



Security

ACE Solutions Architecture Team





Agenda

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

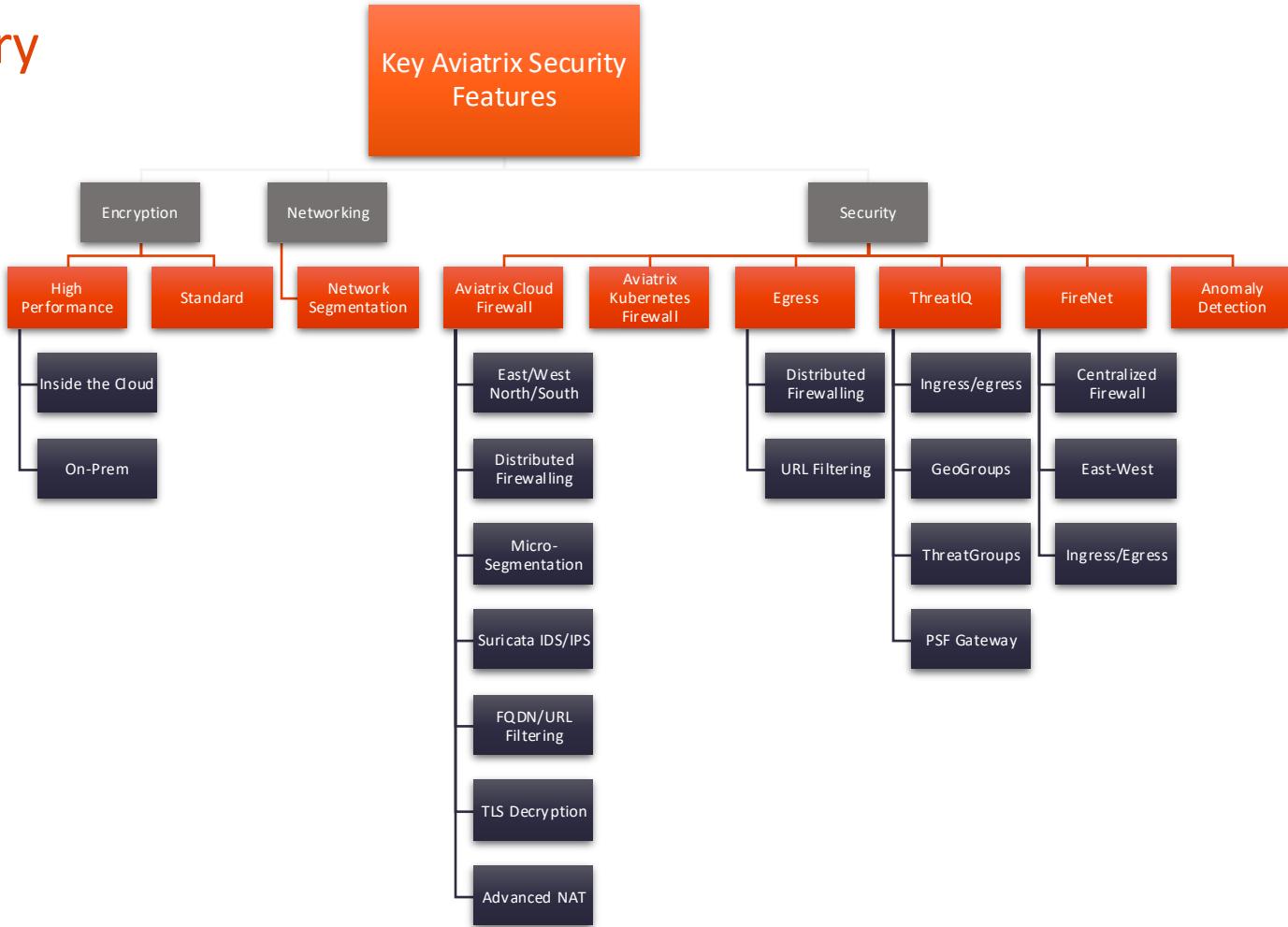
Challenges for CISO, CIO/CTO and NetSec Architects

- 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



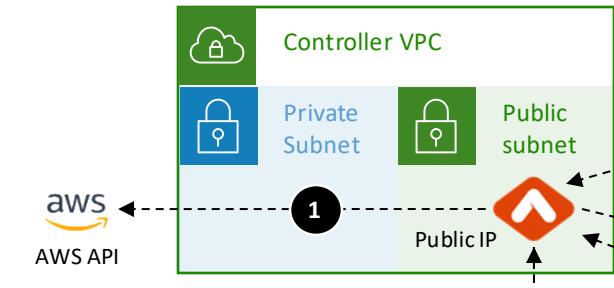


Built-in Security of the Aviatrix Platform

Secure Aviatrix Infrastructure Deployment | Example in AWS & Azure



AWS Cloud

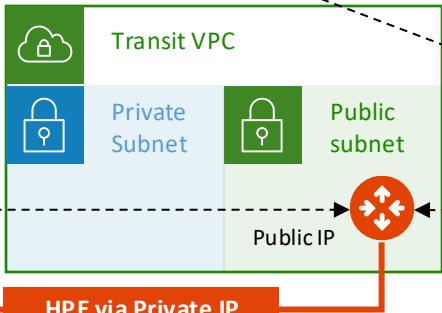
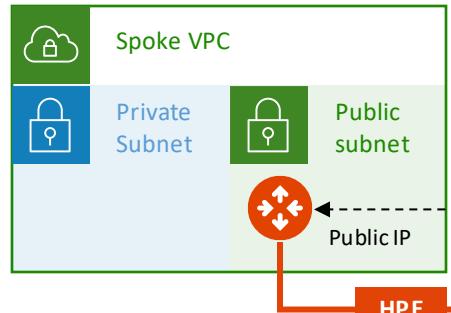


Traffic inside AWS Network Fabric



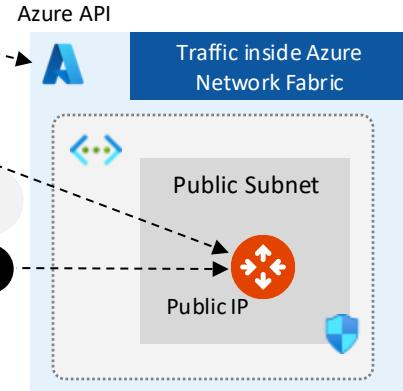
Infra Security Controls

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



Appliance Security

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

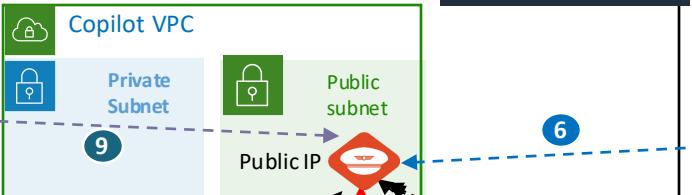


AWS Cloud



Logging/
Audit/
Network
Insight
API

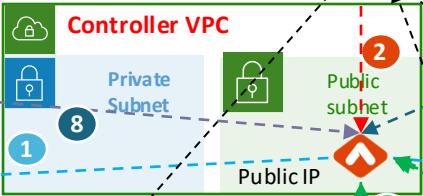
Prometheus
Logstash
Splunk
SumoLogic
Rsyslogic



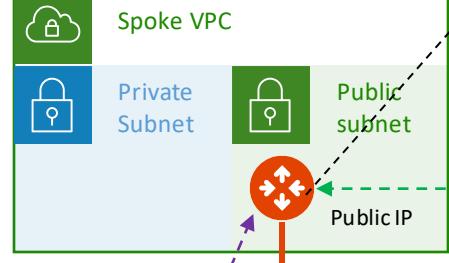
MFA

Duo
Okta
SAML
LDAP etc.

