



# Security

SOLUTIONS ENGINEERING

[www.aviatrix.com](http://www.aviatrix.com)

# Agenda

- Aviatrix Security Features Overview
- Securing Aviatrix Platform
- Egress
- Public Subnet Filtering Gateway

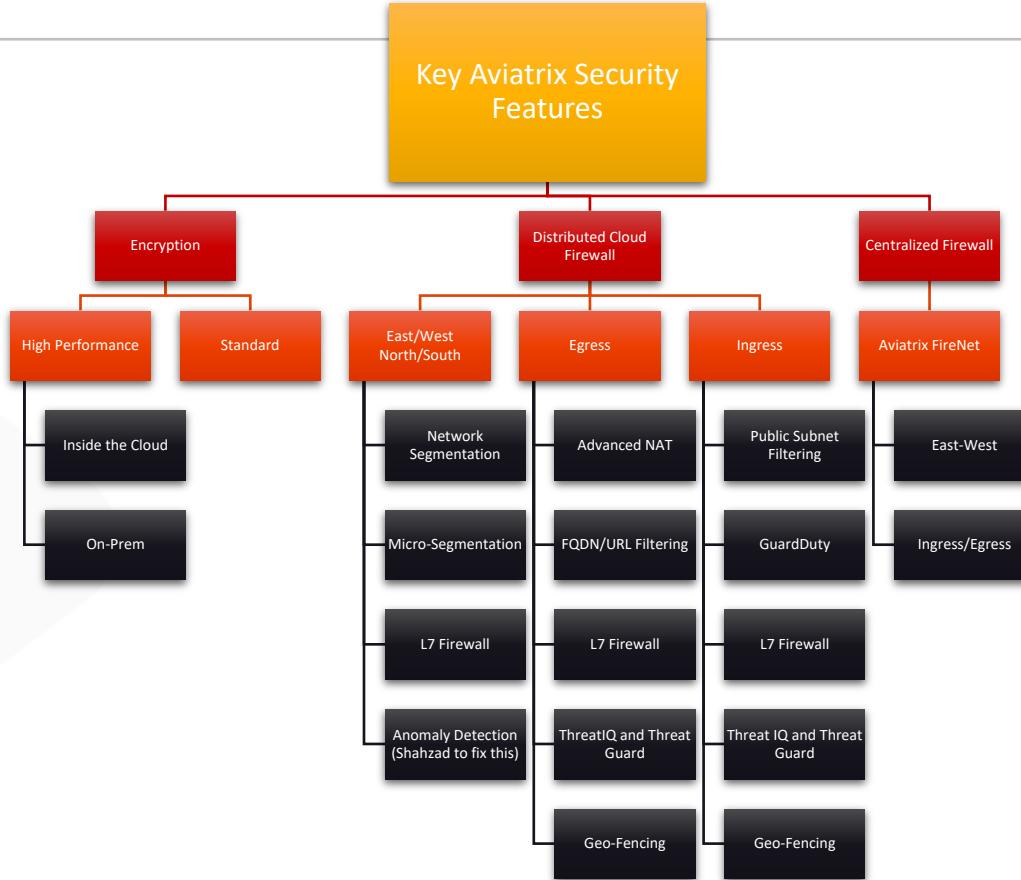
# Challenges for CISO, CIO/CTO and NetSec Architects

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

# Summary



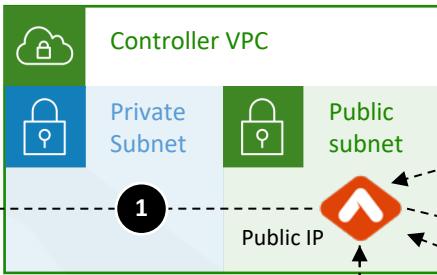


Built-in Security of the Aviatrix Platform

# Secure Aviatrix Infrastructure Deployment | Example in AWS & Azure



AWS Cloud

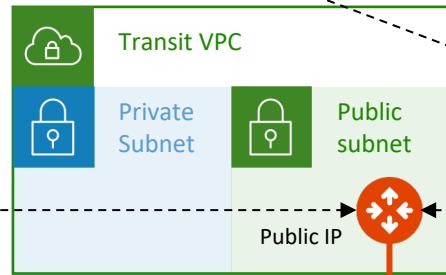
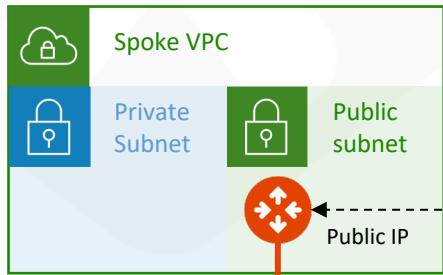


Traffic inside AWS Network Fabric

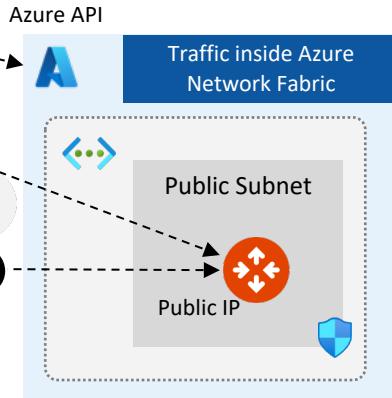


## Infra Security Controls

- Subnet monitoring & notification
- Automatic Security Group lockdown (Controller → GW, GW → GW)
- SAML-based RBAC with MFA



HPE via Private IP



Traffic inside Azure Network Fabric

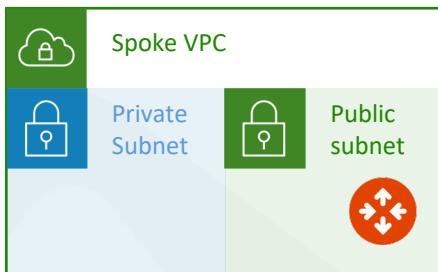
## Appliance Security

- OS Lockdown (hardened: no SSH, limited daemons, etc.)
- EBS Encryption
- FIPS, NESSUS, InfoSec Policy, Pen Testing
- Hitless software/security patching



# Monitor Gateway Subnets

Prevents unauthorized VMs from being launched in the same subnet as the gateways



Monitor Gateway Subnets [Info](#)

[ENABLE](#) [DISABLE](#)

Instances to Exclude

Enter instance Id to be excluded from monitoring separated by comma. Leave it blank if you do not have any. Click OK to finish.

[OK](#) [CANCEL](#)

Monitor Subnets feature has found and stopped user instance(s).

NR no-reply@aviatrix.com  
To

We removed extra line breaks from this message.

You enabled the Monitor Gateway Subnets feature on your Aviatrix controller.  
This feature monitors and stops any user instance that runs on the gateway subnets.

The following user instance(s) have been detected and stopped.

