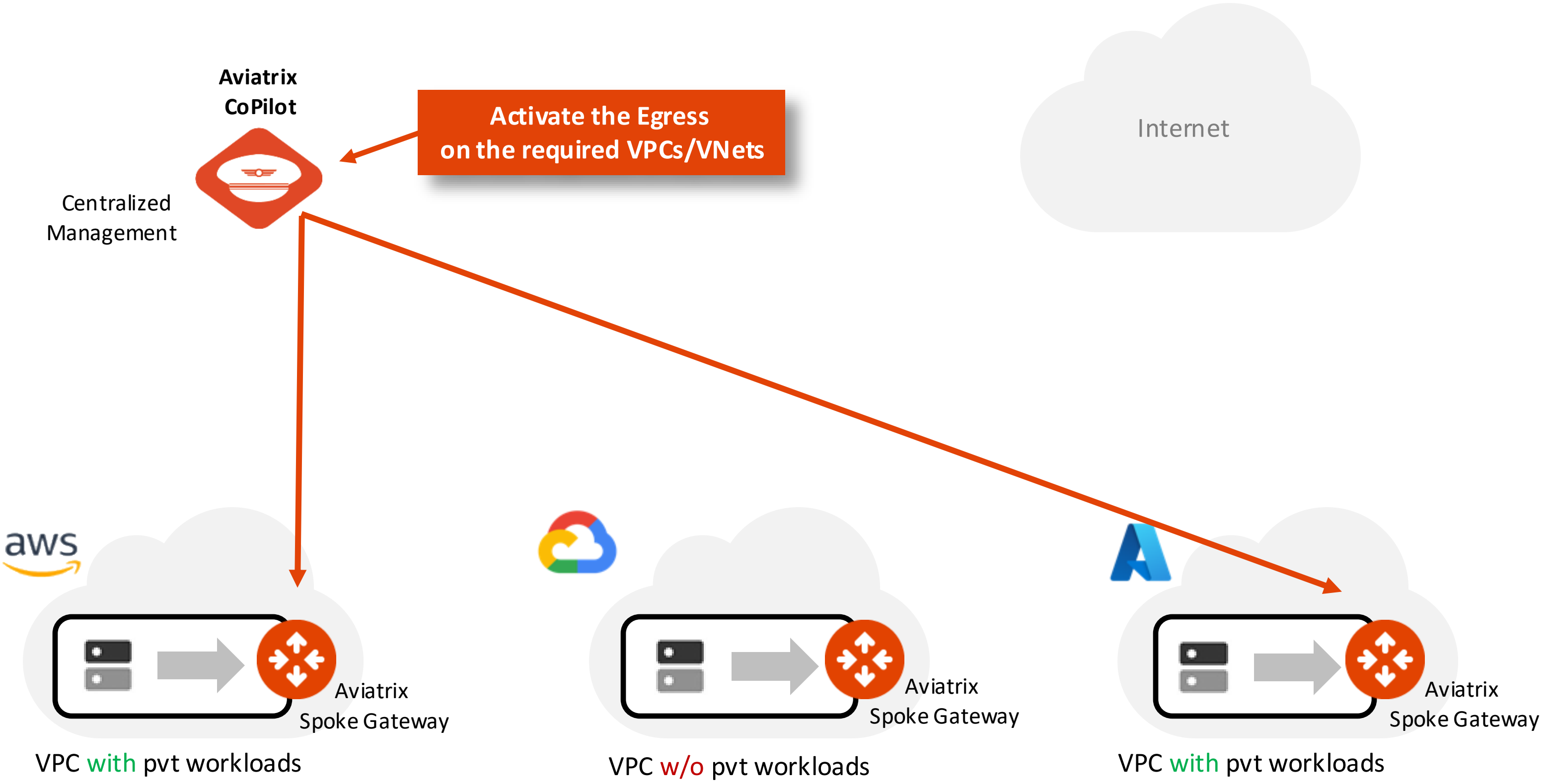


VPC with pvt workloads

VPC w/o pvt workloads

VPC with pvt workloads

Aviatrix Cloud Firewall

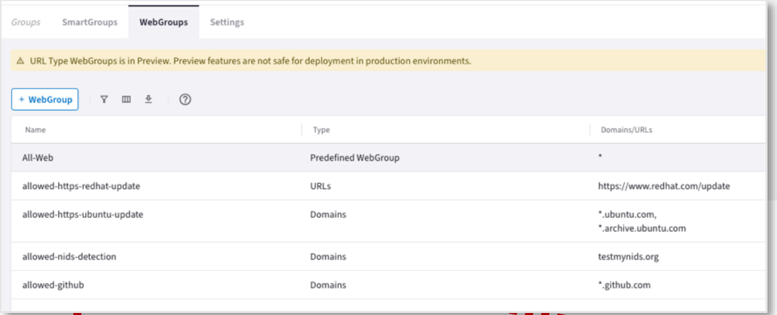


Aviatrix Cloud Firewall

Aviatrix CoPilot

Centralized Management

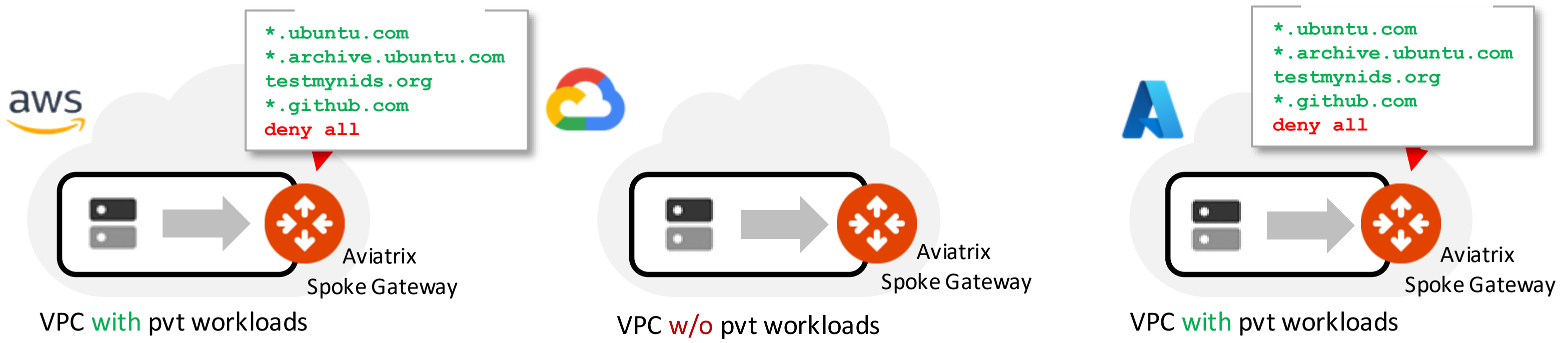
Egress Filtering Policies with **WebGroups** inserted into **DCF rules**