aws API

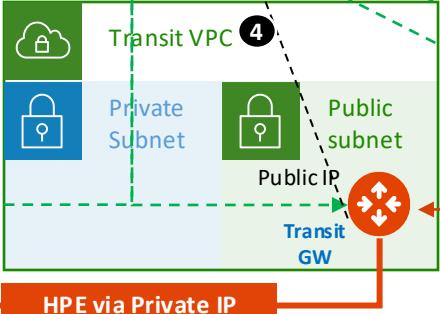


Spoke VPC



On Prem DC/
Branch Office/
B2B Partner

HPE



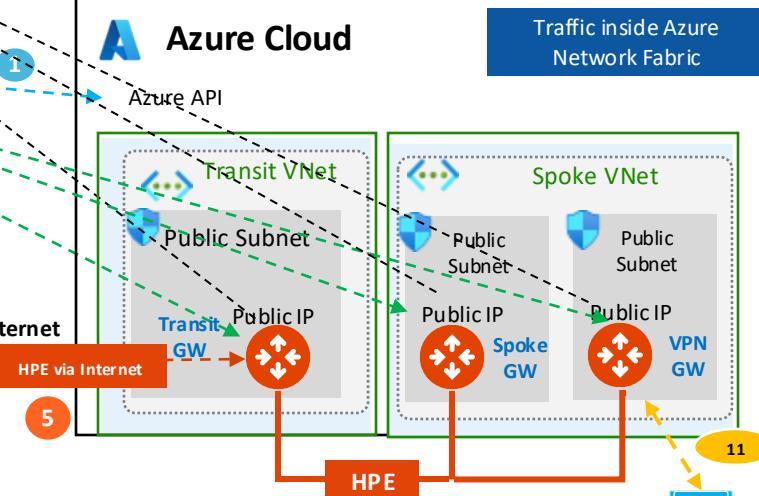
HPE via Private IP

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

Azure Cloud

Traffic inside Azure Network Fabric



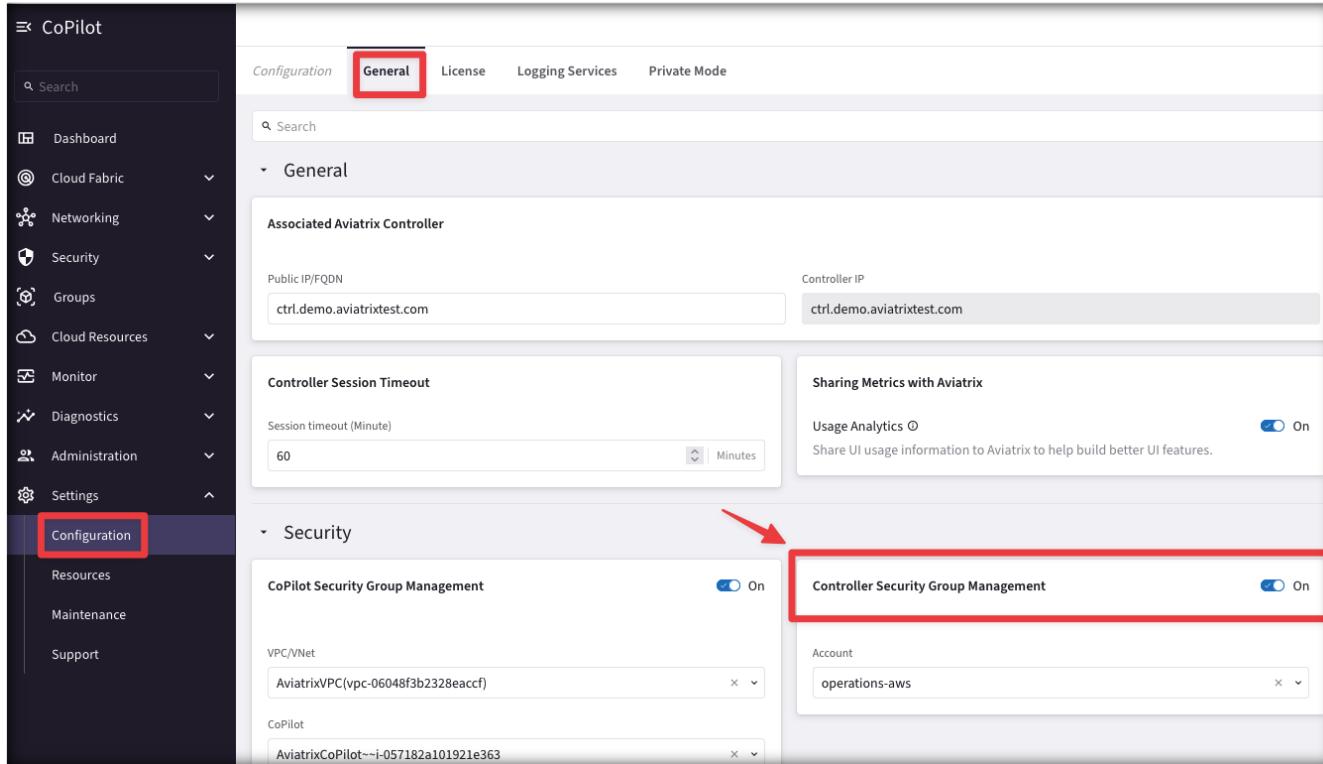
Remote User



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. Under the 'General' section, there is a 'Controller Security Group Management' toggle switch which is turned 'On'. A red box highlights this switch, and a red arrow points from the text below 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.

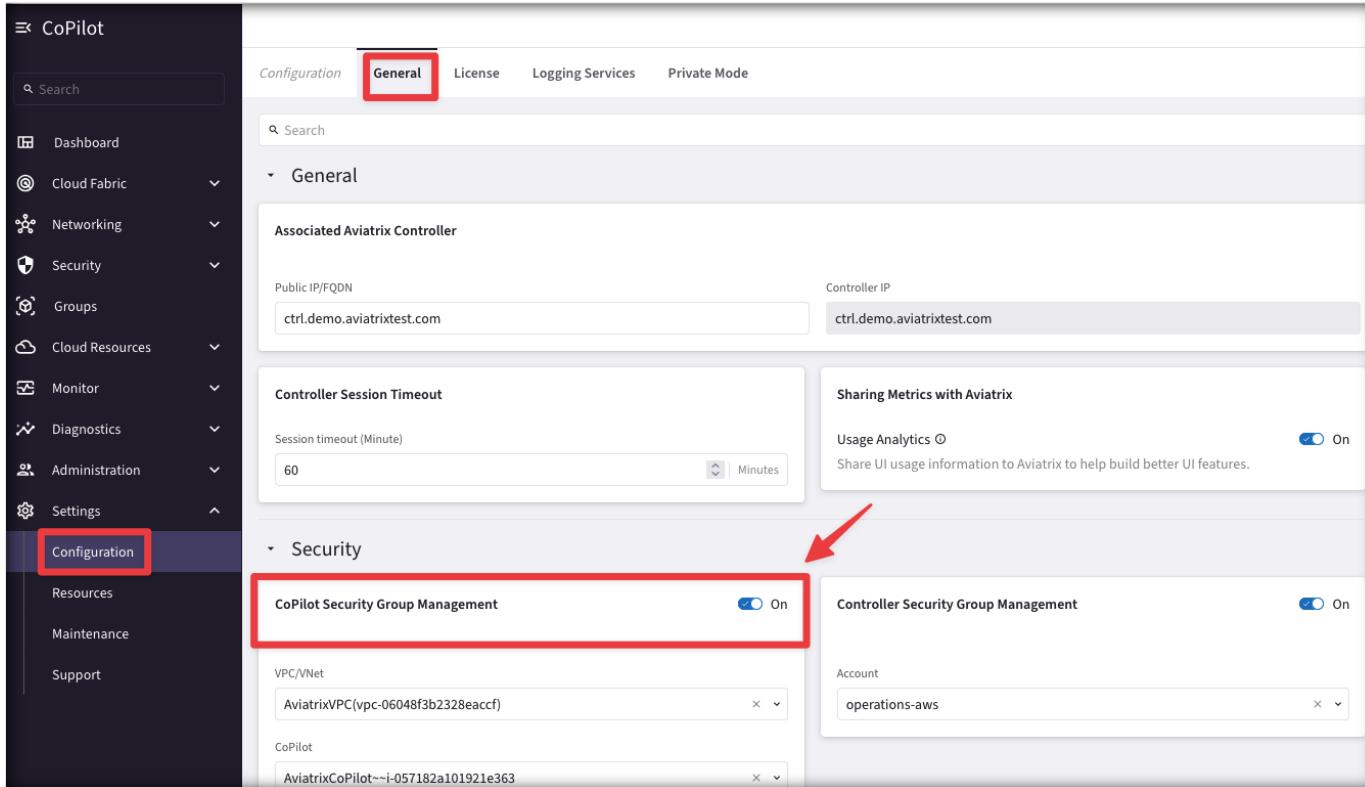
The Controller adds rules to the security group for each gateway IP for the following:

- 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 header has a 'General' tab highlighted with a red box. The 'General' section contains fields for 'Associated Aviatrix Controller' (Public IP/FQDN: ctrl.demo.aviatrixtest.com, Controller IP: ctrl.demo.aviatrixtest.com) and 'Controller Session Timeout' (Session timeout: 60 minutes). The 'Sharing Metrics with Aviatrix' section has an 'On' toggle switch. The 'Security' section is expanded, showing the 'CoPilot Security Group Management' toggle switch set to 'On' (also highlighted with a red box), and the 'Controller Security Group Management' toggle switch also set to 'On'. A red arrow points from the 'CoPilot Security Group Management' section towards the 'Controller Security Group Management' section.

