



Security

SOLUTIONS ENGINEERING

www.aviatrix.com

Agenda

- Aviatrix Security Features Overview
- Securing Aviatrix Platform
- Layer-4 Stateful Firewall
- Egress

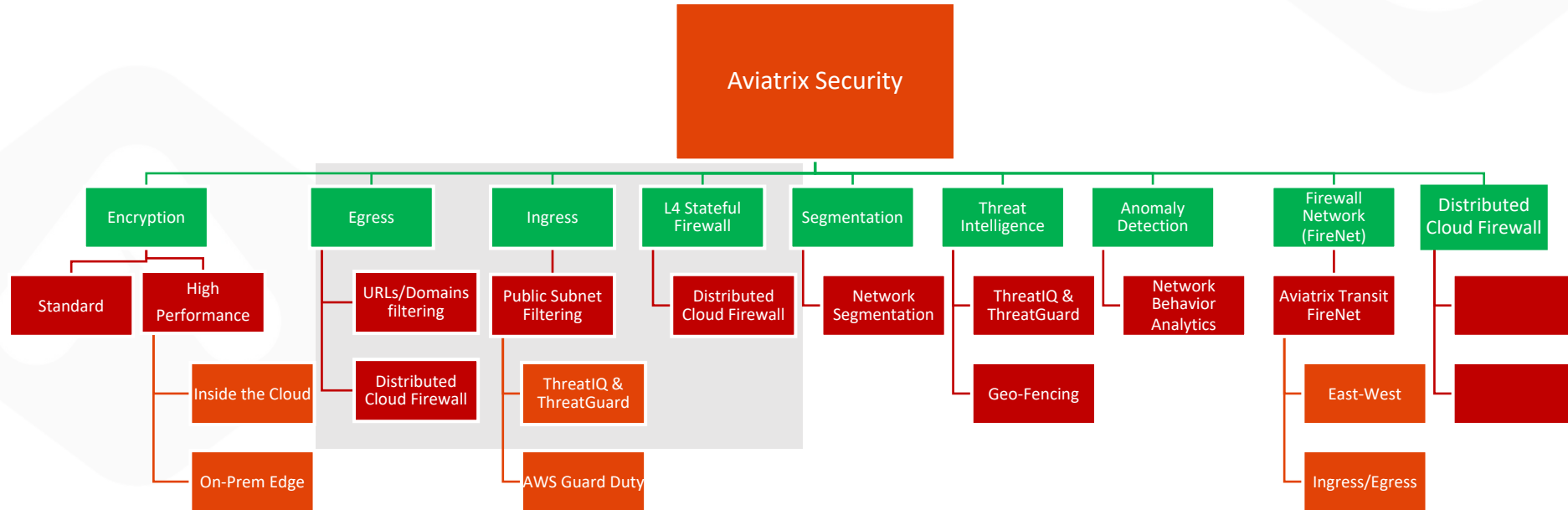
Challenges for CISO, CIO/CTO and NetSec Architects

- 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>

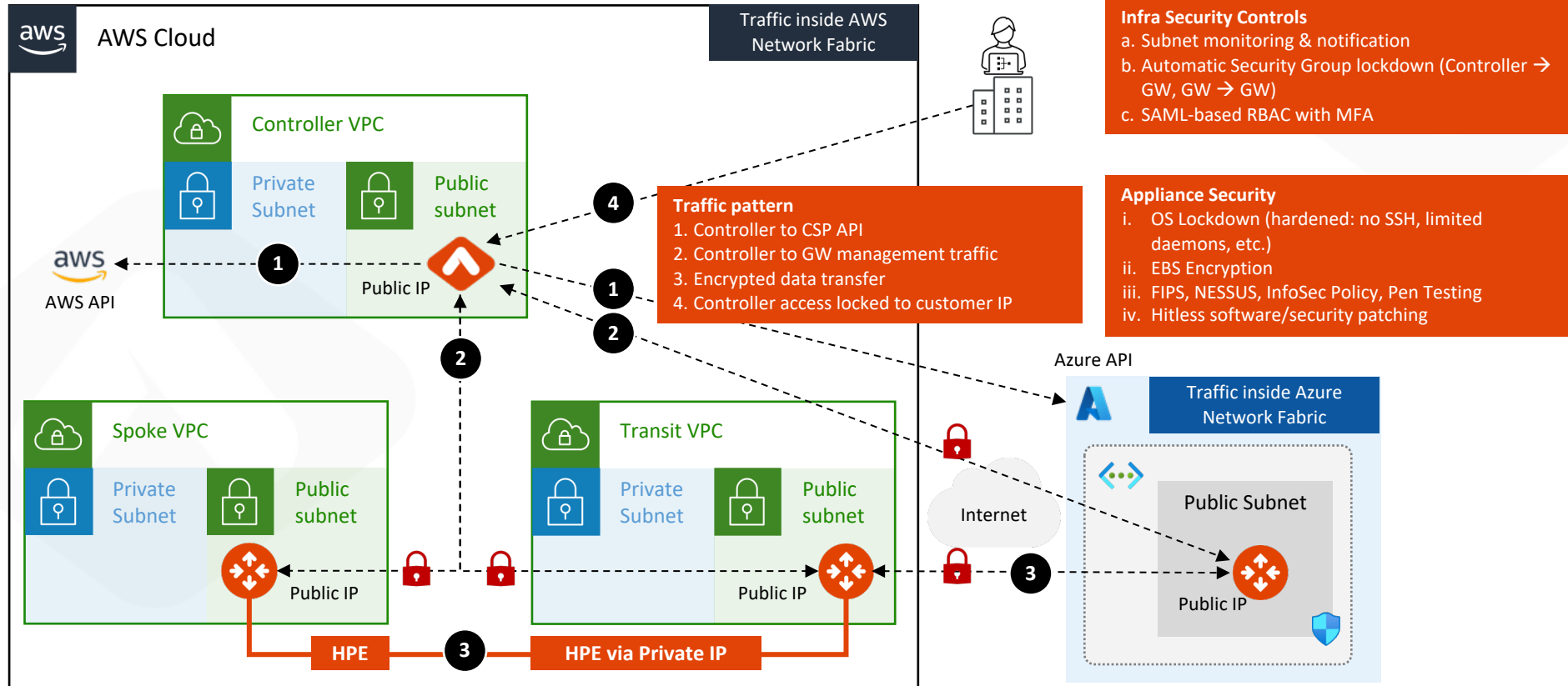
Important Aviatrix Security Features





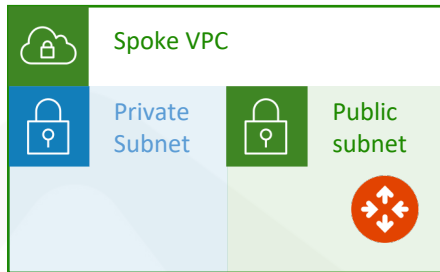
Built-in Security of the Aviatrix Platform

Secure Aviatrix Infrastructure Deployment | Example in AWS & Azure



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).



