



Security

ACE Solutions Architecture Team

Agenda

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

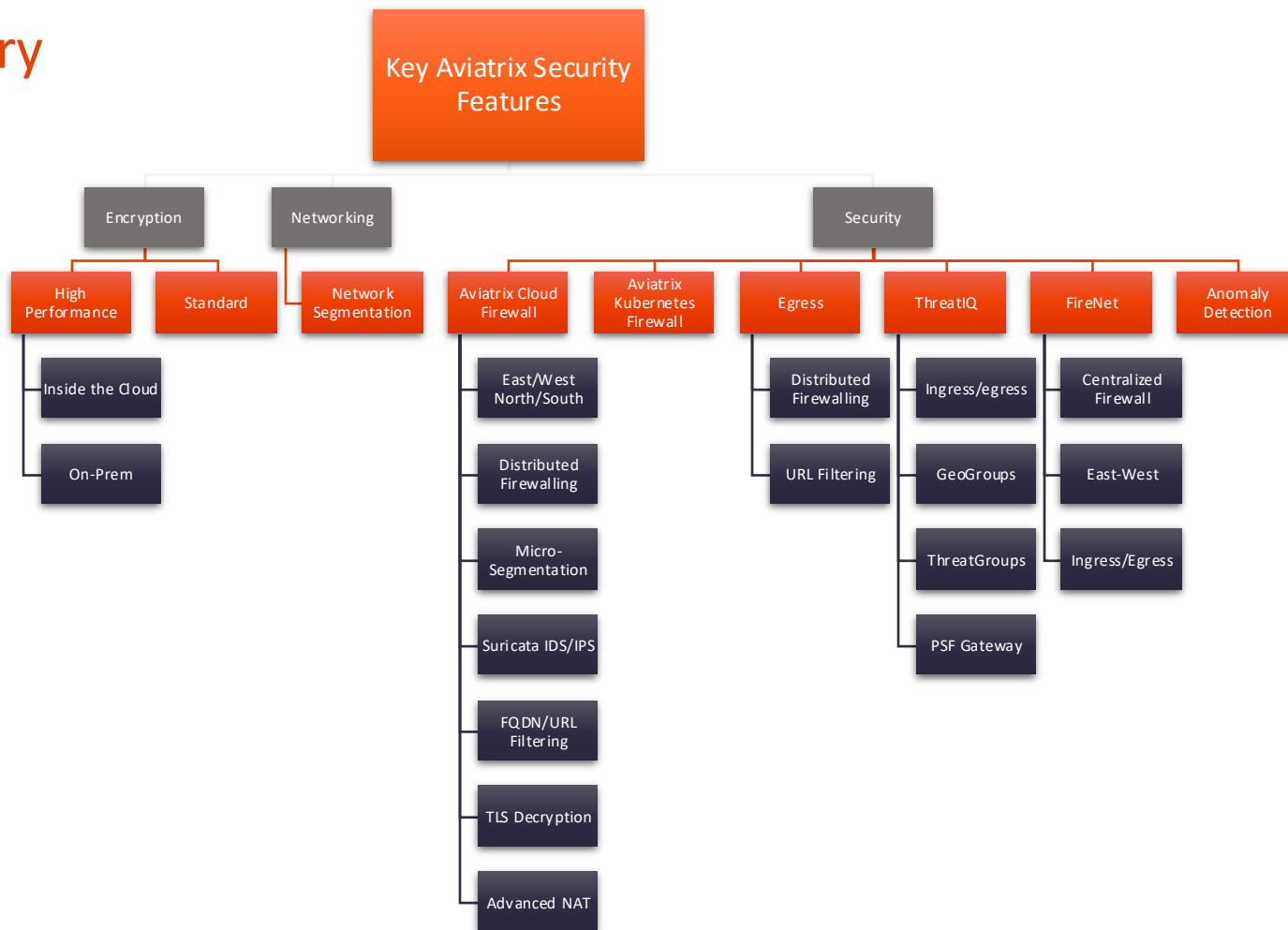
Challenges for CISO, CIO/CTO and NetSec Architects

- 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>

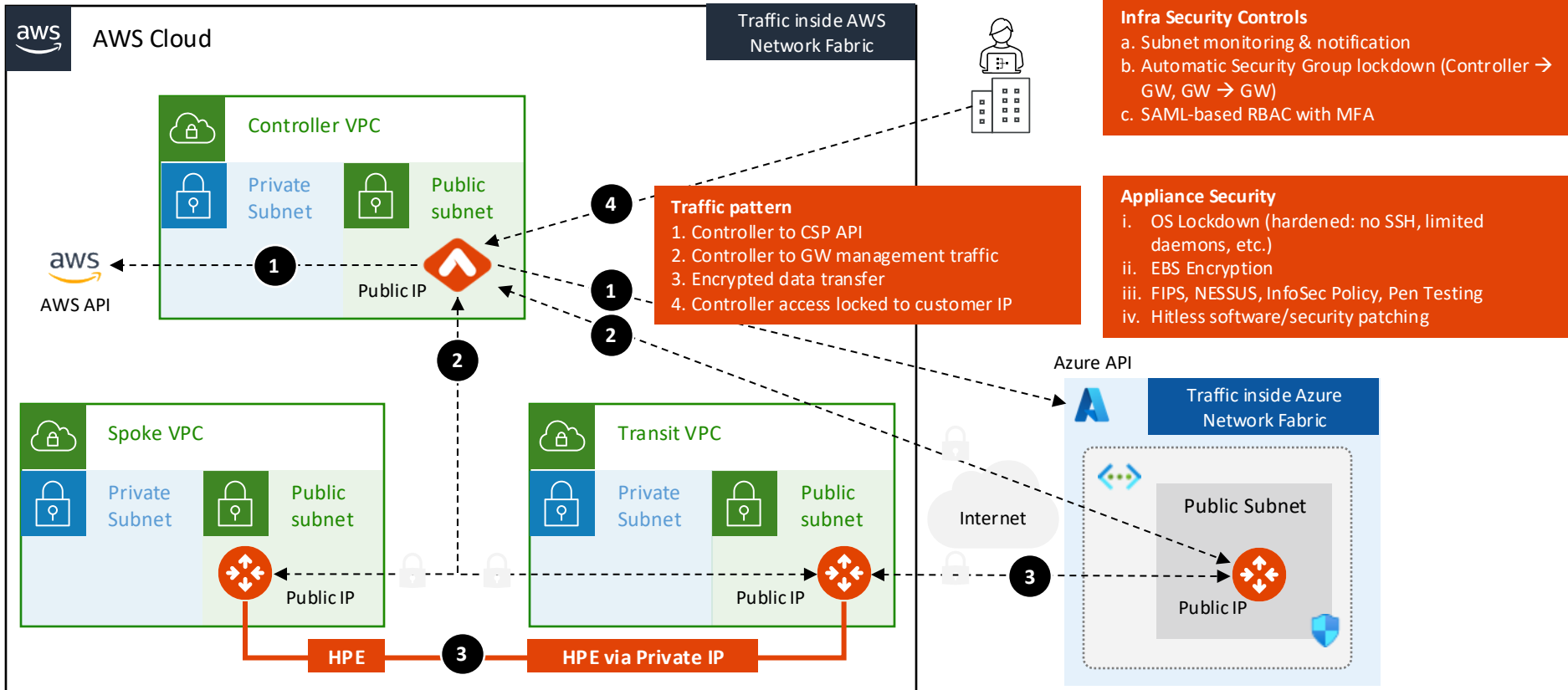
Summary





Built-in Security of the Aviatrix Platform

Secure Aviatrix Infrastructure Deployment | Example in AWS & Azure



AWS Cloud

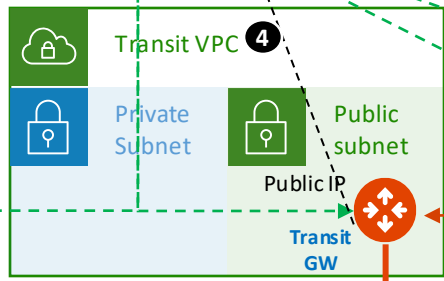
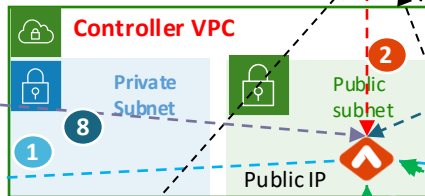
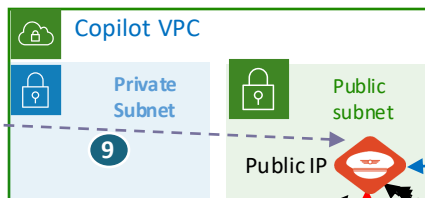
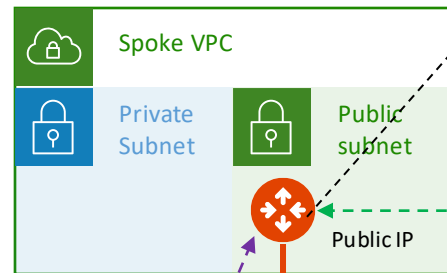