VPC ID	Region	Subnet ID	Instance ID
vpc-0cf9032aa9d742c10	ap-southeast-2	subnet-07ce84a5d56de1a4e	i-0f3adcf8937a6dc6

<https://docs.aviatrix.com/HowTos/gateway.html#monitor-gateway-subnet>

# Controller Security Group Management | Automatic Security Group lockdown

**Details**    **Security**

 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-0a8cce5ee8d489ee	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**

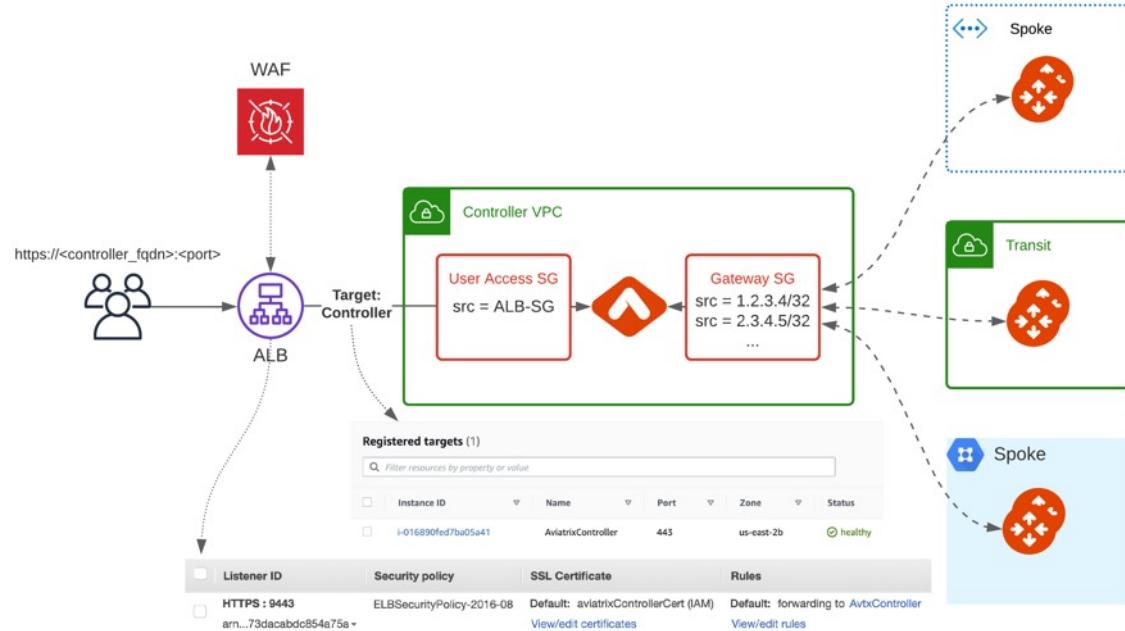
- Around alerts, operational features, logging integration, etc.
  - Putting an LB in front means Controller access can fit right into your existing operational model

- **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

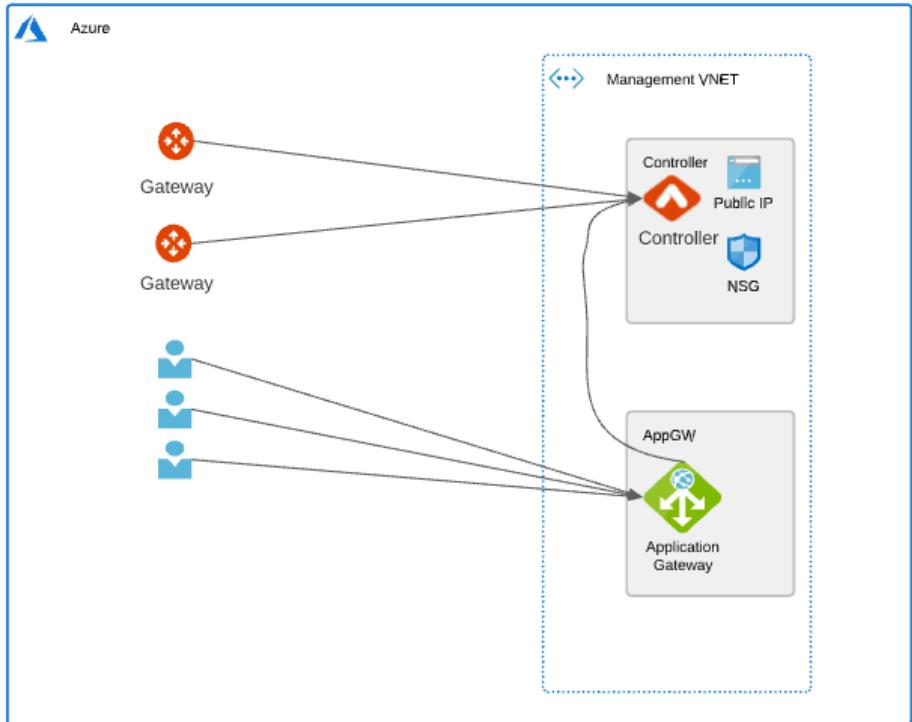
- Any access to controller, including API, UI login, etc., would go through LB, and the LB logging can provide easier, faster integration to existing tools

- Enable Controller Security Group Management to only allow access to the Controller EIP from Aviatrix Gateways
- 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



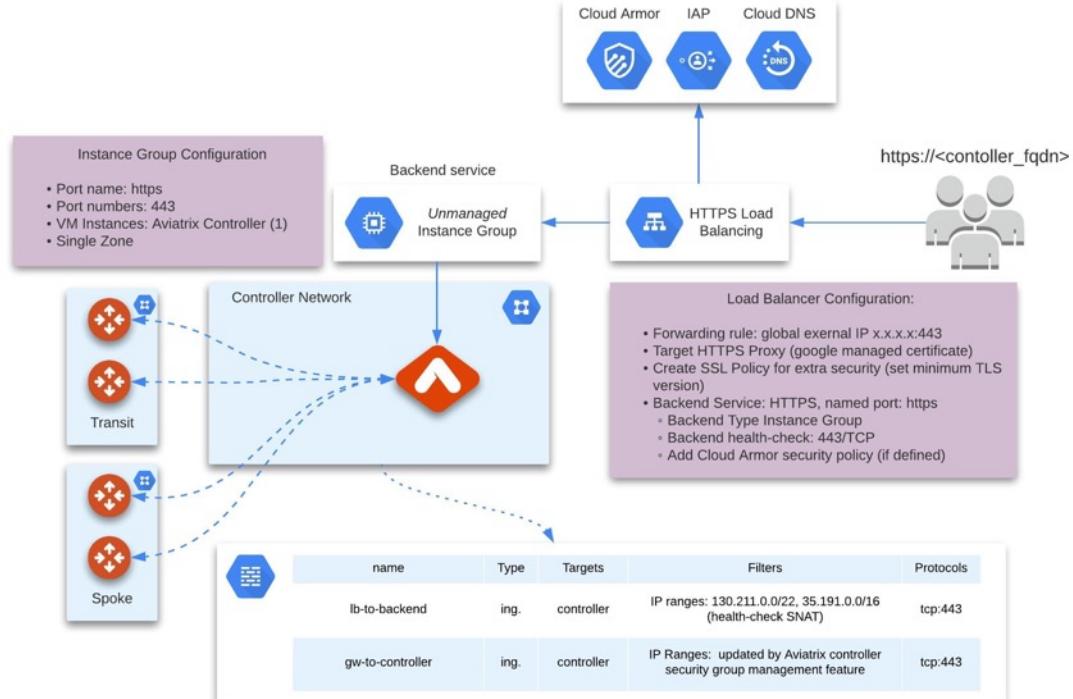
# Azure

- Use WAF with Azure Managed rules on Application Gateway to limit usual web hacks/attacks against Controller
- Only allow user access from the Application Gateway subnet to Controller on port 443 (Controller Security Groups management feature is a pre-requisite for gateway communication to Controller)
- Allow configuring user access on non-standard HTTPS listener port
- Terminate SSL connection on Application Gateway to leverage cloud native certificate management and WAF capability to inspect and log requests
- L7 health-check on the Controller