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-0f3adcfa8937a6dc6

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

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

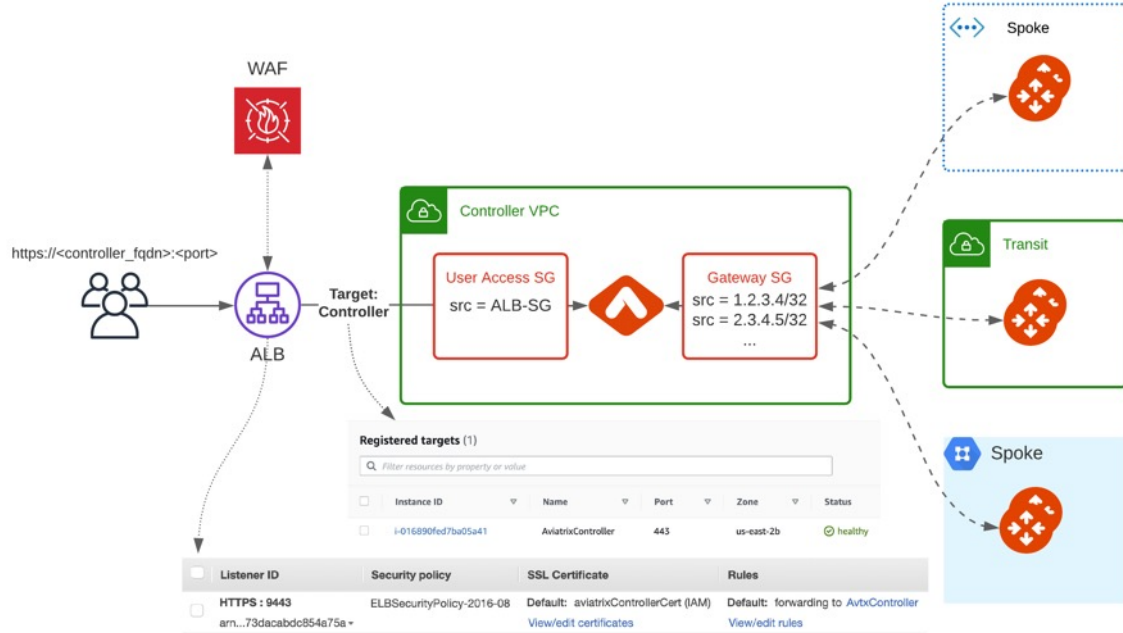
Problem Statement

- 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

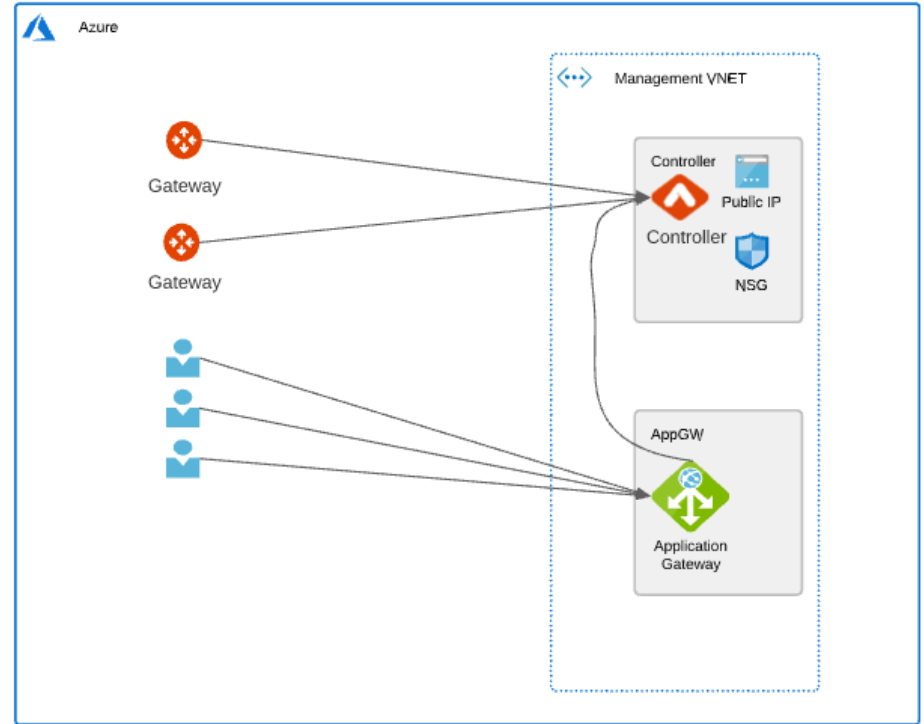
- **Limit management access to Controller**
 - Only allow access from the LB internal IPs to Controller on port 443
- **WAF capability on LBs**
 - Stops usual web hacks/attacks against controller
- **L7 LB managing Controller certificate**
 - Potentially terminating the SSL connection on LB [cloud native 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

- Enable Controller Security Group Management to only allow access to the Controller EP 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



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





Stateful Firewall

Stateful Firewall



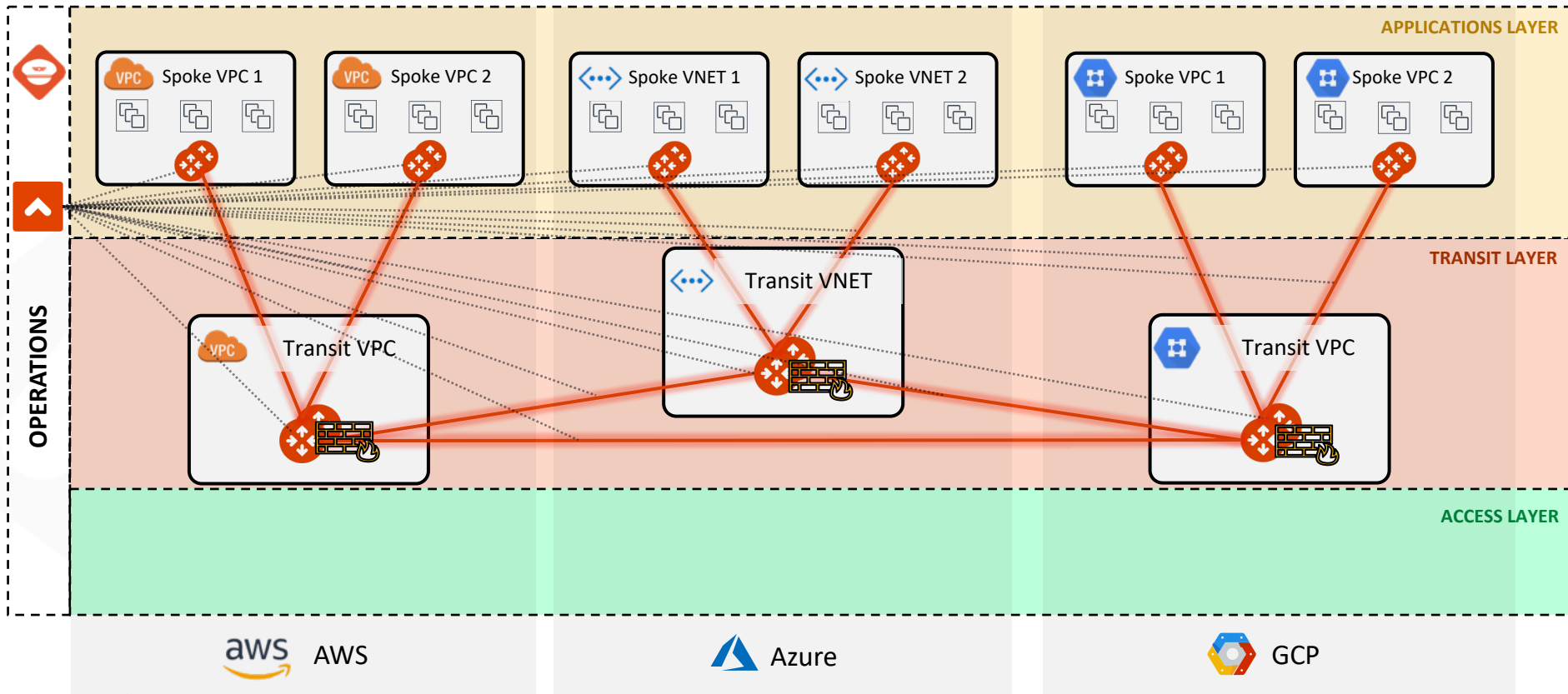
- L4 Stateful Firewall
- Filters network CIDRs, protocols and ports
- Great to be used for Centralized L4 FWs in transit
- Rule:
 - Allow
 - Deny
 - Force Drop
- Up to 1000 rules per Gateway (soft limit)
- This feature is also used in Public Subnet Filtering (Guard Duty Enforcement) to enforce the rules