Logging/
Audit/
Network
Insight
API

Prometheus
Logstash
Splunk
SumoLogic
Rsyslog

MFA

awsAPI



Traffic inside AWS
Network Fabric

HPE

HPE via Private IP



On Prem DC/
Branch Office/
B2B Partner

aviatrix

Traffic Pattern

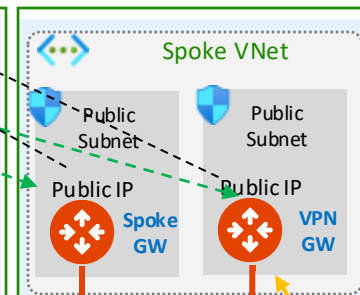
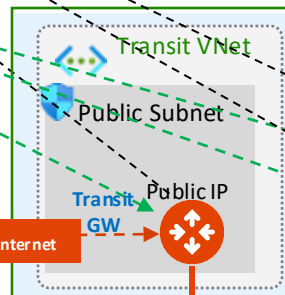
1. Controller to CSP API
2. Controller with Copilot
3. Controller to GW management traffic
4. Gateway to Copilot (Syslog, Netflow etc)
5. Encrypted data transfer
6. Copilot access locked to customer IP
7. Controller access locked to customer IP
8. Controller to MFA
9. Copilot to Customers Network Insight 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

Azure API



Internet

HPE via Internet

HPE



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 Aviatix 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 displays the CoPilot Configuration interface. The left sidebar shows the navigation menu with 'Configuration' highlighted. The main content area is divided into tabs: 'General' (selected), 'License', 'Logging Services', and 'Private Mode'. Under the 'General' tab, the 'Associated Aviatrix Controller' section shows 'Public IP/FQDN' and 'Controller IP' both set to 'ctrl.demo.aviatrixtest.com'. The 'Controller Session Timeout' is set to 60 minutes. The 'Sharing Metrics with Aviatrix' section has 'Usage Analytics' turned on. The 'Security' section is expanded, showing 'CoPilot Security Group Management' and 'Controller Security Group Management' both enabled. The 'Controller Security Group Management' section includes a 'VPC/VNet' dropdown set to 'AviatrixVPC(vpc-06048f3b2328eaccf)' and a 'CoPilot' dropdown set to 'AviatrixCoPilot--i-057182a101921e363'. A red arrow points to the 'Controller Security Group Management' toggle switch.

- 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 displays the Aviatrix CoPilot Configuration interface. The left-hand navigation menu has 'Configuration' selected. The main content area shows the 'General' tab. Under the 'General' section, the 'Associated Aviatrix Controller' is configured with 'ctrl.demo.aviatrixtest.com'. The 'Controller Session Timeout' is set to 60 minutes. The 'Sharing Metrics with Aviatrix' section shows 'Usage Analytics' is turned on. In the 'Security' section, 'CoPilot Security Group Management' is highlighted with a red box and a red arrow, indicating it is enabled. 'Controller Security Group Management' is also enabled. Below these settings, the 'VPC/VNet' is set to 'AviatrixVPC(vpc-06048f3b2328eaccf)' and the 'CoPilot' instance is set to 'AviatrixCoPilot--i-057182a101921e363'.