# GCP

- Create Cloud DNS public Zone for controller domain
- Create instance group and add controller to it
- Configure Cloud Armor Policy
- Create external HTTPS load-balancer
- Add Firewall rules to allow LB health-check to backend service from prefixes
  - 130.211.0.0/22
  - 35.191.0.0/16
- Set appropriate target Tag  
(matching Controller VM instance *network tag*)





Secure Egress

# Problem Statement

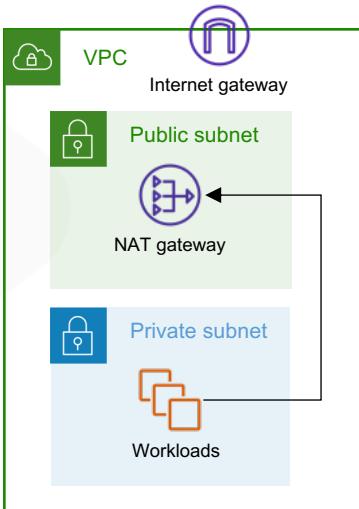
## Private workloads need internet access

- SaaS integration



### NAT Gateway

- NACLs management
- Layer-4 only



- Patching

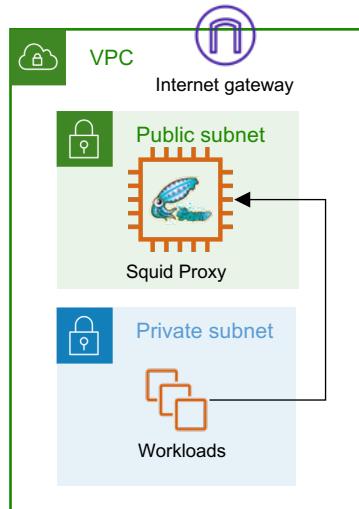


- Updates



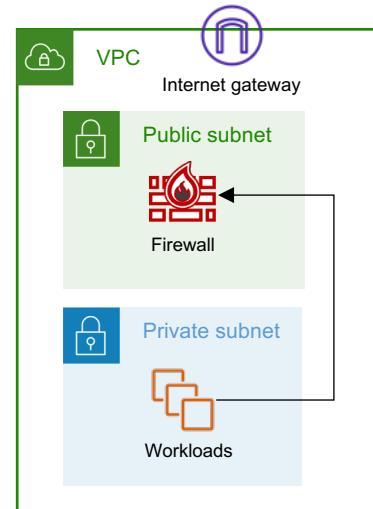
### Squid Proxy

- Hard to manage
- Scale and HA issues

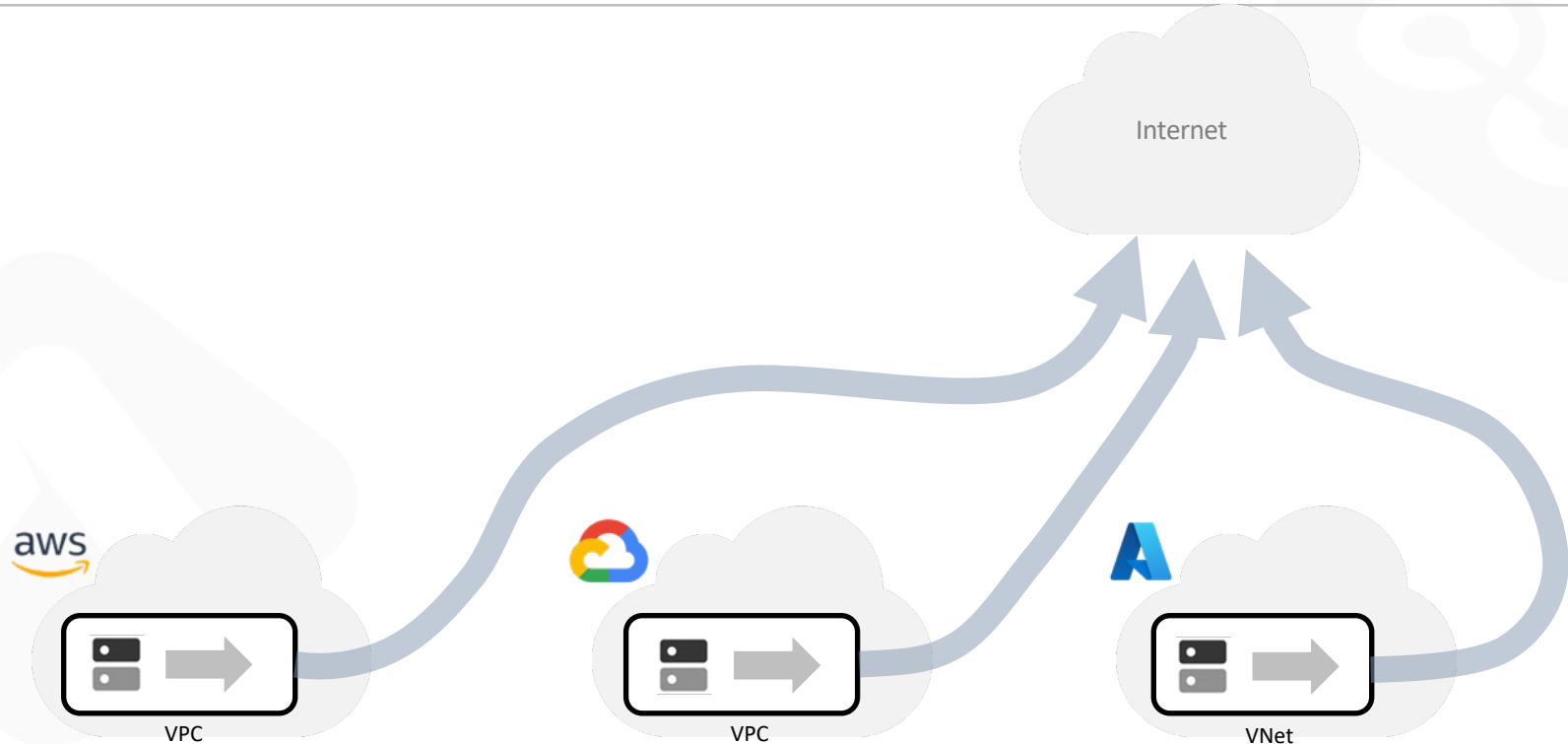


### Layer-7 Firewall

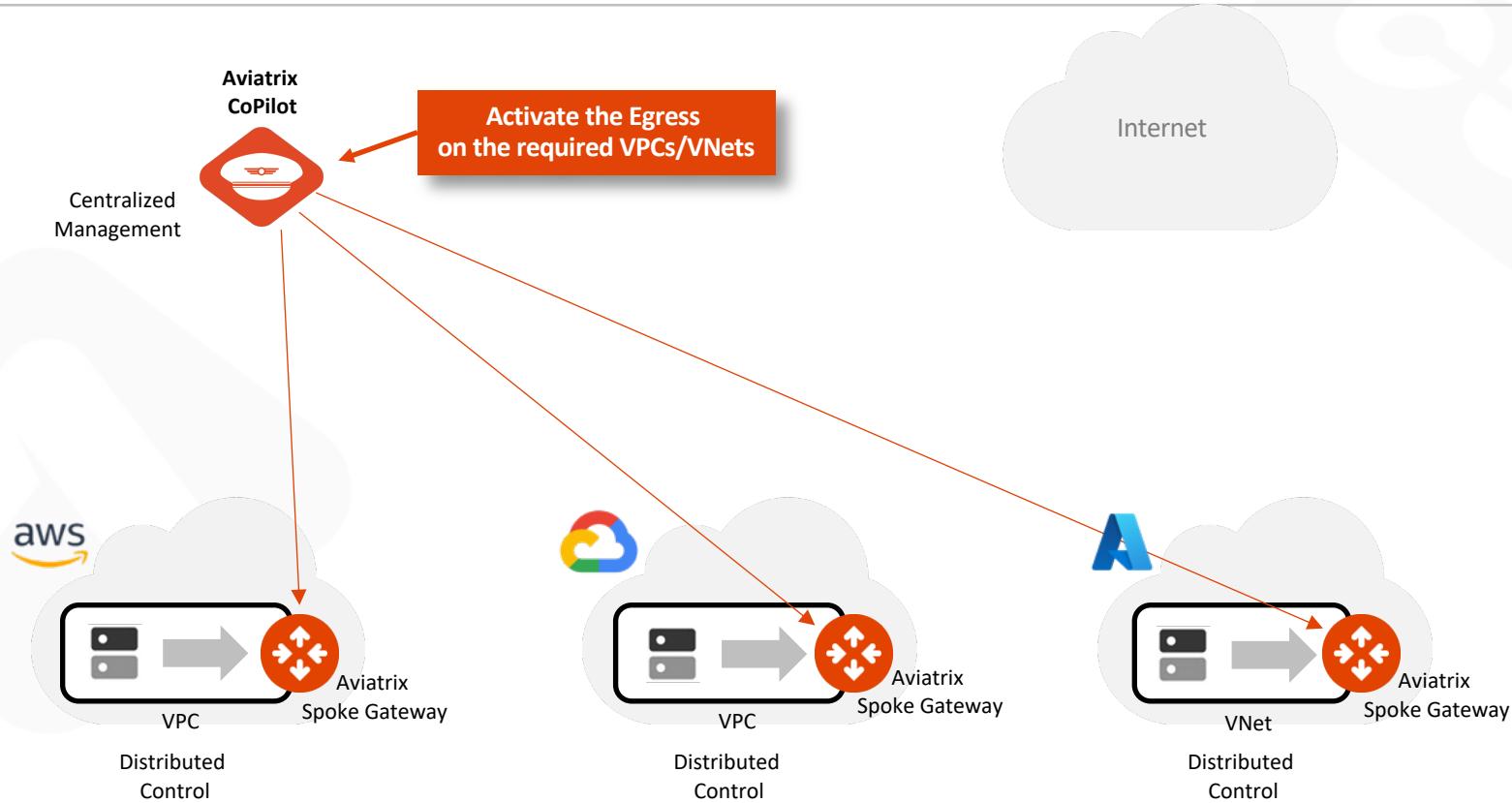
- Overkill
- Expensive



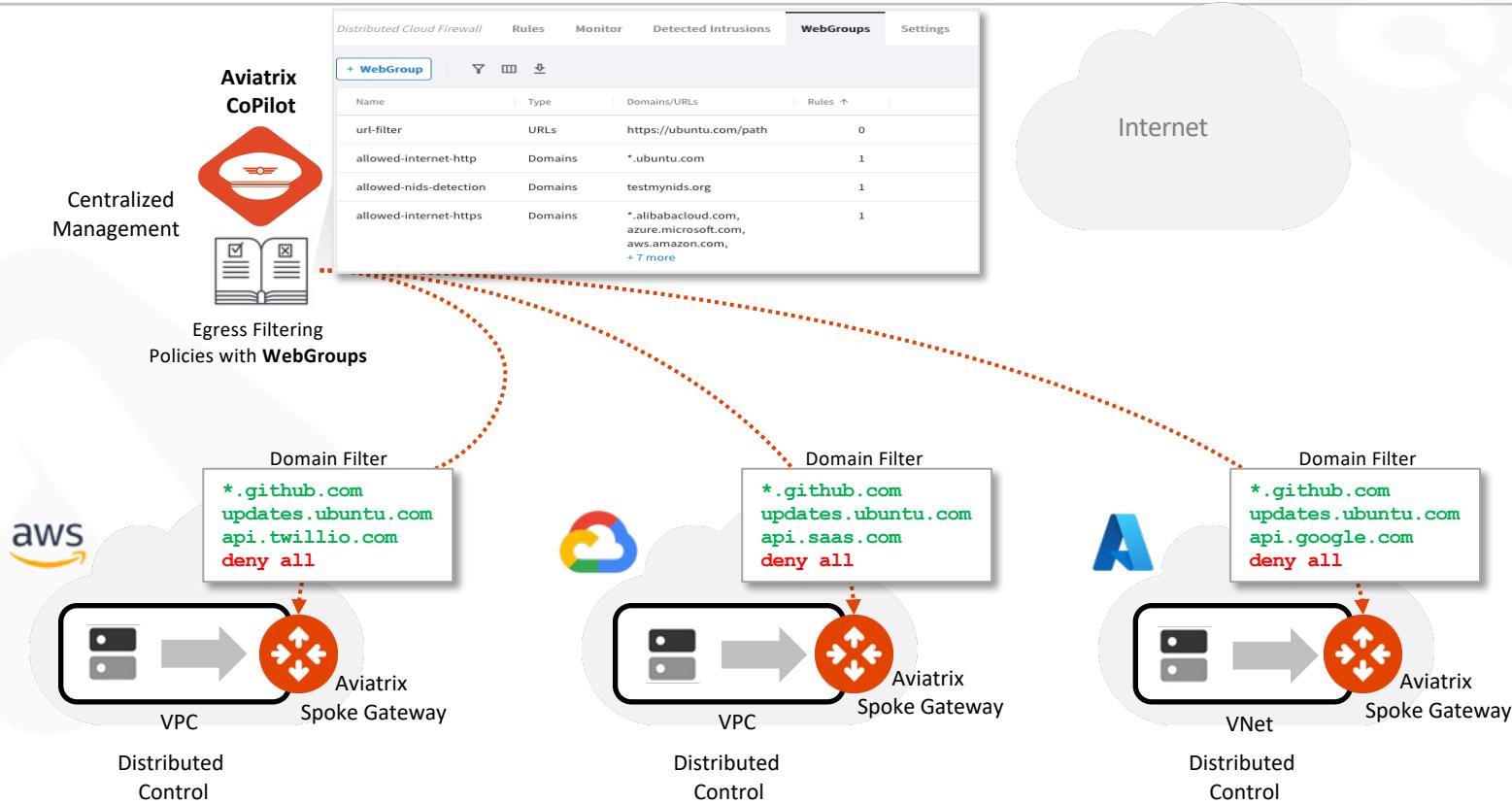
# Aviatrix Secure Egress Filtering Feature