Base Policy ☐ Allow all ☒ Deny all

Enable Packet Logging ☒

SOURCE	DESTINATION	PROTOCOL	PORT RANGE	ACTION	PACKET LOGGING	DESCRIPTION
10.100.100.0/24	10.200.200.0/24	TCP	443	Allow	on	zero-trust

Centralized L4 FWs at Aviatrix Transit



Applying Firewall Rules

1- Group multiple CIDRs in a single tag for ease of use

[Tag Management](#)

Edit tag DatabaseApps

NAME CIDR

App1 192.168.1.0/24

+ INSERT CIDR

DELETE

App2 192.168.2.0/24

+ INSERT CIDR

DELETE

+ ADD NEW

UPDATE

CLOSE

ThreatGuard uses this feature

2- Pick the GW where Policy needs to be enforced

Policy [Info](#)

EDIT

Page Size: 50

Name	State	CIDR	Public IP	Private IP	Size	Cloud	Gateway Zone	Stateful Firewall
avx-demo-all-sydney-transit	up	[10.4.0.0/23]	47.74.88.96	10.4.0.5	ecs.g5ne.large	Alibaba Cloud	ap-southeast-2b	Disabled
avx-demo-all-sydney-transit-hagw	up	[10.4.0.0/23]	47.74.88.81	10.4.0.27	ecs.g5ne.large	Alibaba Cloud	ap-southeast-2b	Disabled
AWS-Spoke1	up	[10.2.0.0/16]	23.21.86.88	10.2.125.94	t3.medium	AWS	us-east-1a	Disabled
AWS-Spoke1-hagw	up	[10.2.0.0/16]	54.147.79.21	10.2.134.189	t3.medium	AWS	us-east-1b	Disabled
AWS-Spoke2	up	[10.3.0.0/16]	3.83.60.121	10.3.115.218	t3.medium	AWS	us-east-1a	Enabled
AWS-Spoke2-hagw	up	[10.3.0.0/16]	18.214.48.229	10.3.131.75	t3.medium	AWS	us-east-1b	Enabled

3- Apply the rules using Tags or CIDRs

Base Policy ☒ Allow all ☐ Deny all

Enable Packet Logging ☐

DISPLAY MODE EDIT MODE DEL ALL

Source	Destination	Protocol	Port Range	Action	Packet Logging	Description
45.88.137.253/32	0.0.0.0/0			force-drop	off	ThreatIQ 2022-01-23T19:09:00.940Z
0.0.0.0/0	45.88.137.253/32			force-drop	off	ThreatIQ 2022-01-23T19:09:00.940Z
107.189.29.142/32	0.0.0.0/0			force-drop	off	ThreatIQ 2022-01-23T21:31:00.599Z
0.0.0.0/0	107.189.29.142/32			force-drop	off	ThreatIQ 2022-01-23T21:31:00.599Z



