



# Security

ACE Solutions Architecture Team



# Agenda

- Aviatrix Security Features Overview
- Securing Aviatrix Platform
- Aviatrix Cloud Firewall
- Public Subnet Filtering Gateway



# Challenges for CISO, CIO/CTO and NetSec Architects

- Apps/Business requirements dictate the Multi-Cloud
  - Some Apps simply operate better in one cloud vs another
  - New Customer Requirements a particular cloud OR M&A
- **Security and Compliance is NOT shared responsibility**
  - It is YOUR responsibility
- SaaS or Managed Services are often a Black-Boxes
- Understaffed Team, Skill Gap and Learning Curve issue
- Time-to-Market causes short-cuts
- Hacked or Not, doesn't matter Audit will happen regardless

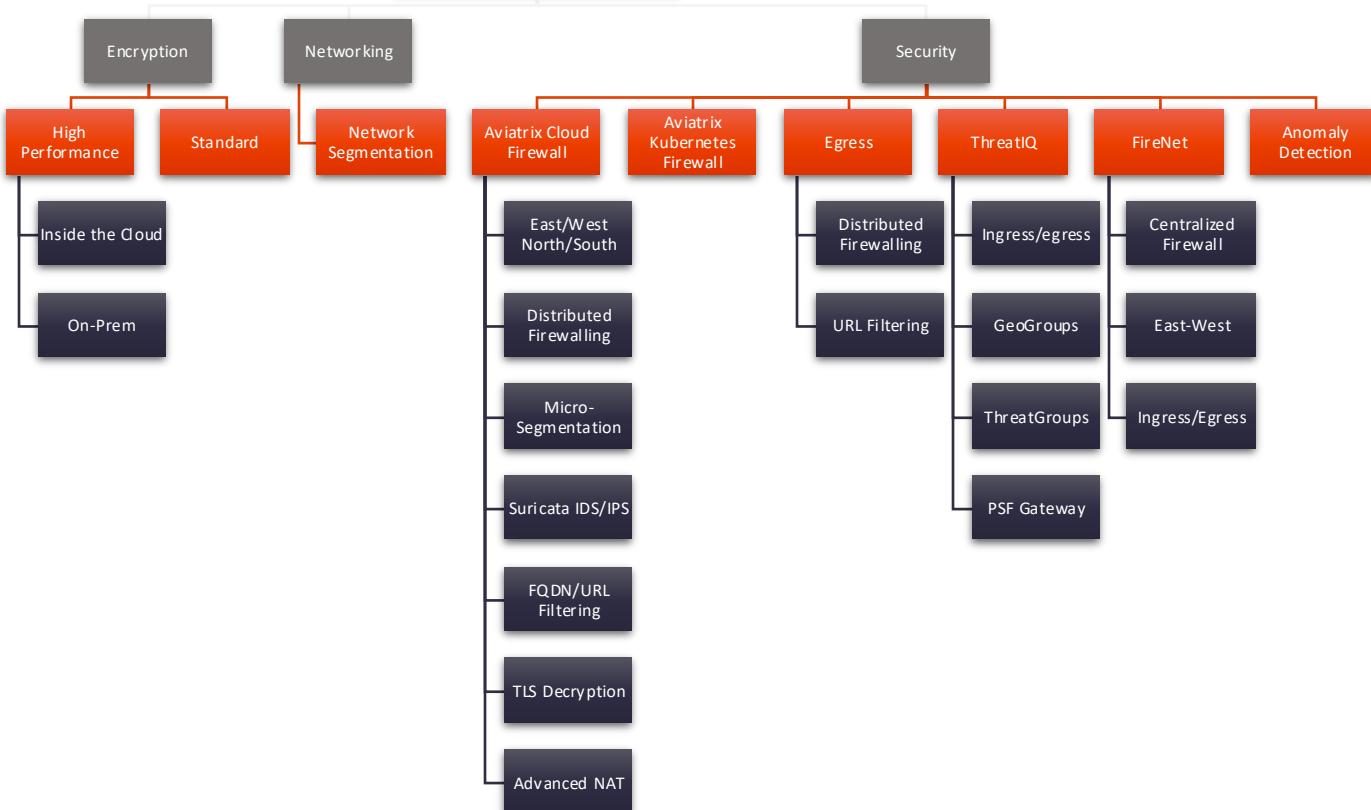


[https://aviatrix.com/resources/ebooks/  
security-architects-guide-multi-cloud-  
networking-v2](https://aviatrix.com/resources/ebooks/security-architects-guide-multi-cloud-networking-v2)

# Summary



## Key Aviatrix Security Features





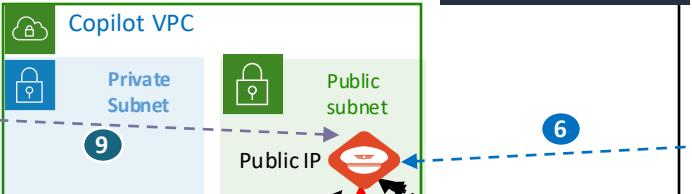
Built-in Security of the Aviatrix Platform

# AWS Cloud



Logging/  
Audit/  
Network  
Insight  
API

Prometheus  
Logstash  
Splunk  
SumoLogic  
Rsyslogic



## MFA

Duo  
Okta  
SAML  
LDAP etc.

aws API

Controller VPC

Private Subnet

Public subnet

Public IP

6

7

8

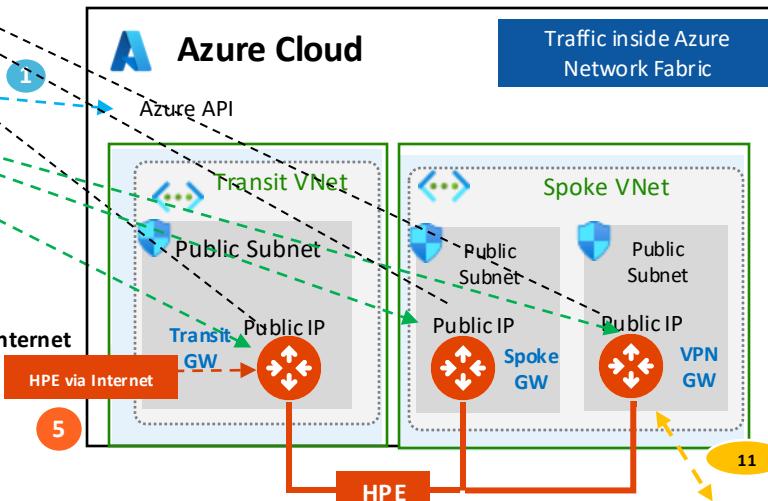
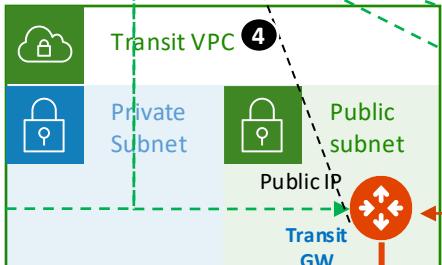
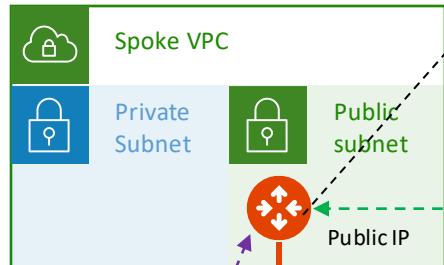
9