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

Name	Type	Domains/URLs
All-Web	Predefined WebGroup	*
allowed-https-redhat-update	URLs	https://www.redhat.com/update
allowed-https-ubuntu-update	Domains	*.ubuntu.com, *.archive.ubuntu.com
allowed-nids-detection	Domains	testmynids.org
allowed-github	Domains	*.github.com

Internet



Domain/URL Filter

```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

Domain/URL Filter

```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

VPC with pvt workloads

VPC w/o pvt workloads

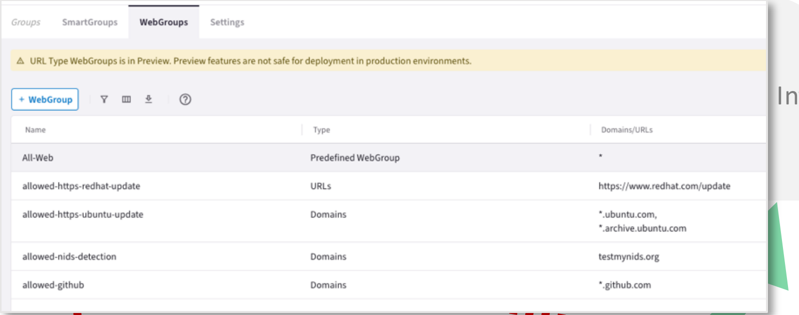
VPC with pvt workloads

Aviatrix Cloud Firewall

Aviatrix CoPilot

Centralized Management

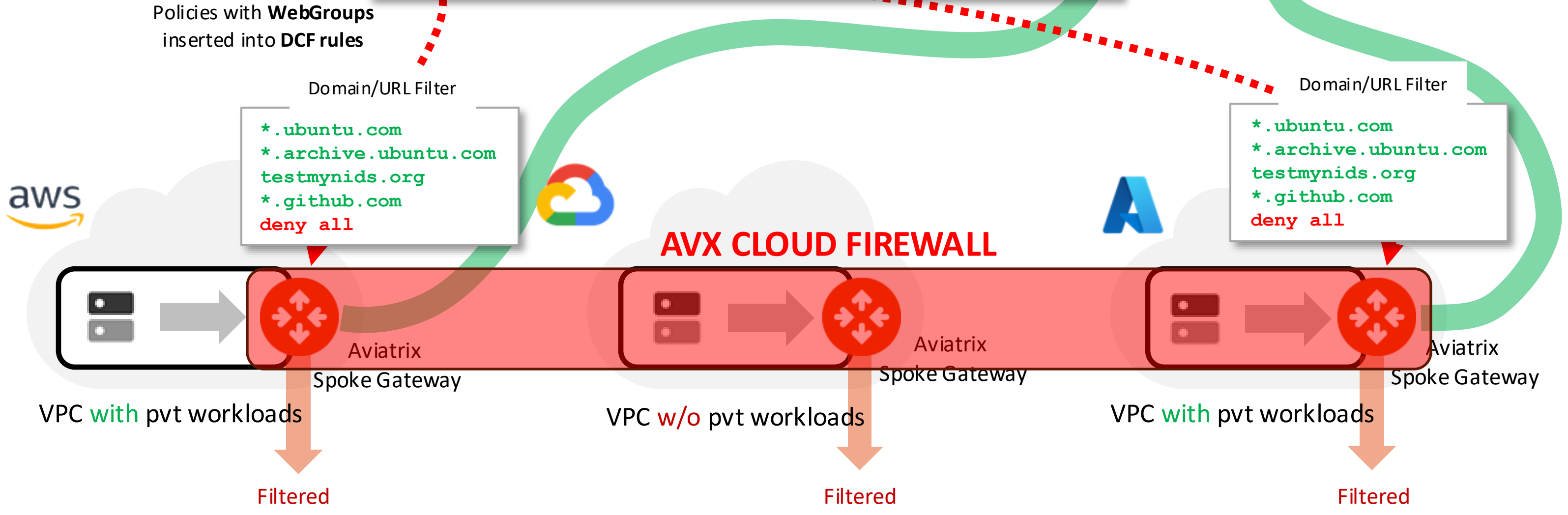
Egress Filtering Policies with **WebGroups** inserted into **DCF rules**



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

Name	Type	Domains/URLs
All-Web	Predefined WebGroup	*
allowed-https-redhat-update	URLs	https://www.redhat.com/update
allowed-https-ubuntu-update	Domains	*.ubuntu.com, *.archive.ubuntu.com
allowed-nids-detection	Domains	testmynids.org
allowed-github	Domains	*.github.com