Egress

Problem Statement

Private workloads need internet access

- SaaS integration



- Patching

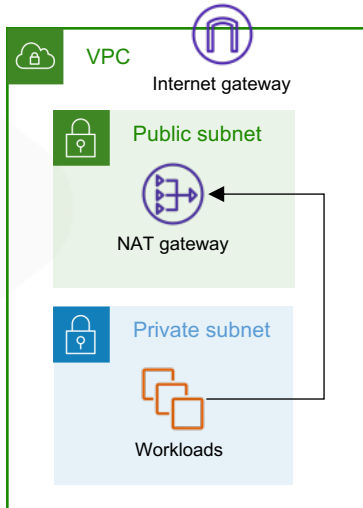


- Updates



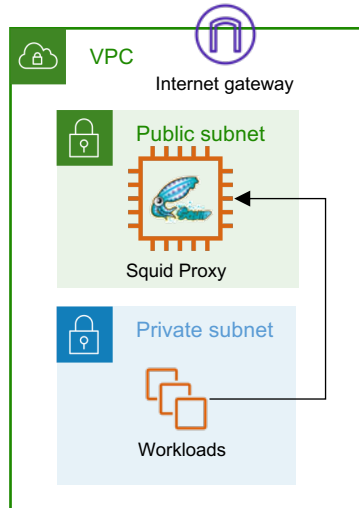
NAT Gateway

- NACLs are necessary
- Unrestricted access



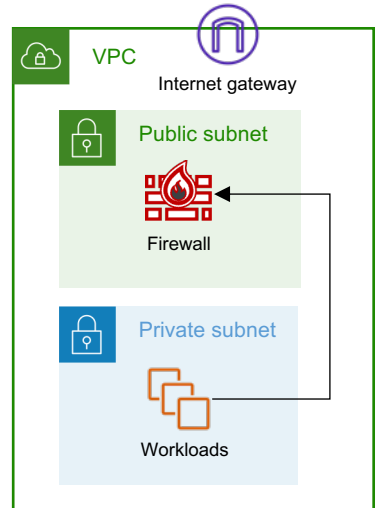
Squid Proxy

- Hard to manage