10

11

## 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



On Prem DC/  
Branch Office/  
B2B Partner



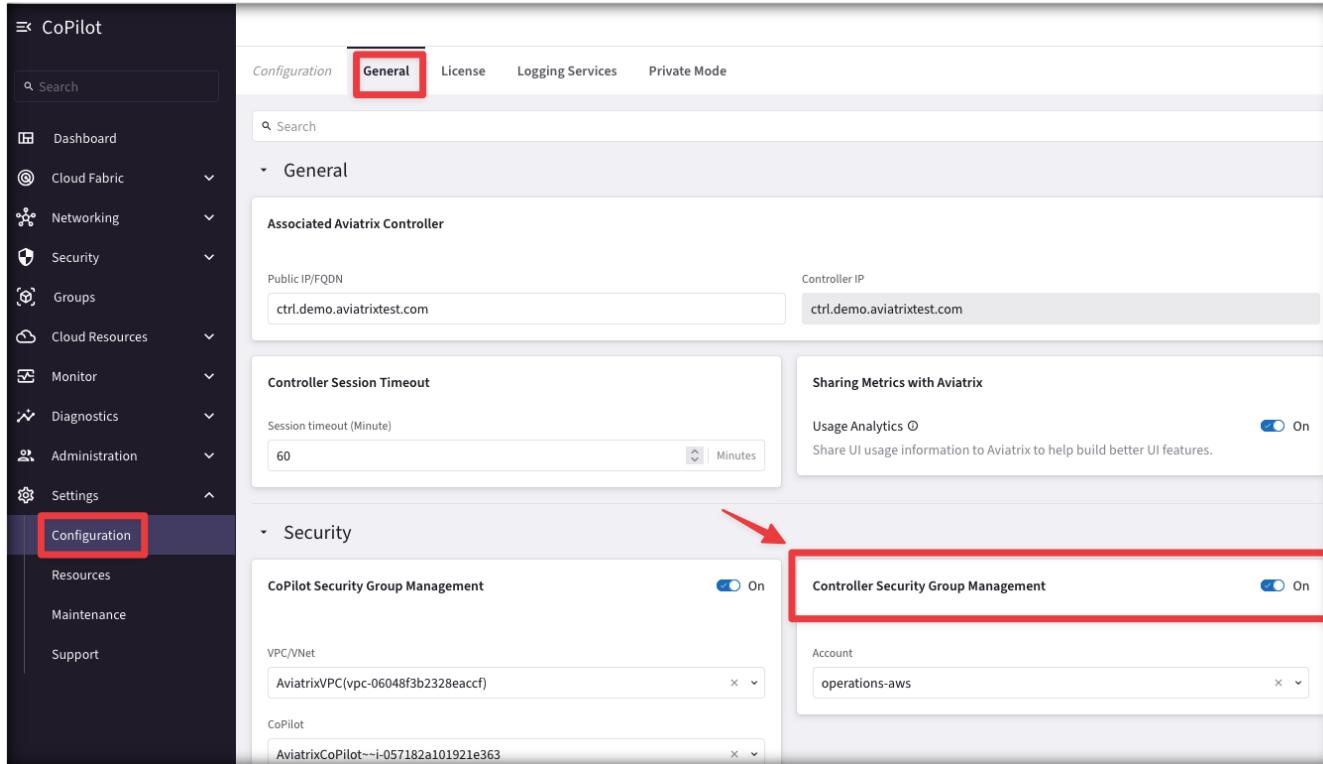
Remote User



## 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)



The screenshot shows the CoPilot interface with the 'Configuration' tab selected. In the 'General' section, there is a 'Controller Security Group Management' toggle switch which is turned 'On'. This section also includes fields for 'VPC/VNet' (set to 'AviatrixVPC(vpc-06048f3b2328eaccf)') and 'CoPilot' (set to 'AviatrixCoPilot~~i-057182a101921e363'). A red box highlights this entire section. A red arrow points from the 'Security' section in the sidebar to this highlighted area.

- 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.

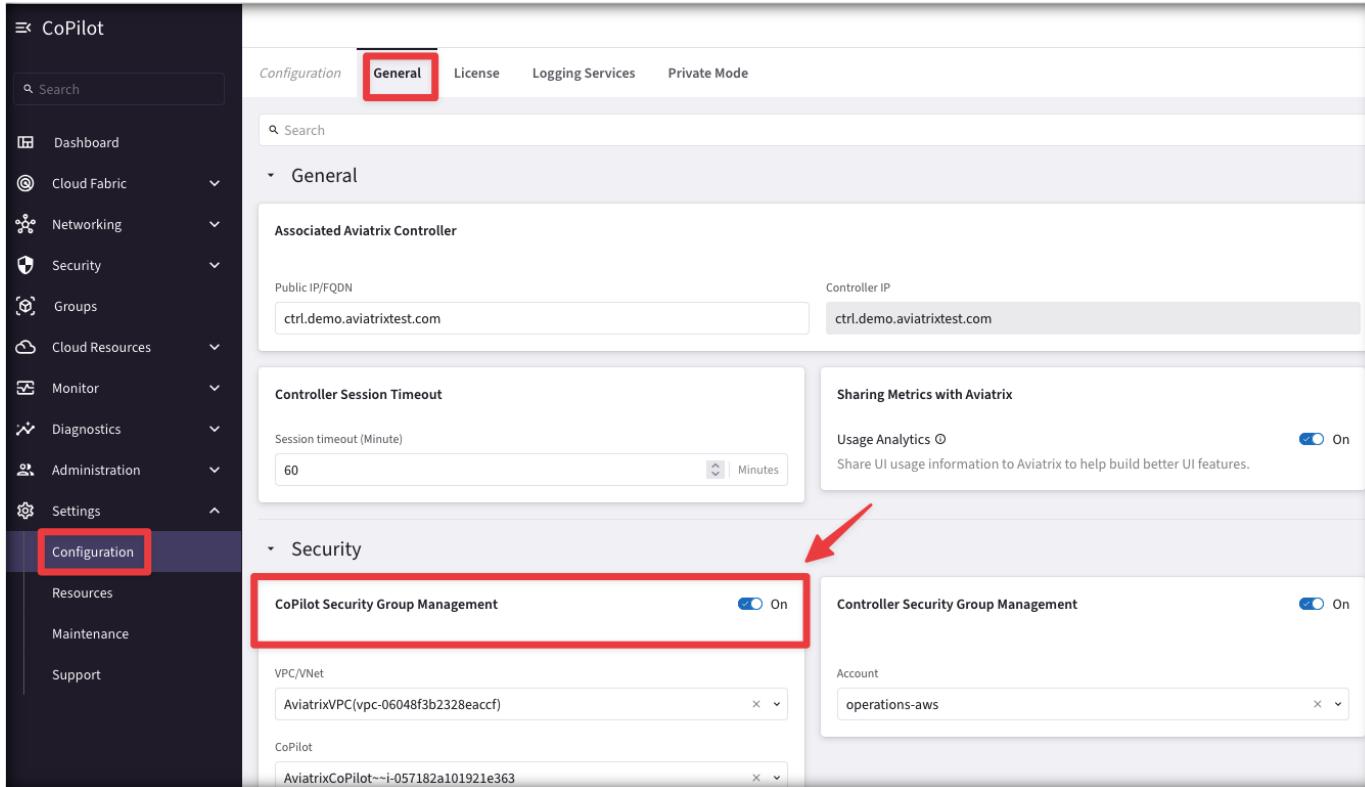
The Controller adds rules to the security group for each gateway IP for the following:

- 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)



The screenshot shows the CoPilot configuration interface. The left sidebar has a 'Configuration' tab highlighted with a red box. The main content area has a 'General' tab highlighted with a red box. Below 'General' is a 'Security' section, which also has a red box around its first item, 'CoPilot Security Group Management'. A red arrow points from the 'Security' section up towards the 'CoPilot Security Group Management' item.

