



Security

ACE Solutions Architecture Team



# Agenda

Aviatrix Security Features Overview

Securing Aviatrix Platform

Secure Egress

Public Subnet Filtering Gateway

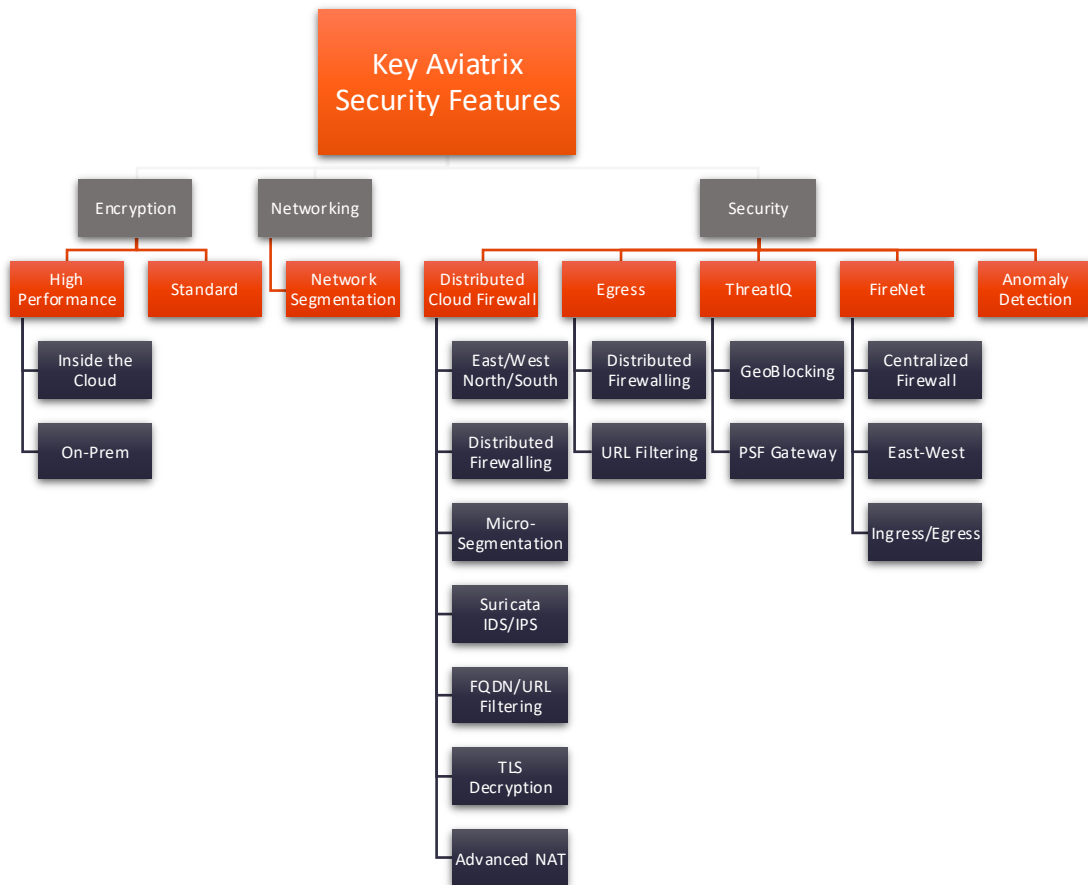
# Challenges for CISO, CIO/CTO and NetSec Architects