- Scale and HA issues

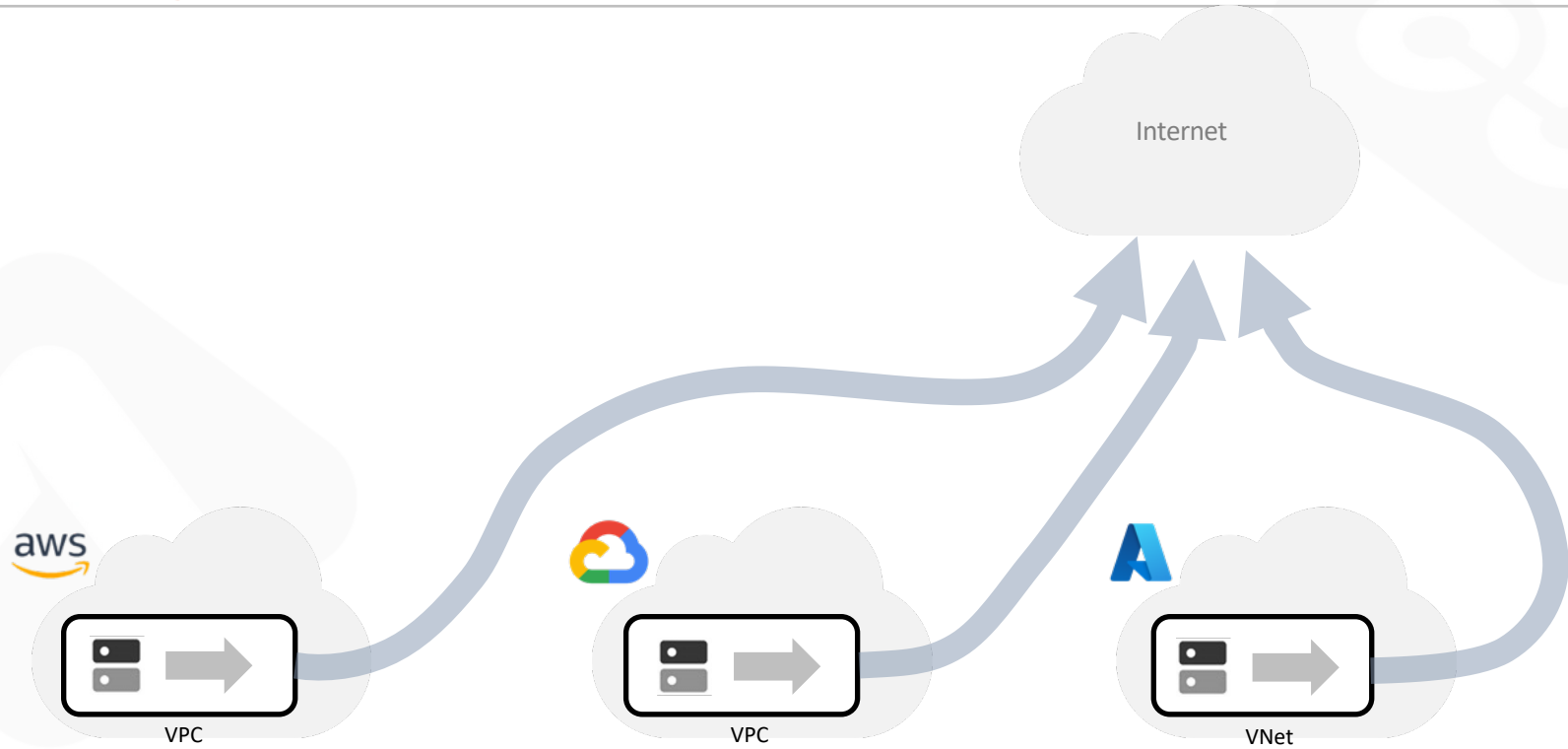


Layer-7 Firewall

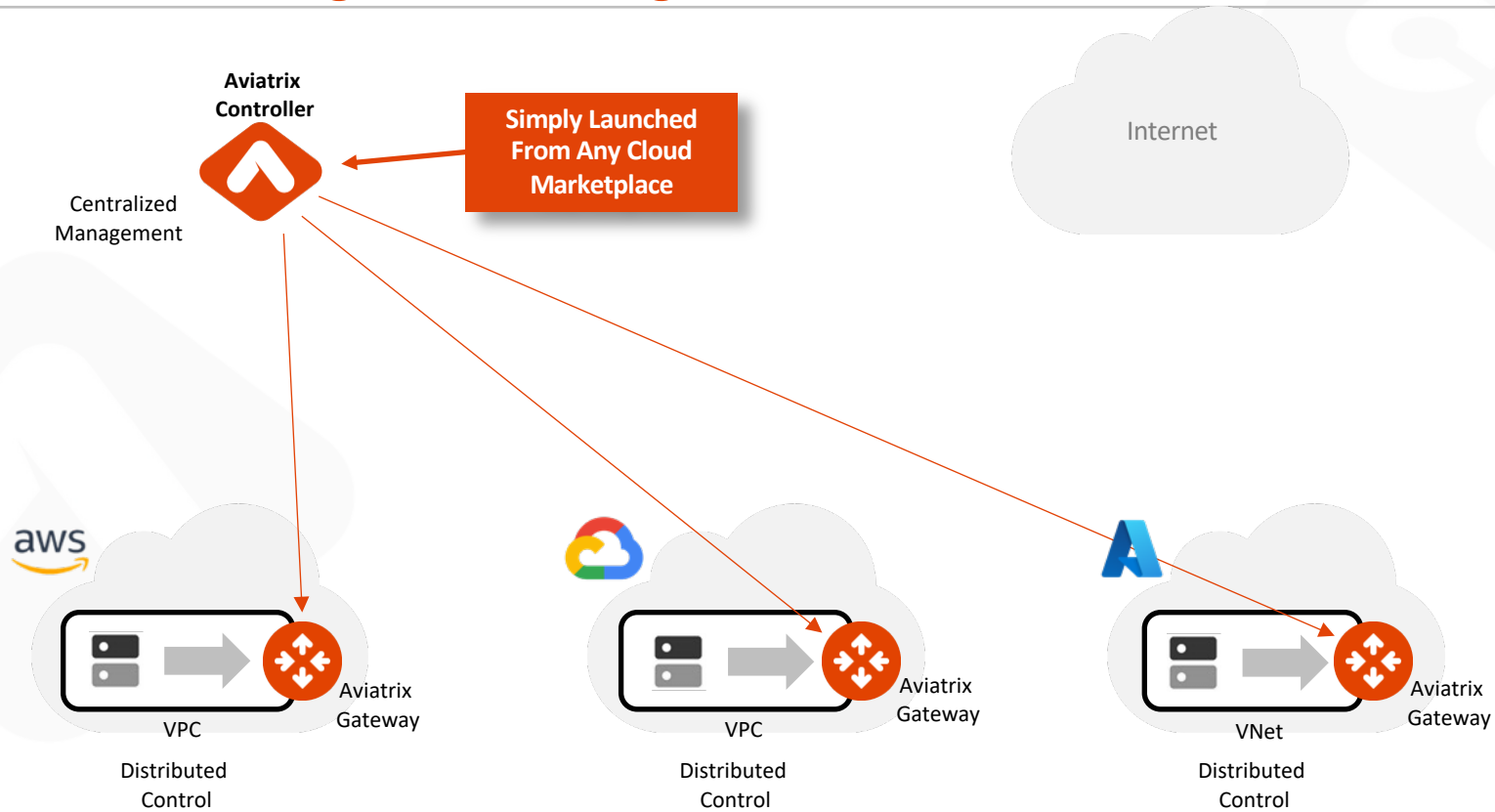
- Overkill
- Expensive



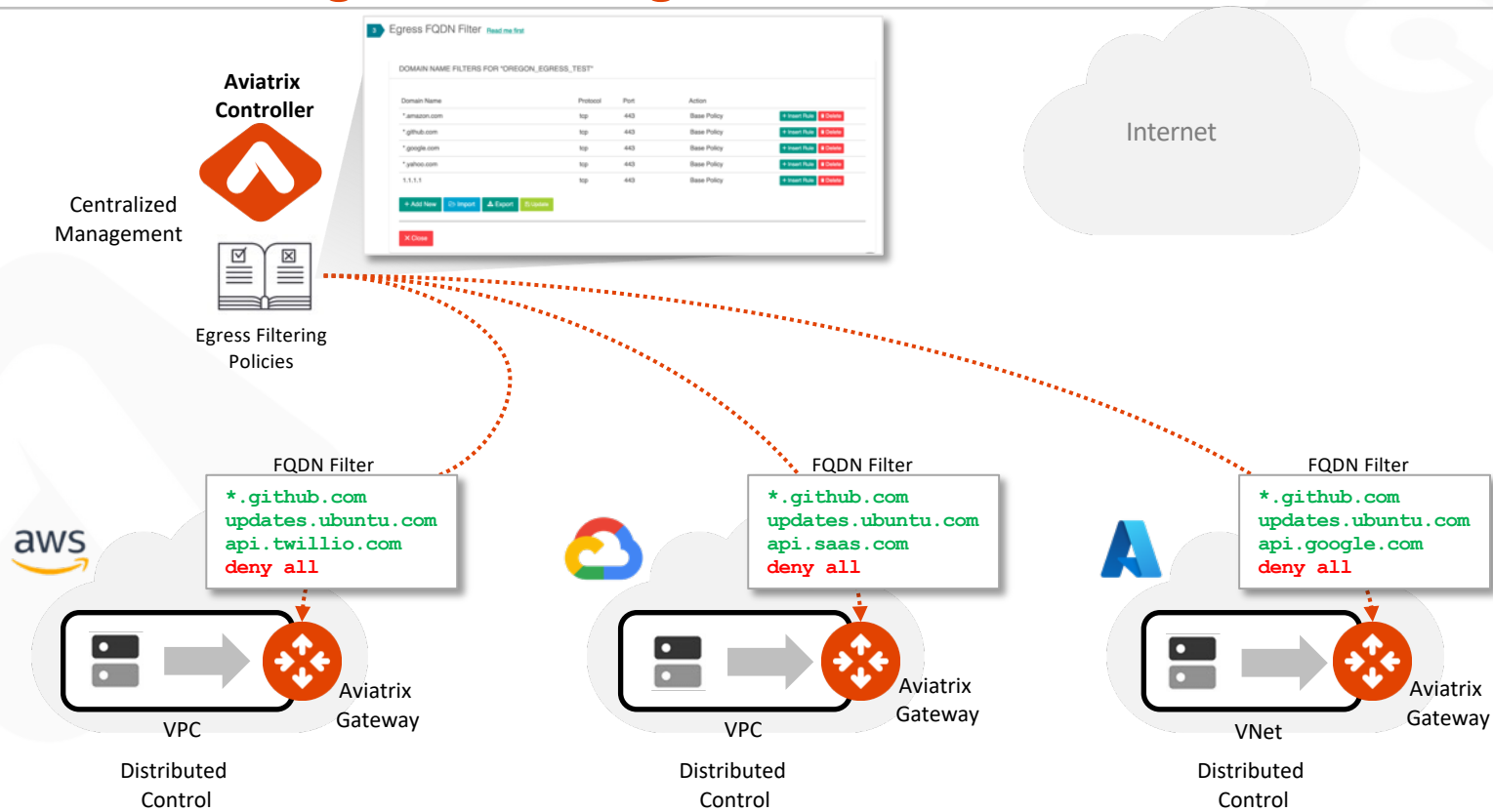
Aviatrix Egress Feature



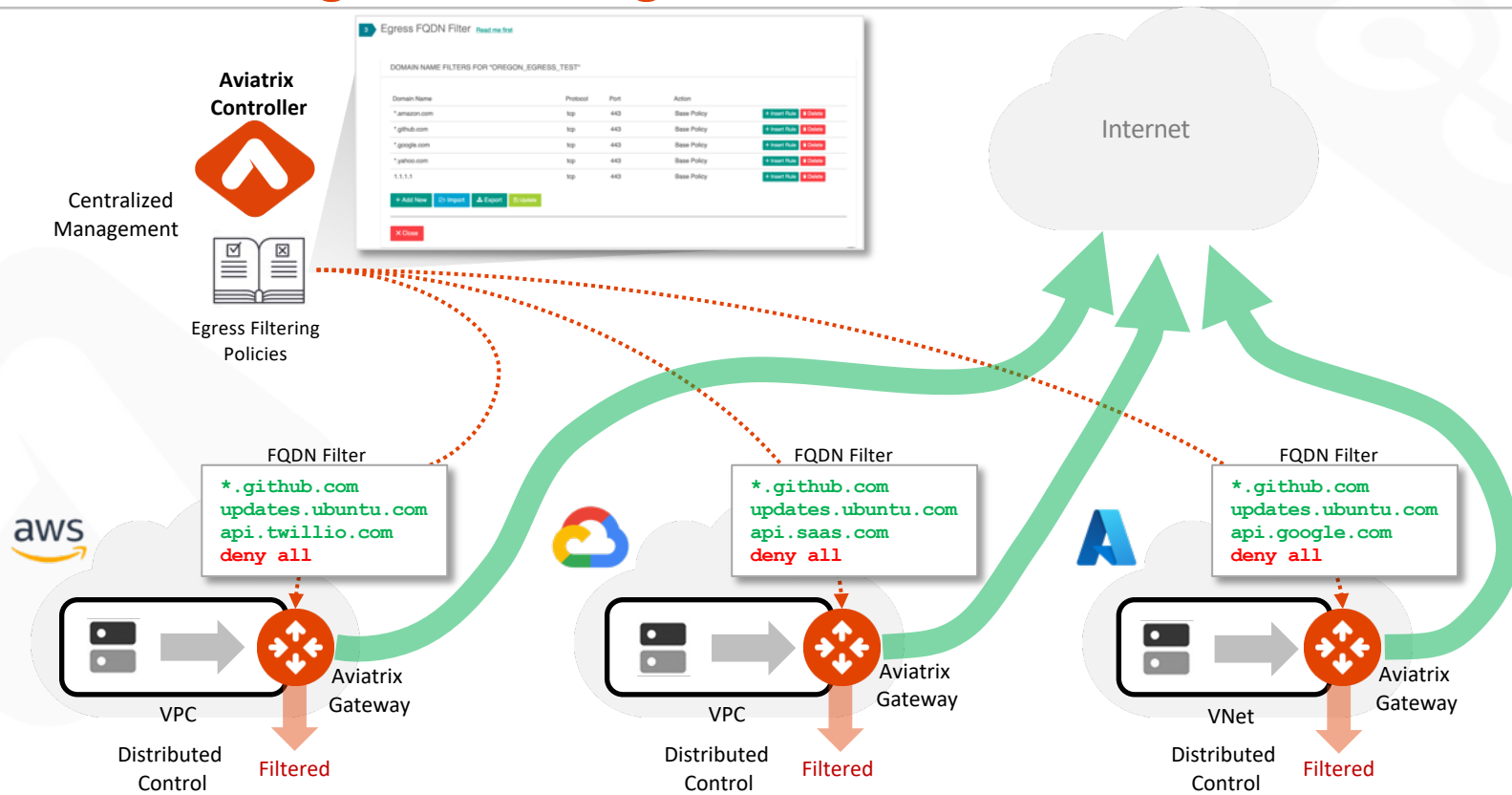
Aviatrix FQDN Egress Filtering



Aviatrix FQDN Egress Filtering