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



Securing the Platform with Cloud Native Load Balancers

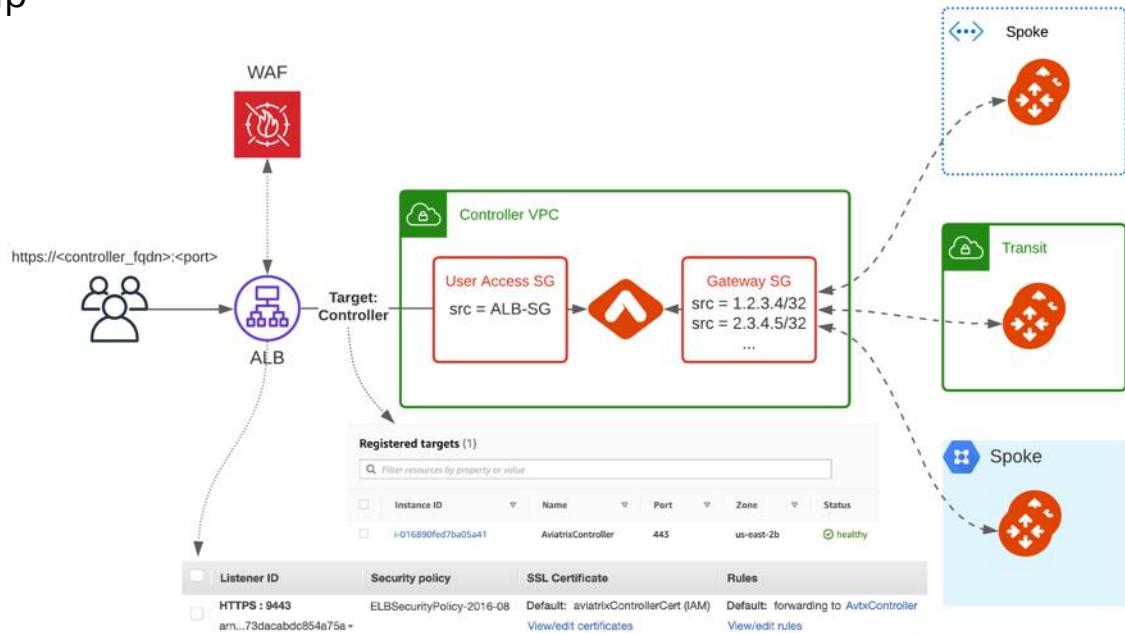


Problem Statement

- 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

- 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



- Patching



- Updates



Understanding the Pain

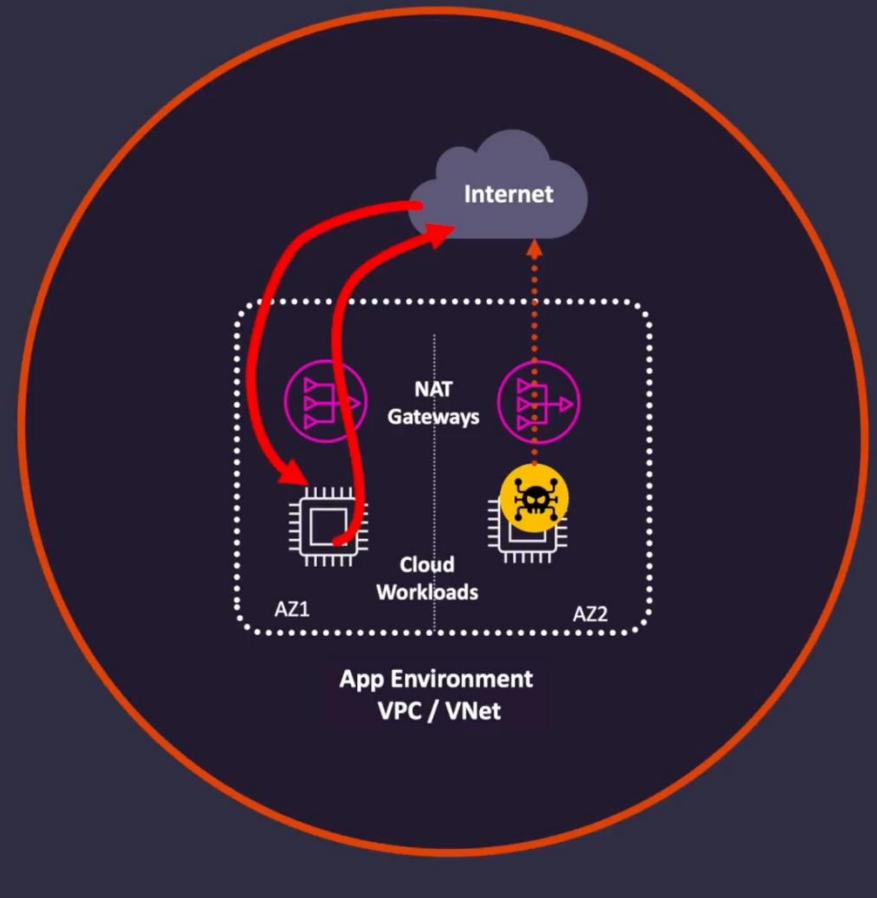
Improve Security and Lower Cloud Costs

- **Business Pain**

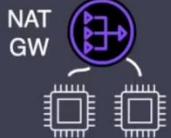
- Excessive Cloud Costs
- Lack of Compliance & Governance
- Risk to Business-Critical Workloads
- Regulatory Fines and Penalties
- Brand Health and Customer Trust

- **Technical Pain**

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



Two Common Paths



VPC / VNET



VPC / VNET



Flow Logs


Analytics

1. Distributed Cloud Provider Services

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

DARK
READING

Secure your 2025
Marketing Dollars Today

LEARN MORE

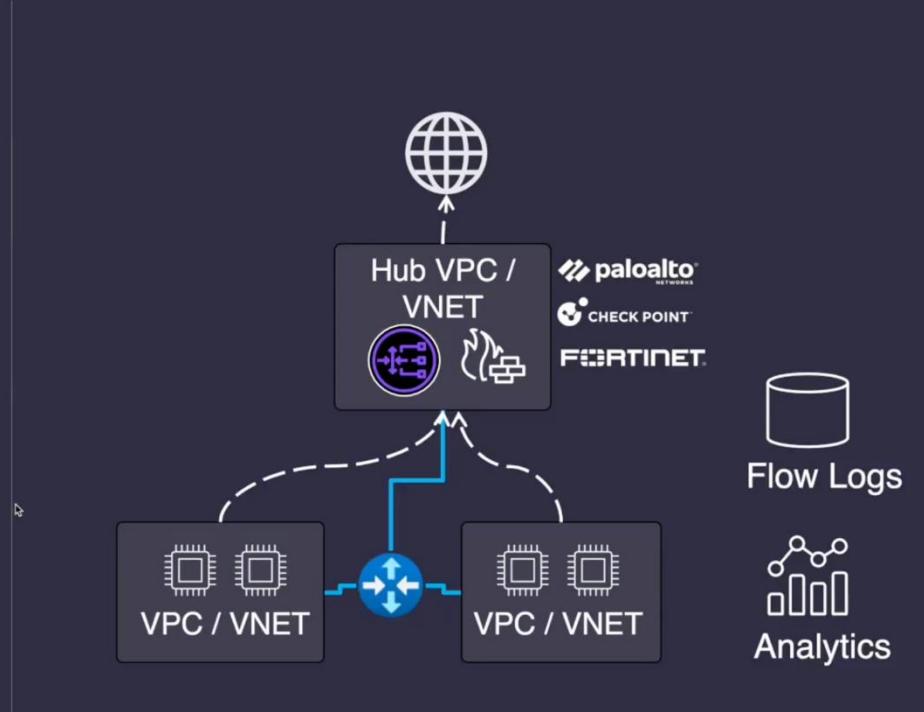
CyberRatings.org Announces Test Results for Cloud Service Provider Native Firewalls

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



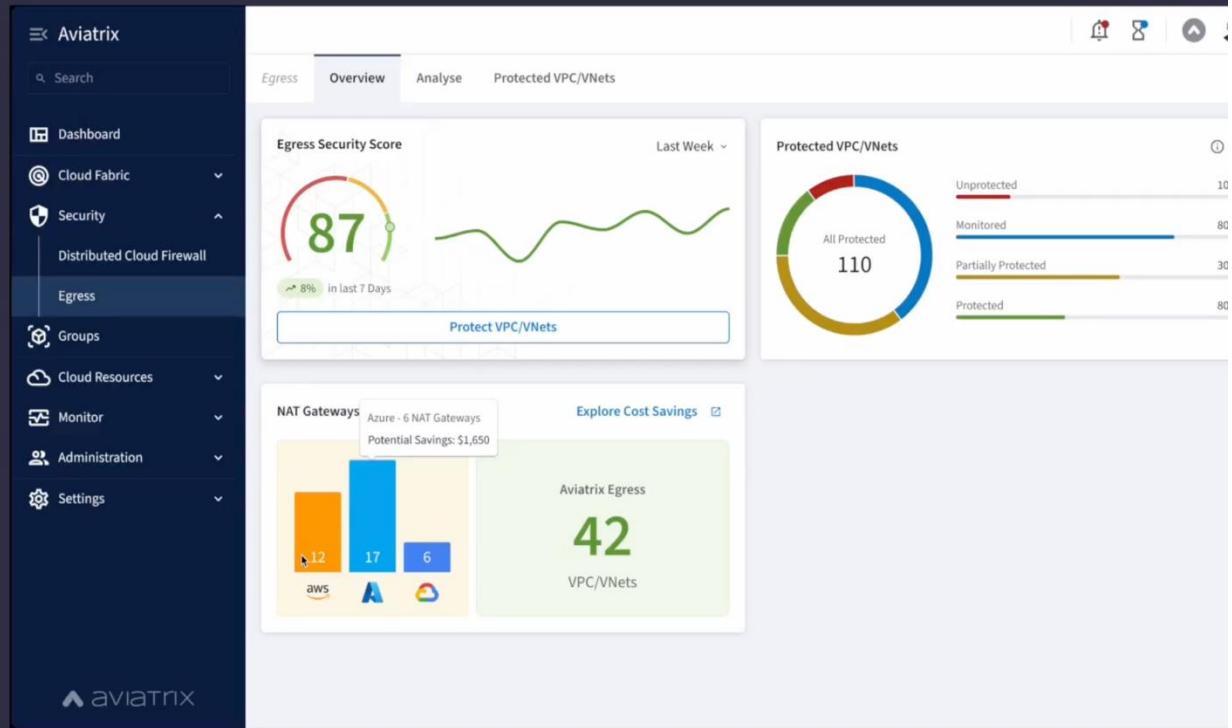
Aviatrix Cloud Firewall

What it is:

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

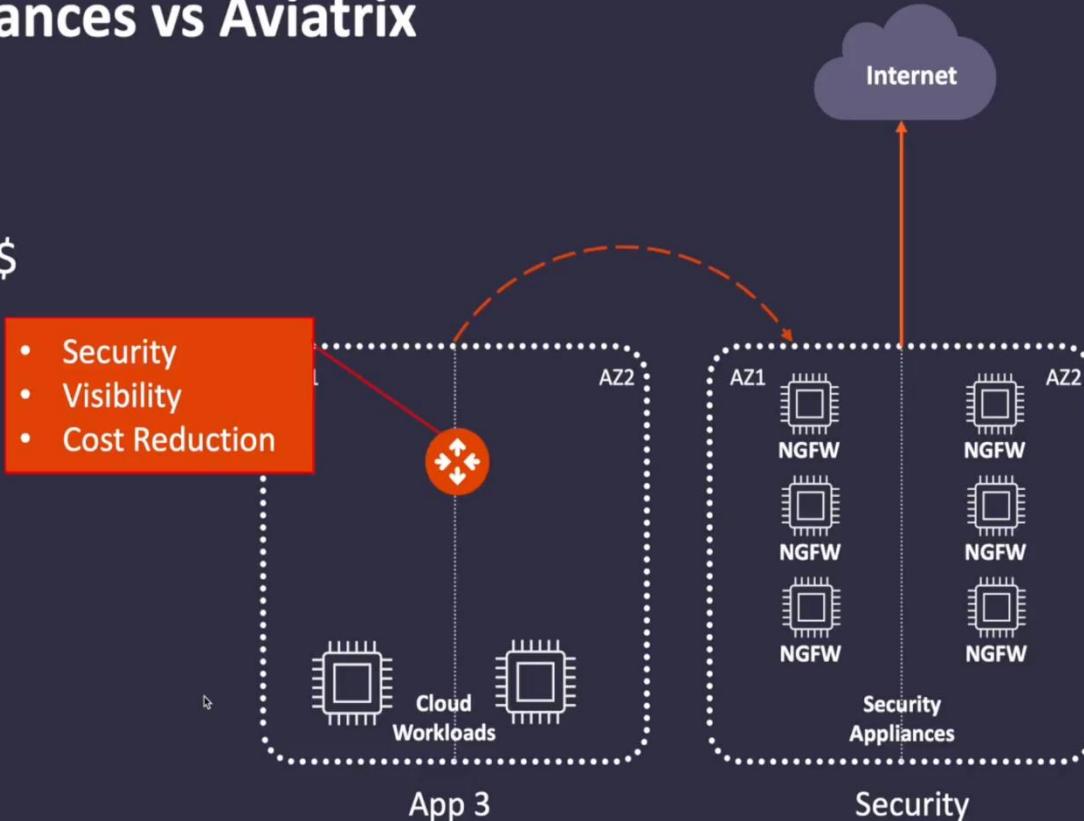
What you get:

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



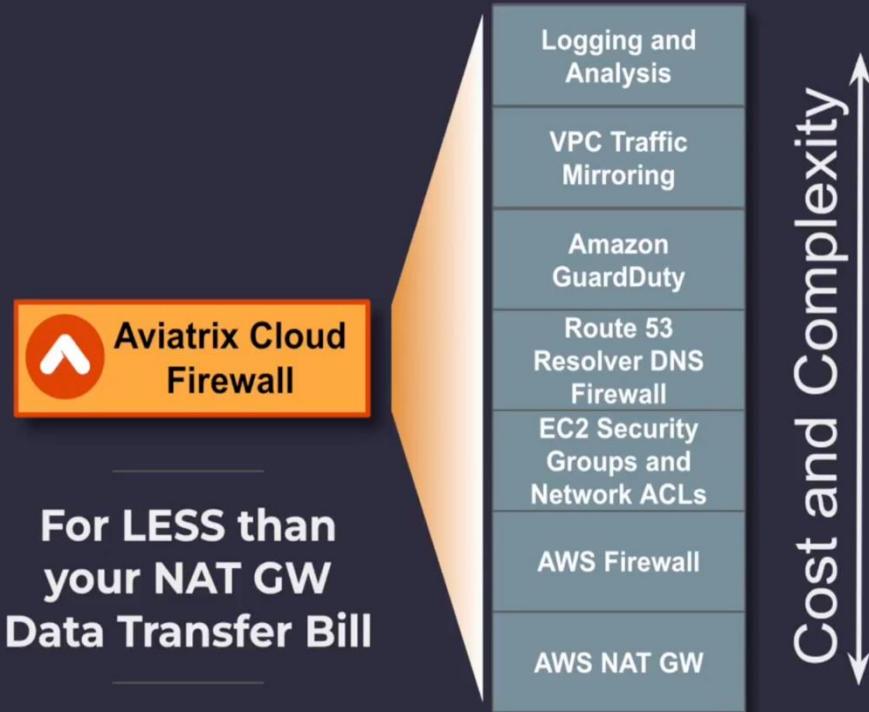
Central Virtualized Appliances vs Aviatrix

- Reduce Data Transfer Costs:
 - Enforcement at the Workload
- Reduced Data Transfer Costs \$\$\$
- Reduced Route Complexity
- Reduced Operational Pain



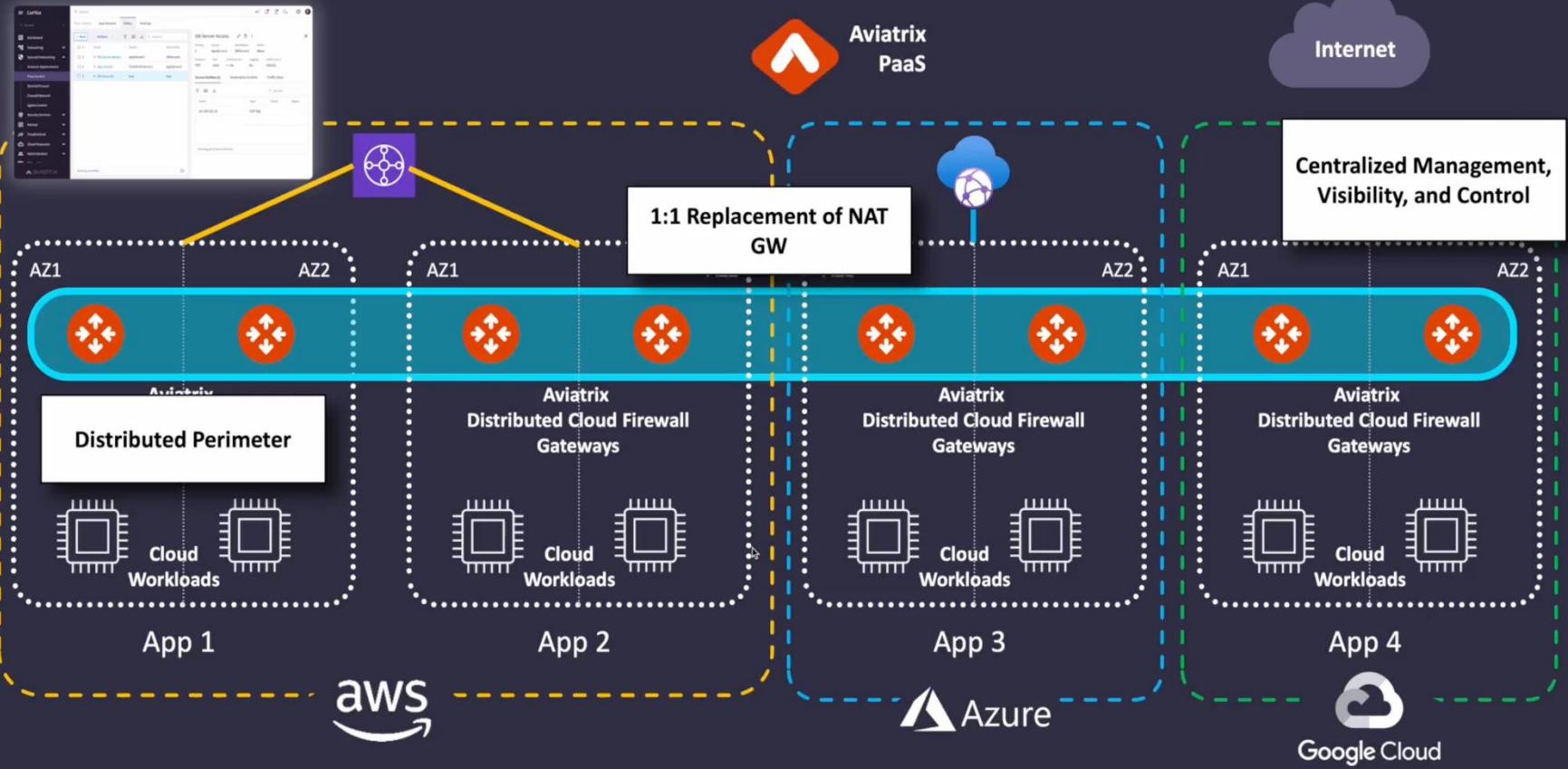
Distributed Cloud Provider Services vs Aviatrix