**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.

**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



# Advantages: L7 Load Balancer in Front of Aviatrix Controller

- **Limit management access to Controller**

- Only allow access from the LB internal IPs to Controller on port 443

- **WAF capability on LBs**

- Stops usual web hacks/attacks against controller

- **L7 LB managing Controller certificate**

- Potentially terminating the SSL connection on LB [cloud native process]

- **Adhere to SoPs and best practices**

- Around alerts, operational features, logging integration, etc.
  - Putting an LB in front means Controller access can fit right into your existing operational model

- **Leverage LB health checks**

- Monitor the Controller at an application layer
  - If the LB health check goes down, it again fits right into existing operational best practices and SoPs of customer making it easier for them to monitor the control plane

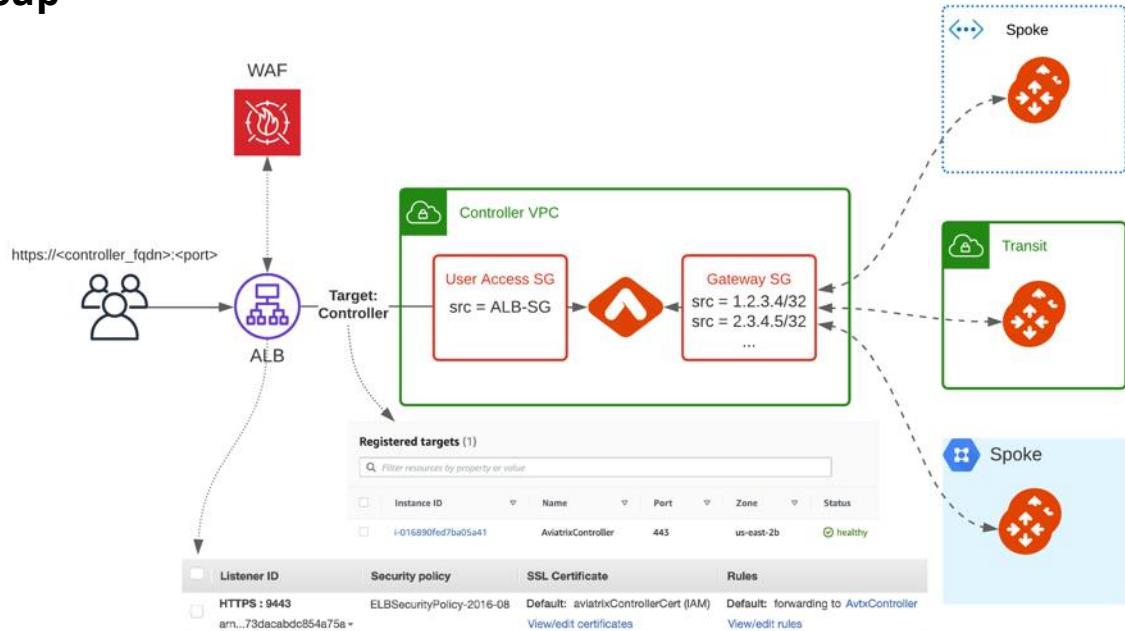
- Any access to controller, including API, UI login, etc., would go through LB, and the LB logging can provide easier, faster integration to existing tools