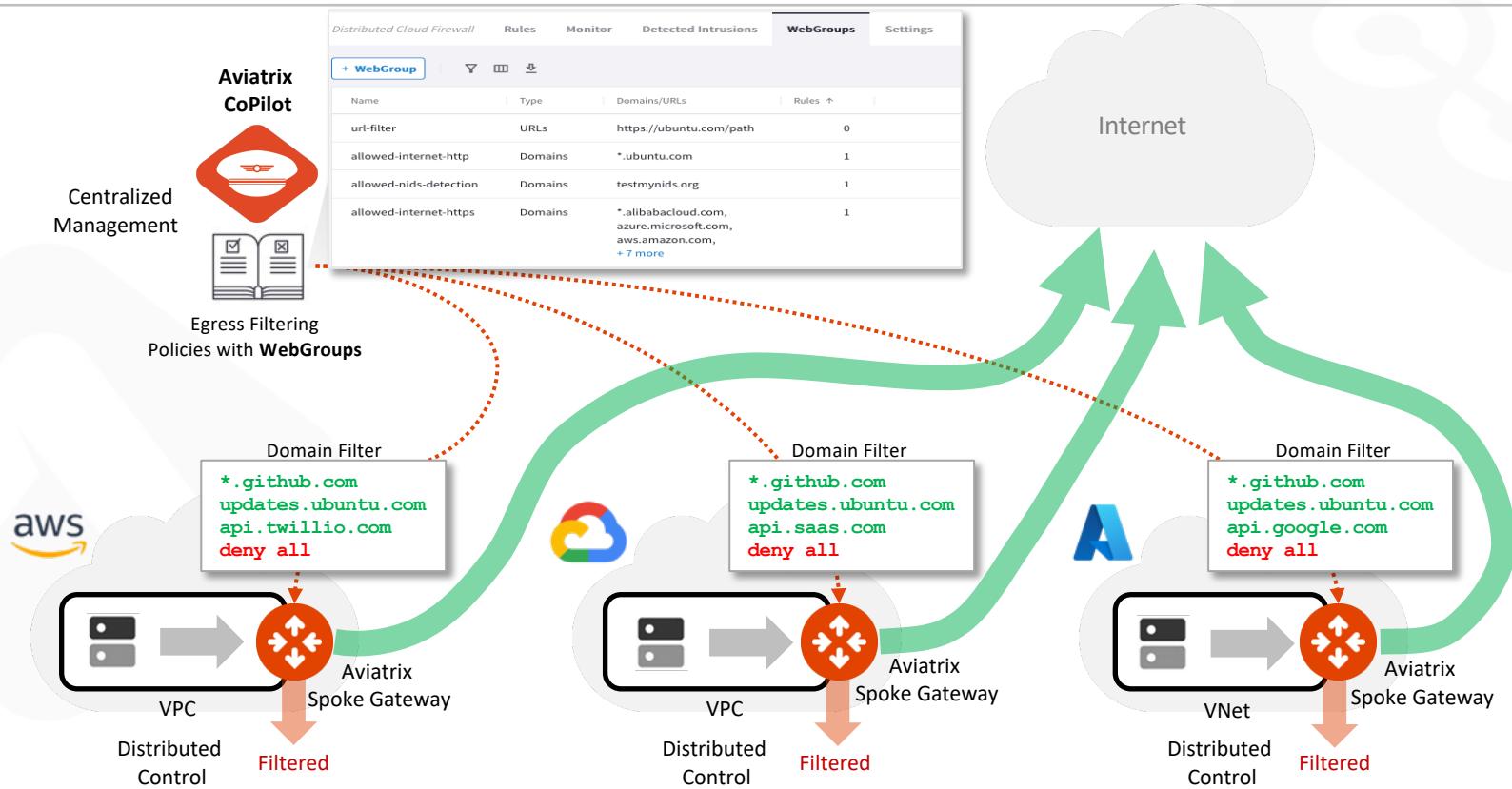
# Aviatrix Secure Egress Filtering



# Aviatrix Secure Egress Filtering

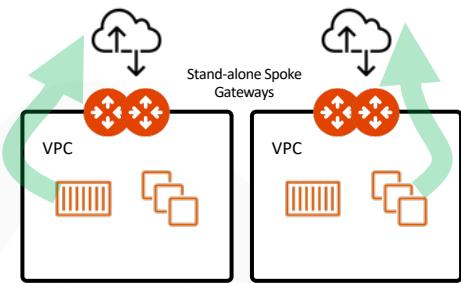


# Aviatrix Secure Egress Filtering

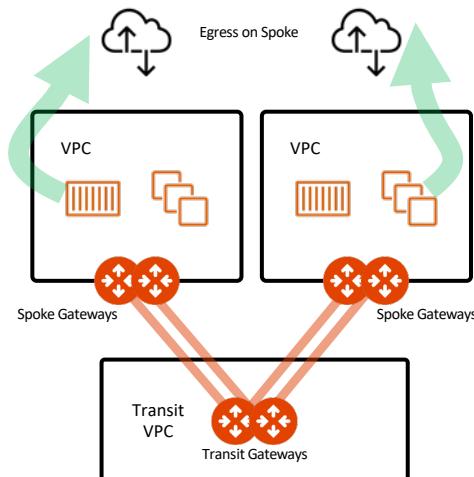


# Aviatrix Secure Egress Filtering Design Patterns

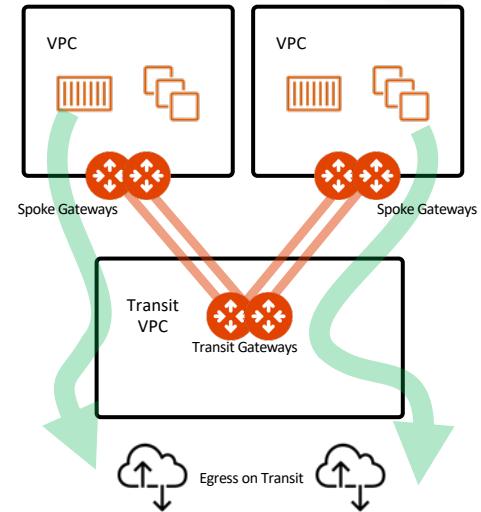
**Stand-alone Spoke GW  
(Distributed)**