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

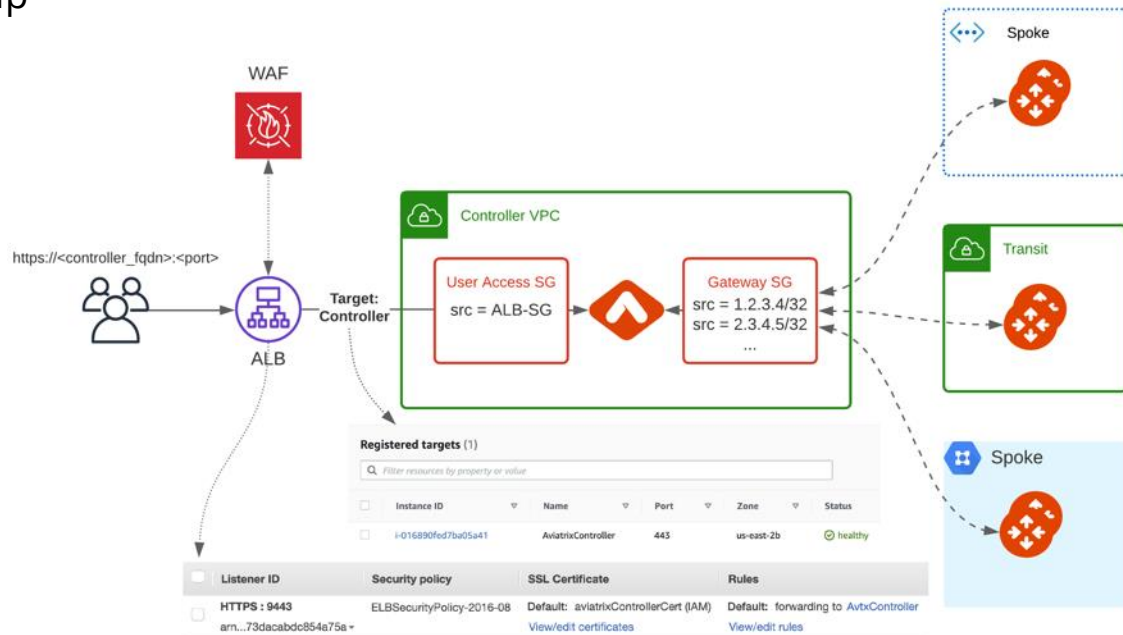


Securing the Platform with Cloud Native Load Balancers

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

Private workloads need internet access

- SaaS integration

- Patching



- Updates



Understanding the Pain

Improve Security and Lower Cloud Costs

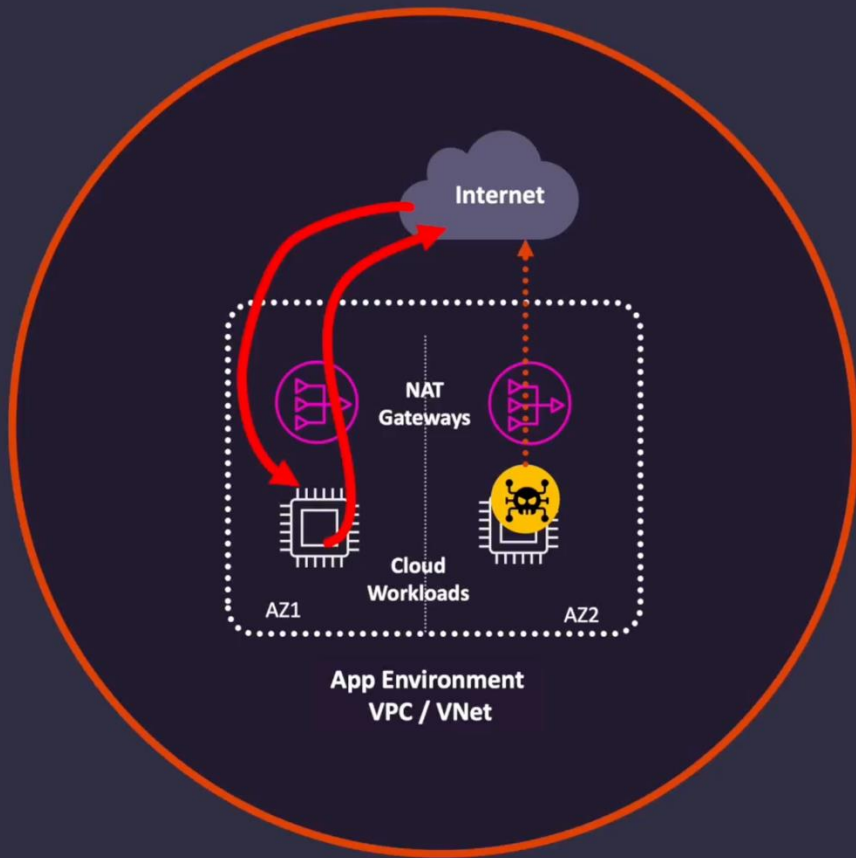


- **Business Pain**

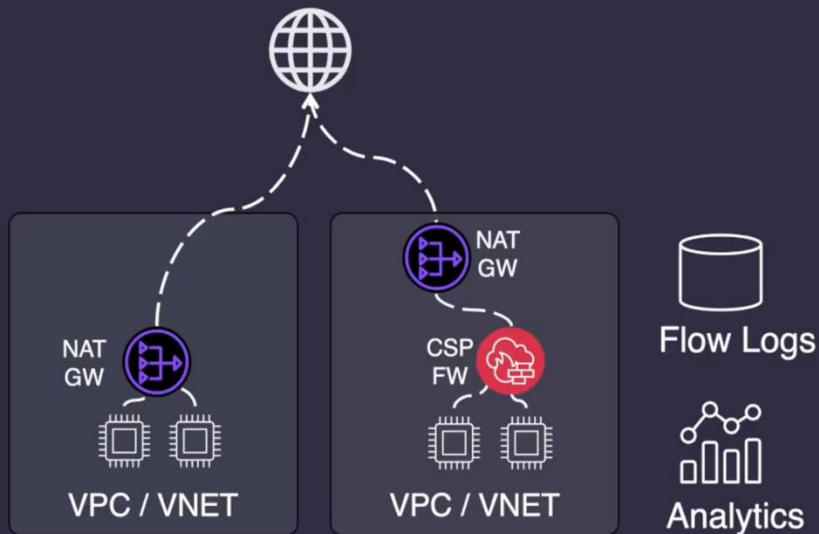
- Excessive Cloud Costs
- Lack of Compliance & Governance
- Risk to Business-Critical Workloads
- Regulatory Fines and Penalties
- Brand Health and Customer Trust

- **Technical Pain**

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



Two Common Paths



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](#)

CLOUD SECURITY