# 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





# Aviatrix Cloud Firewall

# Problem Statement

## Private workloads need internet access

- SaaS integration



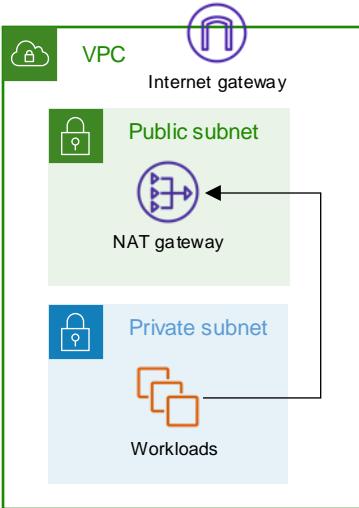
### NAT Gateway

- NACLs are necessary
- Layer-4 only

- Patching

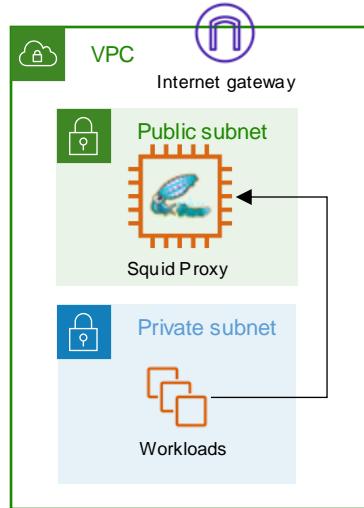


- Updates



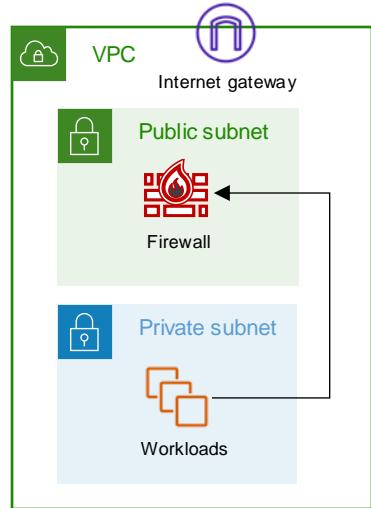
### Squid Proxy

- Hard to manage
- Scale and HA issues

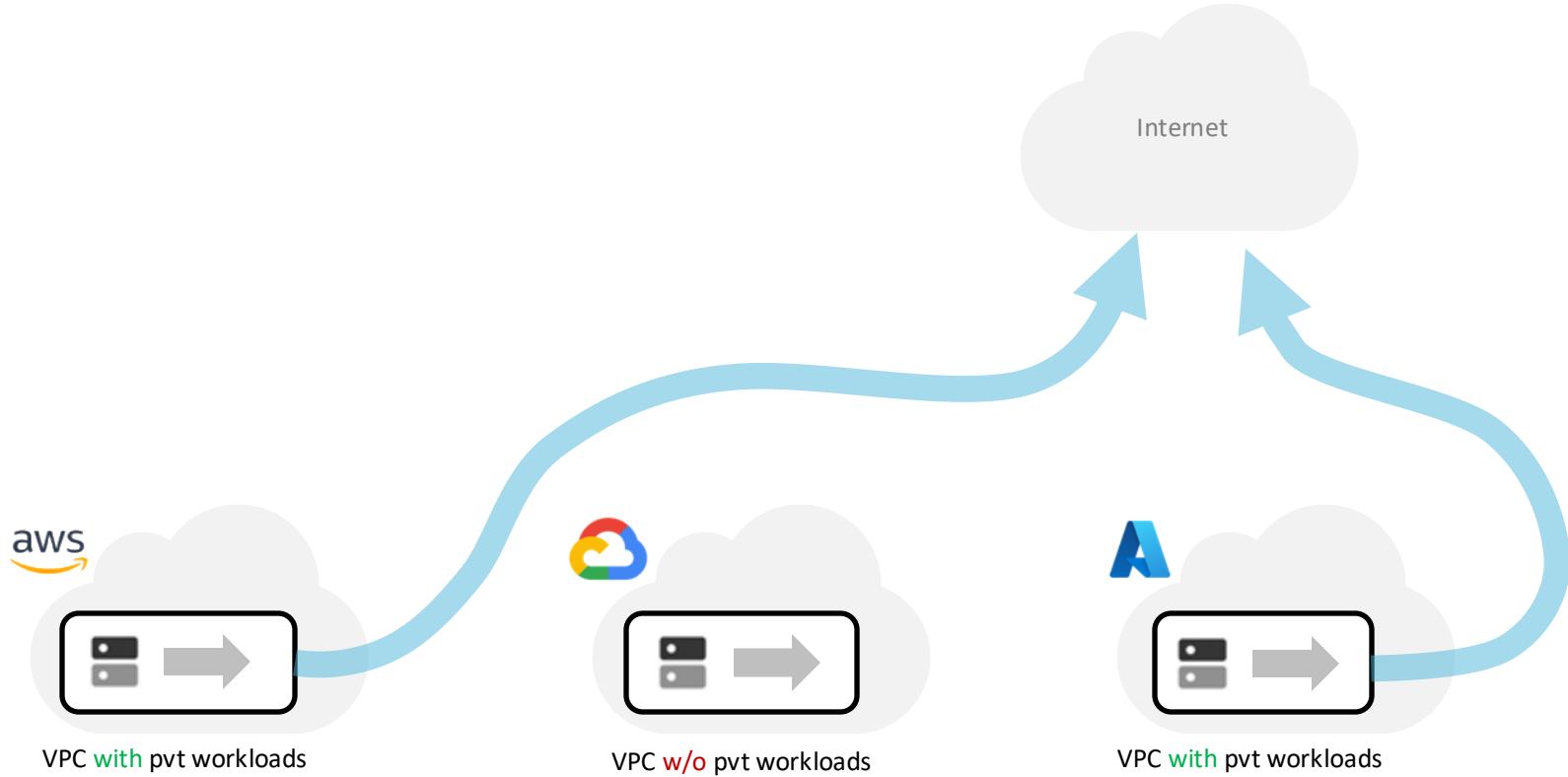


### Layer-7 Firewall

- Overkill
- Expensive

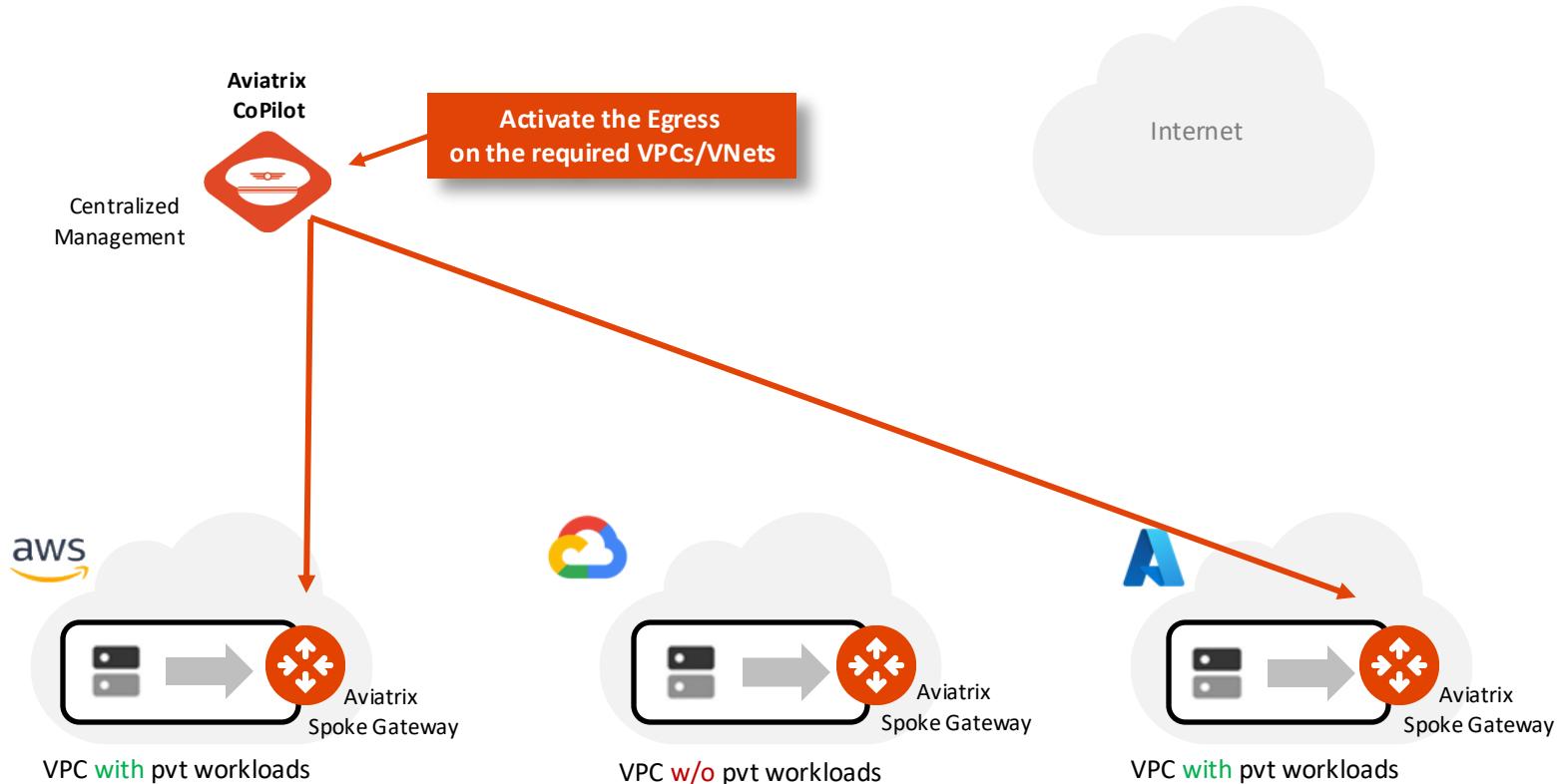


# Aviatrix Cloud Firewall

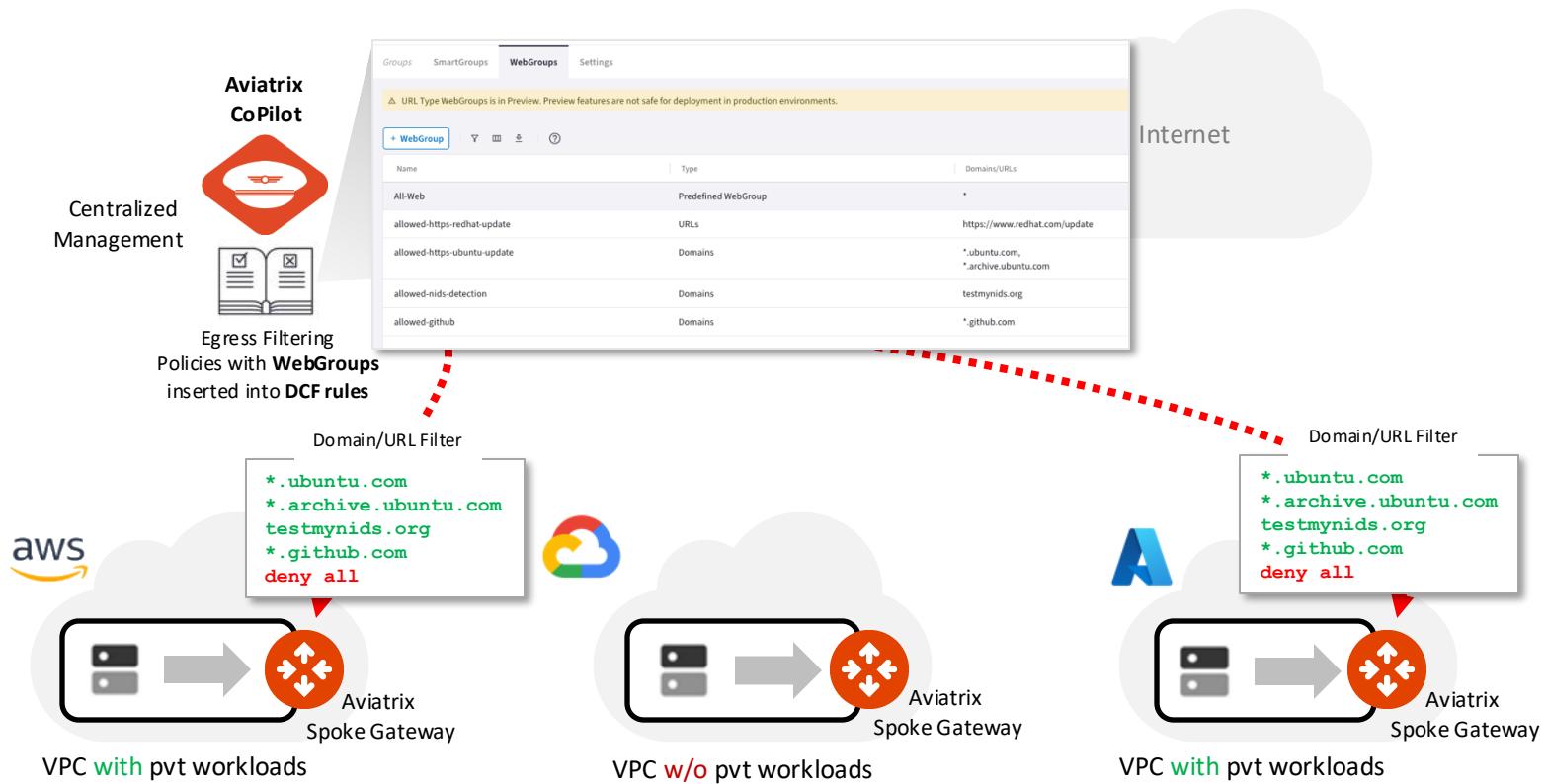




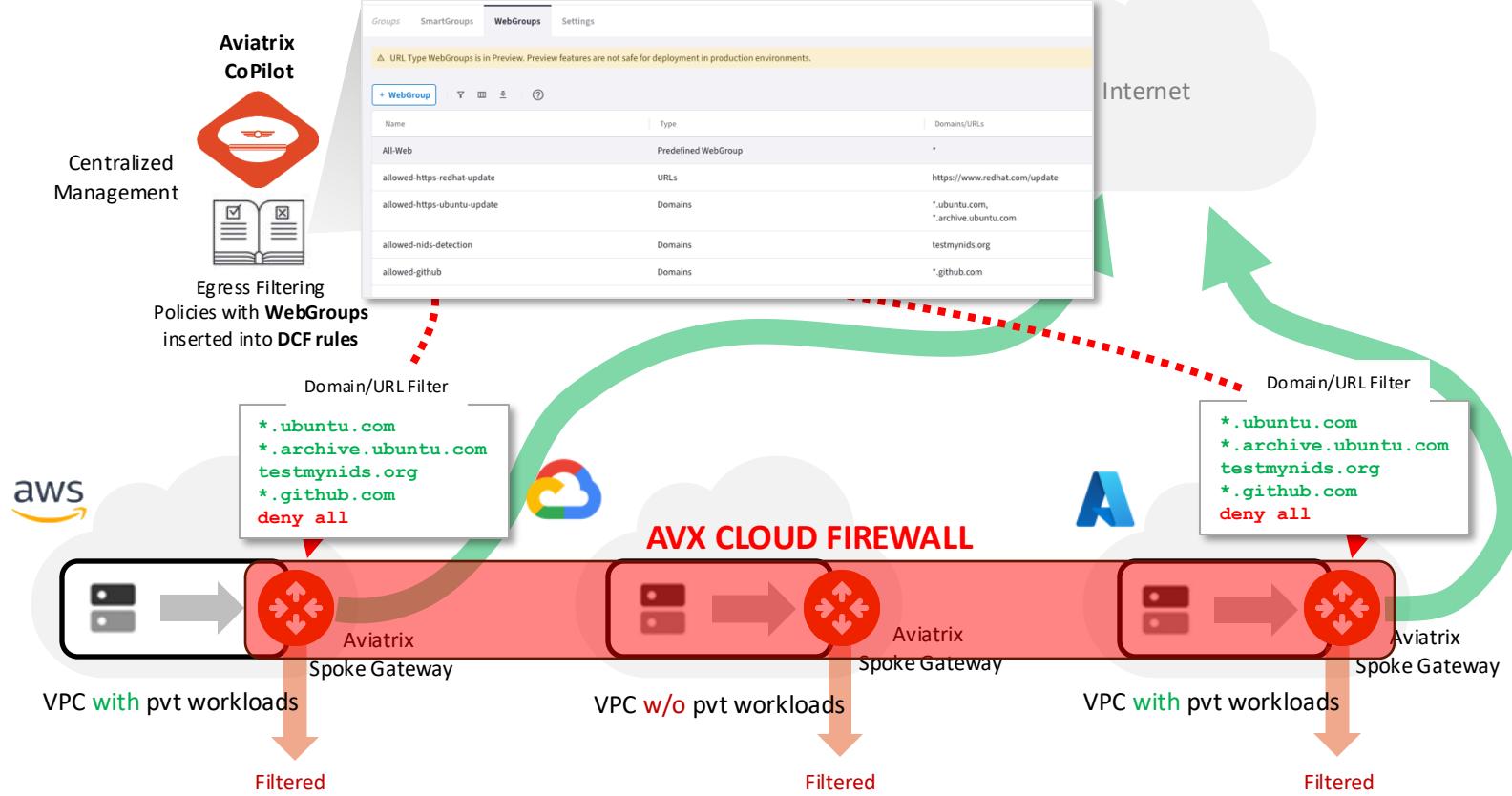
# Aviatrix Cloud Firewall



# Aviatrix Cloud Firewall



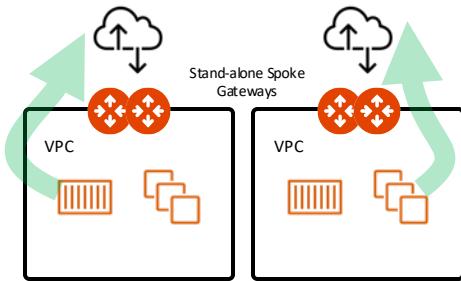