- Consolidation of Egress Security Stack
- Reduction in complexity
- Reduction in Data Transfer Costs \$\$\$
- Reduction in Operational Pain

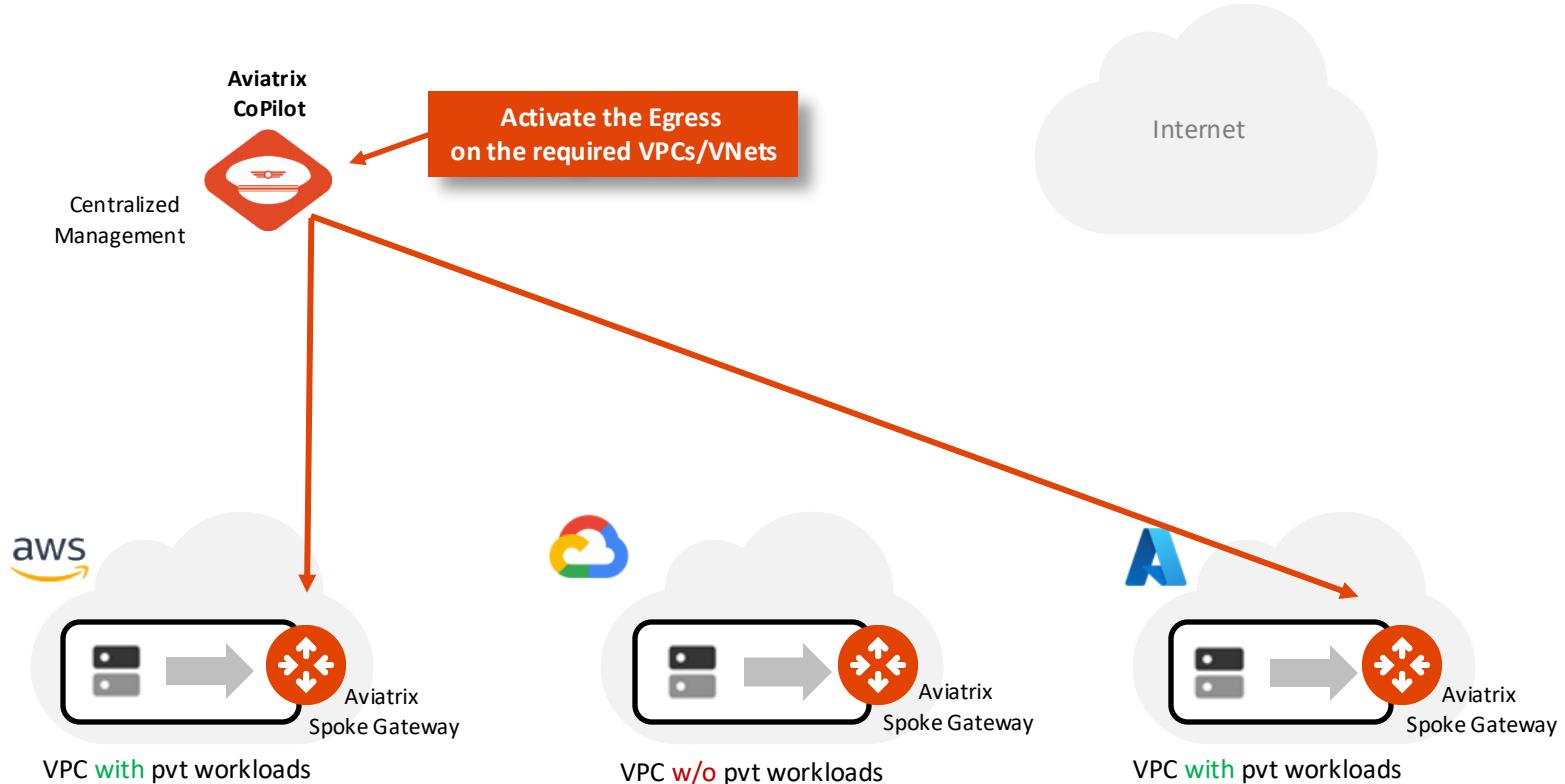


<https://aviatrix.com/aviatrix-paas>

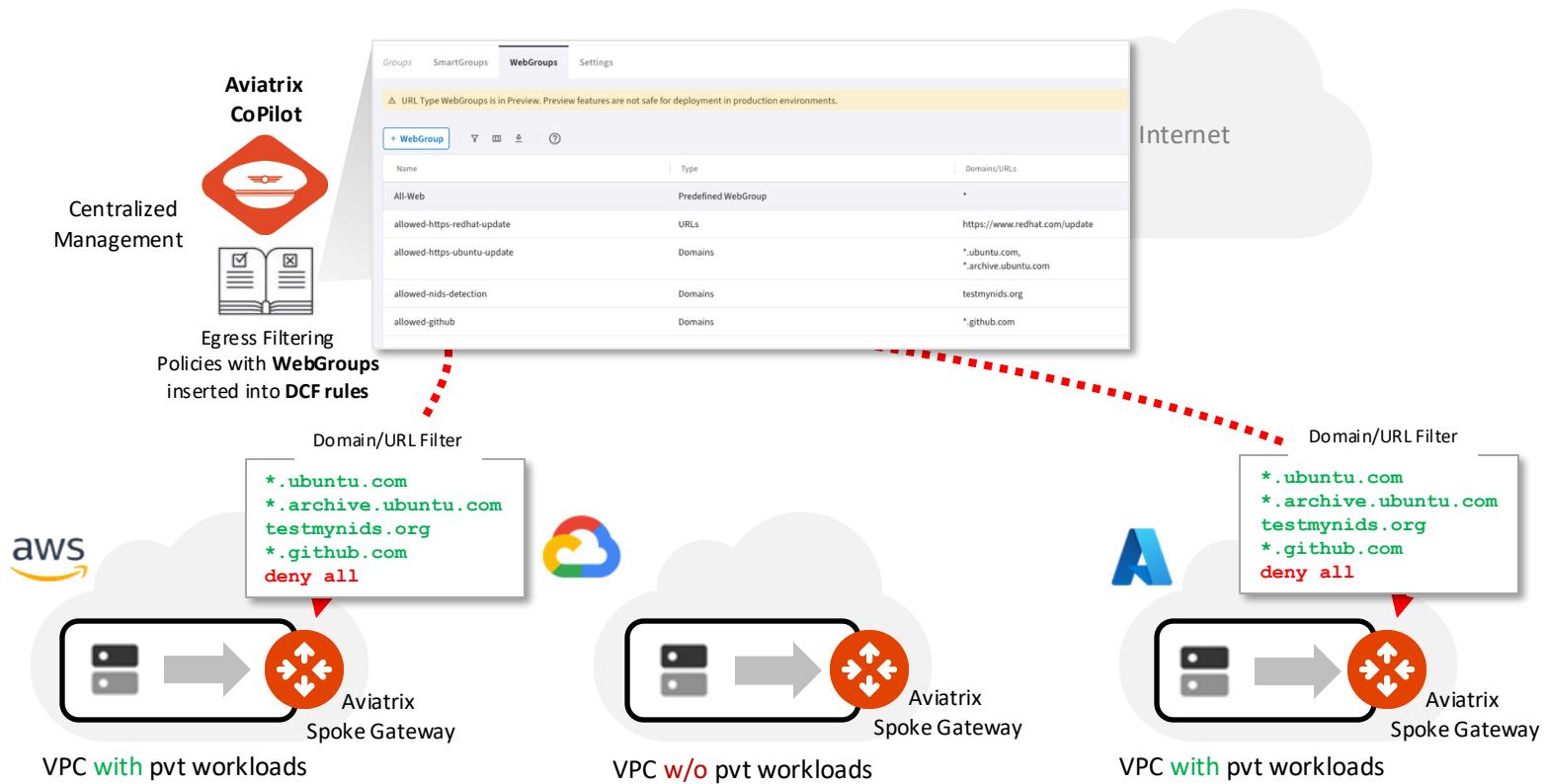
Achieve 25% Cost Savings over 1st Party NAT GWs



