Security

SOLUTIONS ENGINEERING

www.aviatrix.com

Agenda

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

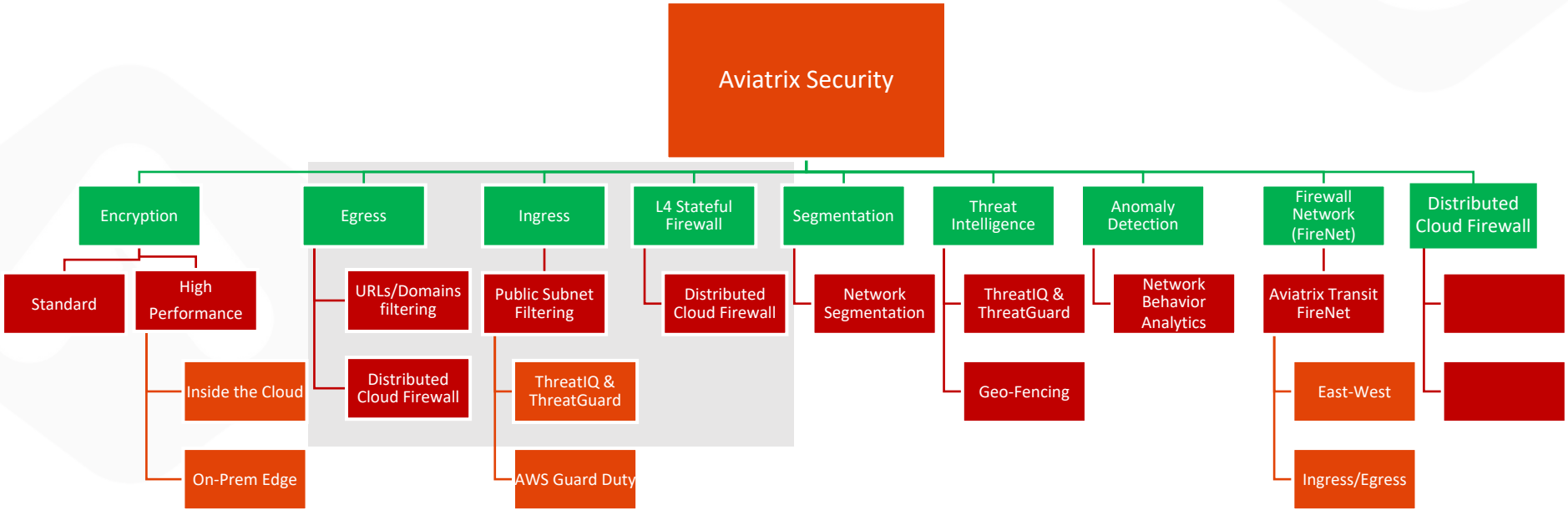
aviatrix

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

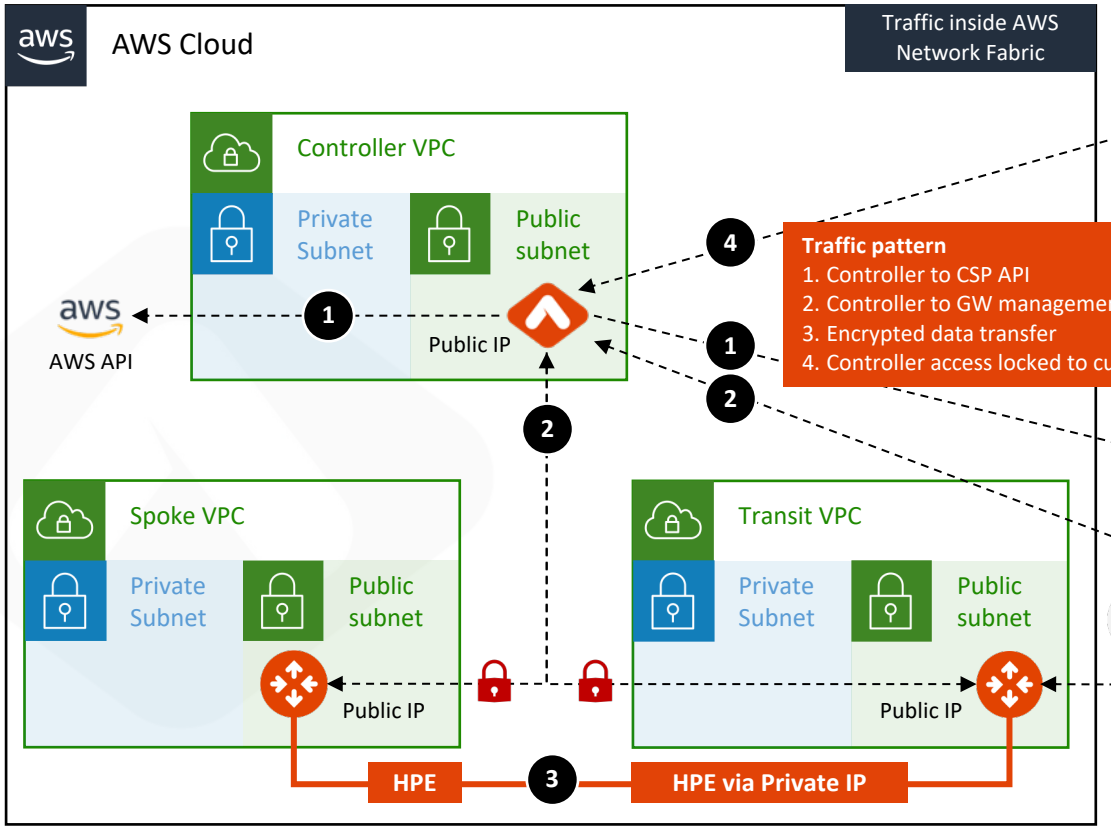
https://aviatrix.com/resources/ebooks/security-architects-guide-multi-cloud-networking-v2