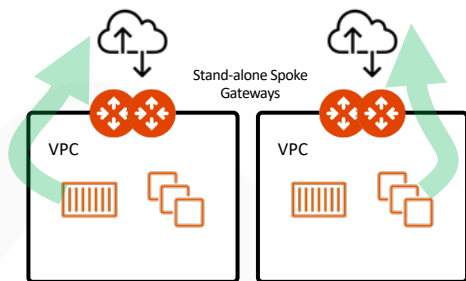


Aviatrix FQDN Egress Filtering

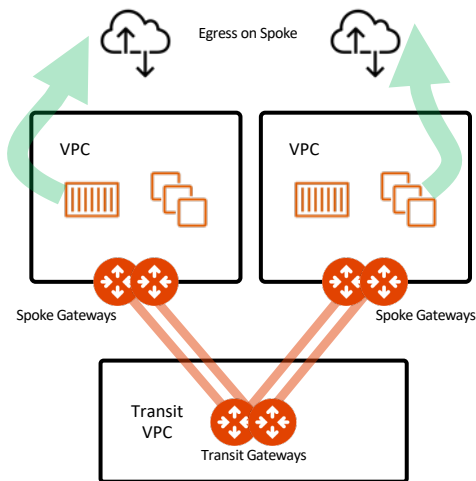


Aviatrix Egress Design Patterns

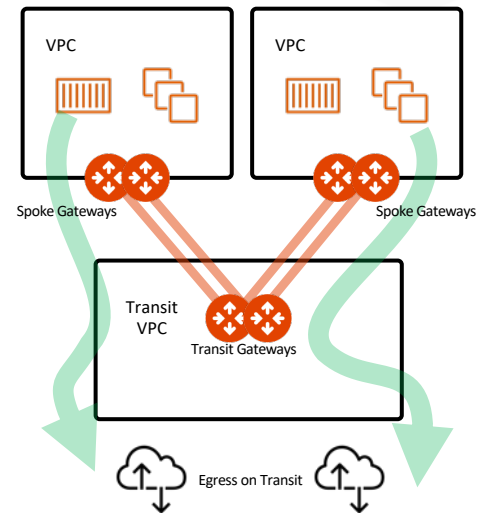
Stand-alone Spoke GW (Distributed)



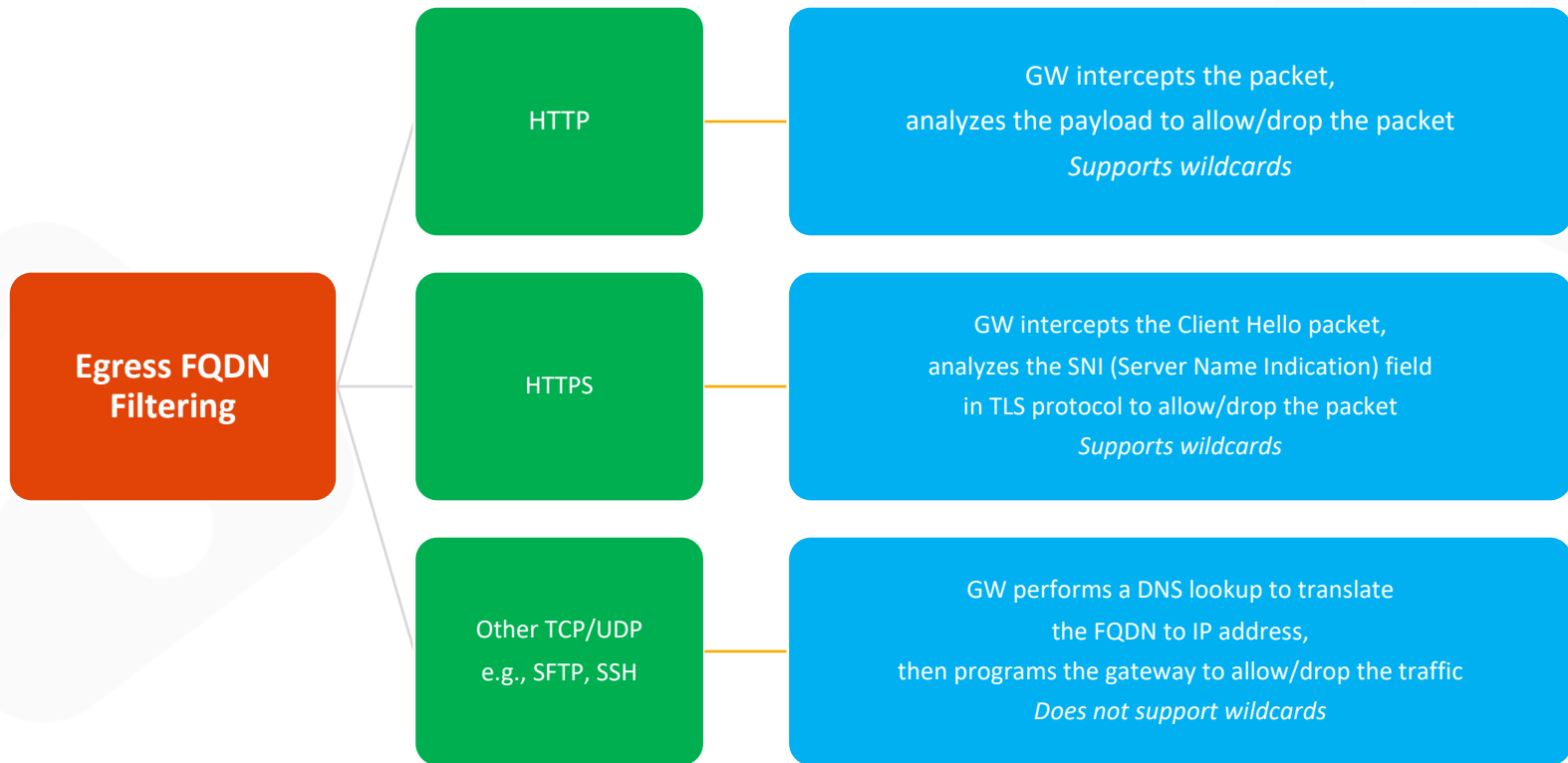
Local Egress (Distributed) with Aviatrix Spoke