- 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>

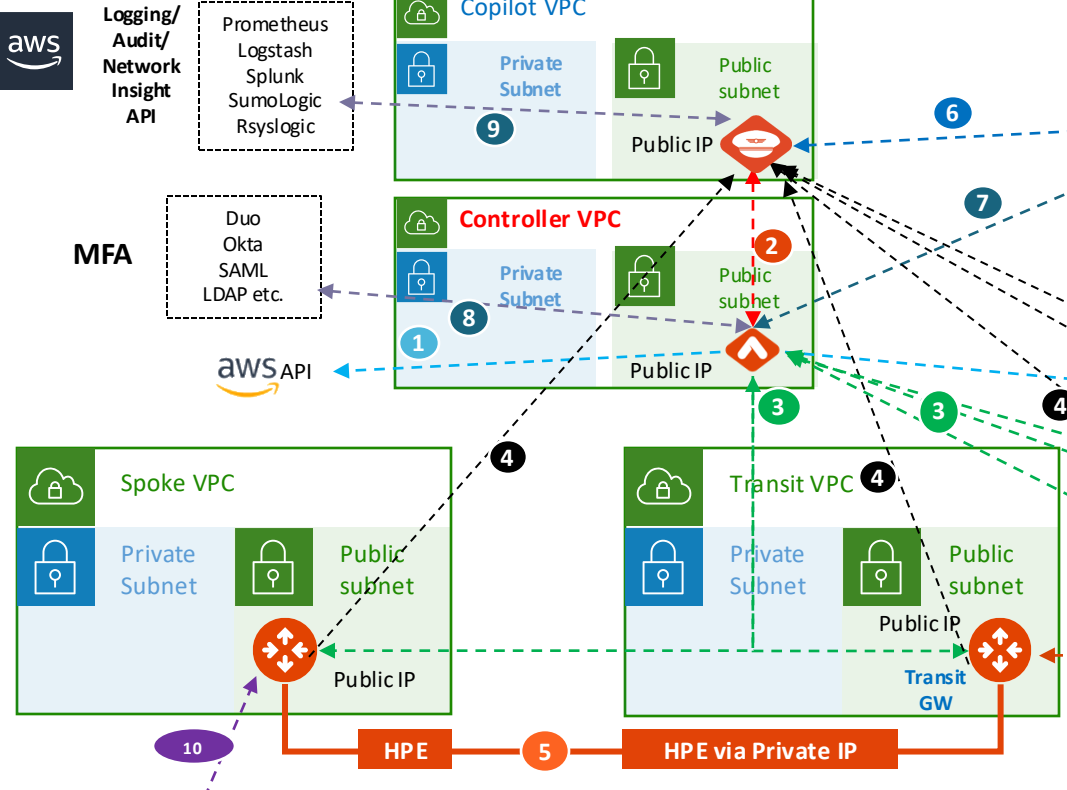
# Summary





# Built-in Security of the Aviatrix Platform

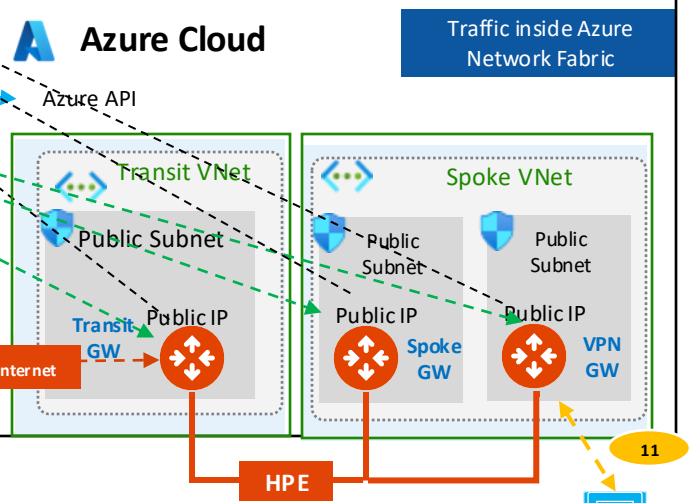
# AWS Cloud



Traffic inside AWS Network Fabric

- ### 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 3<sup>rd</sup> Party devices
  11. Remote user to Aviatrix VPN gateway

# Azure Cloud



Traffic inside Azure Network Fabric

On Prem DC/  
Branch Office/  
B2B Partner



Remote User

# Controller Security Group Management | Automatic Security Group lockdown



Details | **Security**

Security groups

- sg-054a744afb30dcb01 (ss-controller-AviatrixSG-YHFSUVZBB9Q9)
- sg-08a351c5c83665c38 (Aviatrix-SG-54.206.174.209-2)
- sg-0cb4cc125e9c69ed8 (Aviatrix-SG-54.206.174.209)
- sg-0ea9afb4e373b3264 (Aviatrix-SG-54.206.174.209-1)
- sg-05186521ae82c605d (Aviatrix-SG-54.206.174.209-3)



Instance: i-0ea8d13e979fb9be6 (ss-controller)

▼ Inbound rules

| Security group rule ID | Port range | Protocol | Source          | Security groups                       |
|------------------------|------------|----------|-----------------|---------------------------------------|
| sgr-01ffba9d6c84d825d  | 443        | TCP      | 3.106.76.93/32  | ss-controller-AviatrixSG-YHFSUVZBB... |
| sgr-0a11c67bf190b7be7  | 443        | TCP      | 3.105.63.97/32  | Aviatrix-SG-54.206.174.209            |
| sgr-0a8ccee5ee8d489ee  | 443        | TCP      | 3.104.18.207/32 | Aviatrix-SG-54.206.174.209            |



Instance: i-042eb8b6912e0acc0 (aviatrix-spoke1)

Security groups

- sg-09ef033544630561b (spoke1)

▼ Inbound rules

| Security group rule ID | Port range | Protocol | Source            | Security groups |
|------------------------|------------|----------|-------------------|-----------------|
| sgr-0288b5beddfa495b2  | All        | All      | 10.1.1.0/24       | spoke1          |
| sgr-03e3c293b614e73c7  | 443        | TCP      | 54.206.174.209/32 | spoke1          |