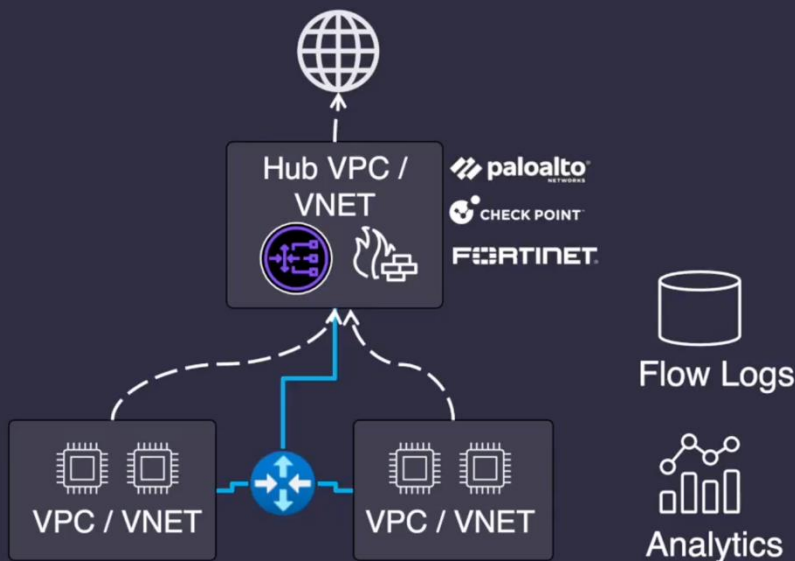
CyberRatings.org Announces Test Results for Cloud Service Provider Native Firewalls

Protection ranged from 0.38% to 50.57% for security effectiveness.

Two Common Paths

2. Central Virtualized Appliances

- Very Expensive
- Not built for cloud: operational complexity
- No support for Island VPCs / VNets
- Requires Overly Complex Routing Architecture
- Security Hub Connectivity dependent
- No centralized network and security intelligence
- Additional troubleshooting issues
- Not multi-cloud deployable



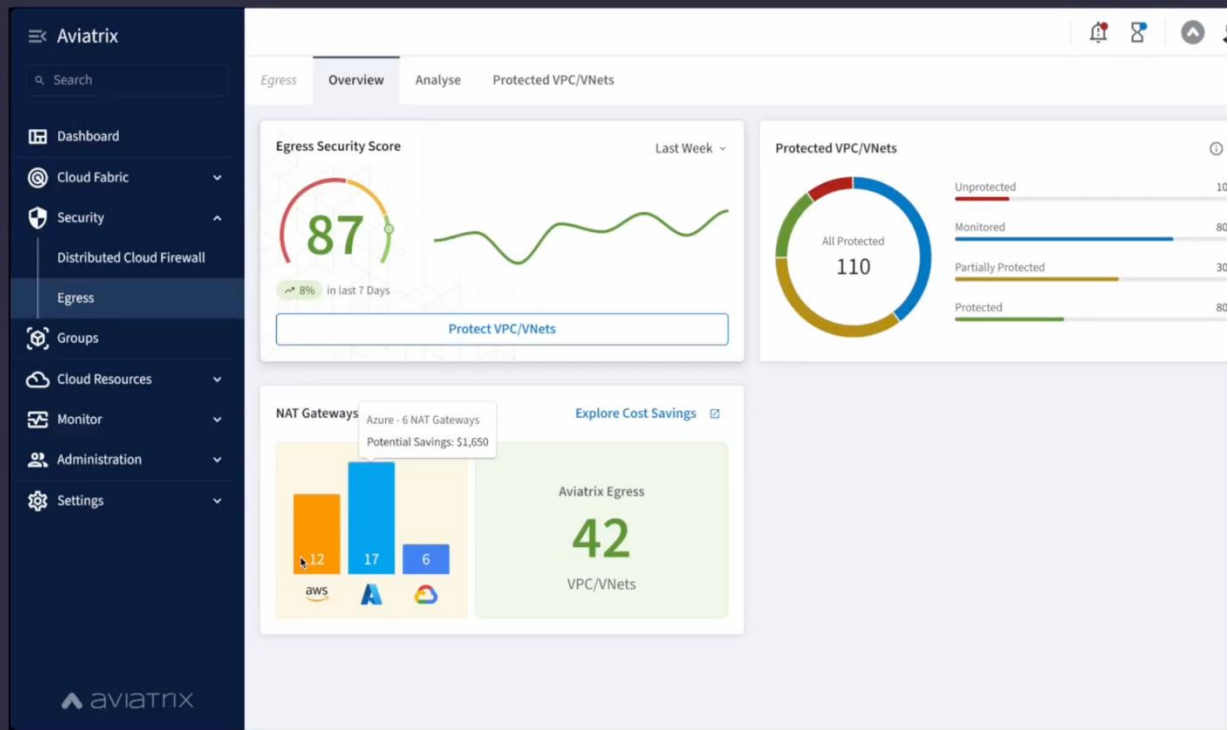
Aviatrix Cloud Firewall

What it is:

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

What you get:

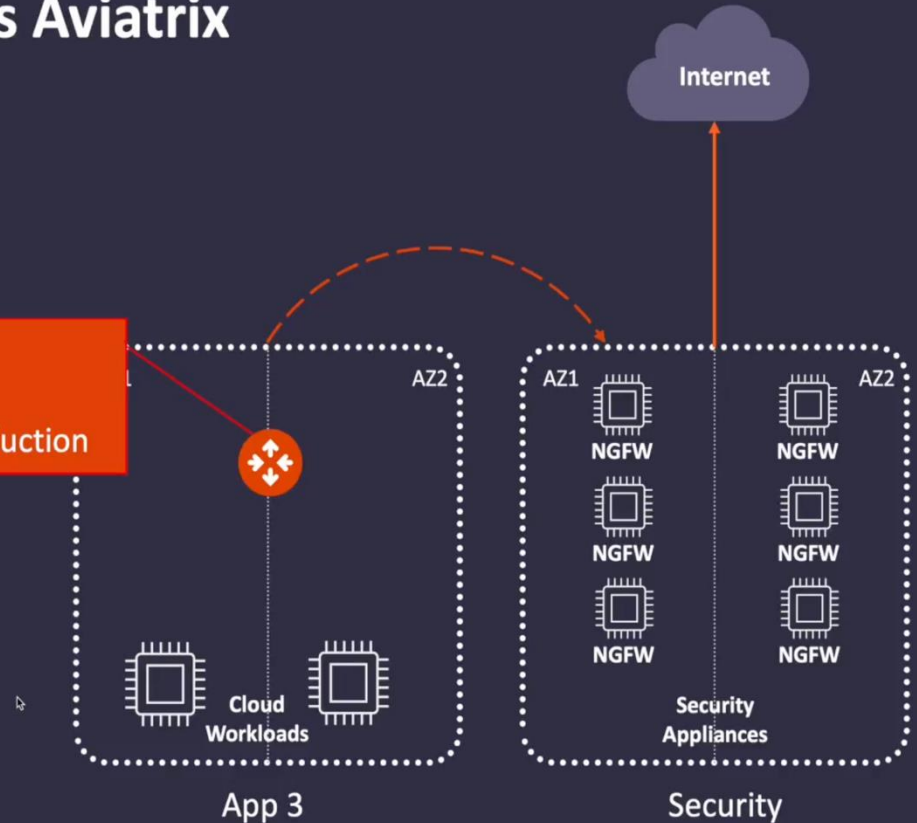
- Secure Networking that's:
 - Agile,
 - Reduces Costs & Complexity
 - Increases Visibility