Important Aviatrix Security Features



Built-in Security of the Aviatrix Platform

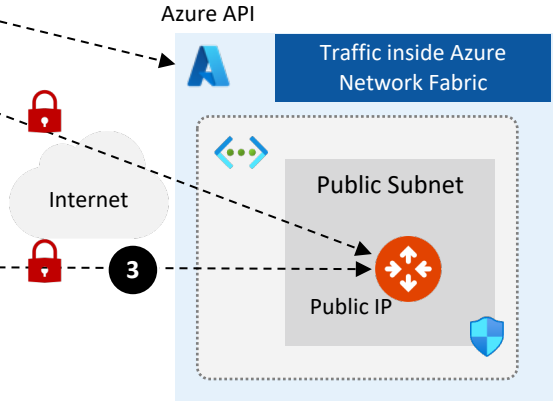
Secure Aviatrix Infrastructure Deployment | Example in AWS & Azure



Traffic pattern
1. Controller to CSP API
2. Controller to GW management traffic
3. Encrypted data transfer
4. Controller access locked to customer IP

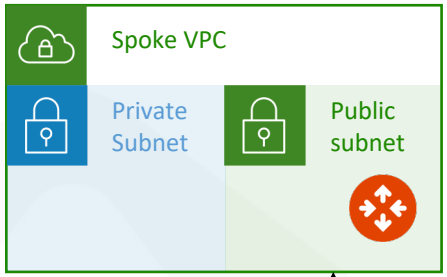
Infra Security Controls
a. Subnet monitoring & notification
b. Automatic Security Group lockdown (Controller → GW, GW → GW)
c. SAML-based RBAC with MFA

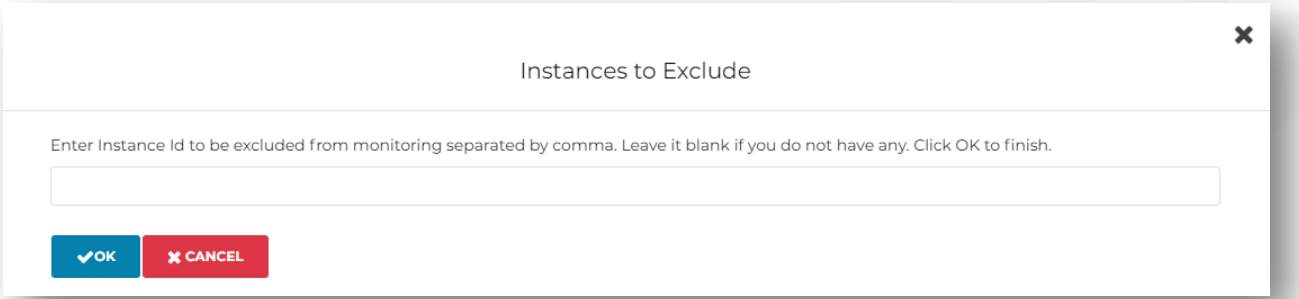
Appliance Security
i. OS Lockdown (hardened: no SSH, limited daemons, etc.)
ii. EBS Encryption
iii. FIPS, NESSUS, InfoSec Policy, Pen Testing
iv. Hitless software/security patching