Internet



Domain/URL Filter

```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

Domain/URL Filter

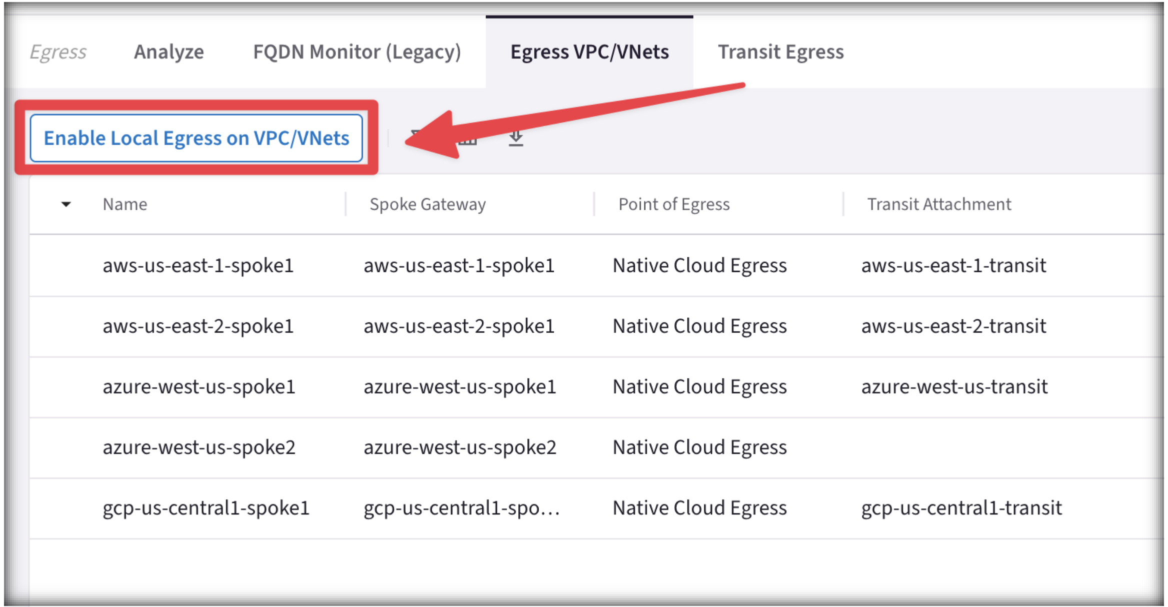
```
*.ubuntu.com
*.archive.ubuntu.com
testmynids.org
*.github.com
deny all
```

AVX CLOUD FIREWALL

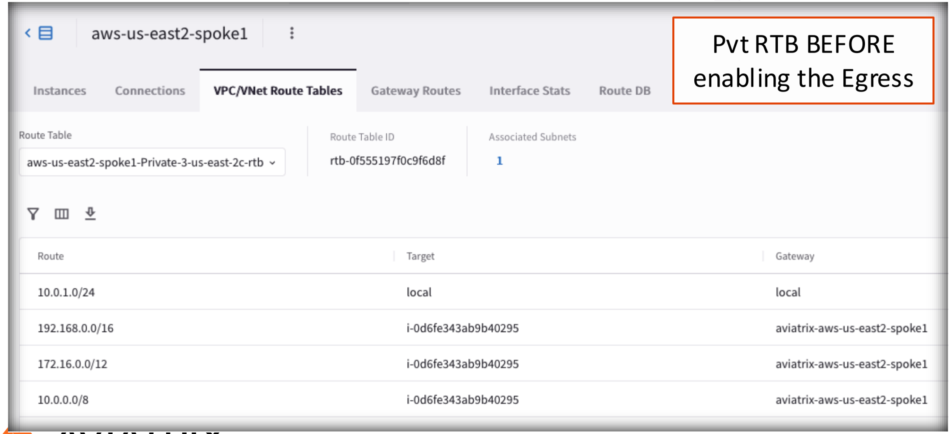
- The Aviatrix Cloud Firewall can be extended also to the Edge

Enabling Egress

- Adding Egress Control on VPC/VNet changes the default route on VPC/VNet to point to the Spoke Gateway and enables **SNAT**.
- In addition to the **Local route**, the **three RFC1918 routes**, also a **default route** will be injected.
- 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.



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



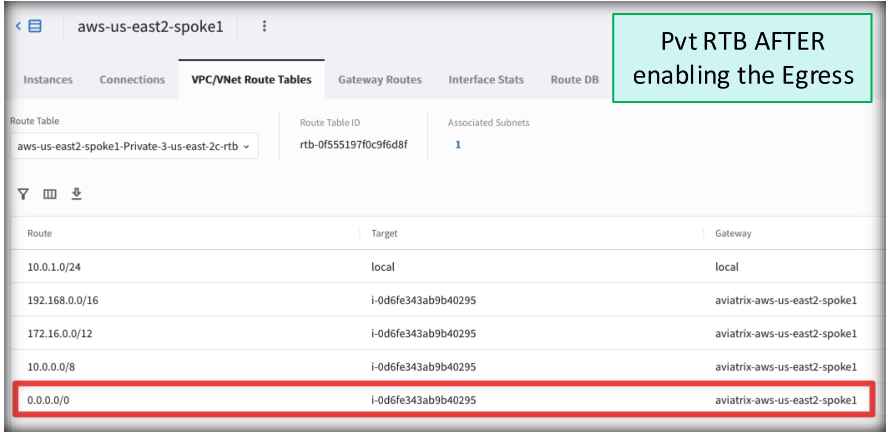
Pvt RTB BEFORE enabling the Egress

Route Table: aws-us-east2-spoke1-Private-3-us-east-2c-rtb

Route Table ID: rtb-0f555197f0c9f6d8f

Associated Subnets: 1

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 Table: aws-us-east2-spoke1-Private-3-us-east-2c-rtb

Route Table ID: rtb-0f555197f0c9f6d8f