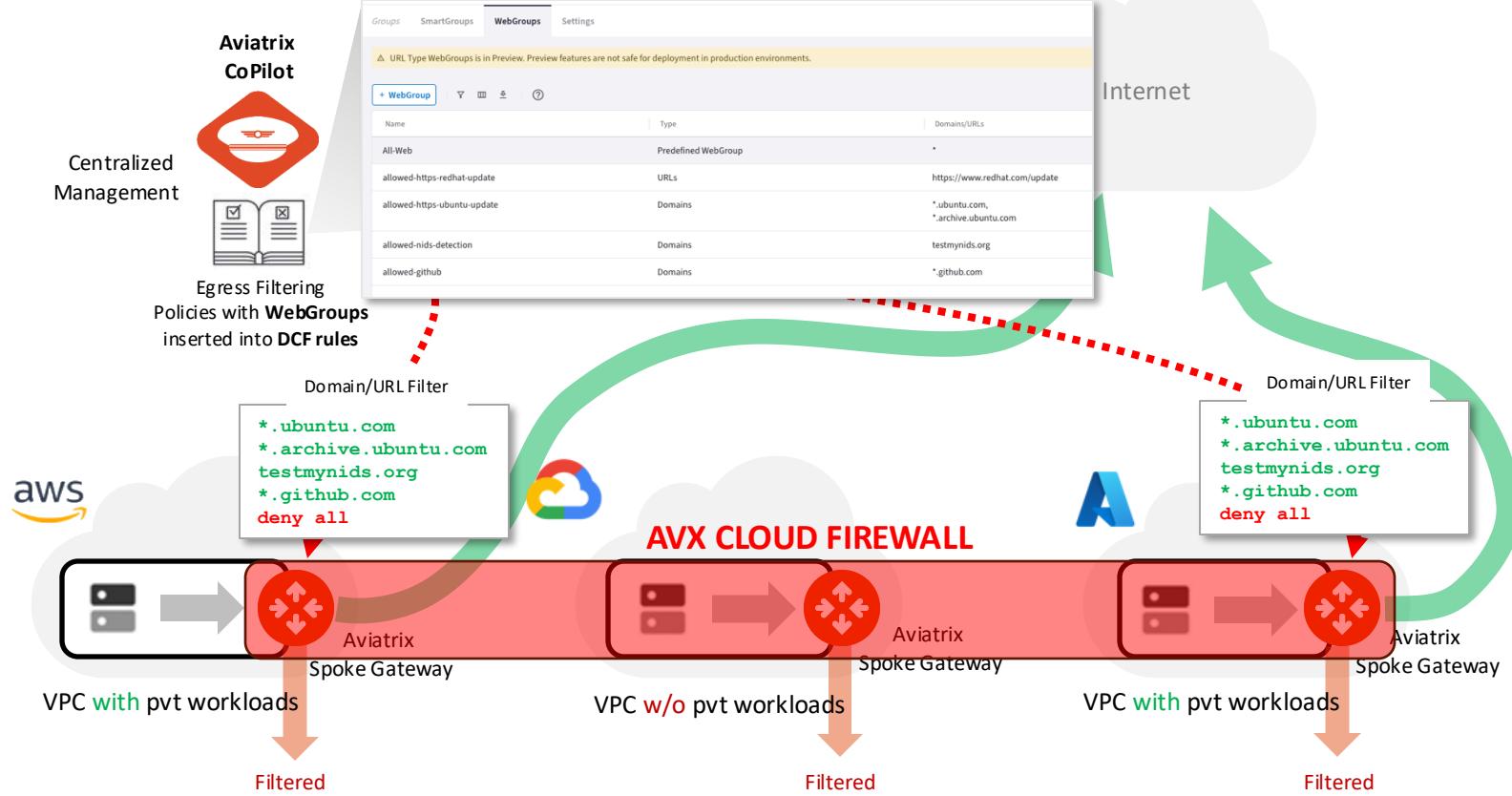
Aviatrix Cloud Firewall



Aviatrix Cloud Firewall



Aviatrix Cloud Firewall



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

Problem Statement

Private workloads need internet access

- SaaS integration



Customer Priority

Protection Against Data Exfiltration Breaches

- Patching



Customer Needs

Cloud-fluent Policy /
Security Posture

Agile Workload
Observability

- Updates



Aviatrix Bundles (SKU)

Aviatrix Cloud Firewall
(ACF)

Aviatrix K8s Firewall
(AKF)

Aviatrix Features

DCF

NAT

Security
Score

PaaS

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 highlighted. A red box surrounds the 'Enable Local Egress on VPC/VNets' button, and a red arrow points to it from the top right. Below the button is a table listing VPC/VNets, Spoke Gateways, Points of Egress, and Transit Attachments.

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

The screenshot shows the AWS VPC/VNet Route Tables interface for 'aws-us-east2-spoke1'. A red box highlights the 'Route Table' section, which displays a single entry: 'aws-us-east2-spoke1-Private-3-us-east-2c-rtb' with Route Table ID 'rtb-0f555197f0c9f6d8f' and Associated Subnets '1'. Below this, the 'Route DB' section shows four routes:

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

The screenshot shows the AWS VPC/VNet Route Tables interface for 'aws-us-east2-spoke1' after enabling Egress. A red box highlights the 'Route' section, which now includes a new default route: '0.0.0.0/0' with Target 'i-0d6fe343ab9b40295' and Gateway 'aviatrix-aws-us-east2-spoke1'. The rest of the table remains the same as the previous screenshot.

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

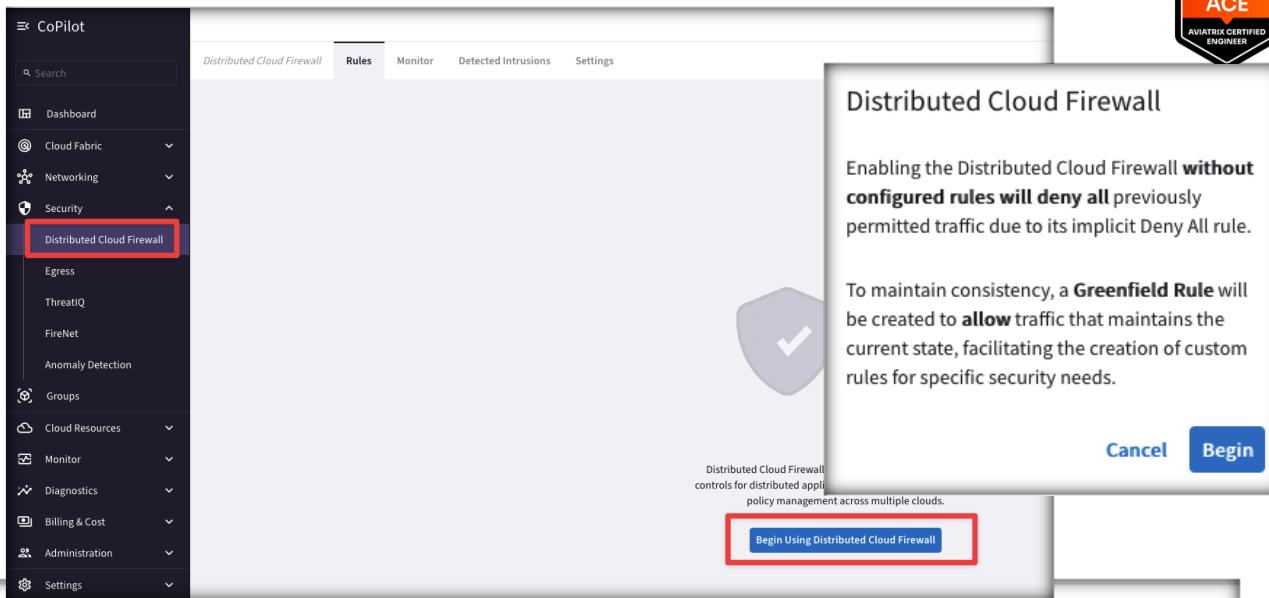
- If you want to apply policies on your Egress traffic, you must enable the Distributed Cloud Firewall.
- The Egress control requires the activation of the Distributed Cloud Firewall.
- The **Greenfield-Rule** is automatically added to allow all kind of traffic.
- An Explicit Deny Rule, named **DefaultDenyAll**,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

Distributed Cloud Firewall

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.

Cancel **Begin**



Distributed Cloud Firewall

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.

Cancel **Begin**

Rules						
Actions		Priority	Name	Source	Destination	Protocol
<input type="checkbox"/>	<input checked="" type="checkbox"/>	214748...	Greenfield-Rule	Anywhere (0.0.0.0...)	Anywhere (0.0.0.0...)	Any
<input type="checkbox"/>	<input checked="" type="checkbox"/>	214748...	DefaultDenyAll	Anywhere (0.0.0.0...)	Anywhere (0.0.0.0...)	Any