# Aviatrix Cloud Firewall



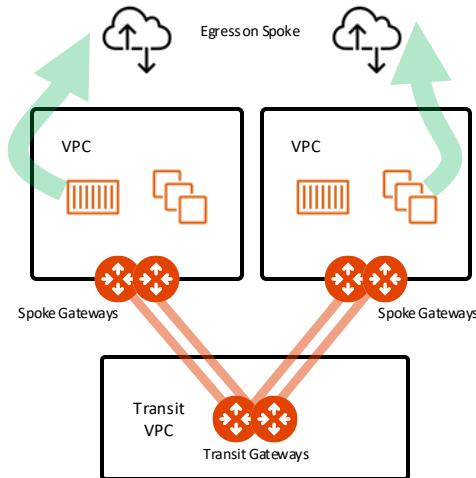
- The Aviatrix Cloud Firewall can be extended also to the Edge

# Aviatrix Cloud Firewall - Filtering Design Patterns

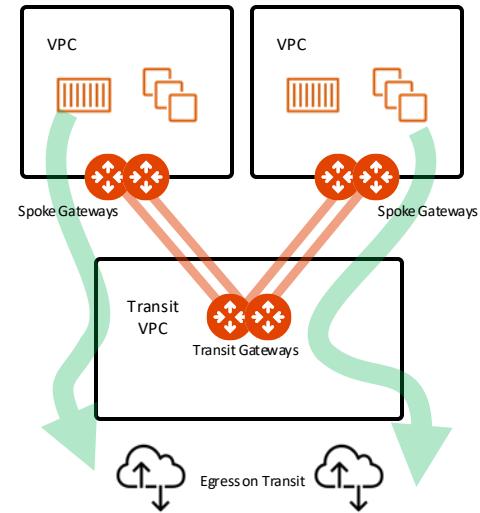
**Stand-alone Spoke GW (Distributed)**



**Local Egress (Distributed) with Aviatrix Spoke GW**



**Centralized Egress with Aviatrix Transit GW**



# 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.

The screenshot shows the CoPilot interface with the Egress tab selected. The 'Egress VPC/VNets' tab is active. A red box highlights the 'Enable Local Egress on VPC/VNets' button, and a red arrow points to the tab header. The table below lists various spoke gateways and their settings.