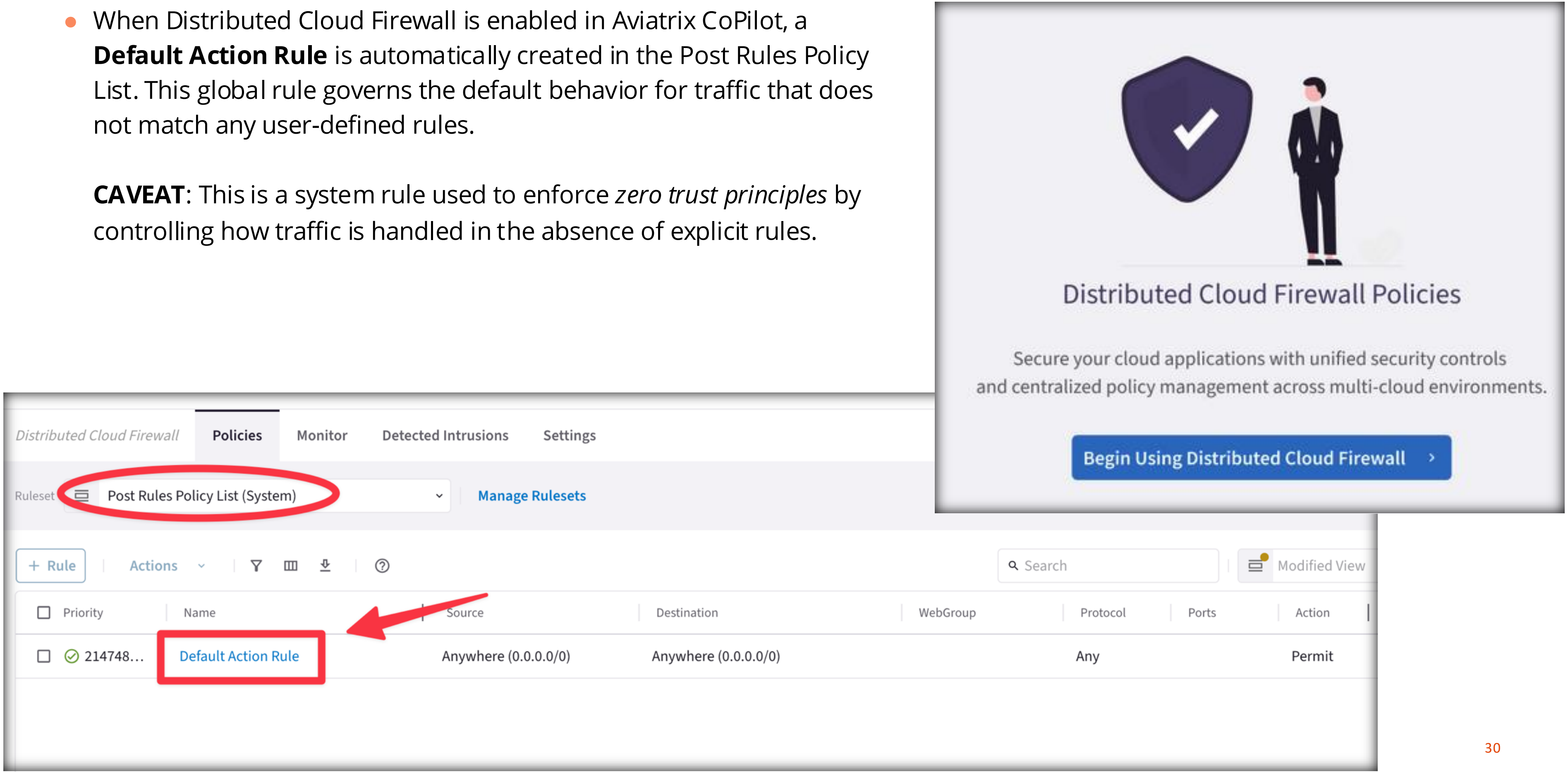
Associated Subnets: 1

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

Enabling Distributed Cloud Firewall (DCF)

- When Distributed Cloud Firewall is enabled in Aviatrix CoPilot, a **Default Action Rule** is automatically created in the Post Rules Policy List. This global rule governs the default behavior for traffic that does not match any user-defined rules.

  CAVEAT: This is a system rule used to enforce *zero trust principles* by controlling how traffic is handled in the absence of explicit rules.



Distributed Cloud Firewall Policies

Secure your cloud applications with unified security controls and centralized policy management across multi-cloud environments.

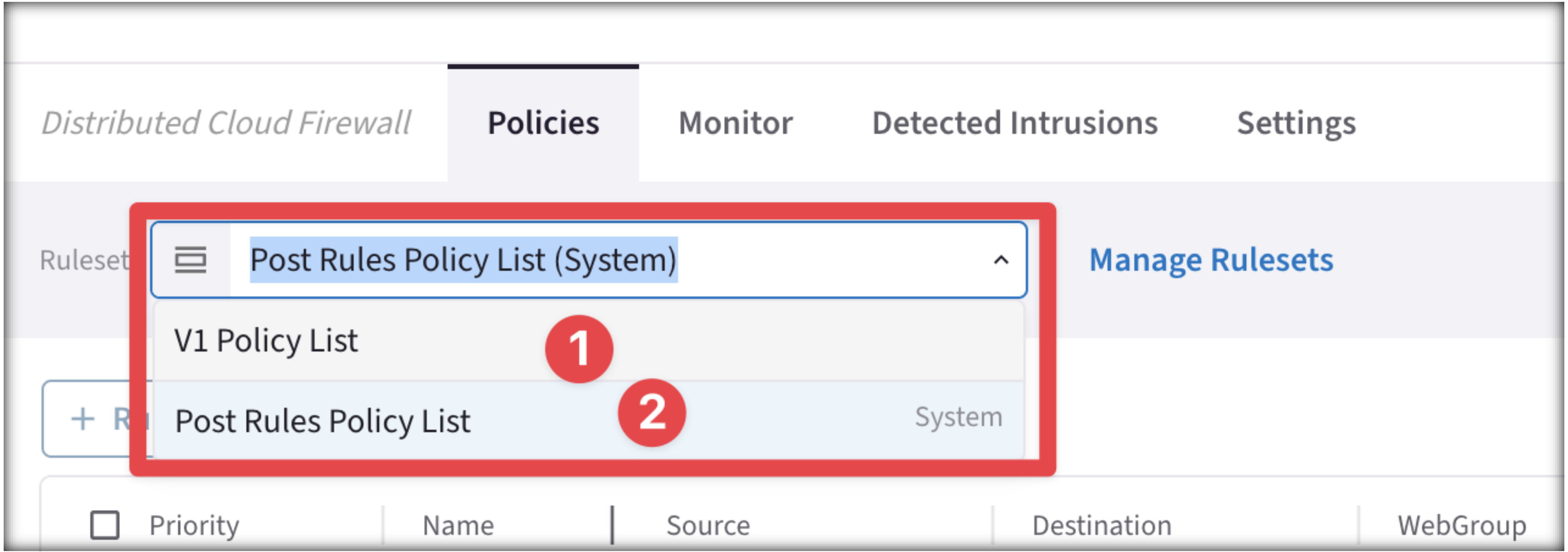
Ruleset: Post Rules Policy List (System)

□	Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
□	✓ 214748…	Default Action Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit

Managing Distributed Cloud Firewall Rulesets

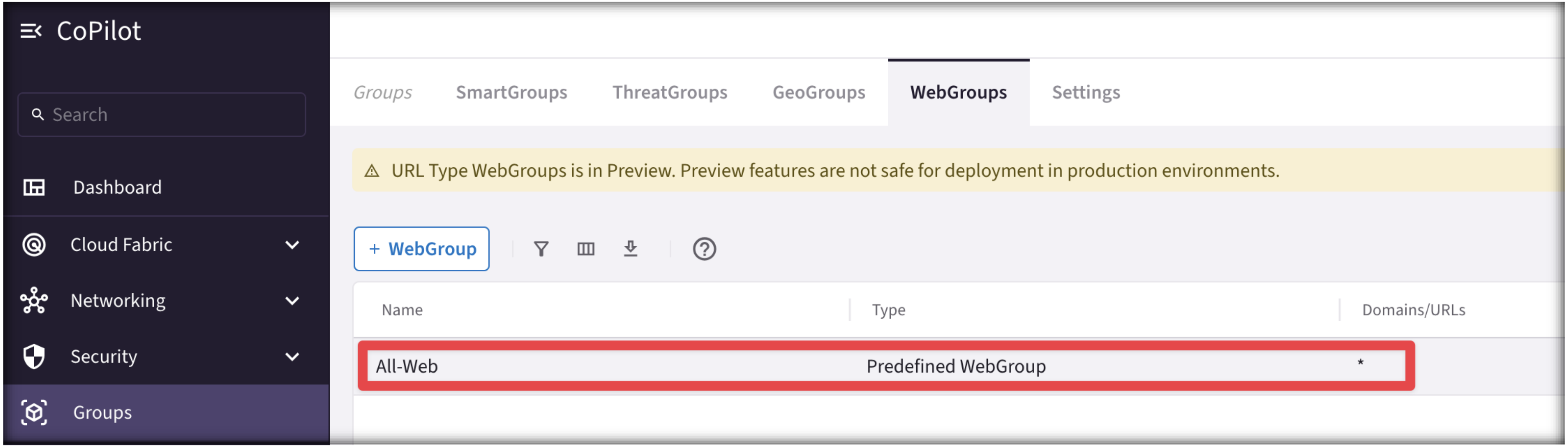
- Two rulesets are initially available when you start using the Rulesets feature:
  - **Post Rules Policy List**: System-based ruleset that contains the DefaultDenyAll Rule. You cannot delete this ruleset or the DefaultDenyAll Rule. This ruleset is executed last in the ruleset list.
  - **V1 Policy List**: Ruleset added by Aviatrix. You can add rules to this ruleset, but you cannot delete it.

CAVEAT: After enabling the Distributed Cloud firewall, configure the Ruleset to the **V1 Policy List** and begin populating it with your custom rules.



Predefined WebGroup: All-Web

- When you navigate to **CoPilot > Groups**, a predefined WebGroup, *All-Web*, has already been created for you.
- This is an *"allow-all"* WebGroup that you must select in a Distributed Cloud Firewall rule if you do not want to limit the Internet-bound traffic for that rule, but you still want to log the FQDNs that are being accessed.

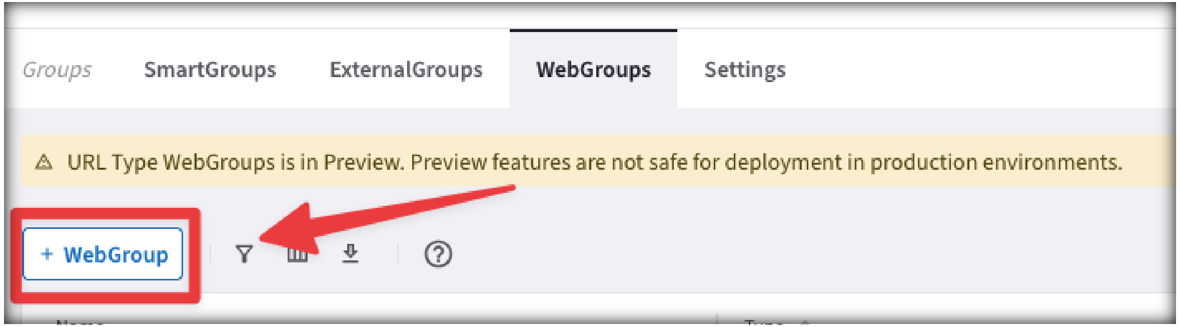


⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments.

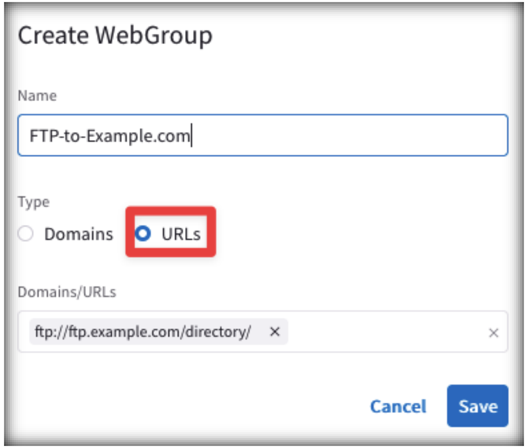
Name	Type	Domains/URLs
All-Web	Predefined WebGroup	*