# 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

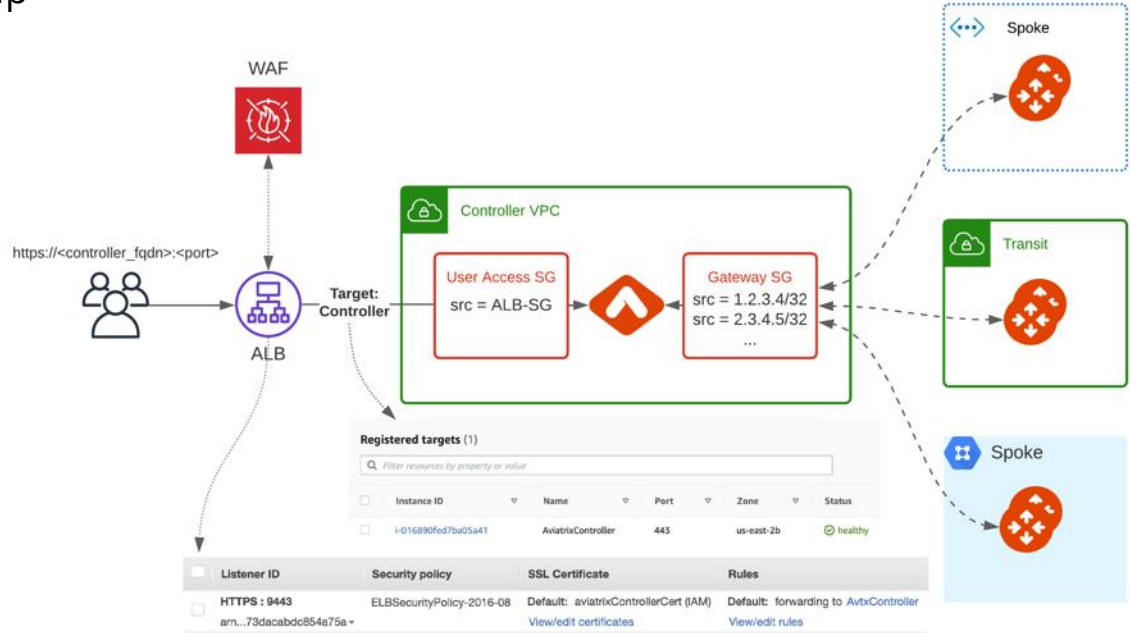


## Advantages: L7 Load Balancer in Front of Aviatrix Controller

- **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





# Cloud Perimeter Security

With Aviatrix Secure Cloud Egress

# Problem Statement

## Private workloads need internet access

- SaaS integration



- Patching

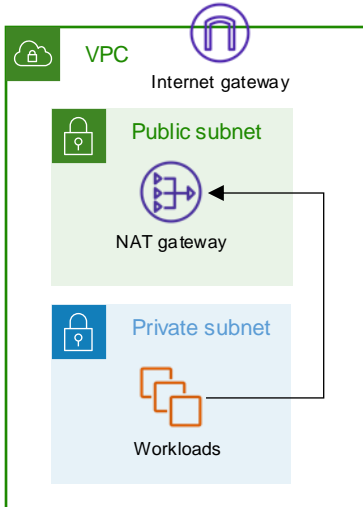