Central Virtualized Appliances vs Aviatrix

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

- Security
- Visibility
- Cost Reduction



Distributed Cloud Provider Services vs Aviatrix

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



For LESS than
your NAT GW
Data Transfer Bill

Logging and
Analysis

VPC Traffic
Mirroring

Amazon
GuardDuty

Route 53
Resolver DNS
Firewall

EC2 Security
Groups and
Network ACLs

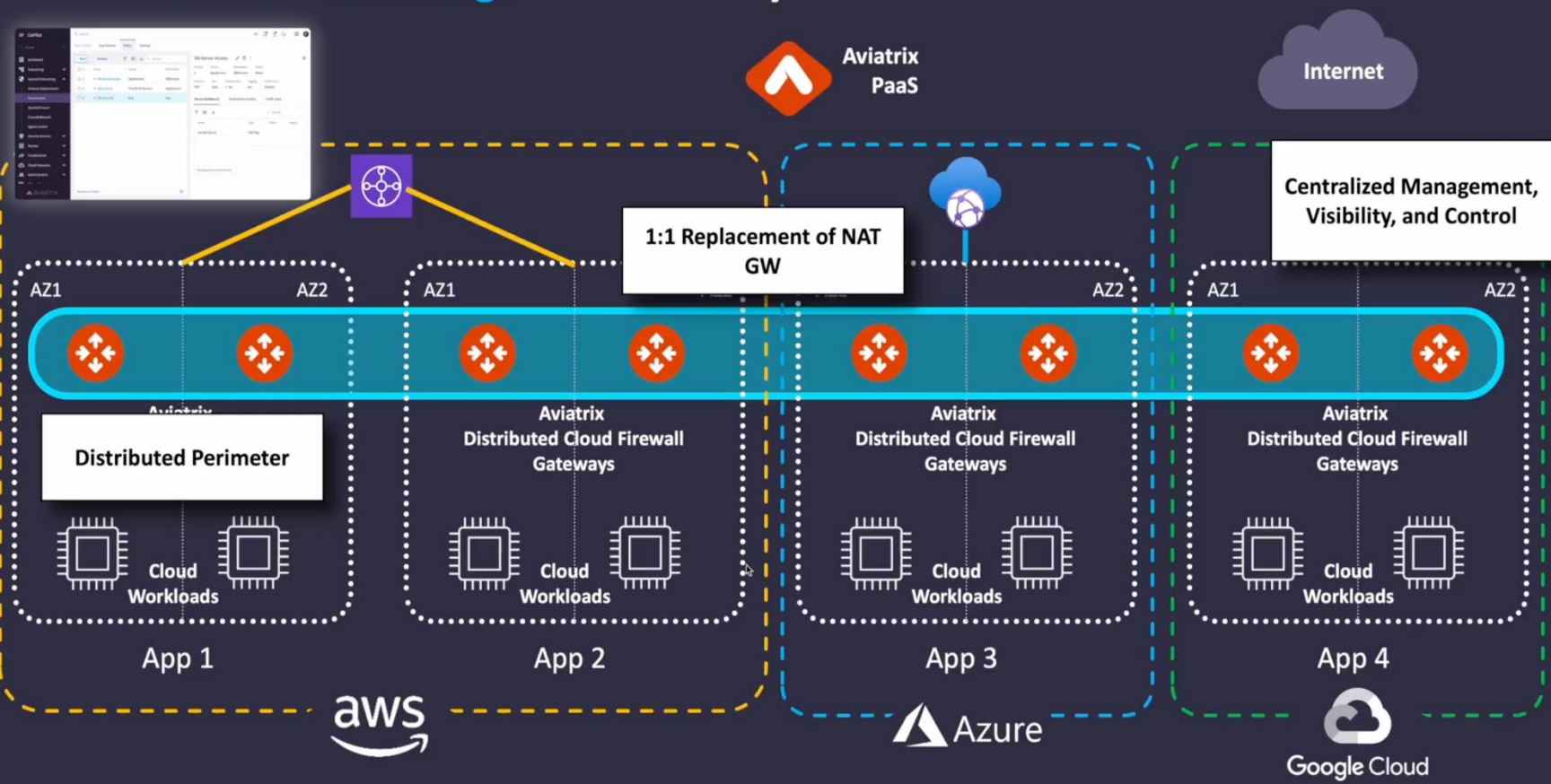
AWS Firewall

AWS NAT GW

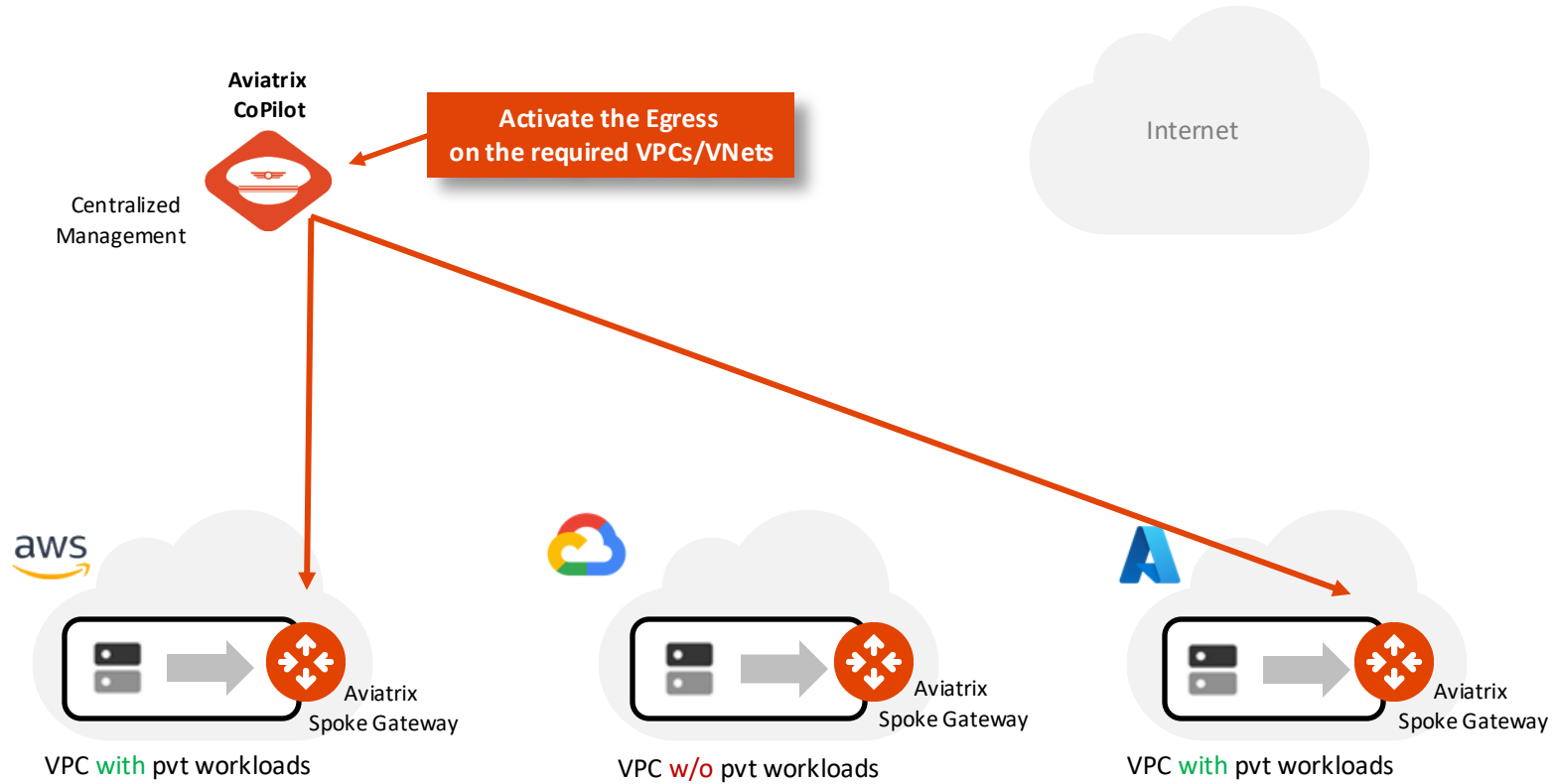
Cost and Complexity

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

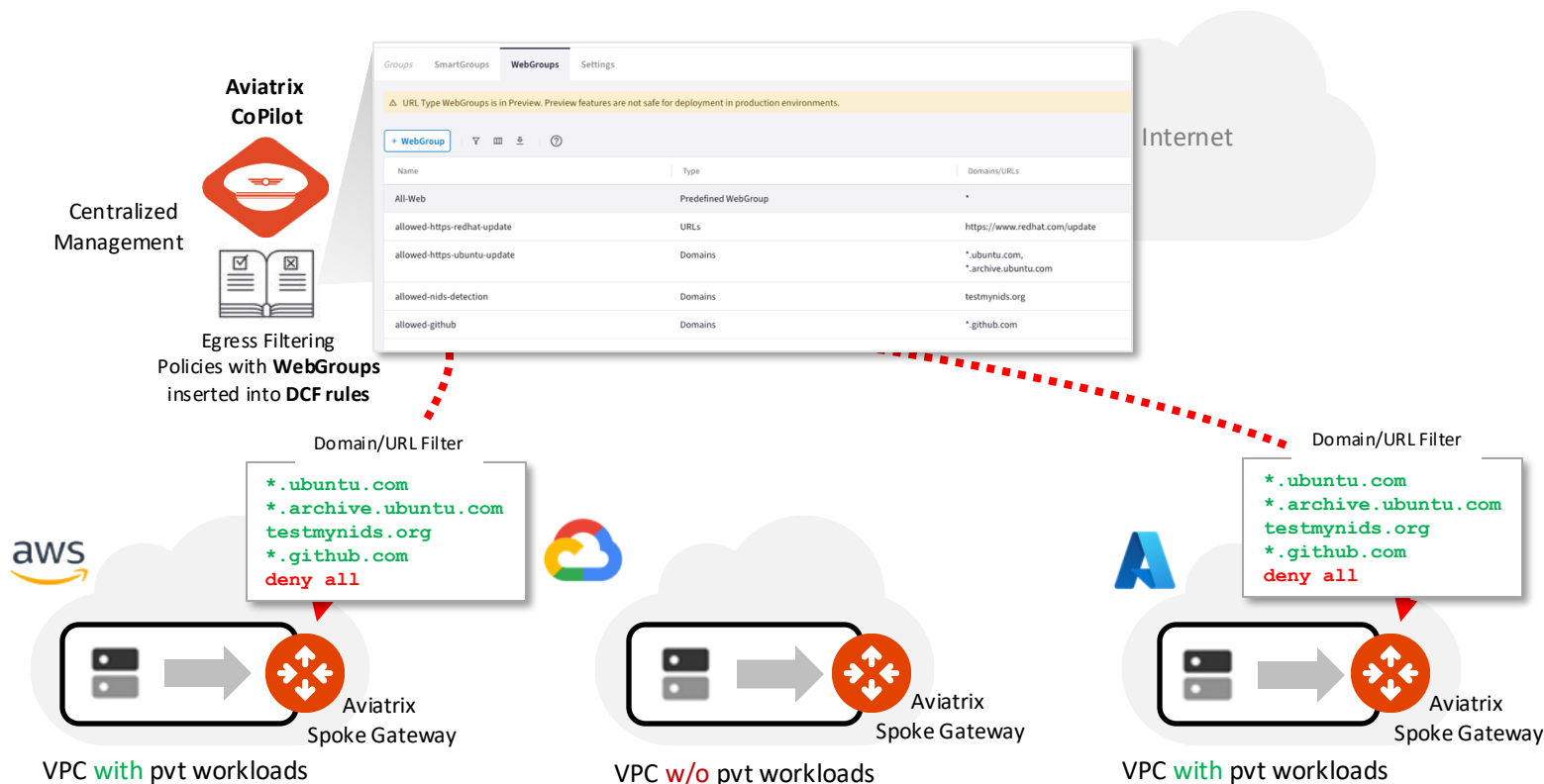
Achieve 25% Cost Savings over 1st Party NAT GWs