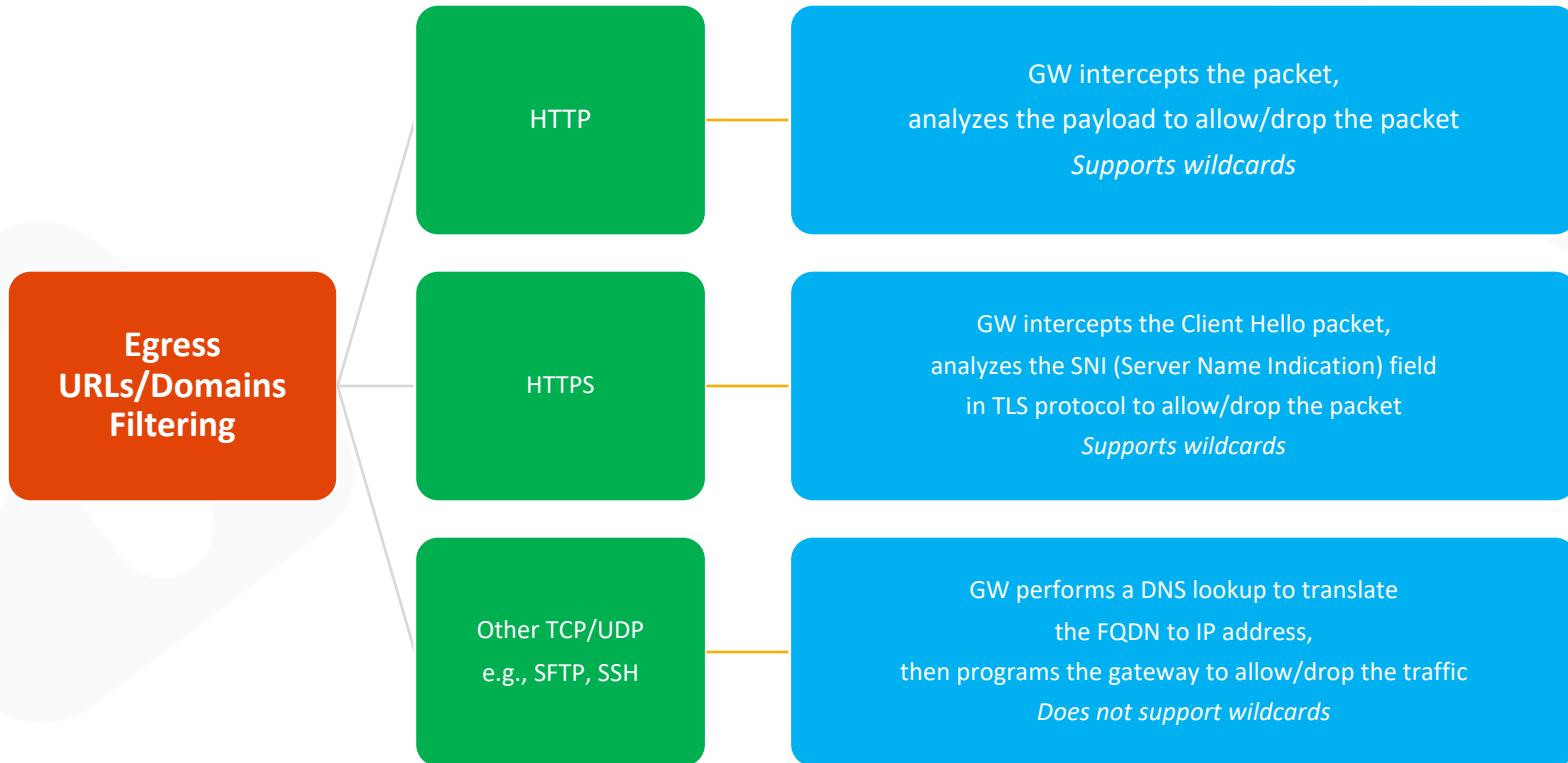
**Local Egress (Distributed)  
with Aviatrix Spoke GW**



**Centralized Egress  
with Aviatrix Transit GW**



# Egress FQDN Filter – Traffic Types



# 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 in the left sidebar. The main area displays a table of Egress configurations. A red box highlights the 'Egress VPC/VNets' tab in the top navigation bar, and another red box highlights the '+ Local Egress on VPC/VNets' button in the table header. The table lists five entries:

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**

VPC/VNet Route Tables		
Instances	Connections	Route DB
aws-us-east2-spoke1		
Route Table	Route Table ID	Associated Subnets
aws-us-east2-spoke1-Private-3-us-east-2c-rtb	rtb-0f555197f0c9f6d8f	1
<b>VPC/VNet Route Tables</b>		
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**

VPC/VNet Route Tables		
Instances	Connections	Route DB
aws-us-east2-spoke1		
Route Table	Route Table ID	Associated Subnets
aws-us-east2-spoke1-Private-3-us-east-2c-rtb	rtb-0f555197f0c9f6d8f	1
<b>VPC/VNet Route Tables</b>		
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 = Deny-List Model

- 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.

The screenshot shows the Avantix CoPilot interface. On the left is a sidebar with various options like Dashboard, Cloud Fabric, Networking, Security, and Distributed Cloud Firewall. The 'Distributed Cloud Firewall' option is highlighted with a red box. The main area has tabs for Rules, Monitor, Detected Intrusions, WebGroups, and Settings. The Rules tab is selected. In the center, there's a shield icon with a checkmark and a person icon, indicating the firewall is active. Below the icons, text states: 'Distributed Cloud Firewall provides granular network security controls for distributed applications in the cloud, and a centralized policy management across multiple clouds.' A blue button labeled 'Begin Using Distributed Cloud Firewall' is at the bottom, also with a red box around it. To the right, a large callout box titled 'Distributed Cloud Firewall' contains text: 'Enabling the Distributed Cloud Firewall **without configured rules will deny all** previously permitted traffic due to its implicit Deny All rule. To maintain consistency, a **Greenfield Rule** will be created to **allow** traffic that maintains the current state, facilitating the creation of custom rules for specific security needs.' At the bottom right of the callout are 'Cancel' and 'Begin' buttons.

Distributed Cloud Firewall		Rules	Monitor	Detected Intrusions	WebGroups	Settings	
		+ Rule	Actions				
Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
<input type="checkbox"/>	21474... 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 as *Source SmartGroup*, the SmartGroup that is identifying the private workloads affected by the Egress feature, previously enabled.
  - b) Attach as *Destination SmartGroup*, the Predefined SmartGroup "**Public Internet**".
  - c) Attach the Predefined **Any-Web** WebGroup.
  - d) Turn On the "**Logging**" 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 display on the **Monitor TAB**.

The screenshot shows the Avantix Distributed Cloud Firewall interface. The top navigation bar includes tabs for Rules, Monitor, Detected Intrusions, WebGroups, and Settings. Below this, the Rules tab is active, showing a list of rules. A red box highlights the "Discovery-Rule" entry, which has a green checkmark next to its ID (2147483644). Another red box highlights the "Greenfield-Rule" entry, which also has a green checkmark next to its ID (2147483645). The columns in the table include Priority, Name, Source, Destination, WebGroup, Protocol, Ports, Action, and SG Orchestrator.

Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	SG Orchestrator
2147483644	Discovery-Rule	AVX-FRANKFURT-PROD1	Public Internet	Any-Web	Any	All	Permit	
2147483645	Greenfield-Rule	Anywhere (0.0.0.0/0)	Anywhere (0.0.0.0/0)		Any		Permit	

The screenshot shows the "Create Rule" dialog box. At the top, a note states: "Rules will be applied only on AWS, AWS Gov, ARM, ARM Gov, and GCP". The "Name" field is set to "Discovery-Rule". The "Source SmartGroups" dropdown contains "AVX-FRANKFURT-PROD1". The "Destination SmartGroups" dropdown contains "Public Internet". The "WebGroups" dropdown is highlighted with a red box and contains "Any-Web". The "Protocol" dropdown is set to "Any" and the "Port" dropdown is set to "All". In the "Rule Behavior" section, the "Action" is set to "Permit", "Ensure TLS" is off, and "TLS Decryption" is off. The "Enforcement" toggle is on, and the "Logging" toggle is also on, highlighted with a red box. In the "Rule Priority" section, the "Place Rule" dropdown is set to "Above" and the "Existing Rule" dropdown is set to "Greenfield-Rule". A red box highlights both of these dropdowns. At the bottom right are "Cancel" and "Save In Drafts" buttons.