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	Local 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	azure-west-us-transit
gcp-us-central1-spoke1	gcp-us-central1-spo...	Native Cloud Egress	gcp-us-central1-transit

Pvt RTB BEFORE enabling the Egress

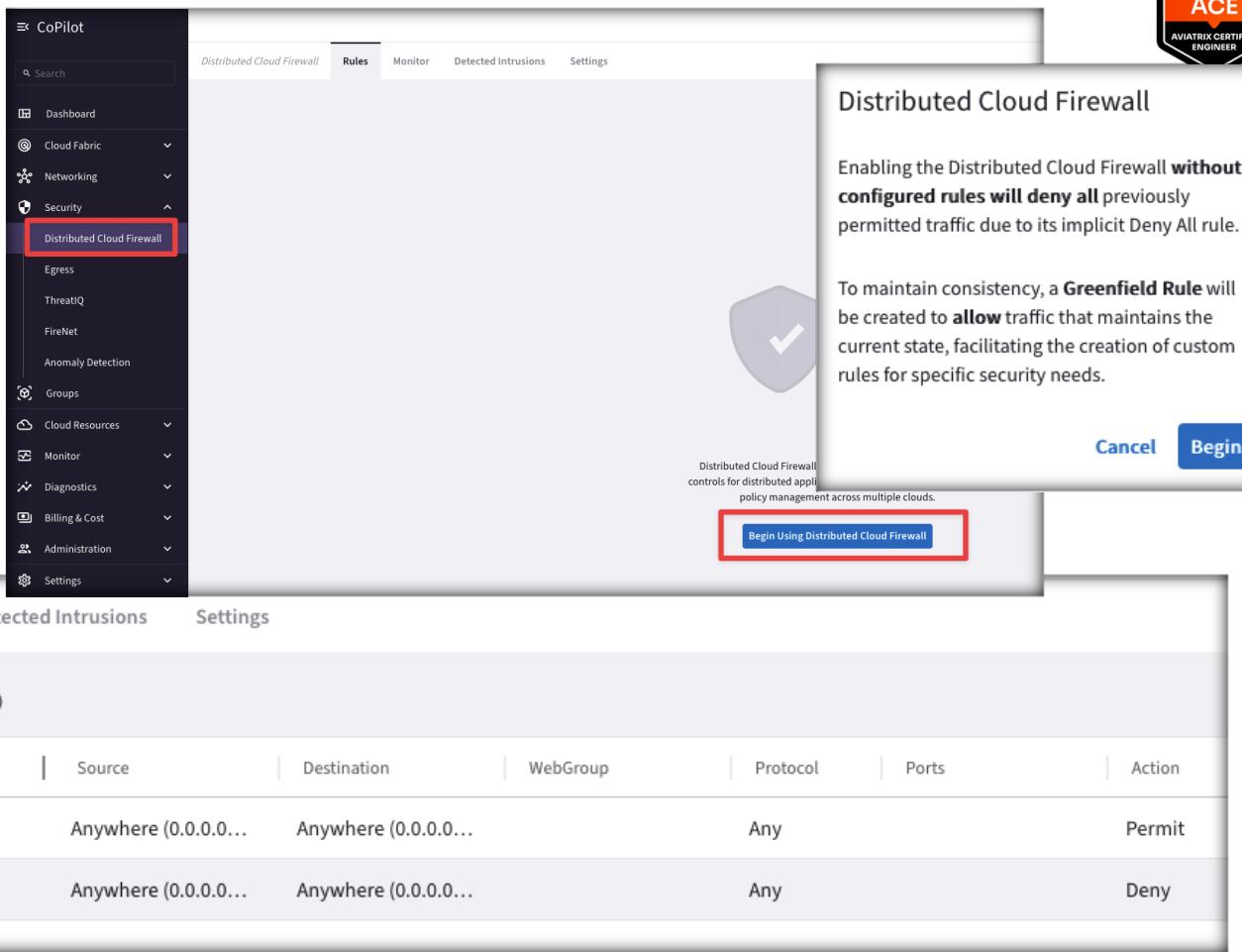
Route	Target	Gateway
10.0.1.0/24	local	local
192.168.0.0/16	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
172.16.0.0/12	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
10.0.0.0/8	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1

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

# The Greenfield-Rule

- If you want to apply policies on your Egress traffic, you must enable the Distributed Cloud Firewall.
- The Egress control requires the activation of the Distributed Cloud Firewall.
- The **Greenfield-Rule** is automatically added to allow all kind of traffic.
- An Explicit Deny Rule, named **DefaultDenyAll**, is also added below the Greenfield-Rule.
- Caveat: Logging is disabled by default on the Greenfield-Rule



The screenshot shows the Aviatrix CoPilot interface with the 'Distributed Cloud Firewall' tab selected. On the left, the navigation menu has 'Distributed Cloud Firewall' highlighted with a red box. The main panel displays a shield icon with a checkmark, indicating that enabling the firewall without rules will deny all traffic. Below the shield is a note: 'Enabling the Distributed Cloud Firewall **without configured rules** will **deny all** previously permitted traffic due to its implicit Deny All rule.' A 'Begin' button is visible. At the bottom, the 'Rules' tab is active, showing a table of rules. The table includes columns for Priority, Name, Source, Destination, WebGroup, Protocol, Ports, and Action. It lists two rules: 'Greenfield-Rule' (Priority 214748..., Action Permit) and 'DefaultDenyAll' (Priority 214748..., Action Deny). Both rules have a green checkmark in the Priority column.

Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
<input type="checkbox"/> 214748...	Greenfield-Rule	Anywhere (0.0.0.0...)	Anywhere (0.0.0.0...)		Any		Permit
<input type="checkbox"/> 214748...	DefaultDenyAll	Anywhere (0.0.0.0...)	Anywhere (0.0.0.0...)		Any		Deny

# Discovery Process

- If you are unsure about the sites your applications are accessing, you can temporarily enable an ad-hoc Discovery Rule.
  - Attach the SmartGroup that identifies the private workloads affected by the Egress feature, previously enabled, as *Source SmartGroup*.
  - Attach the Predefined SmartGroup "**Public Internet**", as *Destination SmartGroup*.
  - Attach the Predefined **All-Web** WebGroup.
  - Turn On the "**Logging**" toggle
  - Turn Off the "**Enforcement**" toggle
- The *Discovery-Rule* allows to intercept the logs generated only by HTTP (port 80) and HTTPS (port 443) traffic, from the VPC where the Egress control was enabled.
- Best Practice:* Place your Discovery-Rule always above the Greenfield-Rule.
- The result will be displayed under the **Copilot > Security > Egress > FQDN Monitor (Legacy)** tab