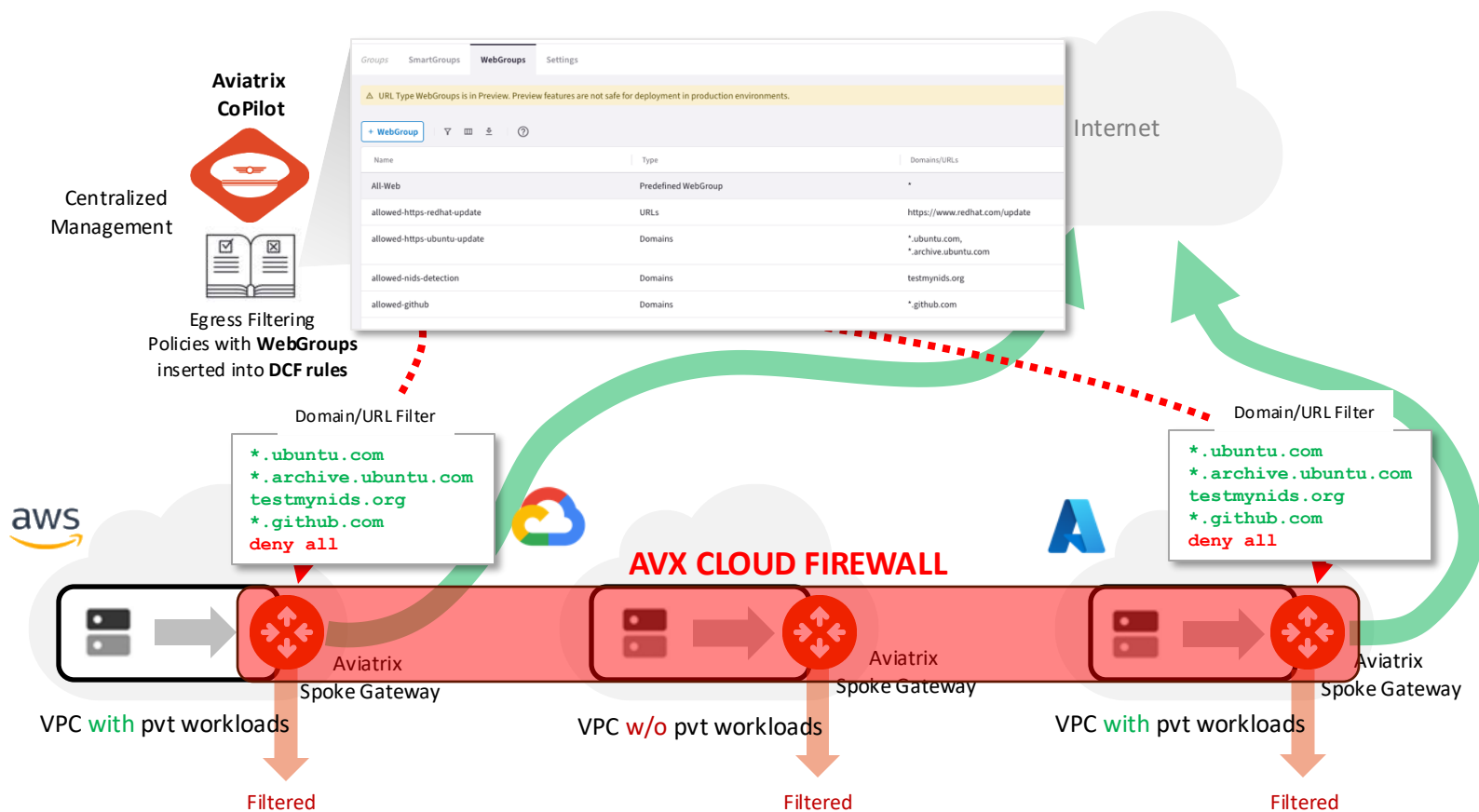
Aviatrix Cloud Firewall



Aviatrix Cloud Firewall



Aviatrix Cloud Firewall



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

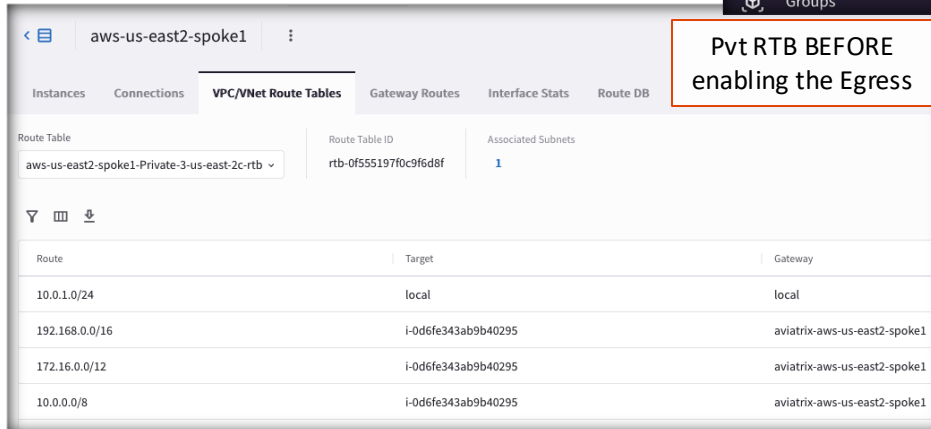
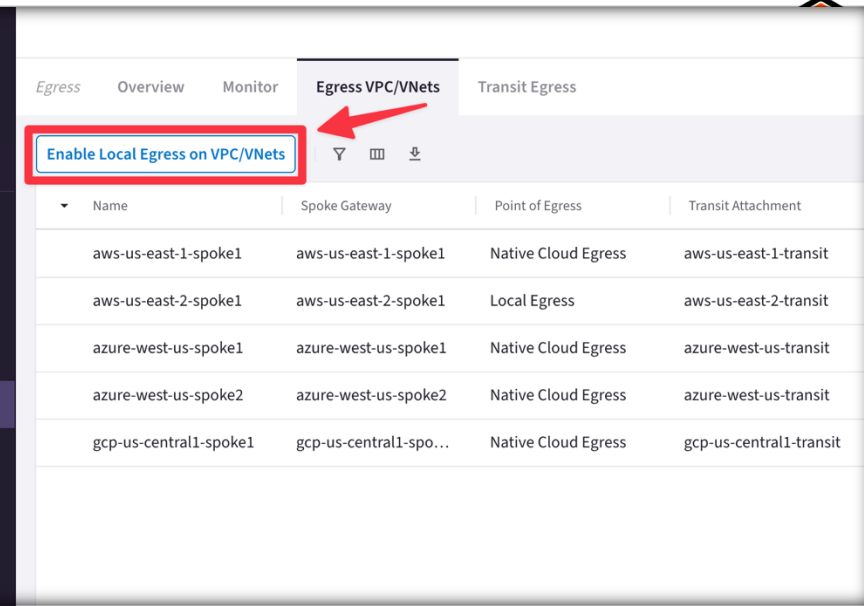
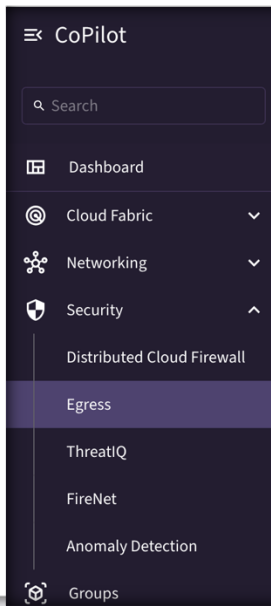
NAT

Security
Score

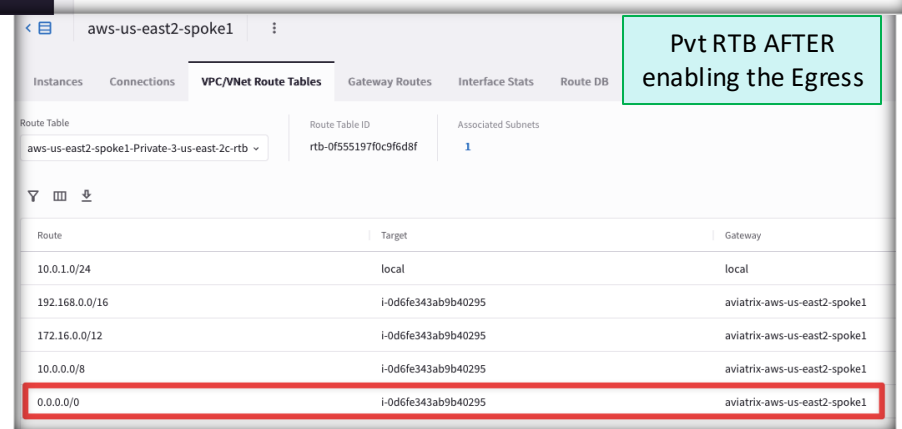
PaaS

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.



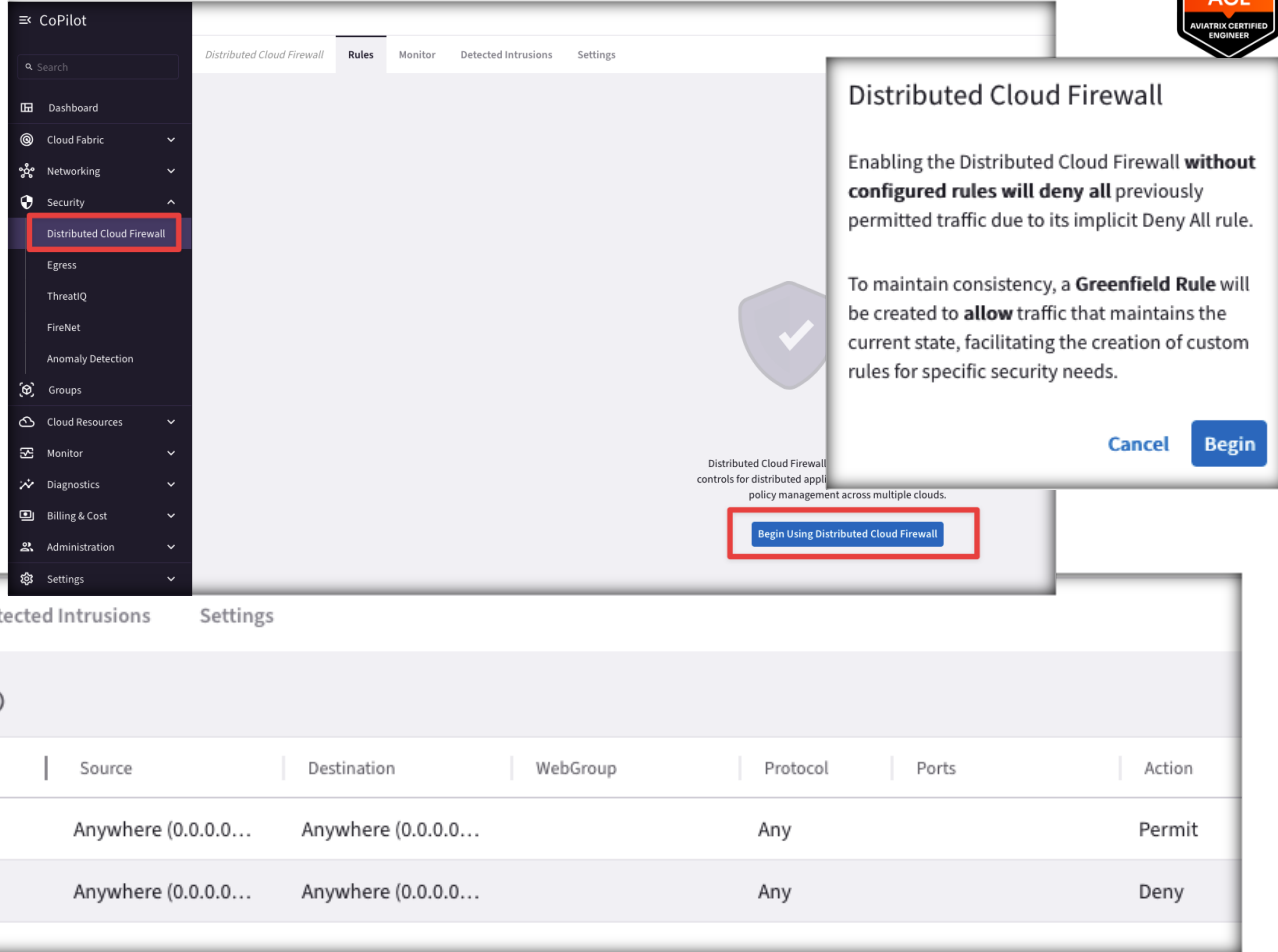
Pvt RTB BEFORE
enabling the Egress



Pvt RTB AFTER
enabling the Egress

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](#)

[Begin Using Distributed Cloud Firewall](#)