# Monitor

- On the Monitor section you can retrieve all the logs and therefore distinguish the domains that should be permitted from those 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 AWS CloudWatch Metrics Insights Monitor interface. The top navigation bar includes tabs for Egress, Overview, Monitor (which is highlighted with a red box), Egress VPC/VNets, and Transit Egress. Below the navigation is a 'Filters' section with a dropdown for 'Time Period' set to 'Last 24 Hours' (Dec 5, 2023 10:40 AM to Now). A 'VPC/VNets' filter is set to 'aws-us-east-2-spoke1'. The main area displays a table of log data with columns: Timestamp, Source IP, VPC/VNet, Domain, Port, Rule Match, and Action. The table lists several log entries from Dec 6, 2023, at 10:40 AM, showing traffic from source IP 10.0.1.10 to various domains (esm.ubuntu.com, security.ubuntu.com, us-east-2.ec2.archive.ubuntu.com, www.football.com, www.espn.com, www.wikipedia.com, www.aviatrix.com) on port 80, all categorized as 'Matched' and 'Allowed'. To the right of the table is a 'Top Rules Hit' section listing the most frequent domains: www.wikipedia.com (80), www.football.com (80), www.espn.com (80), www.aviatrix.com (80), us-east-2.ec2.archive.ubuntu.com (80), security.ubuntu.com (80), and esm.ubuntu.com (443), each with a count of 3.

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

# Predefined WebGroup: Any-Web

- When you navigate to **Security > Distributed Cloud Firewall > WebGroups**, a predefined WebGroup, *Any-Web*, has already been created for you. Edit the Greenfield-Rule:
  - 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 web interface. On the left is a dark sidebar with navigation links: CoPilot, Search, Dashboard, Cloud Fabric, Networking, Security (selected), and Distributed Cloud Firewall. The main area has a light background. At the top, there's a navigation bar with tabs: Distributed Cloud Firewall, Rules, Monitor, Detected Intrusions, WebGroups (which is underlined, indicating it's selected), and Settings. A yellow banner message reads: "⚠️ WebGroups is in Preview. Preview features are not safe for deployment in production environments. [Read more](#) about Aviatrix Feature Modes." Below the banner is a table with a header row: "Name" | "Type" | "Domains/URLs". There is one data row: "Any-Web" | "Predefined WebGroup" | "\*". Below the table are three icons: a plus sign for creating a new WebGroup, a magnifying glass for search, and a downward arrow for sorting.

# WebGroup Creation

- **WebGroups** are groupings of domains and URLs, inserted into Distributed Cloud Firewall rules, that filter (and provide security to) Internet-bound traffic.
- When you navigate to **Security > Distributed Cloud Firewall > WebGroups**, a predefined WebGroup, *Any-Web*, has already been created for you,
- URL: for anything else than HTTP/HTTPS
- Domains: for HTTP and HTTPS traffic

Distributed Cloud Firewall   Rules   Monitor   Detected Intrusions   **WebGroups**   Settings

⚠ WebGroups is in Preview. Preview features are not safe for deployment in production environments. [Read more](#) about Aviatrix Feature Modes.

Name	Type	Domains/URLs
Any-Web	Predefined WebGroup	*

+ WebGroup

Create WebGroup

Name

Type  Domains  URLs

Domains/URLs

**Cancel** **Save**

Create WebGroup

Name

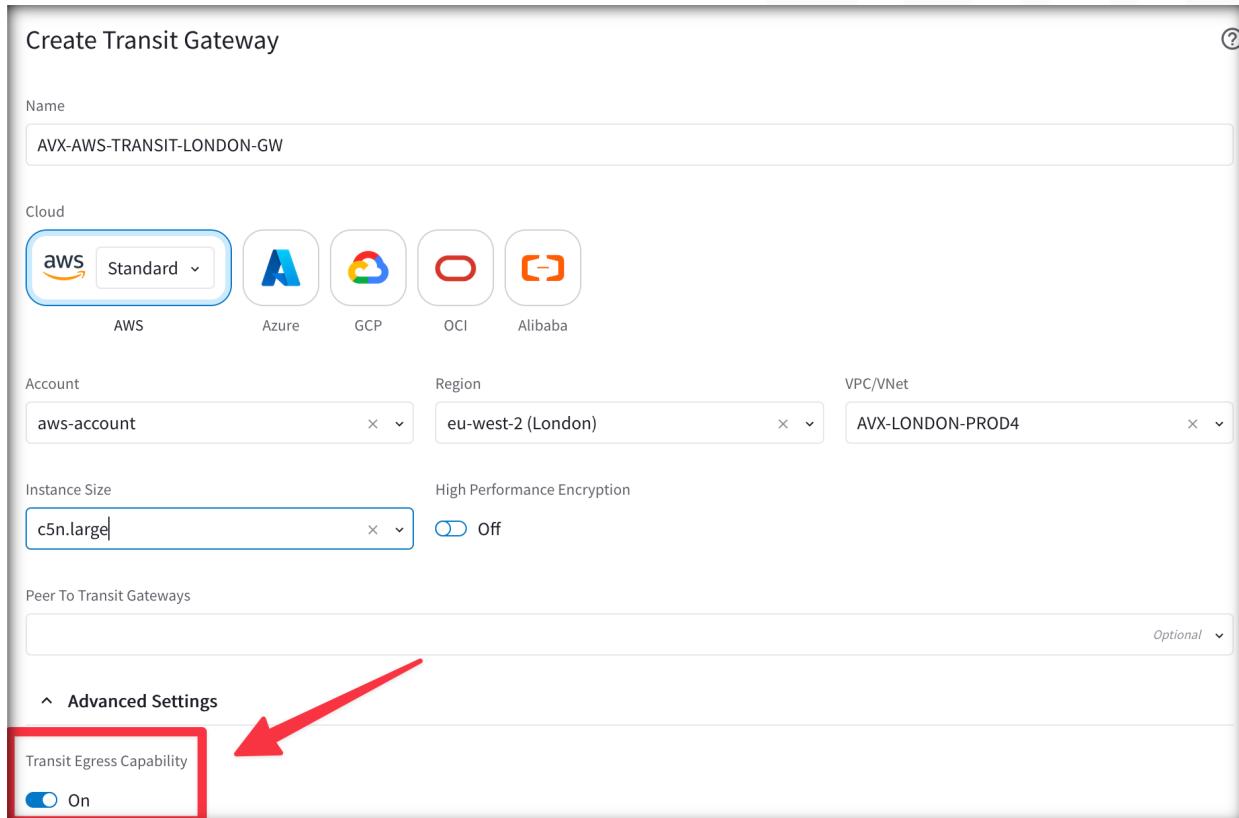
Type  Domains  URLs

Domains/URLs

**Cancel** **Save**

# Transit Egress Capability

- To add *Transit Egress Capability* to a Transit Gateway, set the corresponding toggle to **On**.
- Gateways that turn On Transit Egress Capability are now ready to have attachments added (FireNet or Transit Egress).
- For Azure and GCP, selecting **Transit Egress Capability** must occur when the gateway is created. Otherwise, it will not display as an available Transit Gateway when adding FireNet or Transit Egress to a Transit Gateway.
- CAVEAT: all clouds except OCI and Alibaba.