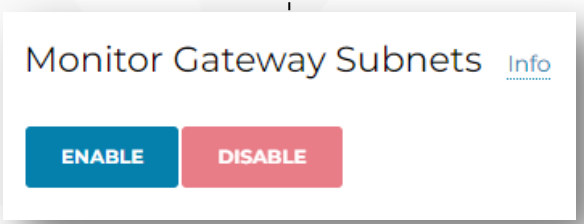


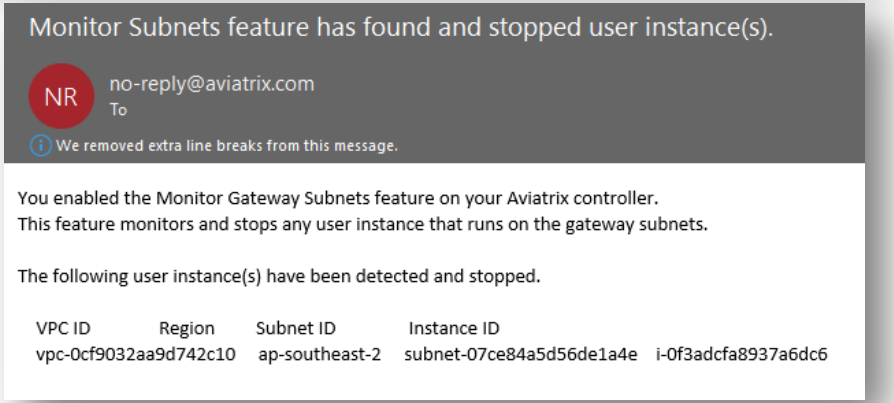
Monitor Gateway Subnets

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









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

Controller Security Group Management | Automatic Security Group lockdown

Instance: i-0ea8d13e979fb9be6 (ss-controller)

▼ Inbound rules

Filter 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

Filter rules

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

Securing the Platform with Cloud Native Load Balancers

Problem Statement

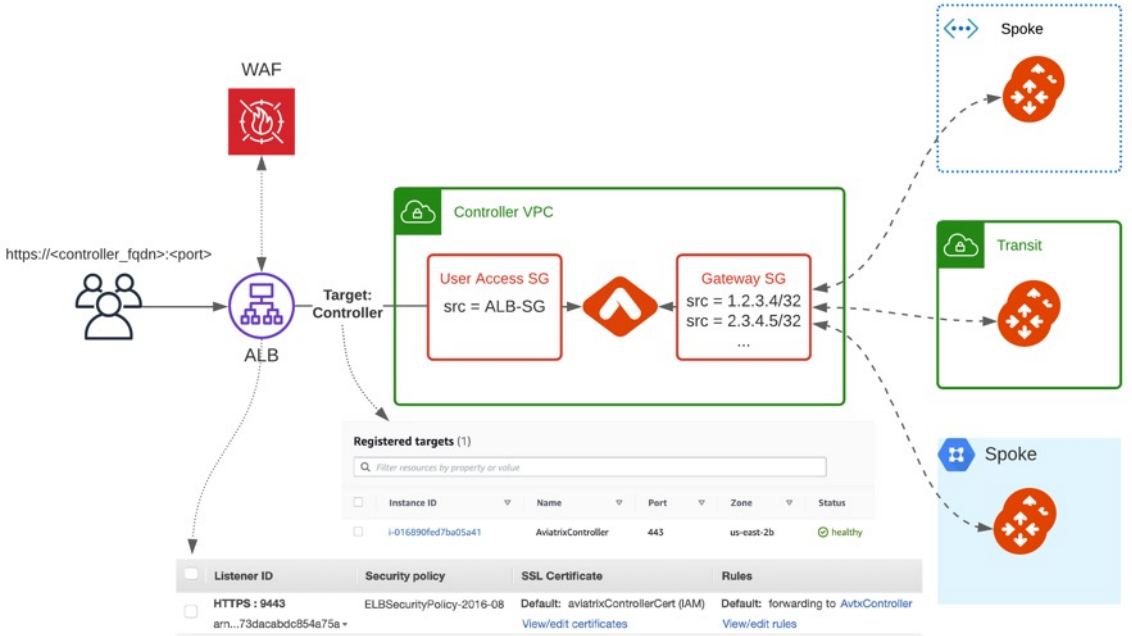
- Enterprise concerns around putting Aviatrix Controller with a public IP in a Public subnet
- Enterprises need tighter security and availability
- What are the options?
    1. Limit access using cloud native L4 stateful firewalls such as:
        - AWS Security Groups
        - Azure Network Security Groups
        - GCP Firewall Rules
    2. Deploy a third-party Firewall in front of controller
    3. Deploy an Application (L7) Load Balancer in front of Aviatrix Controller