Rules

Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action
214748...	Greenfield-Rule	Anywhere (0.0.0.0...	Anywhere (0.0.0.0...		Any		Permit
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.
 - 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 under the **CoPilot > Security > Egress > FQDN Monitor (Legacy)** tab

Priority	Name	Source	Destination	WebGroup	Protocol	Ports	Action	IDS	Logging
0	Discovery-Rule	BU1	Public Internet	All-Web	Any	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

Action: Permit, SG Orchestration: Off

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

Rule Priority

Place Rule: Above, Existing Rule: Greenfield-Rule

Cancel, Save In Drafts

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 displays the 'FQDN Monitor (Legacy)' interface. The top navigation bar includes 'Egress', 'Analyze', 'FQDN Monitor (Legacy)', 'Egress VPC/VNets', and 'Transit Egress'. The 'Filters' section shows 'Time Period' set to 'Last 24 Hours', 'Start' at 'Apr 03, 2025 12:00 PM', 'End' at 'Now', and 'VPC/VNets' set to 'accounting-aws-spoke-dev'. Below the filters is a table with columns: Timestamp, Source IP, VPC/VNet, Domain, Port, Rule Match, and an unlabeled column. The table contains 15 rows of log entries. To the right, a 'Top Rules Hit' sidebar lists domains and their hit counts: 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). Below the sidebar, the 'Allowed' column from the table is visible, showing 'Allowed' for the last three rows.

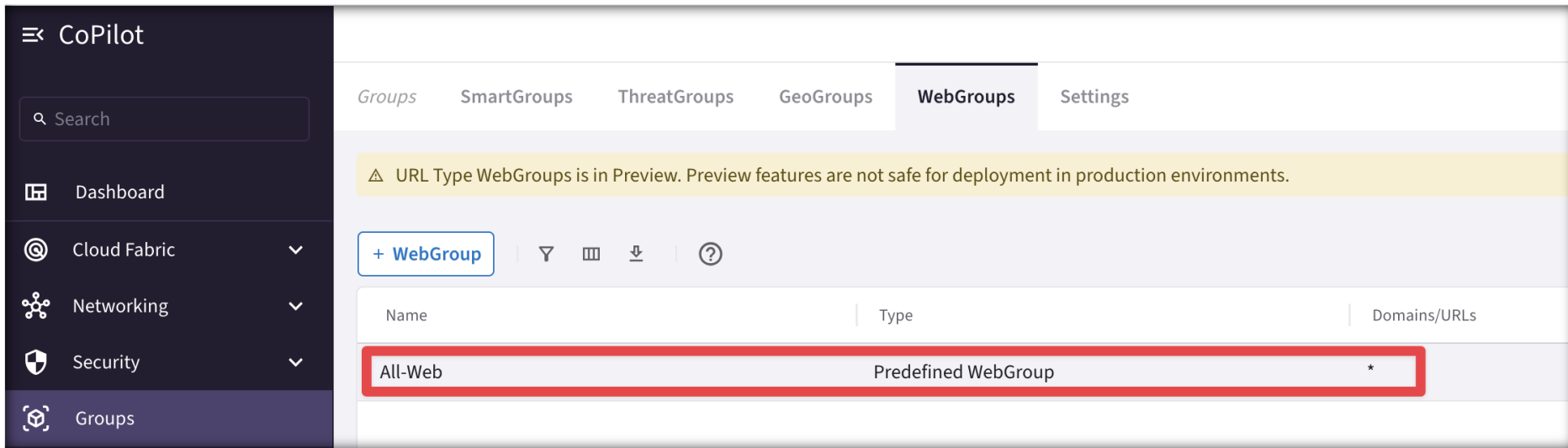
Timestamp	Source IP	VPC/VNet	Domain	Port	Rule Match	
Apr 4, 2025 11:50 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws...	443	Matched	
Apr 4, 2025 11:21 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws...	443	Matched	
Apr 4, 2025 11:11 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 10:53 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws...	443	Matched	
Apr 4, 2025 10:28 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws...	443	Matched	
Apr 4, 2025 9:58 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws...	443	Matched	
Apr 4, 2025 9:31 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws...	443	Matched	
Apr 4, 2025 9:02 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws...	443	Matched	Allowed
Apr 4, 2025 8:32 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws...	443	Matched	Allowed
Apr 4, 2025 8:06 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws...	443	Matched	Allowed

Top Rules Hit

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

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.

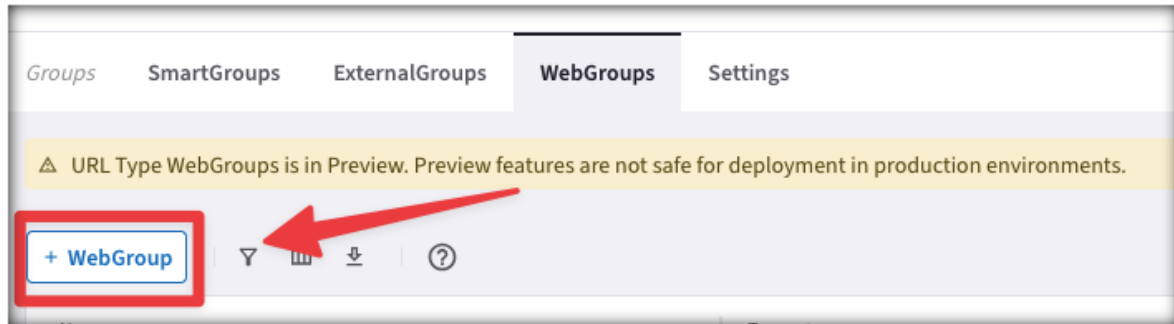
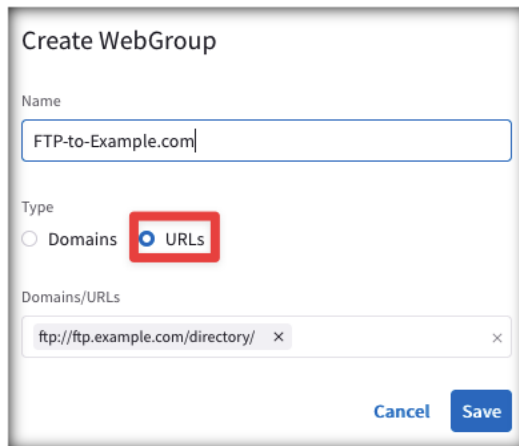
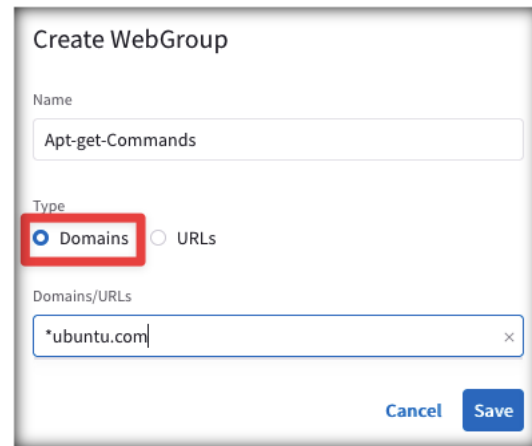


The screenshot shows the Aviatrix CoPilot interface. On the left is a dark sidebar with the 'CoPilot' header and a search bar. Below the search bar are menu items: Dashboard, Cloud Fabric, Networking, Security, and Groups (which is highlighted). The main content area has tabs for Groups, SmartGroups, ThreatGroups, GeoGroups, WebGroups (selected), 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, view, download, and help. A table lists the WebGroups:

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).