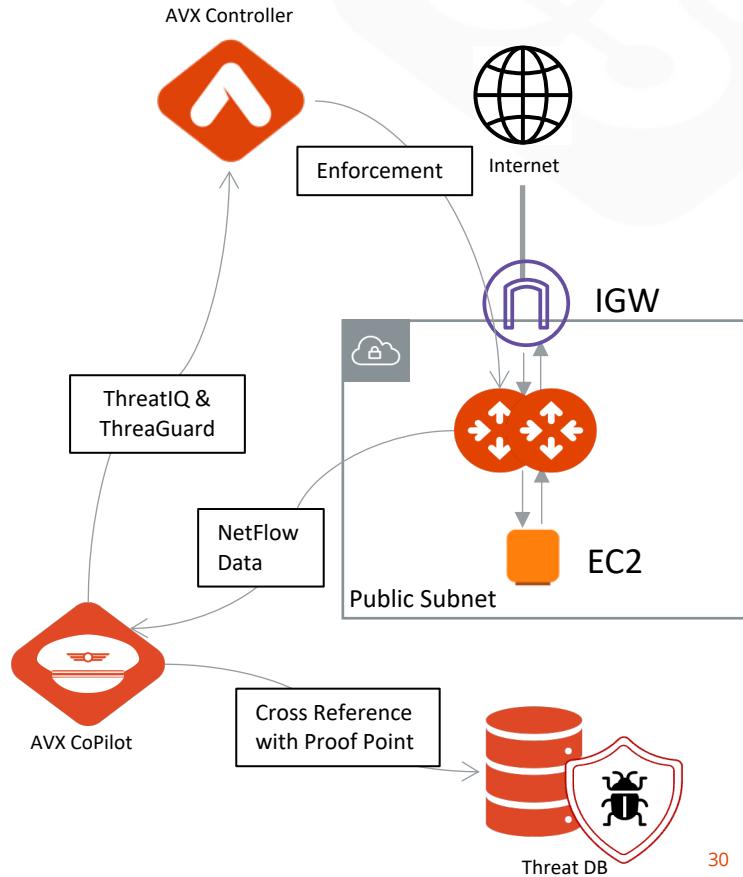




Aviatrix PSF GW(aka Public Subnet  
Filtering Gateway)

# Aviatrix PSF

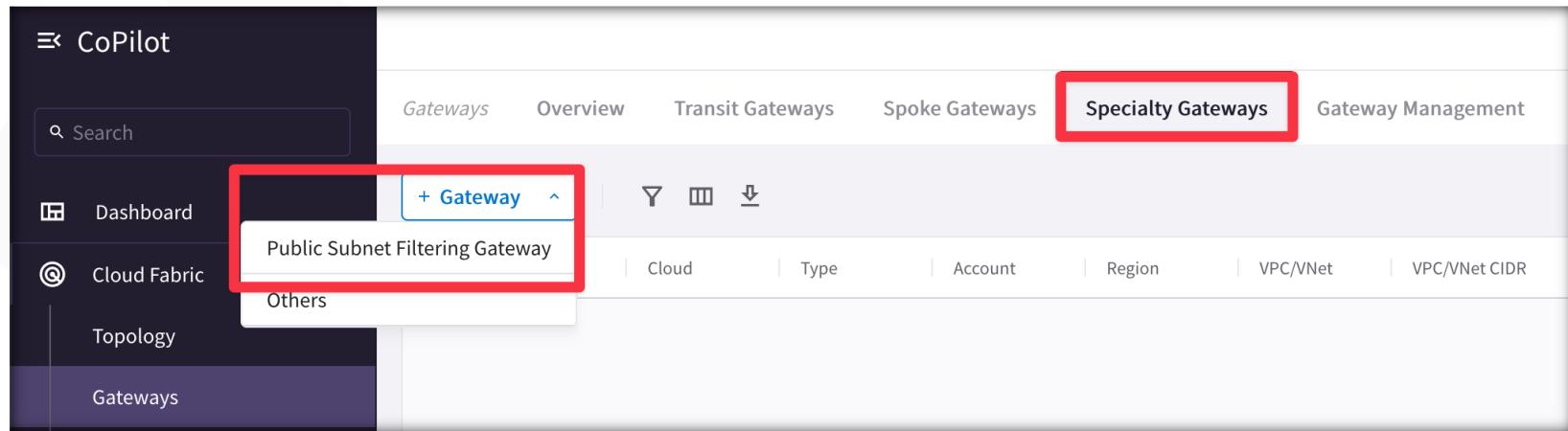
- Public Subnet Filtering Gateways (PSF gateways) provide ingress and egress security for **AWS** public subnets where instances have public IP addresses.
- After the Public Subnet Filtering (PSF) gateway is launched, view or block malicious IPs by activating **ThreatIQ**.
- The PSF gateway generates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



# Aviatrix PSF Deployment Workflow (part.1)

To deploy a Public Subnet Filtering Gateway:

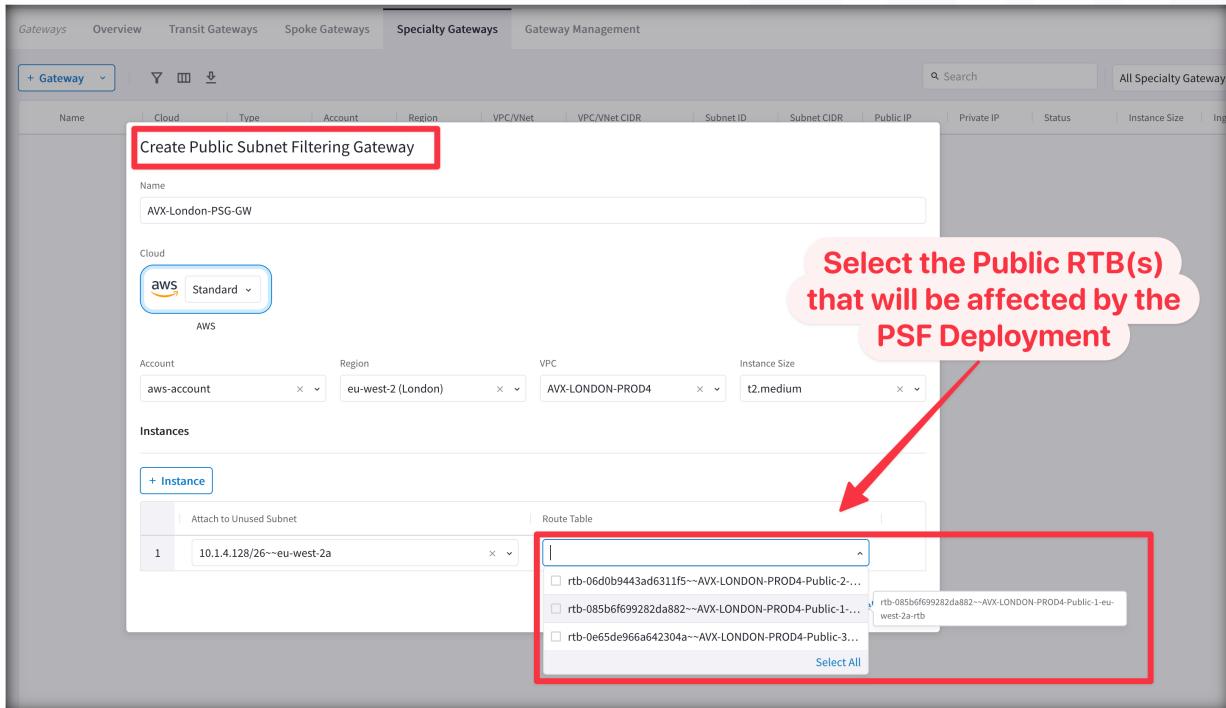
1. In CoPilot, navigate to **Cloud Fabric** > **Gateways** > **Speciality Gateways** tab.
2. Click **+Gateway** and select **Public Subnet Filtering Gateway**.



# 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.





## Lab 6 – Egress