Centralized Egress with Aviatrix Transit

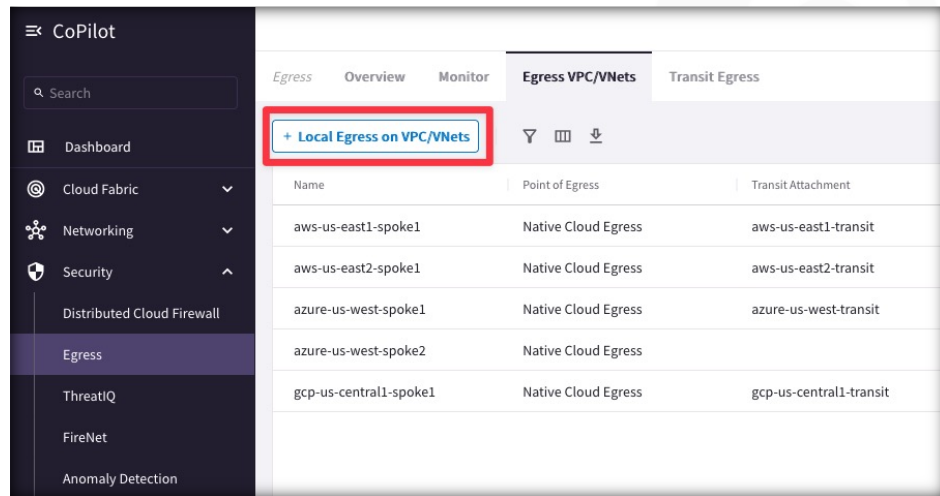


Egress FQDN Filter – Traffic Types



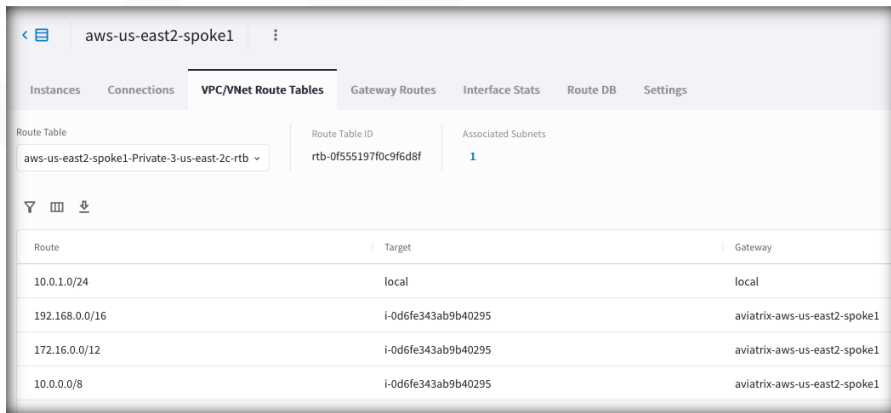
Enable Egress

- Adding Egress Control on VPC/VNet changes the default route on VPC/VNet to point to the Spoke Gateway and enables **SNAT**.
- Egress Control also requires additional resources on the Spoke Gateway.
- In addition to the **Local route**, the **three RFC1918 routes**, also a **default route** will be injected.



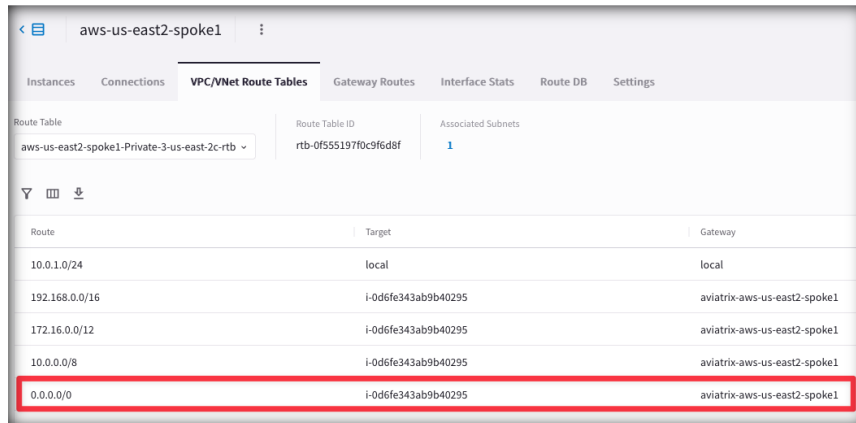
The screenshot shows the CoPilot console interface. On the left is a dark sidebar with a search bar and navigation links: Dashboard, Cloud Fabric, Networking, Security, Egress (selected), ThreatIQ, FireNet, and Anomaly Detection. The main panel has tabs for Egress, Overview, Monitor, Egress VPC/VNets (active), and Transit Egress. Under the active tab, there is a button '+ Local Egress on VPC/VNets' highlighted with a red box. Below the button is a table with columns Name, Point of Egress, and Transit Attachment.

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



The screenshot shows the AWS console interface for the 'aws-us-east2-spoke1' VPC. The 'VPC/VNet Route Tables' tab is active. The table lists routes for 10.0.1.0/24, 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8, all pointing to the 'local' gateway.

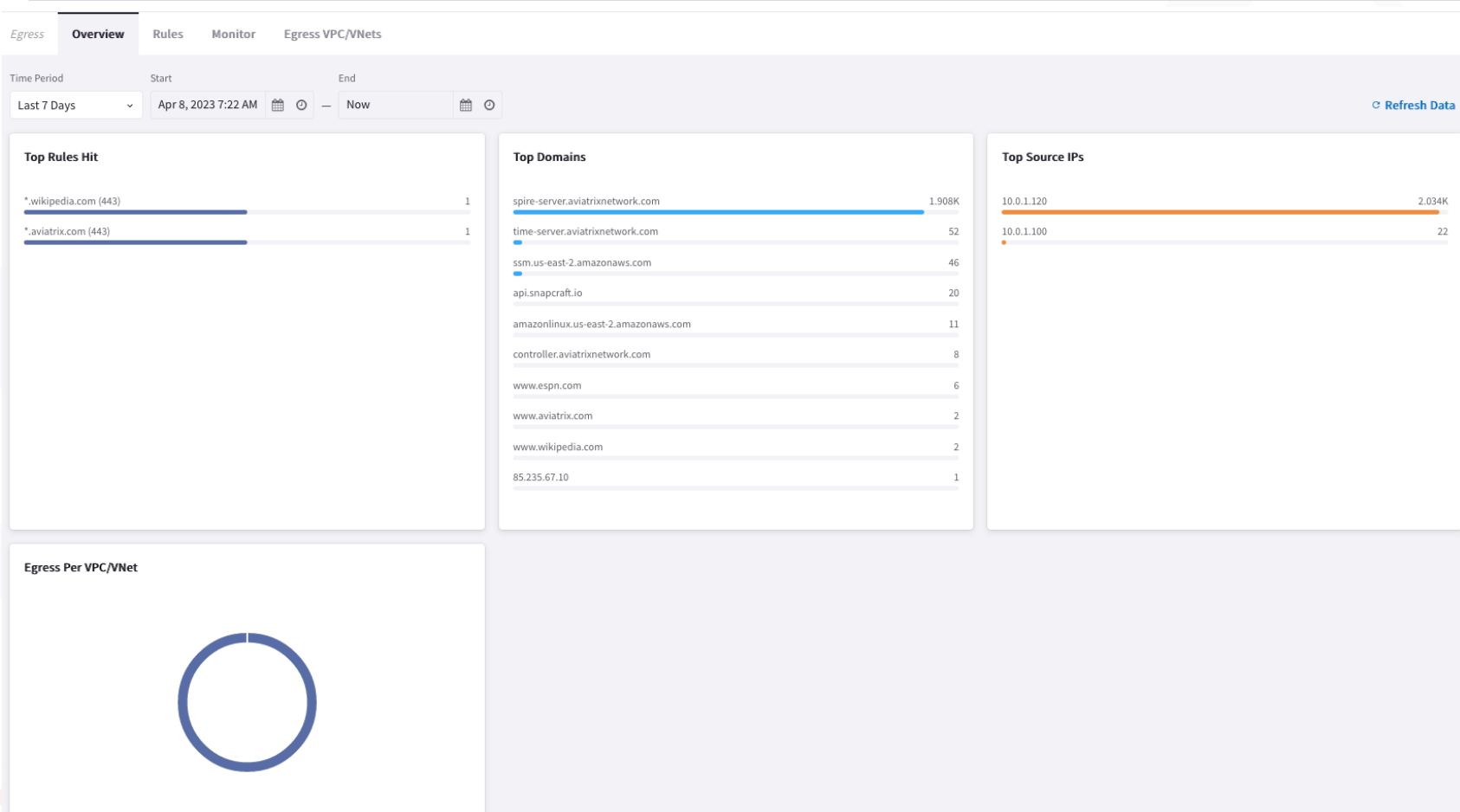
Route	Target	Gateway
10.0.1.0/24	local	local
192.168.0.0/16	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
172.16.0.0/12	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1
10.0.0.0/8	i-0d6fe343ab9b40295	aviatrix-aws-us-east2-spoke1