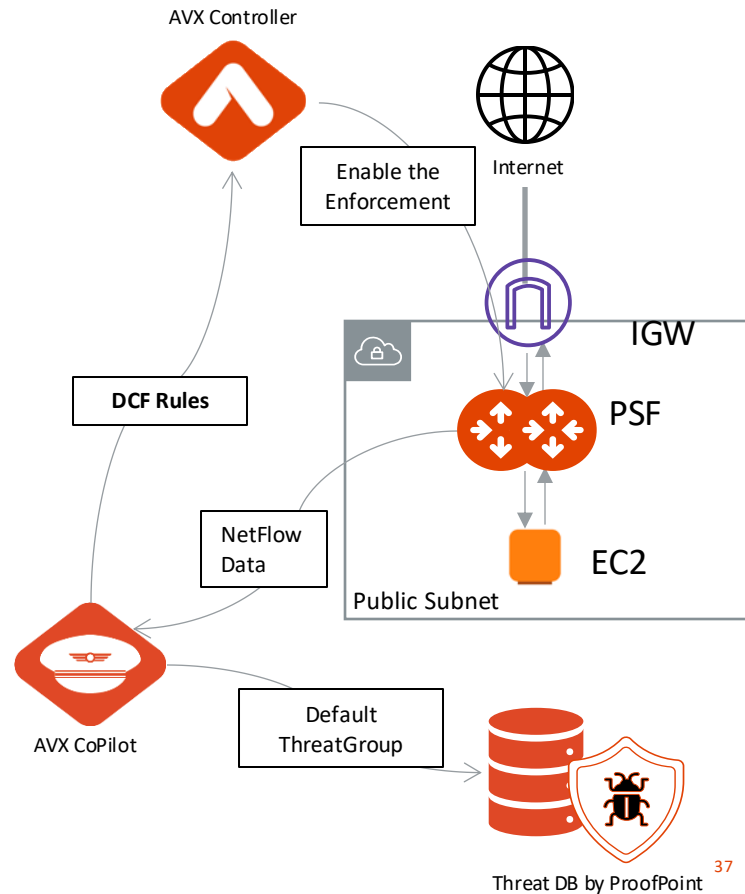






Aviatrix PSF GW(aka Public Subnet Filtering Gateway)

Aviatrix Public Subnet Filtering Gateways (PSF GWs)

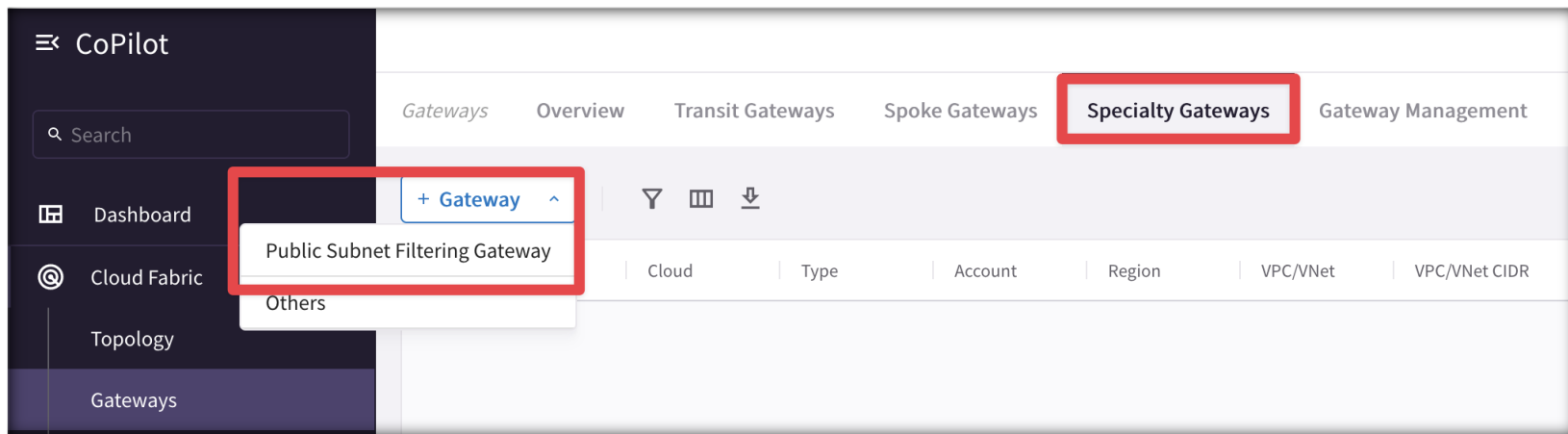
- **Public Subnet Filtering Gateways (PSF** gateways) provide ingress and egress security for **AWS** public subnets where instances have public IP addresses.
- After the Public Subnet Filtering (PSF) gateway is launched, you can apply also DCF (Distributed Cloud Firewall) rules – *enforcement must be enabled*.
- The PSF Gateway acts as a **standalone Gateway** (it's neither a Spoke nor a Transit).
- Leverage the **Default ThreatGroup** (i.e. a Malicious IP addresses DB supplied by ProofPoint) if you want to prevent attacks towards your public-facing workloads.



Aviatrix PSF Deployment Workflow (part.1)

To deploy a Public Subnet Filtering Gateway:

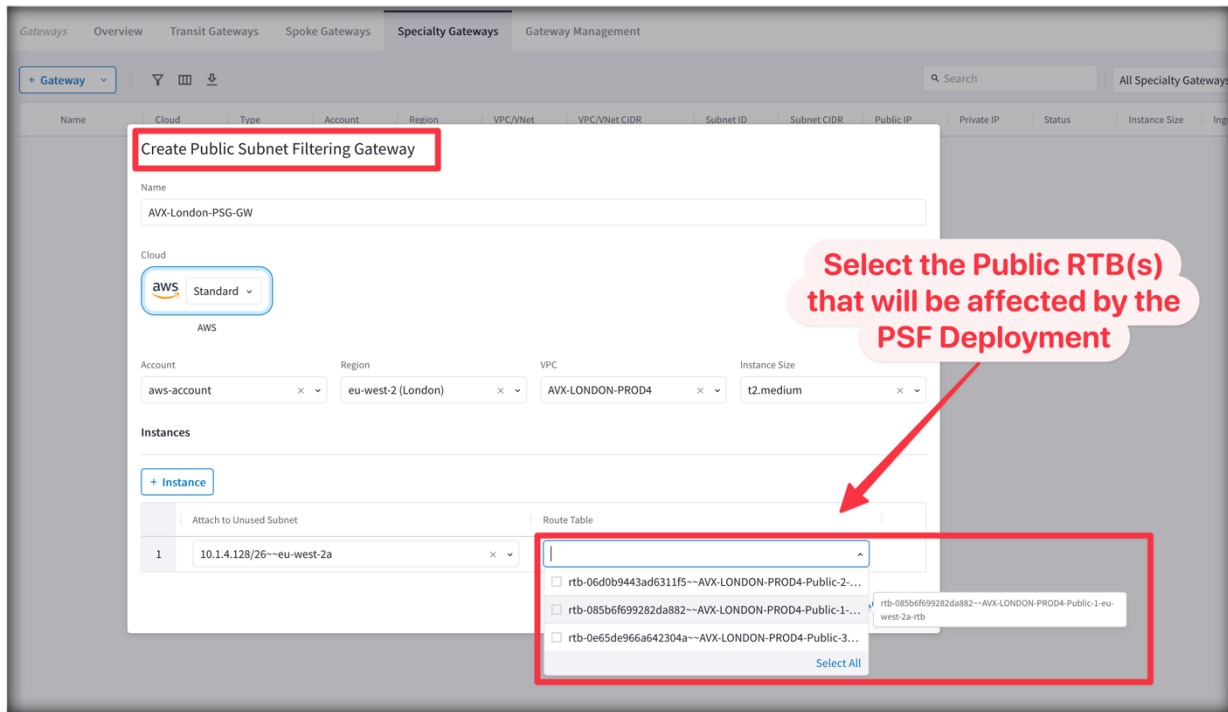
1. In CoPilot, navigate to **Cloud Fabric** > **Gateways** > **Speciality Gateways** tab.
2. Click **+Gateway** and select **Public Subnet Filtering Gateway**.



Aviatrix PSF Deployment Workflow (part.2)

3. Fill up the relevant fields with the required parameters.
4. Select the Public RTB that will get its default route affected (i.e. pointing to the PSF, instead of the IGW)

After the Public Subnet Filtering Gateway is deployed, **Ingress traffic** from IGW is routed to the gateway in a “pass through” manner. **Egress traffic** from instances in the protected public subnets is routed to the PSF gateway in a pass through manner.



The screenshot shows the 'Create Public Subnet Filtering Gateway' form in the Aviatrix console. The form is titled 'Create Public Subnet Filtering Gateway' and includes the following fields:

- Name:** AVX-London-PSG-GW
- Cloud:** AWS (Standard)
- Account:** aws-account
- Region:** eu-west-2 (London)
- VPC:** AVX-LONDON-PROD4
- Instance Size:** t2.medium

Below these fields is a table for 'Instances' with a '+ Instance' button. The table has columns for 'Attach to Unused Subnet' and 'Route Table'. The first row shows a subnet '10.1.4.128/26--eu-west-2a' and a dropdown for 'Route Table'. The dropdown menu is open, showing a list of route tables:

- ☐ rtb-06d0b9443ad6311f5--AVX-LONDON-PROD4-Public-2...
- ☐ rtb-085b6f699282da882--AVX-LONDON-PROD4-Public-1...
- ☐ rtb-0e5de966a642304a--AVX-LONDON-PROD4-Public-3...

A red arrow points to the dropdown menu with the text: '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)