- Updates



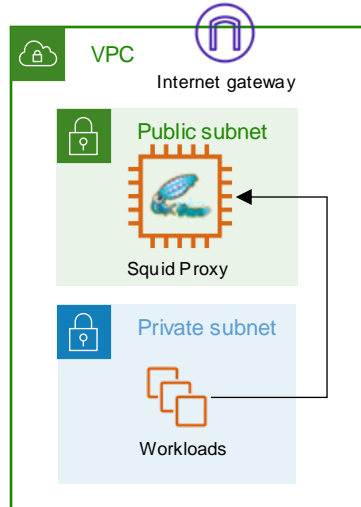
### NAT Gateway

- NACLs are necessary
- Layer-4 only



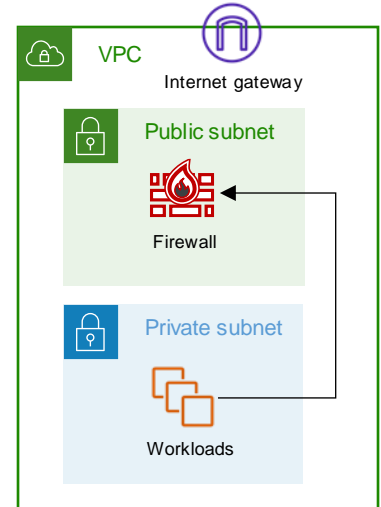
### Squid Proxy

- Hard to manage
- Scale and HA issues

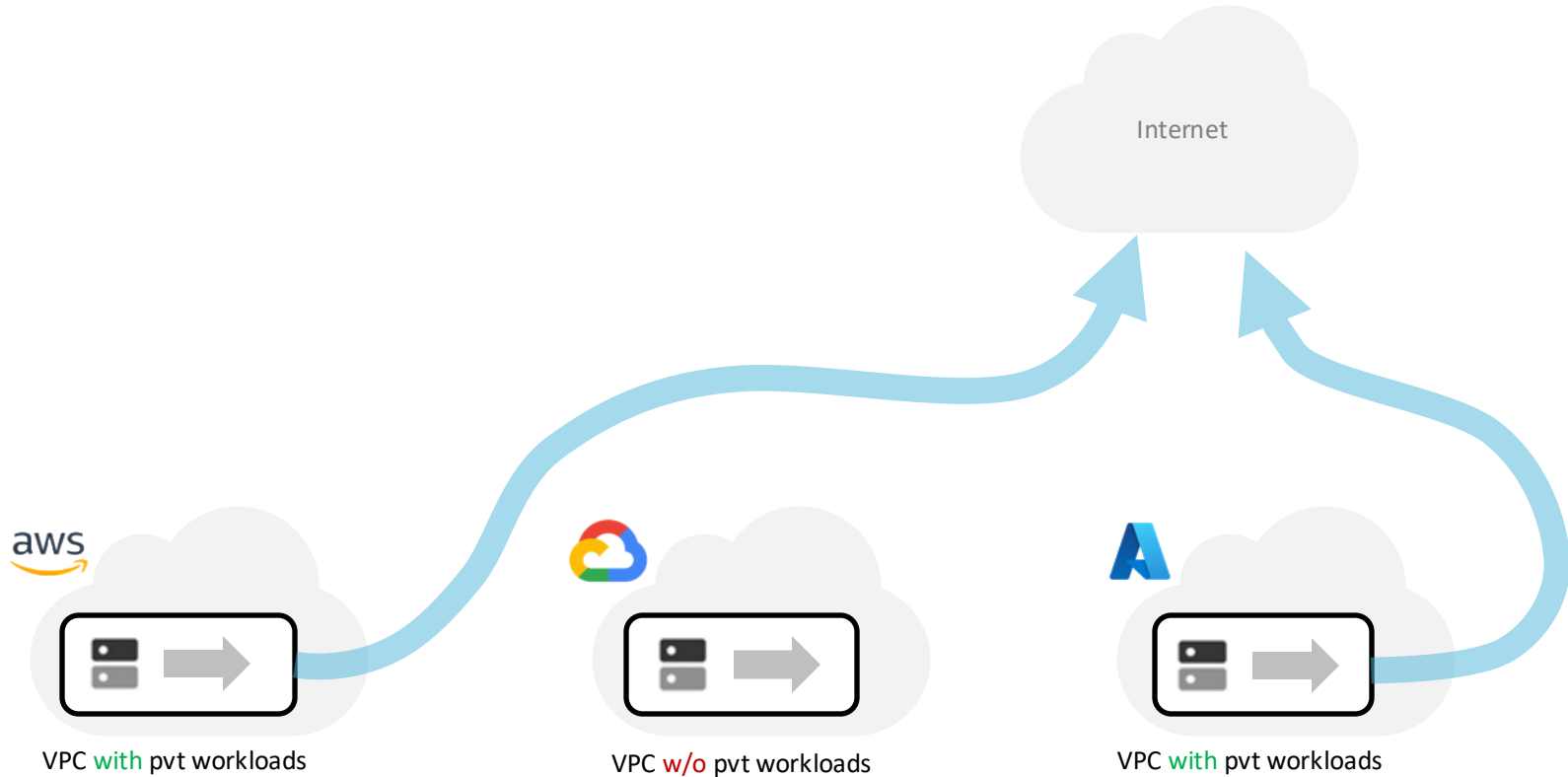


### Layer-7 Firewall

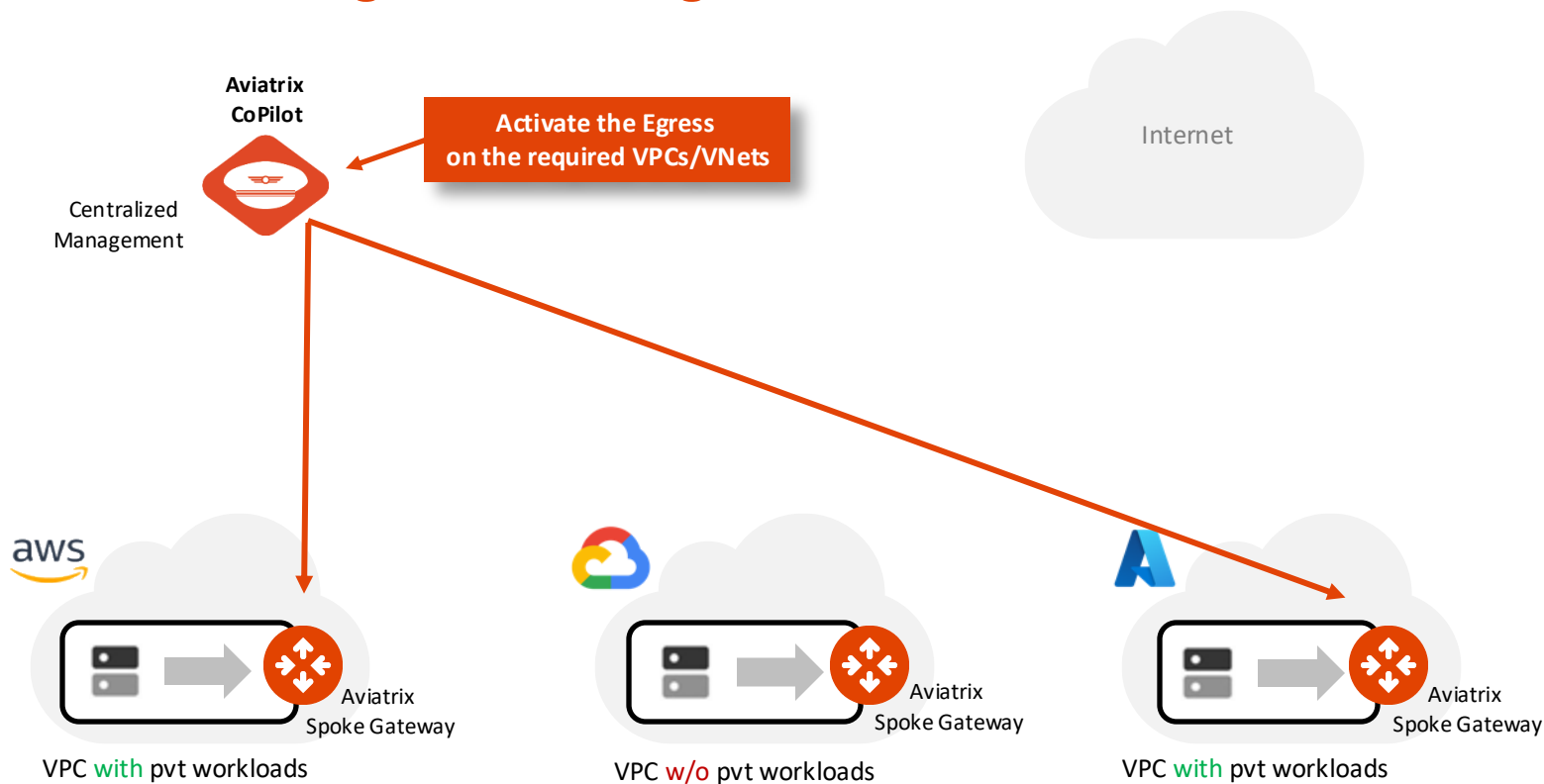
- Overkill
- Expensive



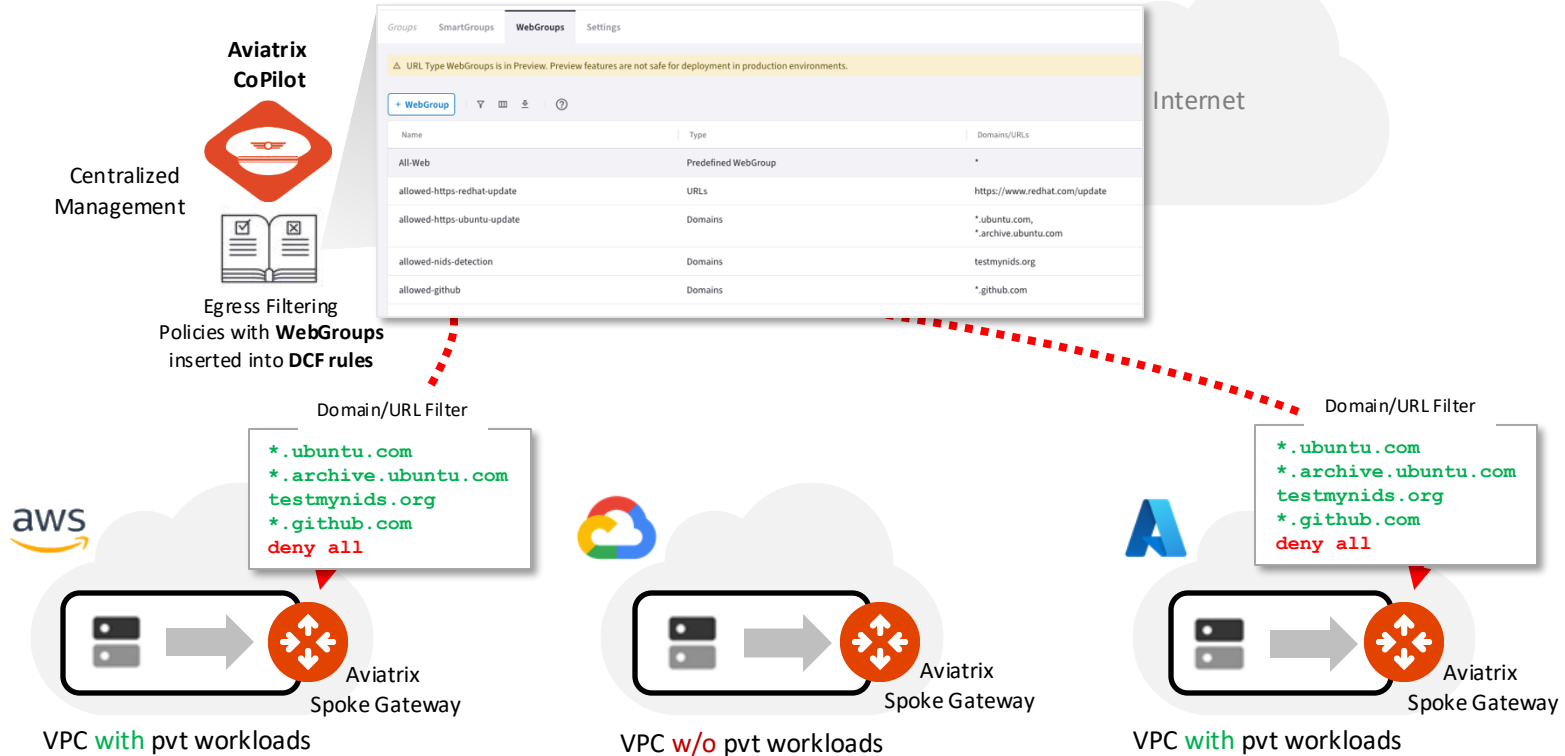
# Aviatrix Secure Egress Filtering Feature