Advantages: L7 Load Balancer in Front of Aviatrix Controller

- **Limit management access to Controller**
  - Only allow access from the LB internal IPs to Controller on port 443
- **WAF capability on LBs**
  - Stops usual web hacks/attacks against controller
- **L7 LB managing Controller certificate**
  - Potentially terminating the SSL connection on LB [cloud native process]
- **Adhere to SoPs and best practices**
  - Around alerts, operational features, logging integration, etc.
  - Putting an LB in front means Controller access can fit right into your existing operational model
- **Leverage LB health checks**
  - Monitor the Controller at an application layer
  - If the LB health check goes down, it again fits right into existing operational best practices and SoPs of customer making it easier for them to monitor the control plane
- Any access to controller, including API, UI login, etc., would go through LB, and the LB logging can provide easier, faster integration to existing tools

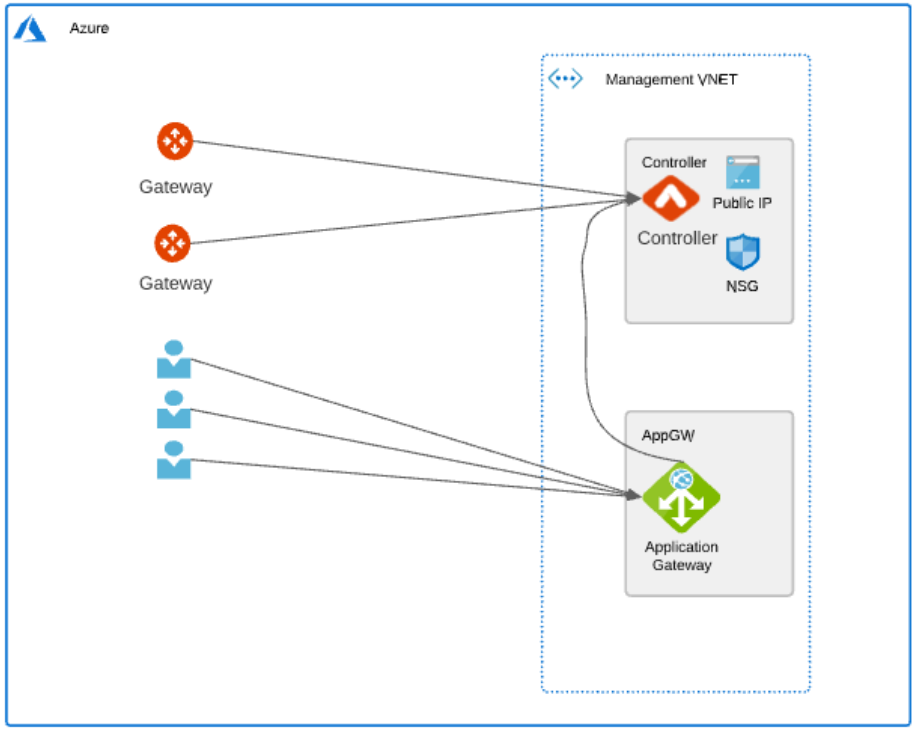
AWS

- 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

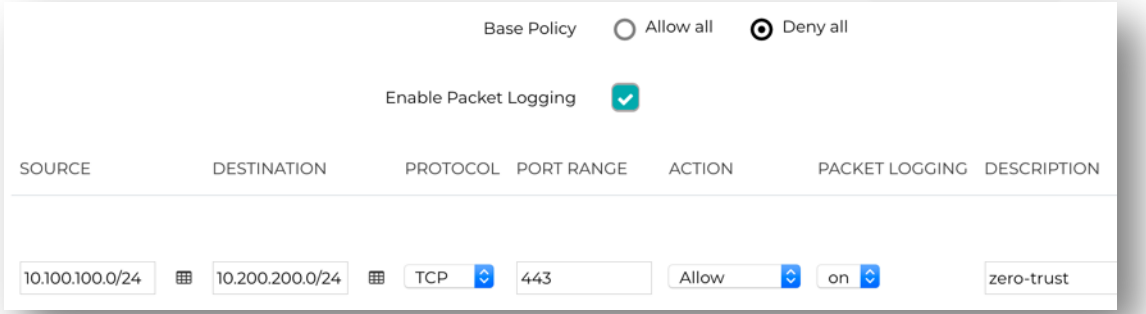
- Use WAF with Azure Managed rules on Application Gateway to limit usual web hacks/attacks against Controller
- Only allow user access from the Application Gateway subnet to Controller on port 443 (Controller Security Groups management feature is a pre-requisite for gateway communication to Controller)
- 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