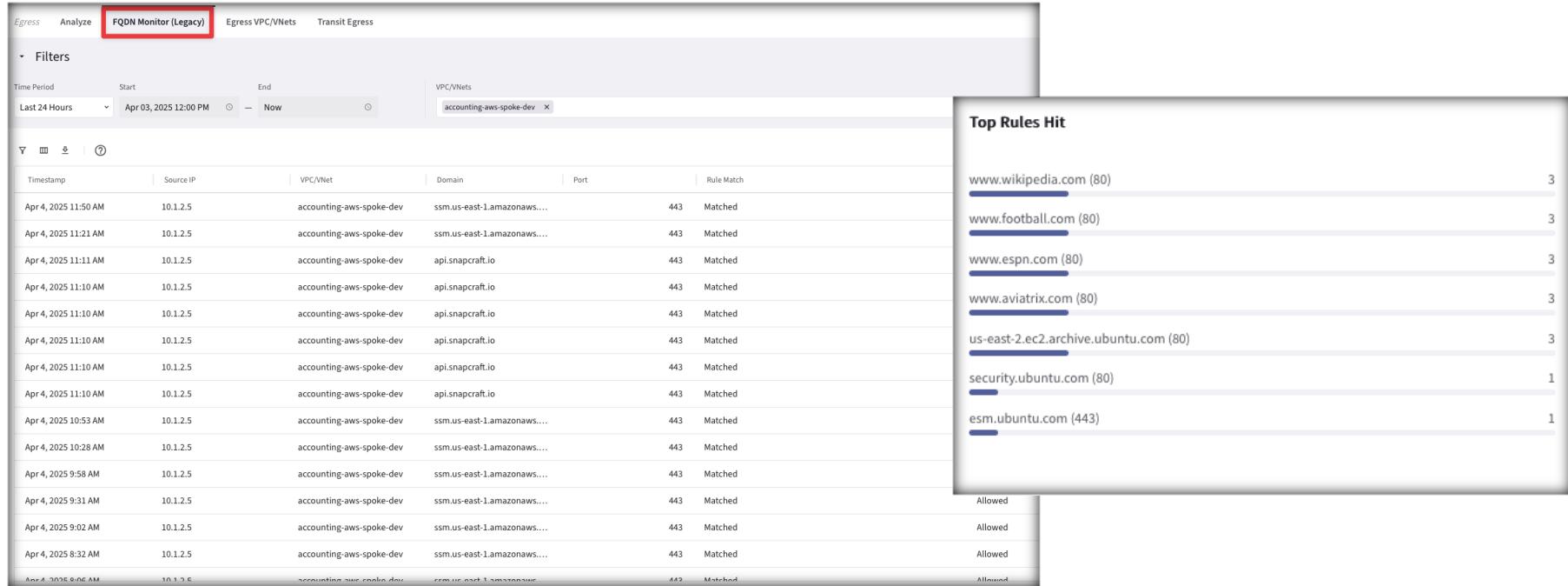
The screenshot shows the Aviatrix Distributed Cloud Firewall Rules interface. At the top, there are tabs for Rules, Monitor, Detected Intrusions, and Settings. The Rules tab is selected. Below the tabs is a toolbar with actions like + Rule, Actions, and a search/filter icon. A table lists the rules:

Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	IDS	Logging
0	Discovery-Rule	BU1	Public Internet	All-Web	Any		Permit		On
2147483...	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit		

The screenshot shows the "Create Rule" dialog box. It has sections for Name, Source SmartGroups, Destination SmartGroups, WebGroups, Protocol, Rule Behavior, and Rule Priority. The "Name" field is set to "Discovery Rule". The "Source SmartGroups" field contains "BU1". The "Destination SmartGroups" field contains "Public Internet". The "WebGroups" field contains "All-Web". The "Protocol" section shows "Any" selected for both Port and Protocol. In the "Rule Behavior" section, the "Enforcement" toggle is off and the "Logging" toggle is on. In the "Rule Priority" section, the "Place Rule" dropdown is set to "Above" and the "Existing Rule" dropdown is set to "Greenfield-Rule".

# 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.
- Best Practice: *The Discovery Process* should be used only temporarily. As soon as you have completed your discovery, kindly proceed to activating the *Allow-List model* (i.e. ZTNA approach).



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 box. Below the tabs, there are filters for Time Period (Last 24 Hours), Start (Apr 03, 2025 12:00 PM), End (Now), and a VPC/VNets filter set to "accounting-aws-spoke-dev".

The main area displays a table of log entries with columns: Timestamp, Source IP, VPC/Net, Domain, Port, and Rule Match. The table shows numerous entries from April 4, 2025, at various times, mostly from source IP 10.1.2.5, connecting to domains like ssm.us-east-1.amazonaws.com, api.snapcraft.io, and www.wikipedia.com, all through port 443 and marked as "Matched".

To the right, a large callout box highlights the "Top Rules Hit" section. It lists the most frequent domains and ports: 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. Each entry has a small blue bar chart next to it.



# Predefined WebGroup: All-Web

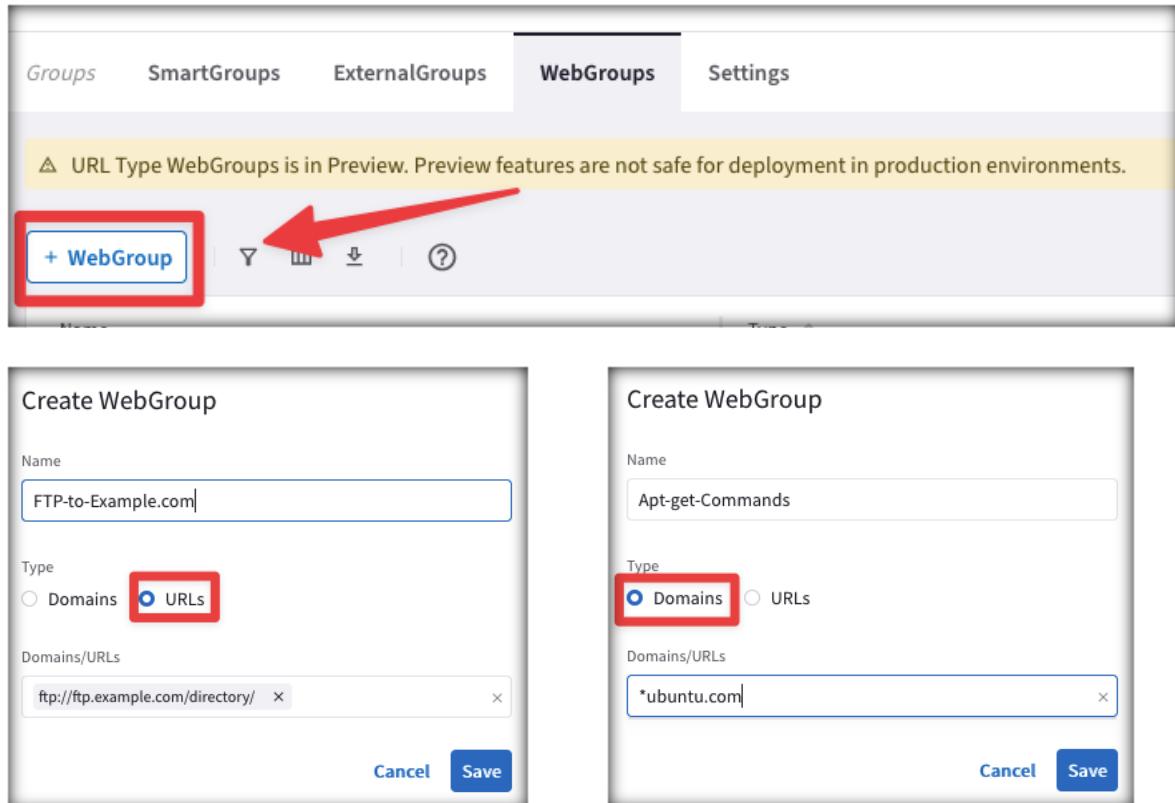
- When you navigate to **CoPilot > Groups**, a predefined WebGroup, *All-Web*, has already been created for you.
- This is an "*allow-all*" WebGroup that you must select in a Distributed Cloud Firewall rule if you do not want to limit the Internet-bound traffic for that rule, but you still want to log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

The screenshot shows the Aviatrix CoPilot interface with the 'Groups' tab selected. A yellow banner at the top states: "⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments." Below the banner, there is a table with columns for Name, Type, and Domains/URLs. The first row, 'All-Web', is highlighted with a red border. The 'Name' column contains 'All-Web', the 'Type' column contains 'Predefined WebGroup', and the 'Domains/URLs' column has an asterisk (\*) indicating it is required.

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).