WebGroup Creation

- **WebGroups** are groupings of domains and URLs, inserted into Distributed Cloud Firewall rules, that filter (and provide security to) Internet-bound traffic.
- In addition to the predefined WebGroup ***All-Web***, you can also create two kind of custom WebGroups:
  1. **URLs WebGroup:** for HTTP/HTTPS and for other protocols, but you need to define the full Path.
     - CAVEAT: TLS Decryption must be turned on when URLs-based WebGroups are used.
  2. **Domains WebGroup:** for HTTP and HTTPS traffic (wild cards are supported – i.e. partial names).



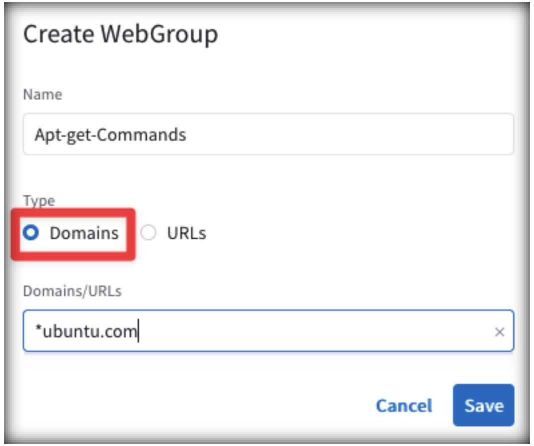
⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments.


Create WebGroup

Name: FTP-to-Example.com

Type: ○ Domains ● URLs

Domains/URLs: ftp://ftp.example.com/directory/ ×


Create WebGroup

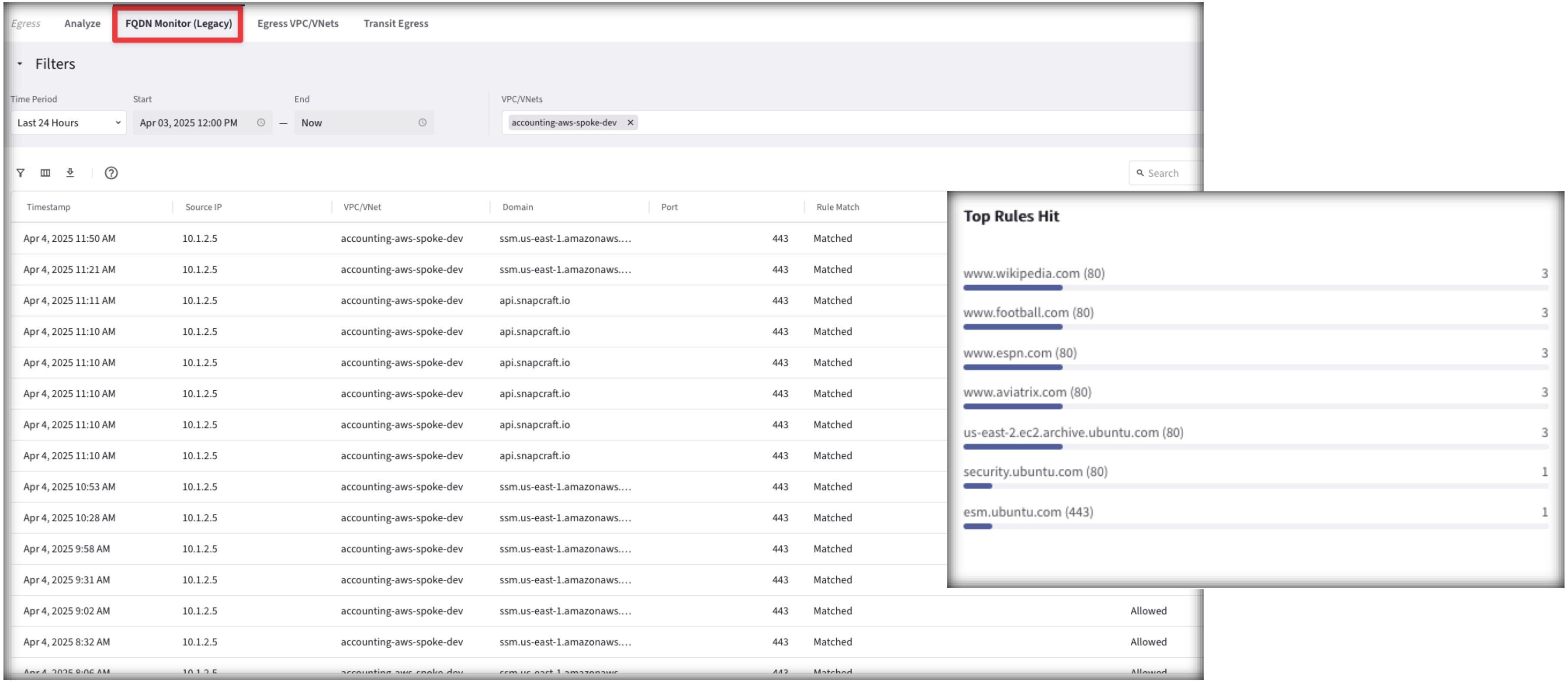
Name: Apt-get-Commands

Type: ● Domains ○ URLs

Domains/URLs: *ubuntu.com

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.



Time Period: Last 24 Hours
Start: Apr 03, 2025 12:00 PM — End: Now