The screenshot shows the AWS console interface for the 'aws-us-east2-spoke1' VPC. The 'VPC/VNet Route Tables' tab is active. The table lists routes for 10.0.1.0/24, 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, and 0.0.0.0/0. The 0.0.0.0/0 route is highlighted with a red box, pointing to the 'local' gateway.

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

Visibility from CoPilot



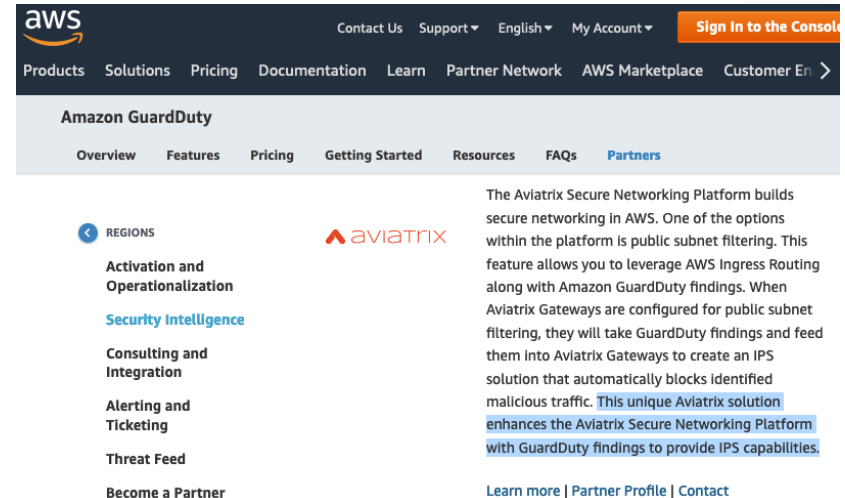


Aviatrix PSF (aka Public Subnet Filtering) with AWS GuardDuty

Problem Statement

- AWS GuardDuty is a managed service for threat detection (IDS)
 - CrowdStrike and ProofPoint provide information to GuardDuty called Indicators of Compromise (IOC)
- GuardDuty does not take any action on the malicious activity it finds
 - <https://aws.amazon.com/guardduty/resources/partners/>

AWS GuardDuty



aws

Contact Us Support English My Account Sign In to the Console

Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer En >

Amazon GuardDuty

Overview Features Pricing Getting Started Resources FAQs **Partners**

REGIONS

Activation and Operationalization

Security Intelligence

Consulting and Integration

Alerting and Ticketing

Threat Feed

Become a Partner

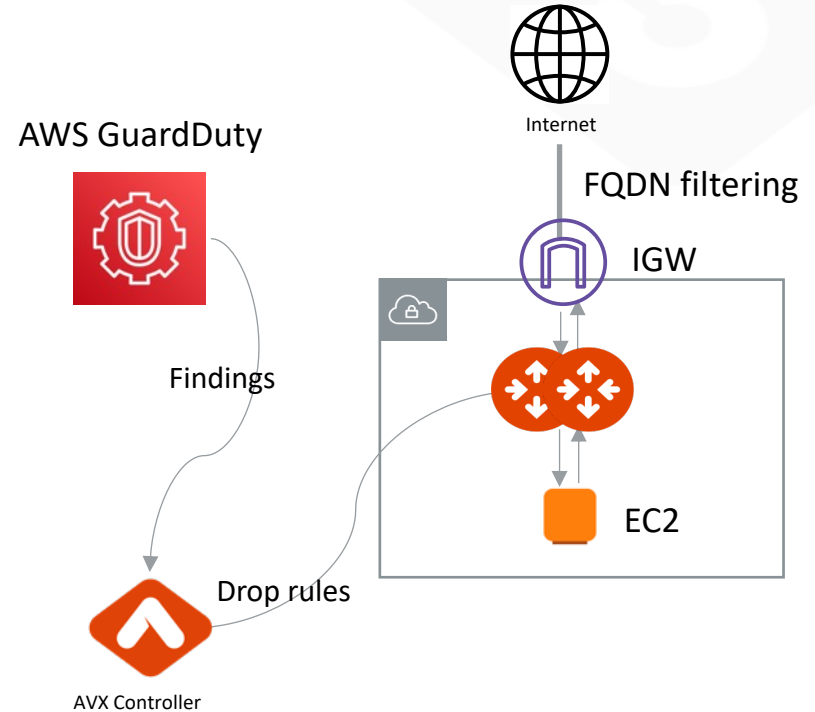
aviatrix

The Aviatrix Secure Networking Platform builds secure networking in AWS. One of the options within the platform is public subnet filtering. This feature allows you to leverage AWS Ingress Routing along with Amazon GuardDuty findings. When Aviatrix Gateways are configured for public subnet filtering, they will take GuardDuty findings and feed them into Aviatrix Gateways to create an IPS solution that automatically blocks identified malicious traffic. This unique Aviatrix solution enhances the Aviatrix Secure Networking Platform with GuardDuty findings to provide IPS capabilities.

[Learn more](#) | [Partner Profile](#) | [Contact](#)

Aviatrix GuardDuty Enforcement

- Integration with the AWS Ingress Routing
- Enables customers to act upon real-time threat intelligence information from AWS GuardDuty
- Uses Aviatrix Gateway's Stateful Firewall
- Aviatrix IPS GW is also called Public Subnet Filtering (PSF) GW





Lab 6 – Egress