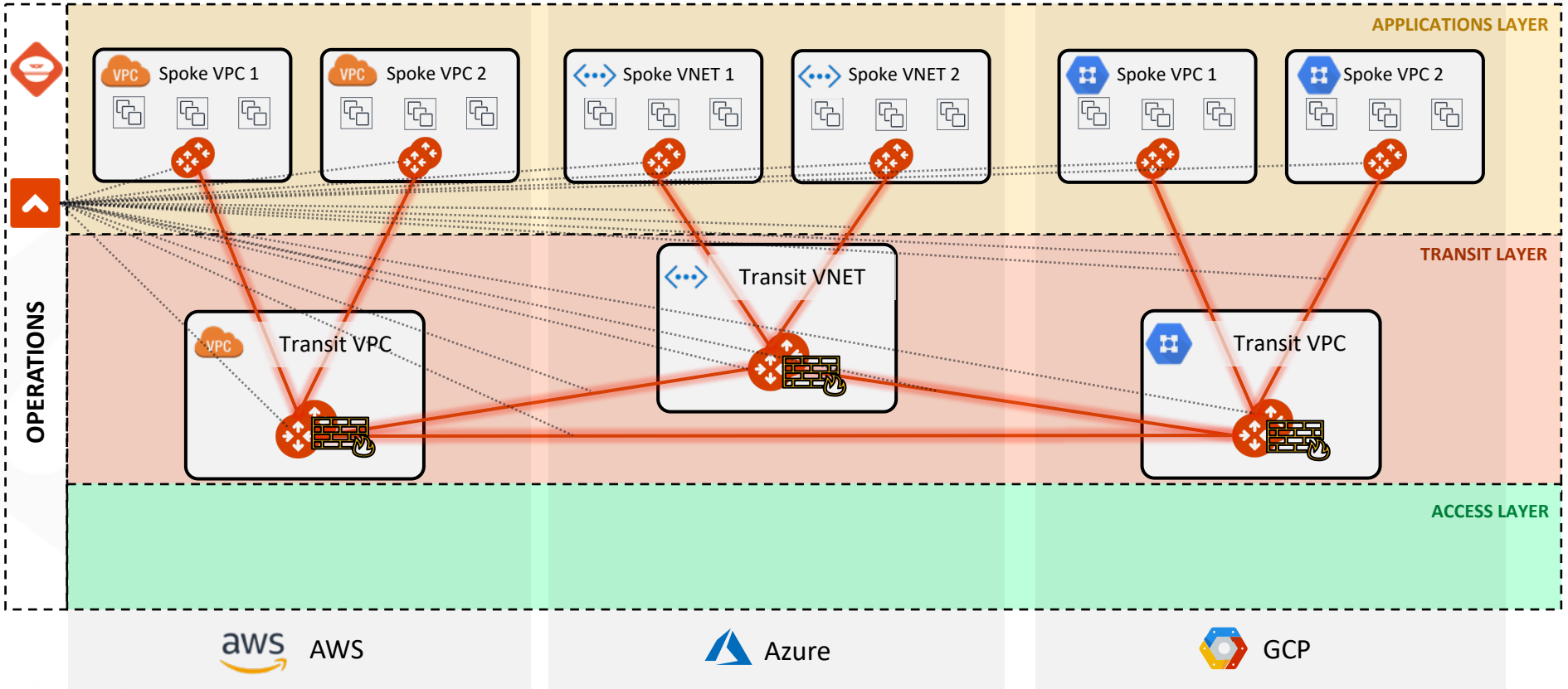
Stateful Firewall

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

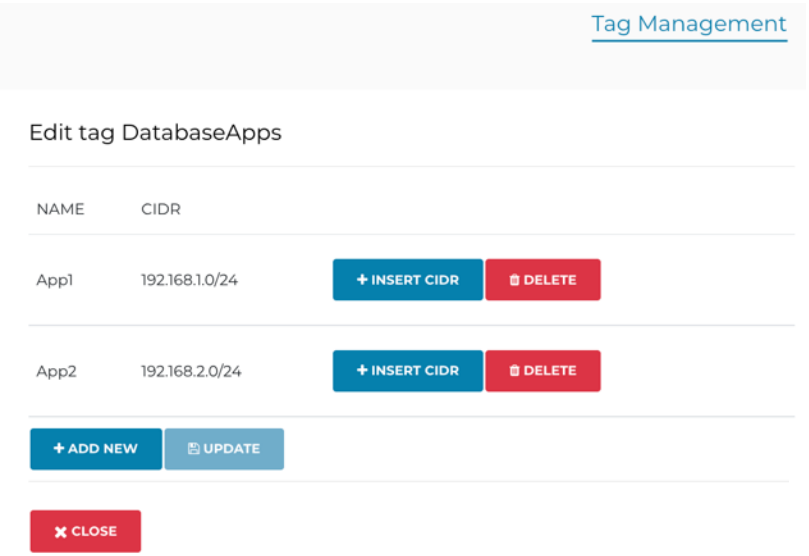


Centralized L4 FWs at Aviatrix Transit