**Create WebGroup**

Name:

Type:  URLs  Domains (highlighted with a red box)

Domains/URLs:

**Cancel** **Save**

**Create WebGroup**

Name:

Type:  Domains  URLs (highlighted with a red box)

Domains/URLs:

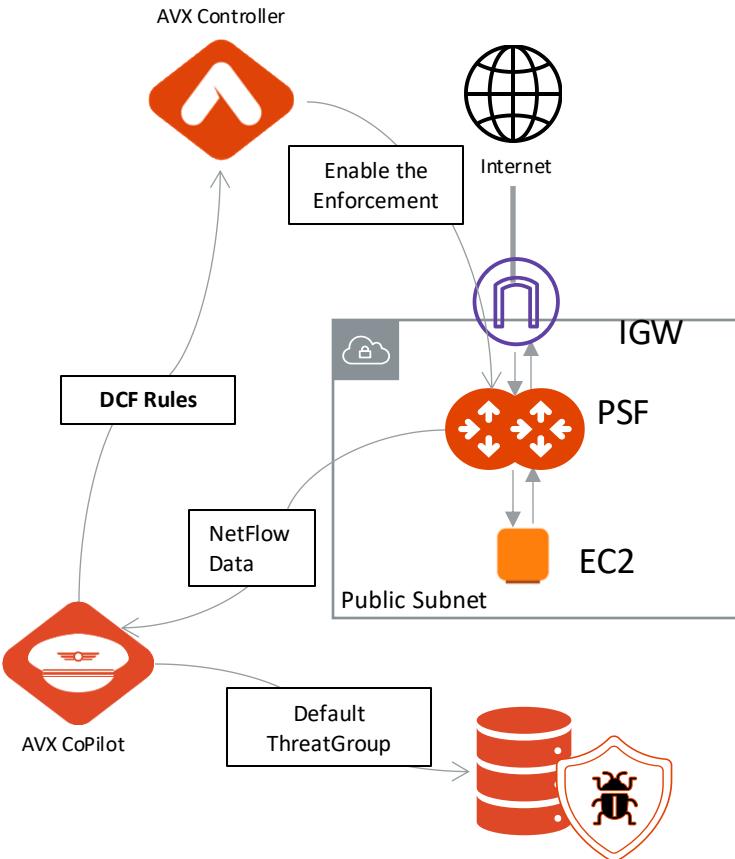
**Cancel** **Save**



# Aviatrix PSF GW(aka Public Subnet Filtering Gateway)

# Aviatrix Public Subnet Filtering Gateways (PSF GWs)

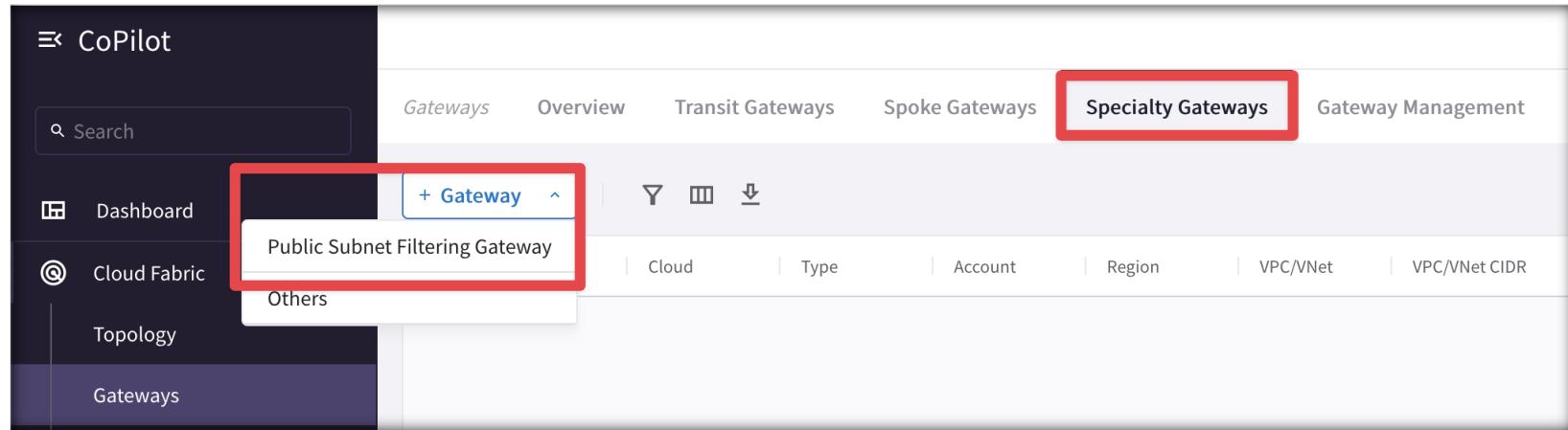
- **Public Subnet Filtering Gateways (PSF gateways)** provide ingress and egress security for **AWS** public subnets where instances have public IP addresses.
- After the Public Subnet Filtering (PSF) gateway is launched, you can apply also DCF (Distributed Cloud Firewall) rules – *enforcement must be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

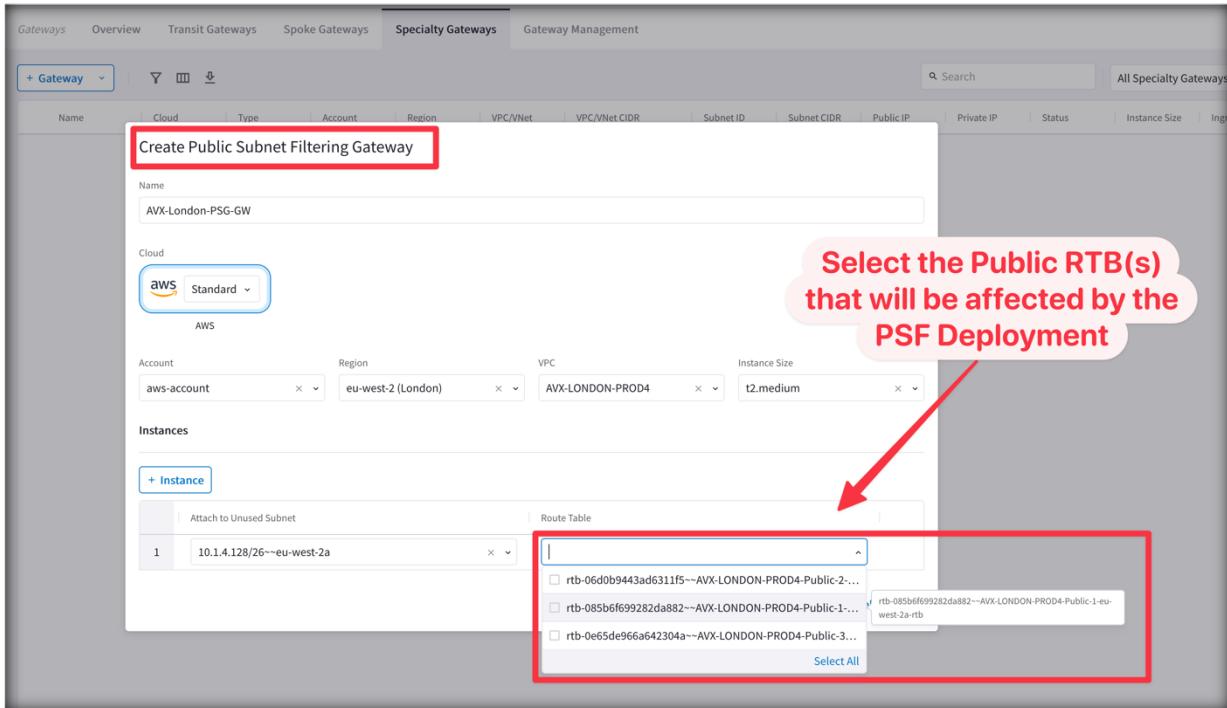
1. In CoPilot, navigate to **Cloud Fabric > Gateways > Specialty Gateways** tab.
2. Click **+Gateway** and select **Public Subnet Filtering Gateway**.



# 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



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