Discovery Process

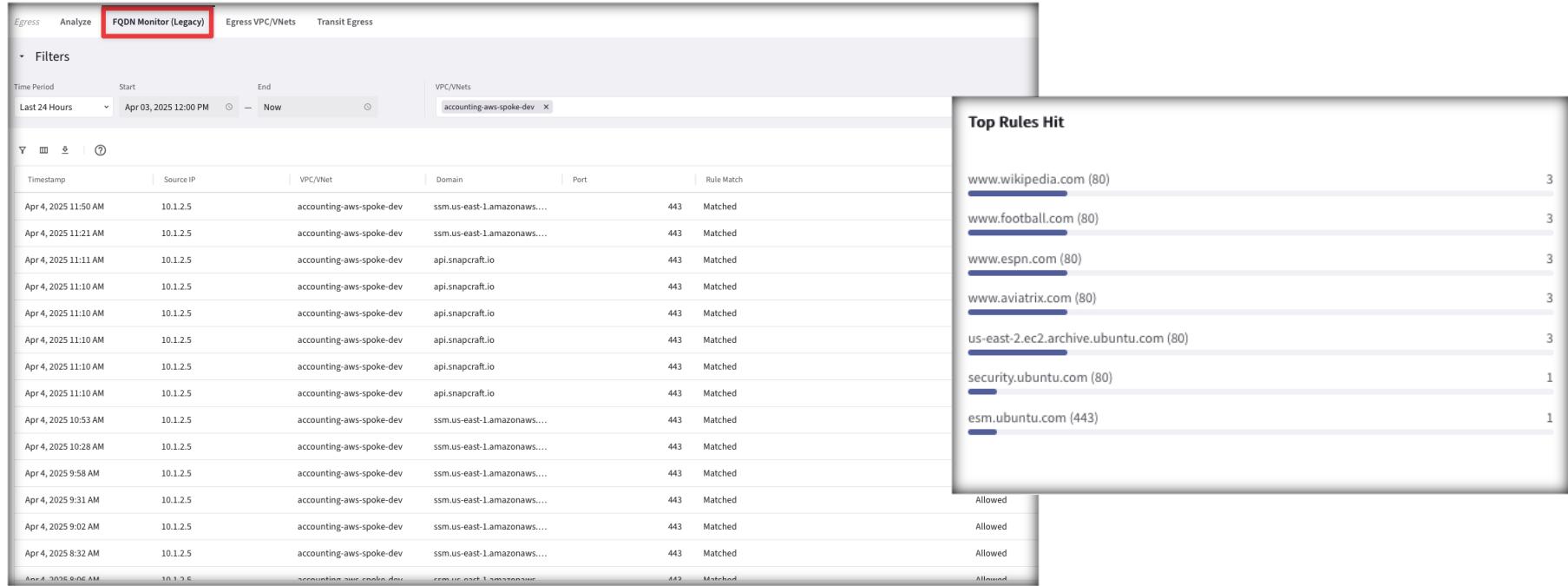
- If you are unsure about the sites your applications are accessing, you can temporarily enable an ad-hoc Discovery Rule.
 - Attach the SmartGroup that identifies the private workloads affected by the Egress feature, previously enabled, as *Source SmartGroup*.
 - Attach the Predefined SmartGroup "**Public 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. The top navigation bar includes tabs for Rules, Monitor, Detected Intrusions, and Settings. Below the navigation is a toolbar with actions like + Rule, Actions, and a search/filter icon. The main table lists rules with columns for Priority, Name, Source, Destination, WebGroup, Protocol, Ports, Action, IDS, and Logging. A red box highlights the first rule, "Discovery-Rule", which has a priority of 0, source "BU1", destination "Public Internet", WebGroup "All-Web", protocol "Any", action "Permit", and logging "On". A second rule, "Greenfield-Rule", is listed below it with a priority of 2147483... and a similar configuration. The "Place Rule" dropdown in the "Rule Priority" section is set to "Above" and is also highlighted with a red box. To the right of the table is a modal window titled "Create Rule" with fields for Name (set to "Discovery Rule"), Source SmartGroups (set to "BU1"), Destination SmartGroups (set to "Public Internet"), and WebGroups (set to "All-Web"). The "Rule Behavior" section includes toggles for "Enforcement" (off) and "Logging" (on). The "Rule Priority" section shows the "Place Rule" dropdown set to "Above" and the "Existing Rule" dropdown set to "Greenfield-Rule", both of which are also highlighted with red boxes. The modal has "Cancel" and "Save In Drafts" buttons at the bottom.

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		

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 logs with columns: Timestamp, Source IP, VPC/Net, Domain, Port, and Rule Match. The logs show multiple entries for the domain "accounting-aws-spoke-dev" connecting to various ports (443) and domains (ssm.us-east-1.amazonaws.com, api.snapcraft.io). All entries show a "Matched" rule match.

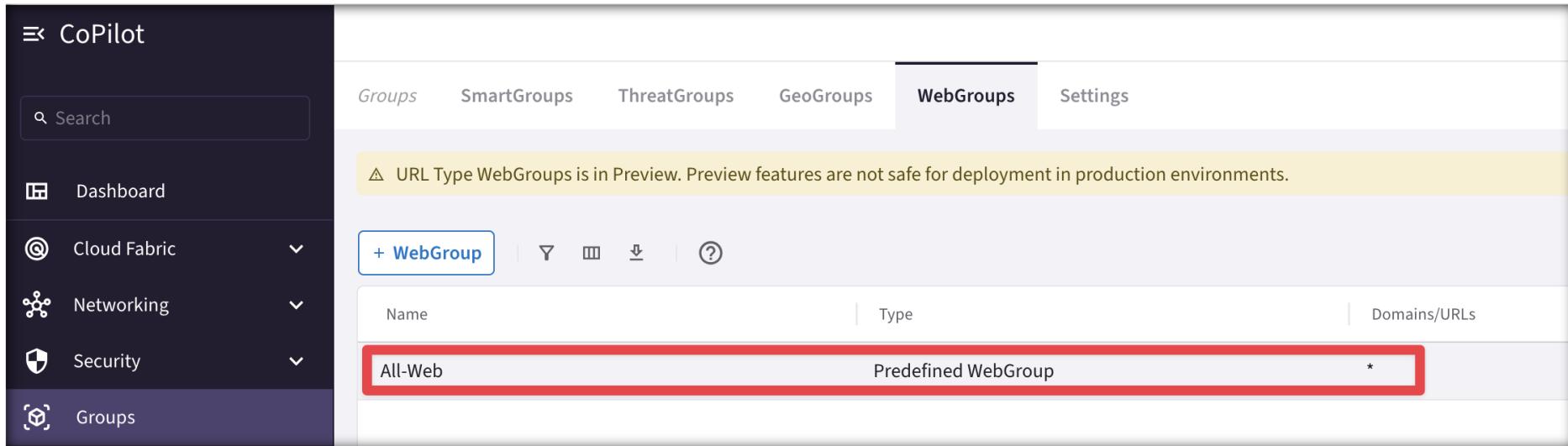
To the right, a chart titled "Top Rules Hit" shows the most frequent domains and ports. The chart has a light gray background with horizontal bars. The data points are:

Domain/Port	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

At the bottom of the log table, there is a column labeled "Action" with values "Allowed" or "Denied".

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.

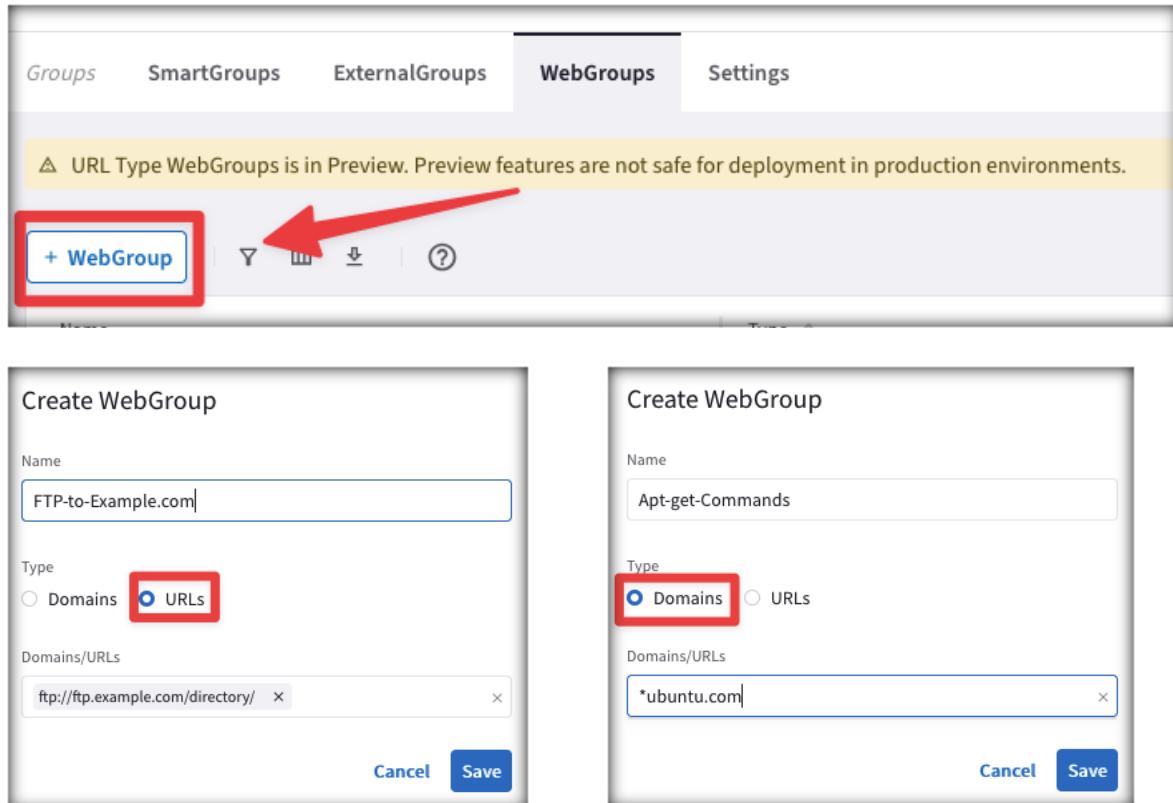


The screenshot shows the Aviatrix CoPilot web interface. On the left is a dark sidebar with navigation links: CoPilot (selected), Search, Dashboard, Cloud Fabric, Networking, Security, and Groups (highlighted with a red box). The main area has a light background. At the top, there are tabs: Groups, SmartGroups, ThreatGroups, GeoGroups, WebGroups (selected and highlighted with a black bar), and Settings. A yellow banner message says: "⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments." Below the banner is a toolbar with icons for creating a new WebGroup (+ WebGroup), deleting, and other actions. A table lists existing WebGroups. The first row, "All-Web", is highlighted with a red border. The table columns are Name, Type, and Domains/URLs. The "All-Web" entry shows "Predefined WebGroup" under Type and an asterisk (*) under Domains/URLs.