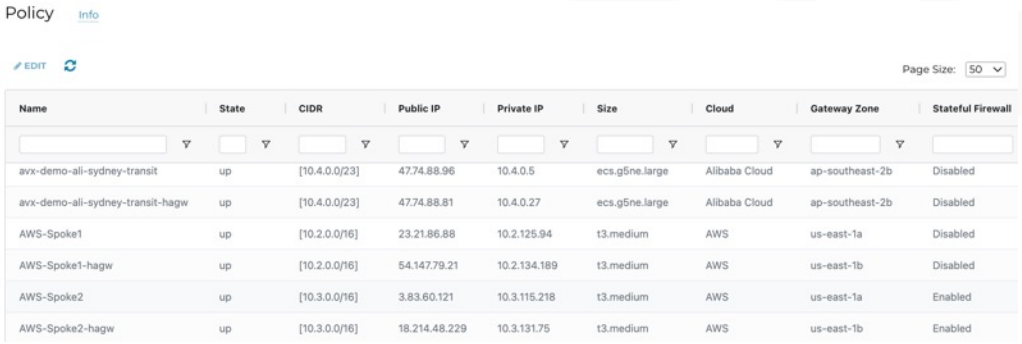


Applying Firewall Rules

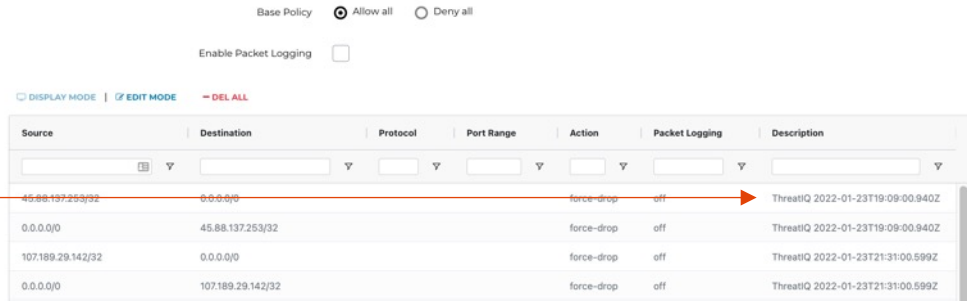
1- Group multiple CIDRs in a single tag for ease of use