# Aviatrix Secure Egress Filtering

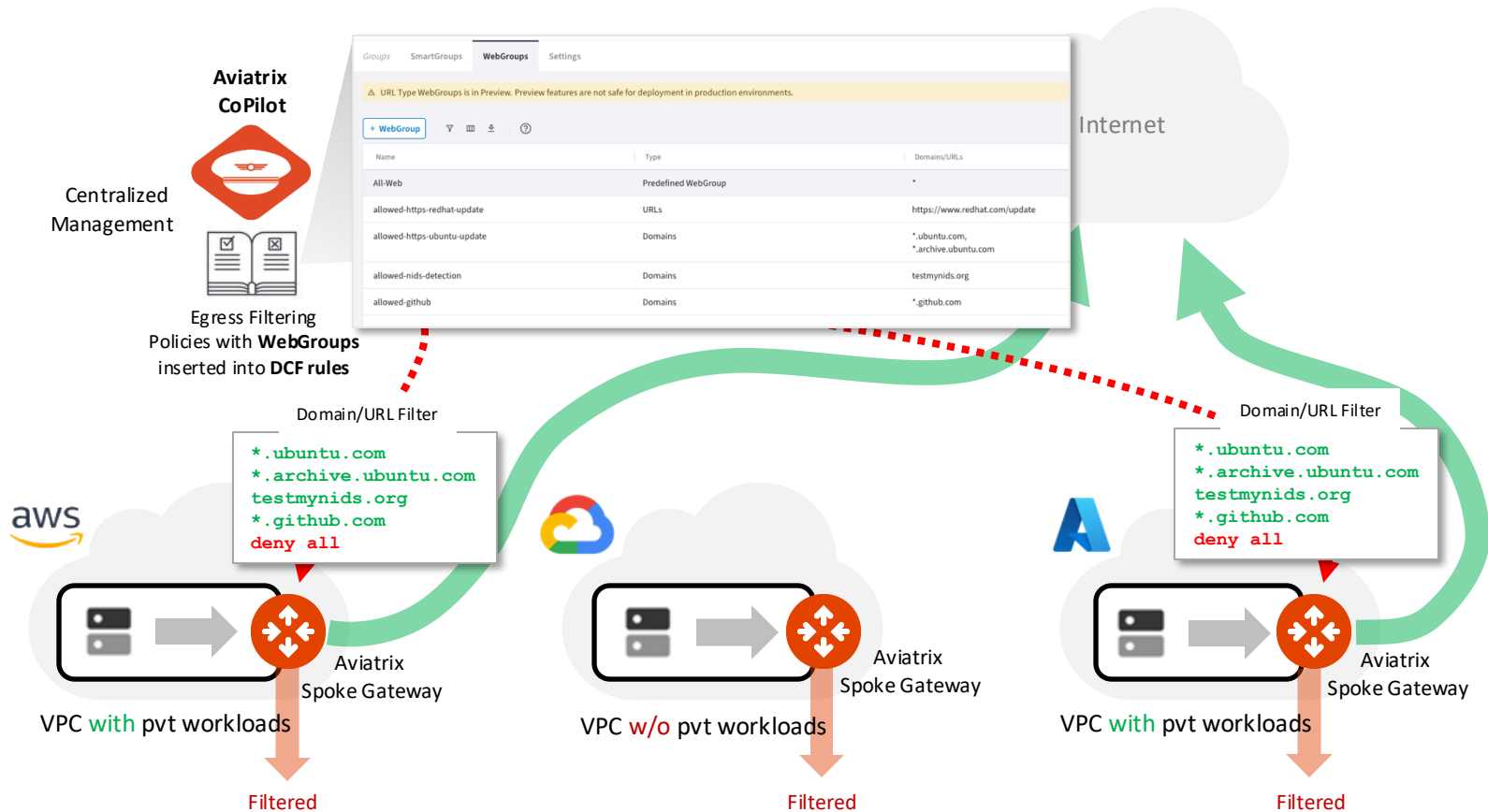


# Aviatrix Secure Egress Filtering



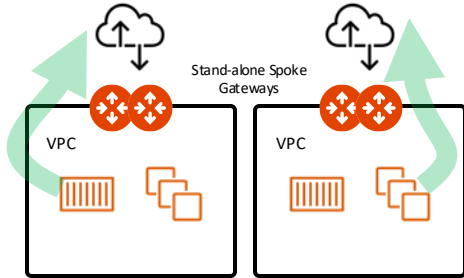


# Aviatrix Secure Egress Filtering

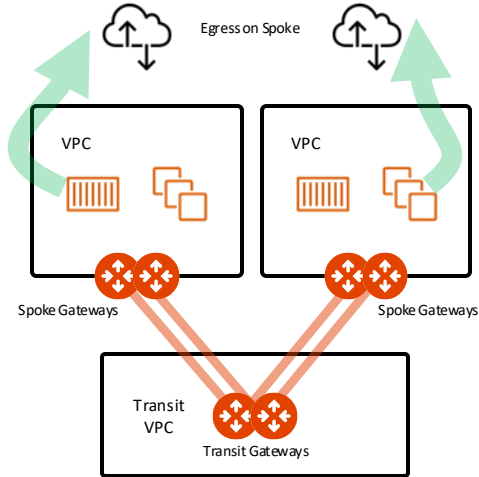


# Aviatrix Secure Egress Filtering Design Patterns

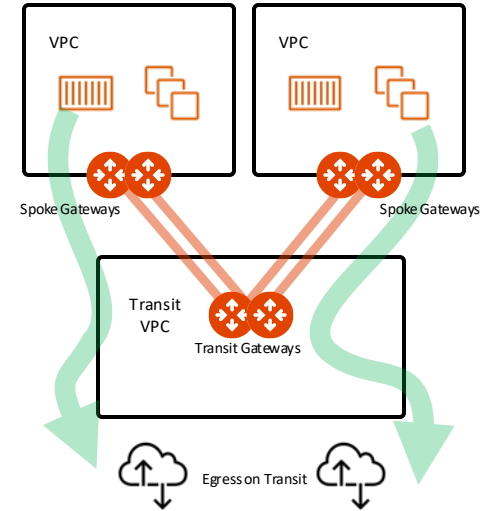
## Stand-alone Spoke GW (Distributed)



## 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.

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

**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.
- *Best Practice: do not edit this rule,* although it can be recreated if it is accidentally deleted.

| Priority                            | Name            | Source               | Destination          | WebGroup | Protocol | Ports | Action |
|-------------------------------------|-----------------|----------------------|----------------------|----------|----------|-------|--------|
| <input type="checkbox"/> 2147483646 | Greenfield-Rule | Anywhere (0.0.0.0/0) | Anywhere (0.0.0.0/0) |          | Any      |       | Permit |

# Discovery Process

- If you don't know the sites that your applications visit, an ad-hoc *Discovery-Rule* can be enabled, temporarily.
  - a) Attach the SmartGroup that identifies the private workloads affected by the Egress feature, previously enabled, as *Source SmartGroup*.
  - b) Attach the Predefined SmartGroup **"Public Internet"**, as *Destination SmartGroup*.