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).



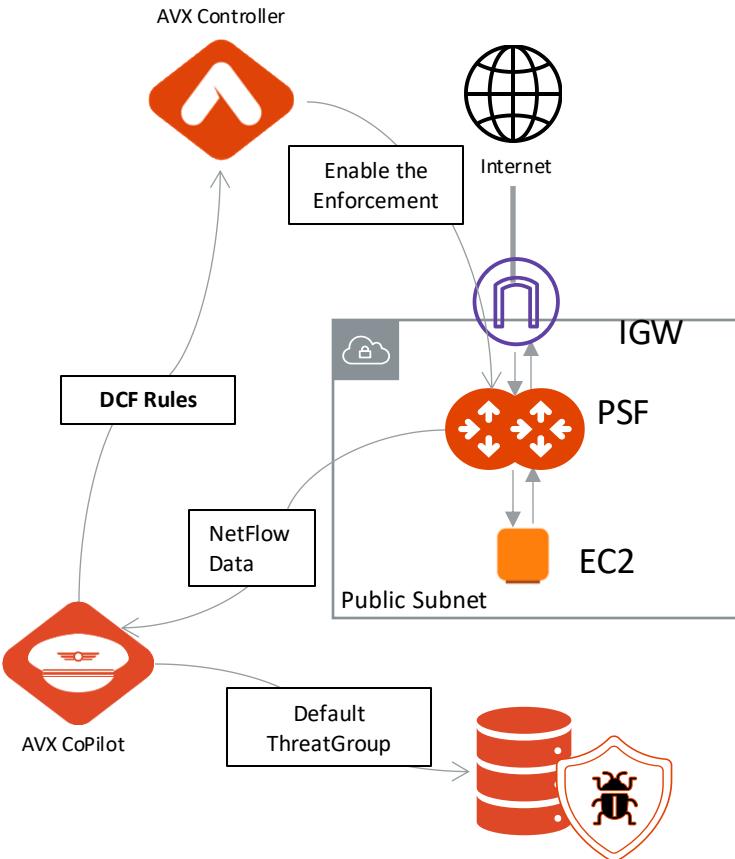
The screenshot illustrates the process of creating a WebGroup in the Aviatrix UI. The top navigation bar includes tabs for Groups, SmartGroups, ExternalGroups, WebGroups (which is selected), and Settings. A yellow warning message states: "⚠ URL Type WebGroups is in Preview. Preview features are not safe for deployment in production environments." Below the tabs is a toolbar with a "+ WebGroup" button (highlighted with a red box and an arrow pointing to it), a dropdown menu, and a help icon. The main area displays two examples of creating a WebGroup. The first example, "Create WebGroup" for "FTP-to-Example.com", shows the "Type" set to "URLs" (radio button highlighted with a red box) and the "Domains/URLs" field containing "ftp://ftp.example.com/directory/". The second example, "Create WebGroup" for "Apt-get-Commands", shows the "Type" set to "Domains" (radio button highlighted with a red box) and the "Domains/URLs" field containing "*ubuntu.com". Both examples include "Cancel" and "Save" buttons at the bottom.



Aviatrix PSF GW(aka Public Subnet Filtering Gateway)

Aviatrix Public Subnet Filtering Gateways (PSF GWs)

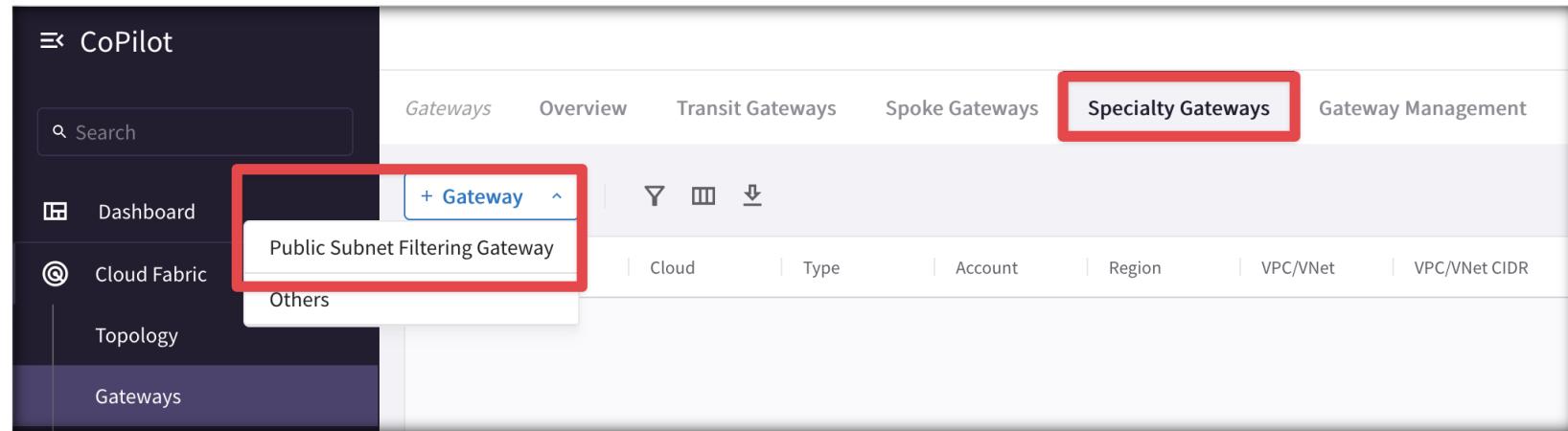
- **Public Subnet Filtering Gateways (PSF gateways)** provide ingress and egress security for **AWS** public subnets where instances have public IP addresses.
- After the Public Subnet Filtering (PSF) gateway is launched, you can apply also DCF (Distributed Cloud Firewall) rules – *enforcement must be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

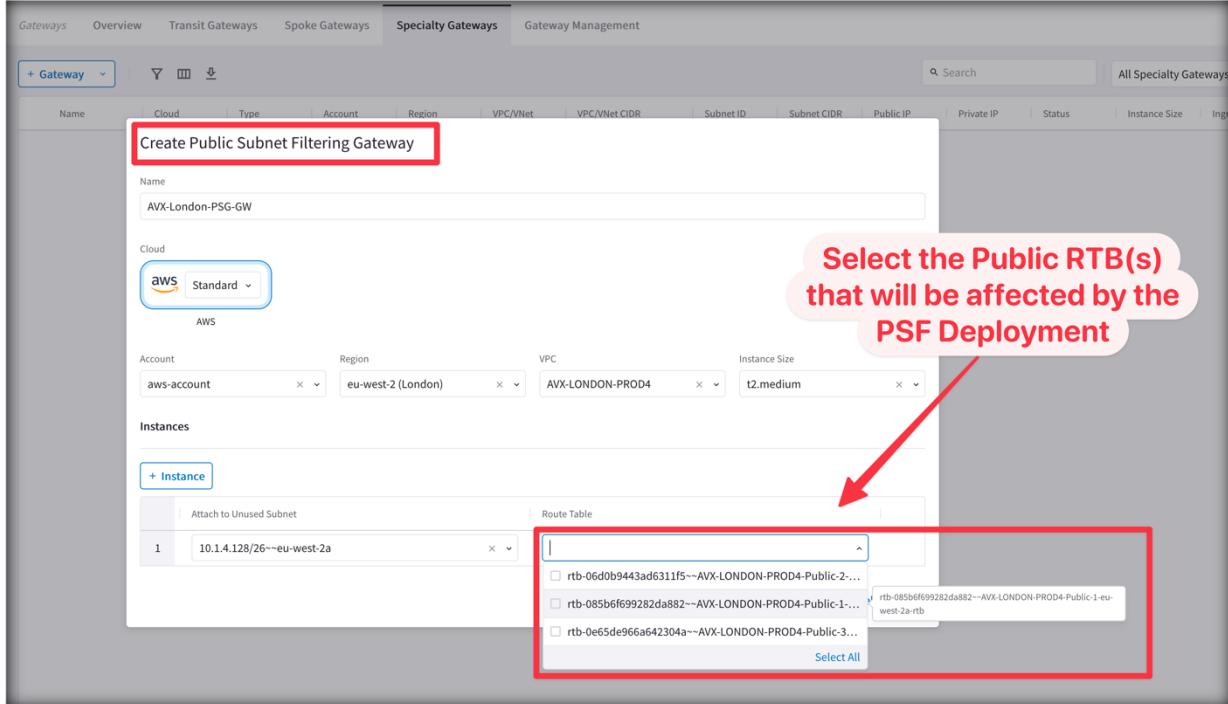
1. In CoPilot, navigate to **Cloud Fabric > Gateways > Specialty Gateways** tab.
2. Click **+Gateway** and select **Public Subnet Filtering Gateway**.



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.



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

Instances:

+ Instance

Route Table:

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

Select All

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

Enable



Lab 5 – Aviatrix Cloud Firewall (with Secure Egress)