VPC/VNets: accounting-aws-spoke-dev ×

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 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	Allowed
Apr 4, 2025 8:32 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws.…	443	Matched	Allowed
Apr 4, 2025 8:06 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws.…	443	Matched	Allowed

Top Rules Hit

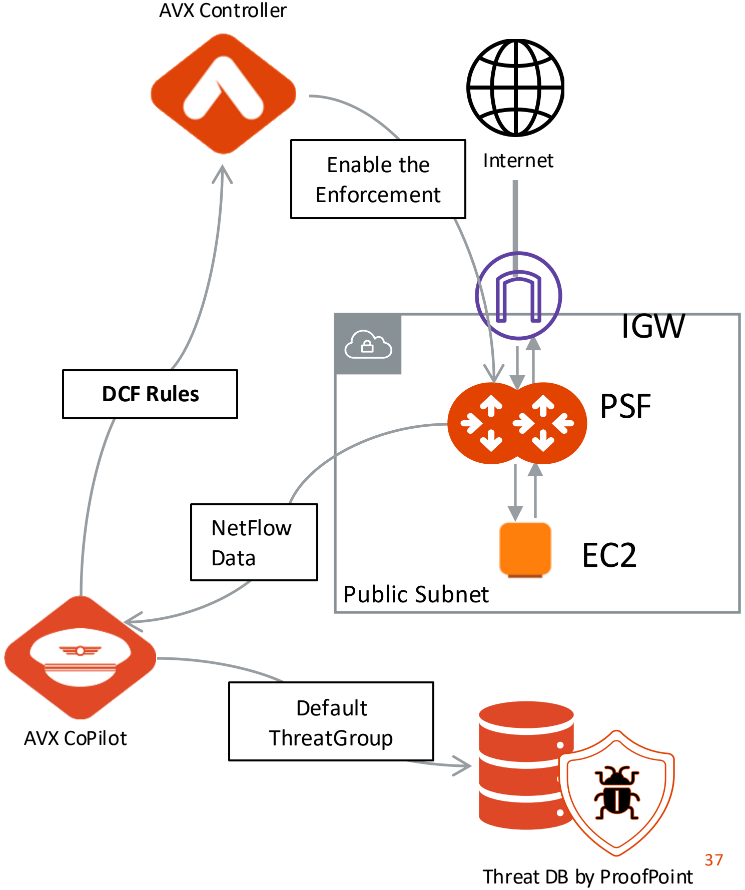
www.wikipedia.com (80)	3
www.football.com (80)	3
www.espn.com (80)	3
www.aviatrix.com (80)	3
us-east-2.ec2.archive.ubuntu.com (80)	3
security.ubuntu.com (80)	1
esm.ubuntu.com (443)	1

AVIATRIX
ACE
★★★★
PROFESSIONAL

Aviatrix PSF GW(aka Public Subnet Filtering Gateway)

Aviatrix Public Subnet Filtering Gateways (PSF GWs)

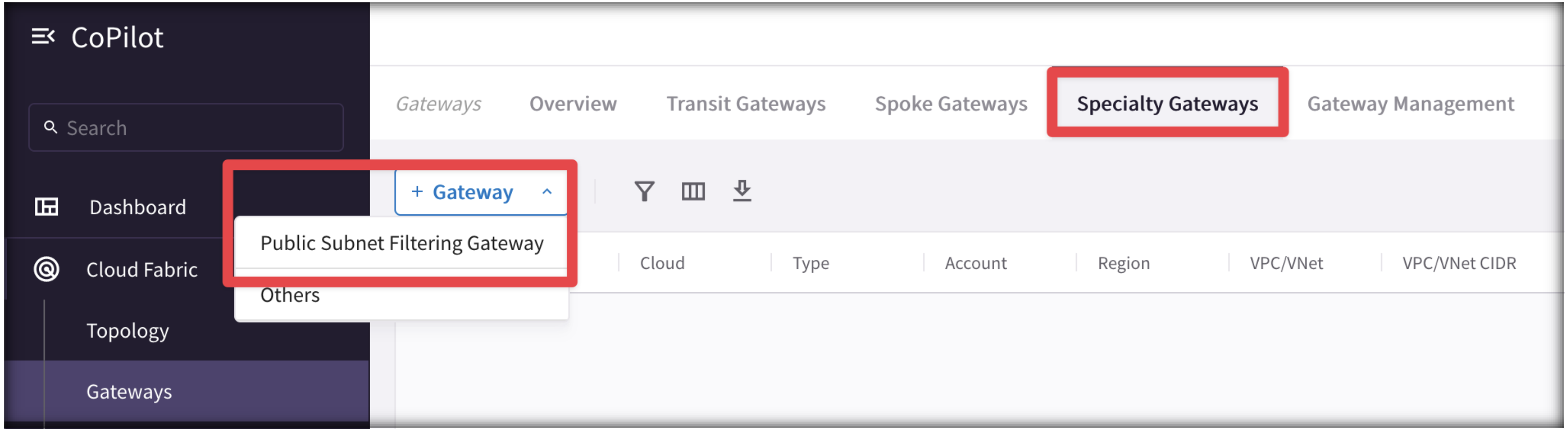
- **Public Subnet Filtering Gateways** (PSF gateways) provide ingress and egress security for **AWS** public subnets where instances have public IP addresses.
- After the Public Subnet Filtering (PSF) gateway is launched, you can apply also DCF (Distributed Cloud Firewall) rules – *enforcement must be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