  - c) Attach the Predefined **All-Web** WebGroup.
  - d) Turn On the **"Logging"** toggle
  - e) 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 on the **Monitor** TAB.

| 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 |     |         |

**Create Rule**

Name: Discovery Rule

Source SmartGroups: BU1

Destination SmartGroups: Public Internet

WebGroups: All-Web

Protocol: Any | Port: All

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

**Rule Behavior**: Enforcement  | Logging

Action: Permit | SG Orchestration  Off

Ensure TLS:  Off | TLS Decryption:  Off | Intrusion Detection (IDS):  Off

**Rule Priority**: Place Rule: Above | Existing Rule: Greenfield-Rule

Buttons: Cancel, Save In Drafts

# Monitor

- On the Monitor 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. *ZTN approach*).

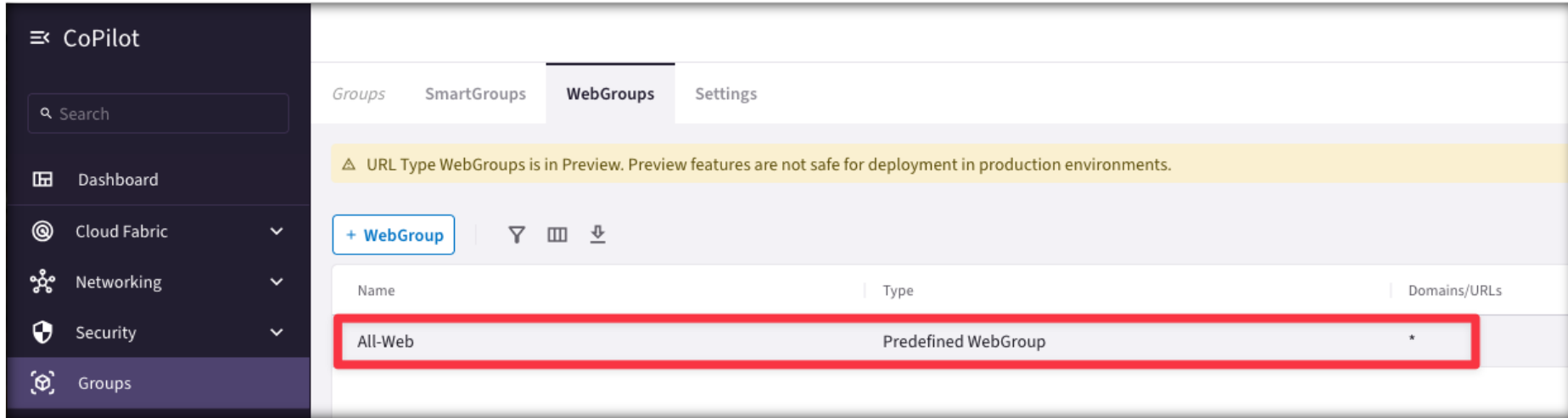
The screenshot shows the 'Monitor' section of the Aviatrix console. The 'Monitor' tab is highlighted with a red box. The interface includes a navigation bar with 'Egress', 'Overview', 'Monitor', 'Egress VPC/VNets', and 'Transit Egress'. Below the navigation bar, there are filters for 'Time Period' (Last 24 Hours), 'Start' (Dec 5, 2023 10:40 AM), 'End' (Now), and 'VPC/VNets' (aws-us-east-2-spoke1). A table of logs is displayed with columns for Timestamp, Source IP, VPC/VNet, Domain, Port, Rule Match, and Action. A sidebar on the right shows 'Top Rules Hit' with a list of domains and their hit counts.

| Timestamp            | Source IP | VPC/VNet             | Domain                           | Port | Rule Match | Action  |
|----------------------|-----------|----------------------|----------------------------------|------|------------|---------|
| Dec 6, 2023 10:40 AM | 10.0.1.10 | aws-us-east-2-spoke1 | esm.ubuntu.com                   | 443  | Matched    | Allowed |
| Dec 6, 2023 10:40 AM | 10.0.1.10 | aws-us-east-2-spoke1 | security.ubuntu.com              | 80   | Matched    | Allowed |
| Dec 6, 2023 10:40 AM | 10.0.1.10 | aws-us-east-2-spoke1 | us-east-2.ec2.archive.ubuntu.com | 80   | Matched    | Allowed |
| Dec 6, 2023 10:40 AM | 10.0.1.10 | aws-us-east-2-spoke1 | us-east-2.ec2.archive.ubuntu.com | 80   | Matched    | Allowed |
| Dec 6, 2023 10:40 AM | 10.0.1.10 | aws-us-east-2-spoke1 | us-east-2.ec2.archive.ubuntu.com | 80   | Matched    | Allowed |
| Dec 6, 2023 10:39 AM | 10.0.1.10 | aws-us-east-2-spoke1 | www.football.com                 | 80   | Matched    | Allowed |
| Dec 6, 2023 10:39 AM | 10.0.1.10 | aws-us-east-2-spoke1 | www.espn.com                     | 80   | Matched    | Allowed |
| Dec 6, 2023 10:39 AM | 10.0.1.10 | aws-us-east-2-spoke1 | www.wikipedia.com                | 80   | Matched    | Allowed |
| Dec 6, 2023 10:39 AM | 10.0.1.10 | aws-us-east-2-spoke1 | www.aviatrix.com                 | 80   | Matched    | Allowed |

| Domain                                | Count |
|---------------------------------------|-------|
| 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     |

# 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.

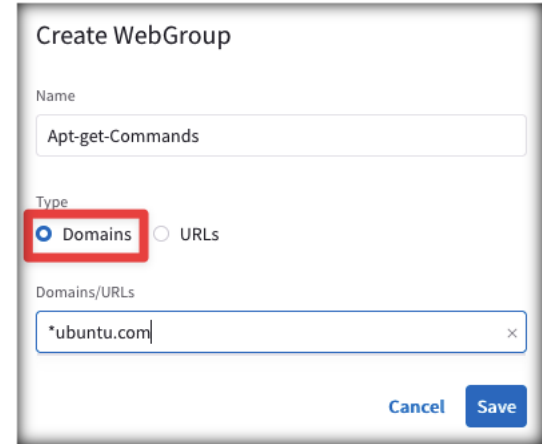
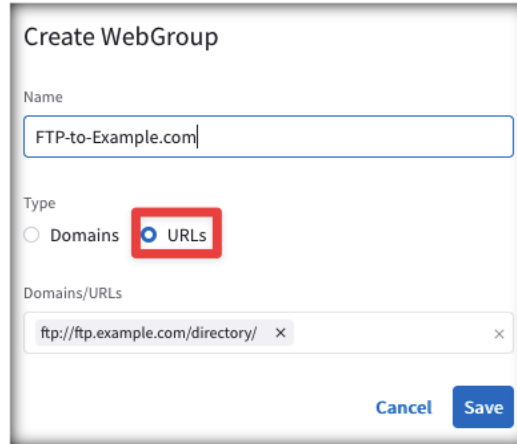
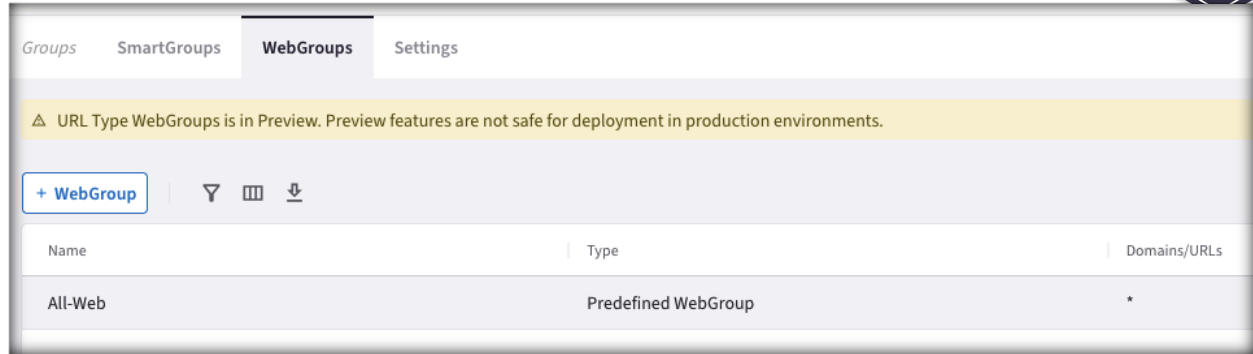


The screenshot shows the Aviatrix CoPilot interface. On the left is a dark sidebar with navigation options: CoPilot, Search, Dashboard, Cloud Fabric, Networking, Security, and Groups. The main content area has tabs for Groups, SmartGroups, WebGroups, and Settings. A yellow warning banner states: "URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments." Below the banner is a "+ WebGroup" button and icons for filter, list, and download. A table lists WebGroups with columns for Name, Type, and Domains/URLs. The "All-Web" entry is highlighted with a red box.

| 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).