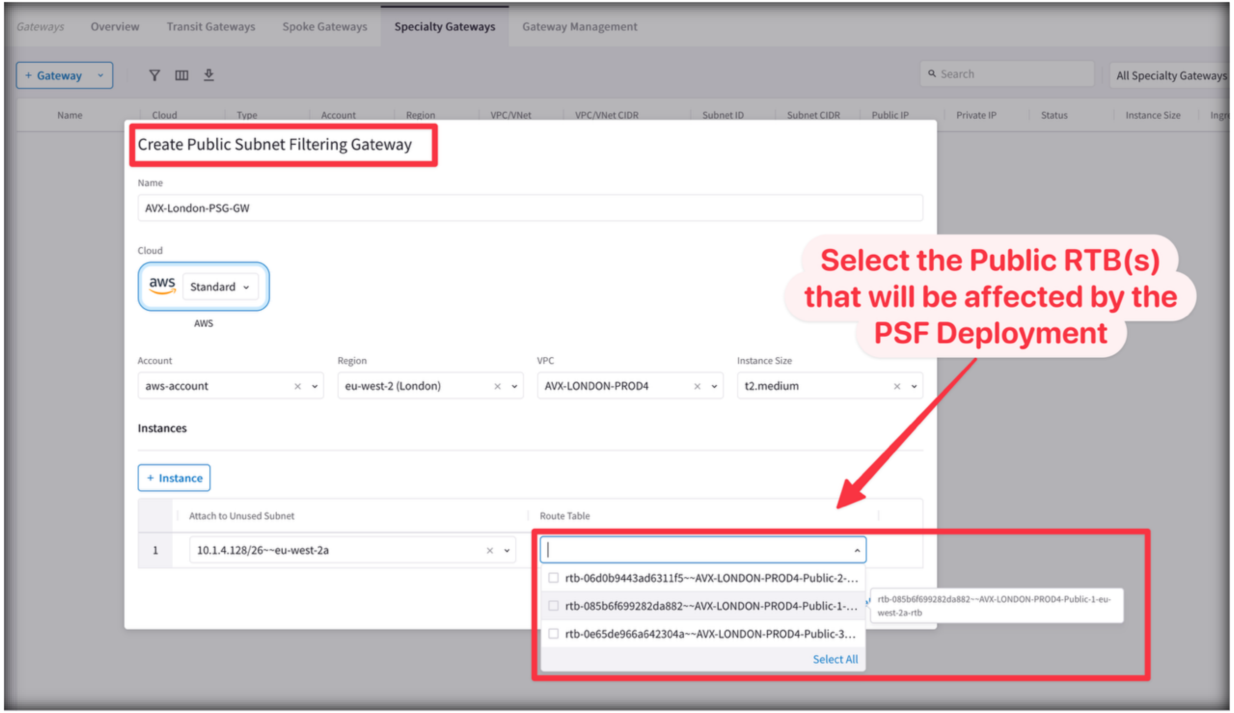
1. In CoPilot, navigate to **Cloud Fabric** > **Gateways** > **Speciality Gateways** tab.
2. Click **+Gateway** and select **Public Subnet Filtering Gateway**.



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.



Create Public Subnet Filtering Gateway

Name: AVX-London-PSG-GW

Cloud: aws Standard (AWS)

Account: aws-account

Region: eu-west-2 (London)

VPC: AVX-LONDON-PROD4

Instance Size: t2.medium

Instances

+ Instance

	Attach to Unused Subnet	Route Table
1	10.1.4.128/26~~eu-west-2a	

□ rtb-06d0b9443ad6311f5~~AVX-LONDON-PROD4-Public-2-...
□ rtb-085b6f699282da882~~AVX-LONDON-PROD4-Public-1-...
□ rtb-0e65de966a642304a~~AVX-LONDON-PROD4-Public-3...
Select All

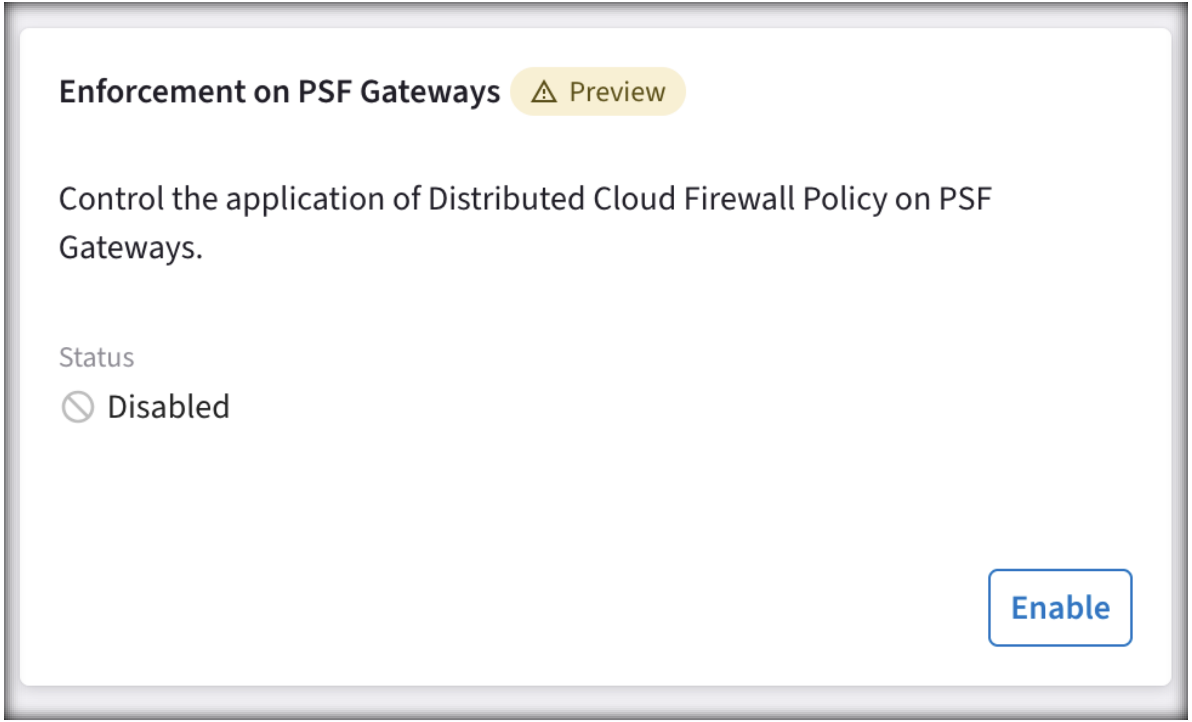
rtb-085b6f699282da882~~AVX-LONDON-PROD4-Public-1-eu-west-2a-rtb

Select the Public RTB(s) that will be affected by the PSF Deployment

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

AVIATRIX

ACE

★★★★

PROFESSIONAL

Lab 5 – **Aviatrix Cloud Firewall (with Secure Egress)**