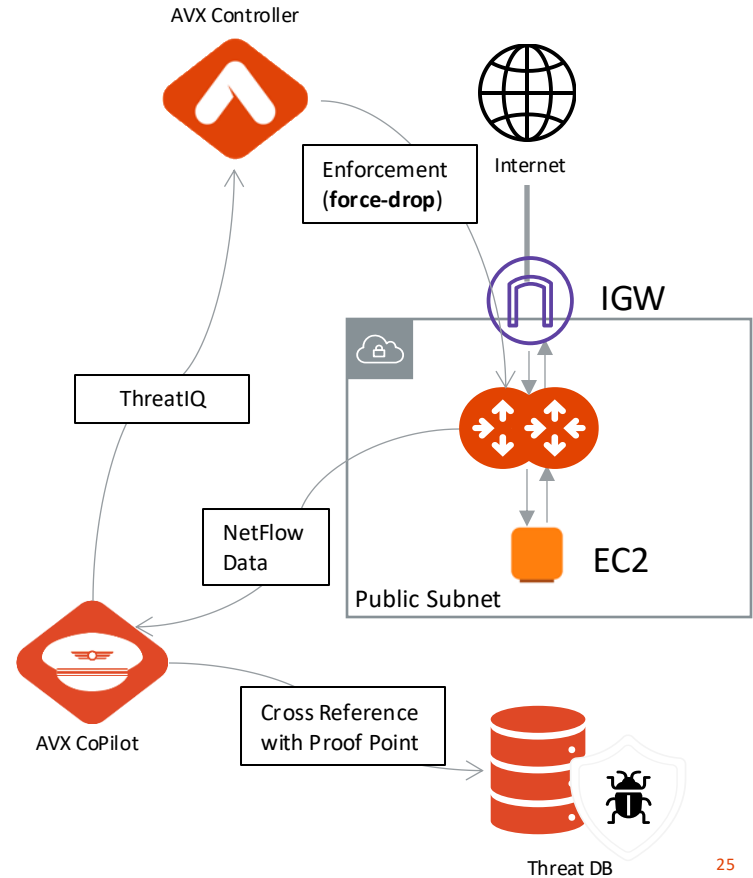


Aviatrix PSF GW(aka Public Subnet Filtering Gateway)

# Aviatrix PSF



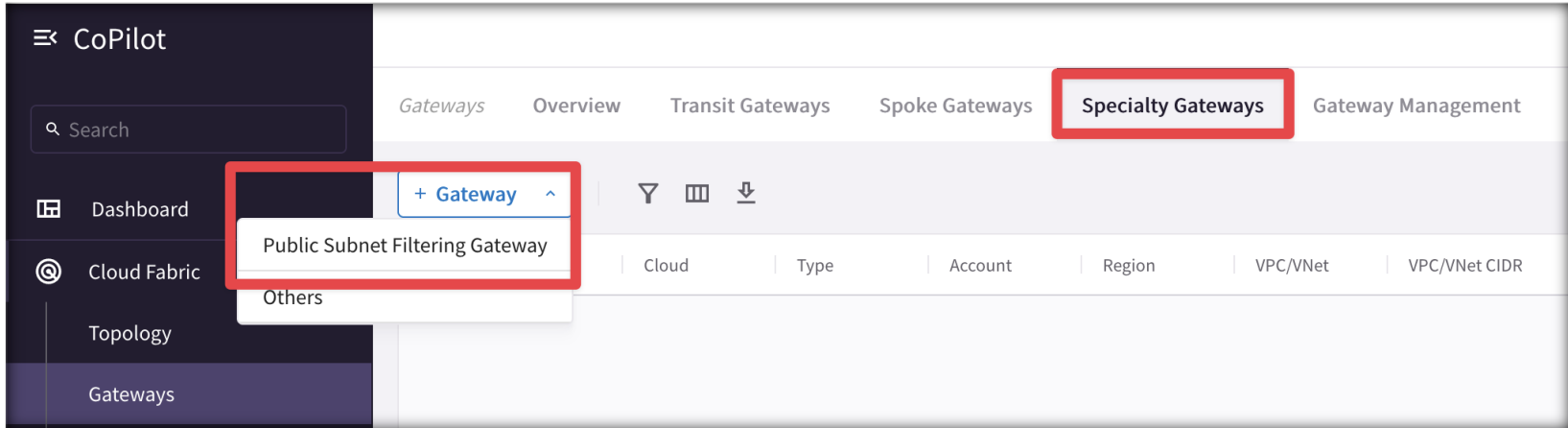
- Public Subnet Filtering Gateways (PSF gateways) provide ingress and egress security for **AWS** public subnets where instances have public IP addresses.
- After the Public Subnet Filtering (PSF) gateway is launched, view or block malicious IPs by activating **ThreatIQ**.
- The PSF gateway generates Netflow data, that is fed to FlowIQ.
- ThreatIQ monitors FlowIQ for any matches, and then alerts or programs a block (i.e. **force-drop**) on the corresponding gateway.



# 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**.



The screenshot shows the Aviatrix CoPilot interface. On the left is a dark sidebar with a search bar and navigation items: Dashboard, Cloud Fabric, Topology, and Gateways. The main area has a top navigation bar with tabs: Gateways, Overview, Transit Gateways, Spoke Gateways, **Speciality Gateways** (highlighted with a red box), and Gateway Management. Below the tabs is a '+ Gateway' button (highlighted with a red box) and a dropdown menu with 'Public Subnet Filtering Gateway' (highlighted with a red box) and 'Others'. Below the menu is a table with columns: Cloud, Type, Account, Region, VPC/VNet, and VPC/VNet CIDR.

# 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 gateway in a pass through manner.

**Create Public Subnet Filtering Gateway**

Name: AVX-London-PSG-GW

Cloud: aws Standard

Account: aws-account Region: eu-west-2 (London) VPC: AVX-LONDON-PROD4 Instance Size: t2.medium

| Attach to Unused Subnet     | Route Table   |
|-----------------------------|---|
| 1 10.1.4.128/26--eu-west-2a | <input type="checkbox"/> rtb-06d0b9443ad6311f5--AVX-LONDON-PROD4-Public-2-...<br><input type="checkbox"/> rtb-085b6f699282da882--AVX-LONDON-PROD4-Public-1-...<br><input type="checkbox"/> rtb-0e55de966a642304a--AVX-LONDON-PROD4-Public-3-... |

Select All

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



## Lab 5 – CLOUD PERIMETER SECURITY (Secure Cloud Egress)