2- Pick the GW where Policy needs to be enforced



3- Apply the rules using Tags or CIDRs



ThreatGuard uses this feature

aviatrix

Egress

Problem Statement

Private workloads need internet access

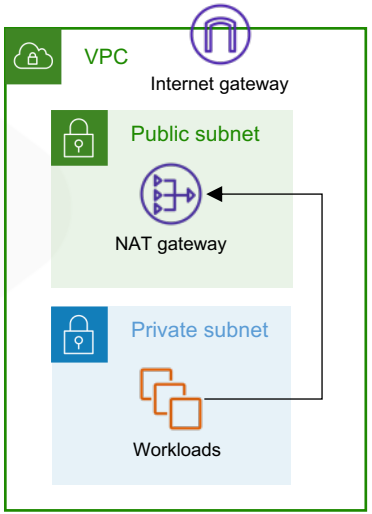
- **SaaS integration**

- **Patching**

- **Updates**

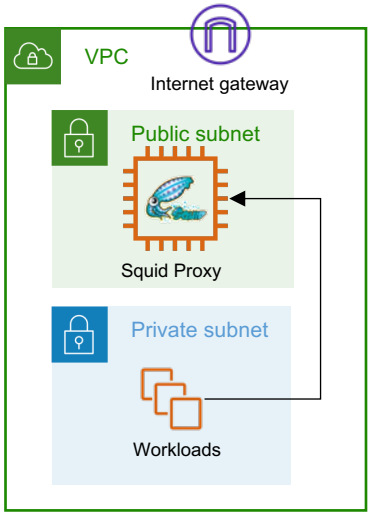
NAT Gateway

- NACLs are necessary
- Unrestricted access



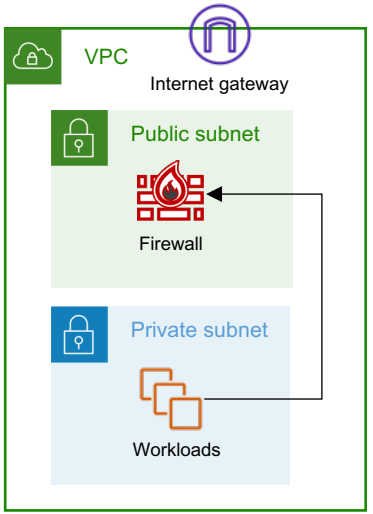
Squid Proxy

- Hard to manage
- Scale and HA issues

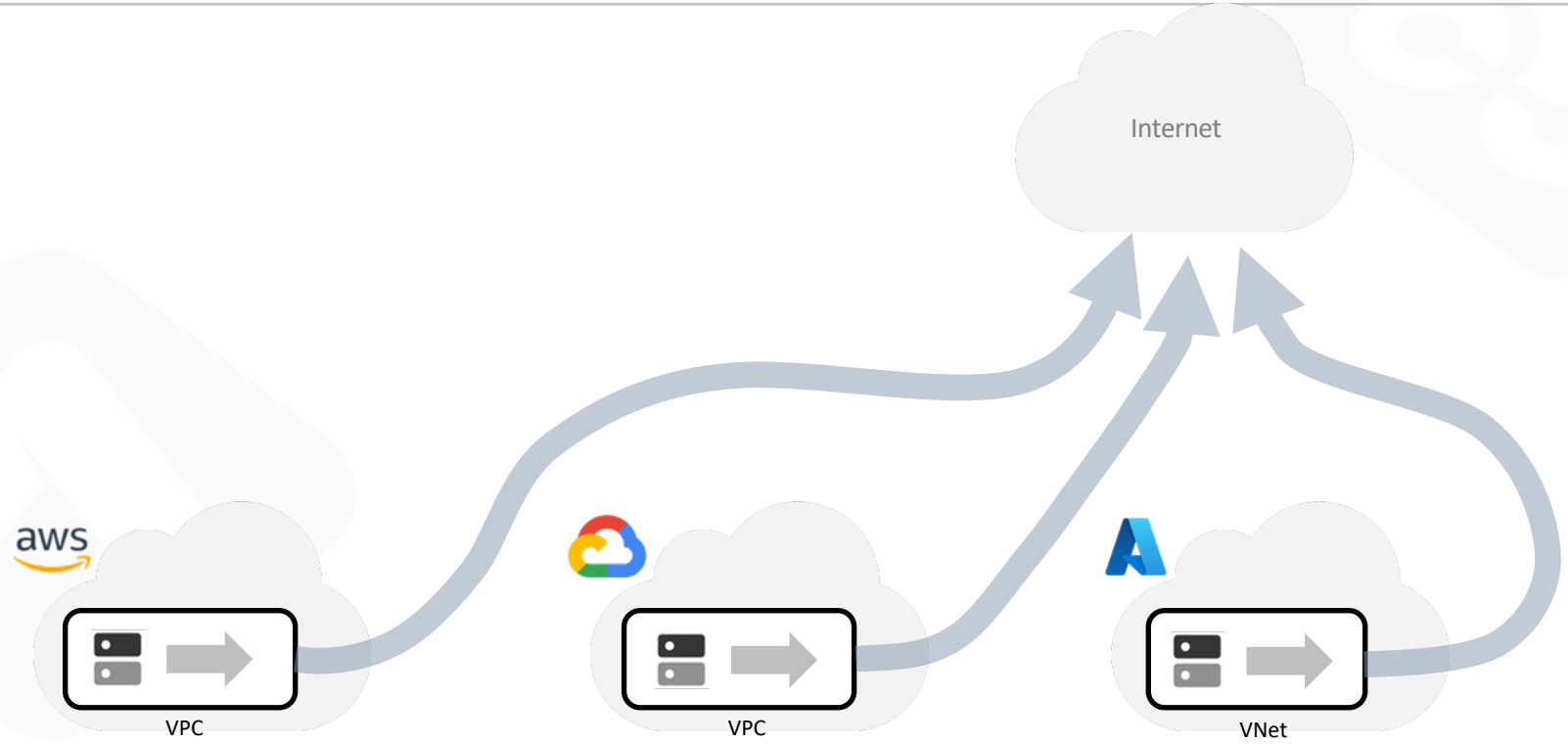


Layer-7 Firewall

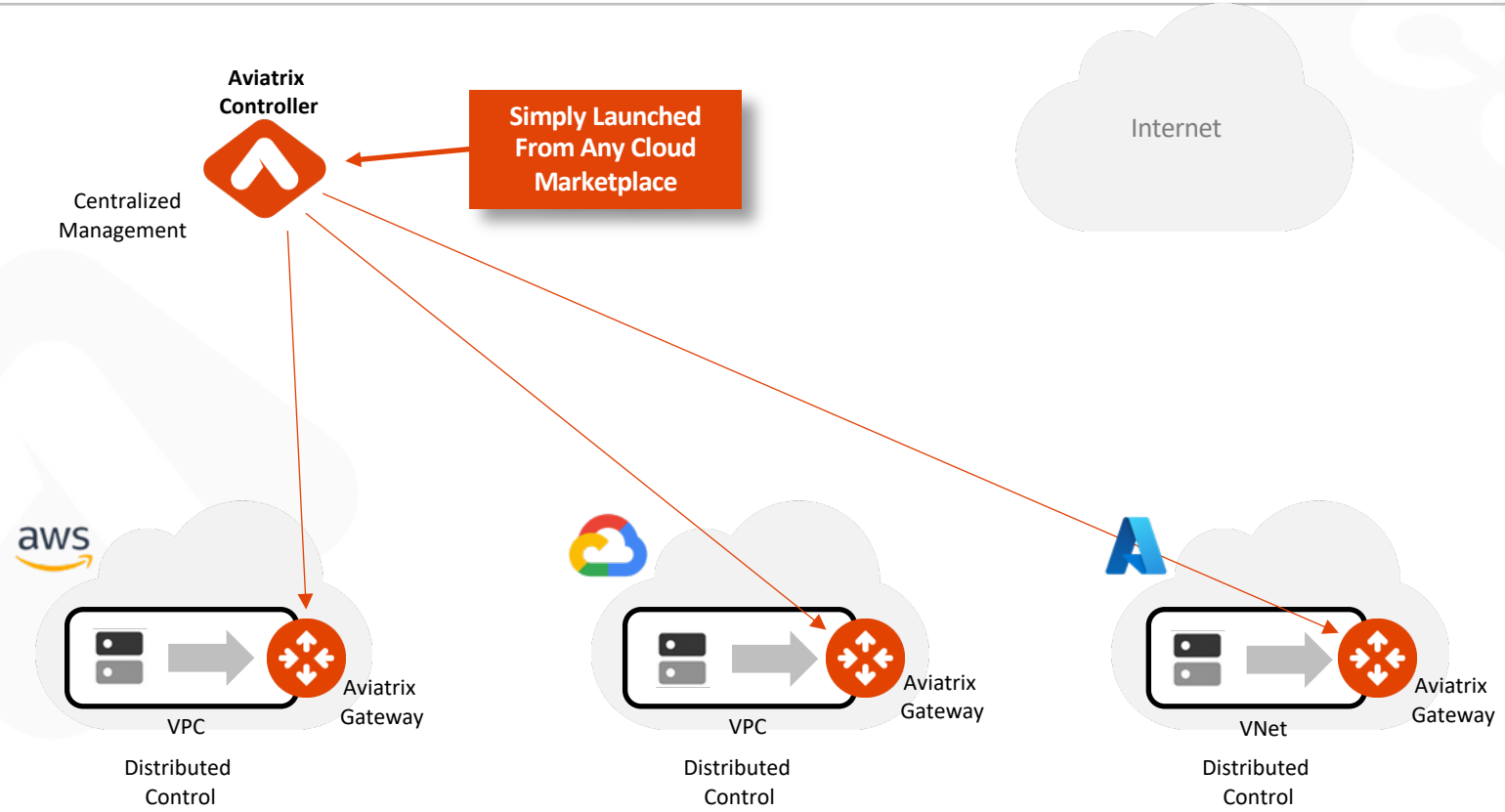
- Overkill
- Expensive



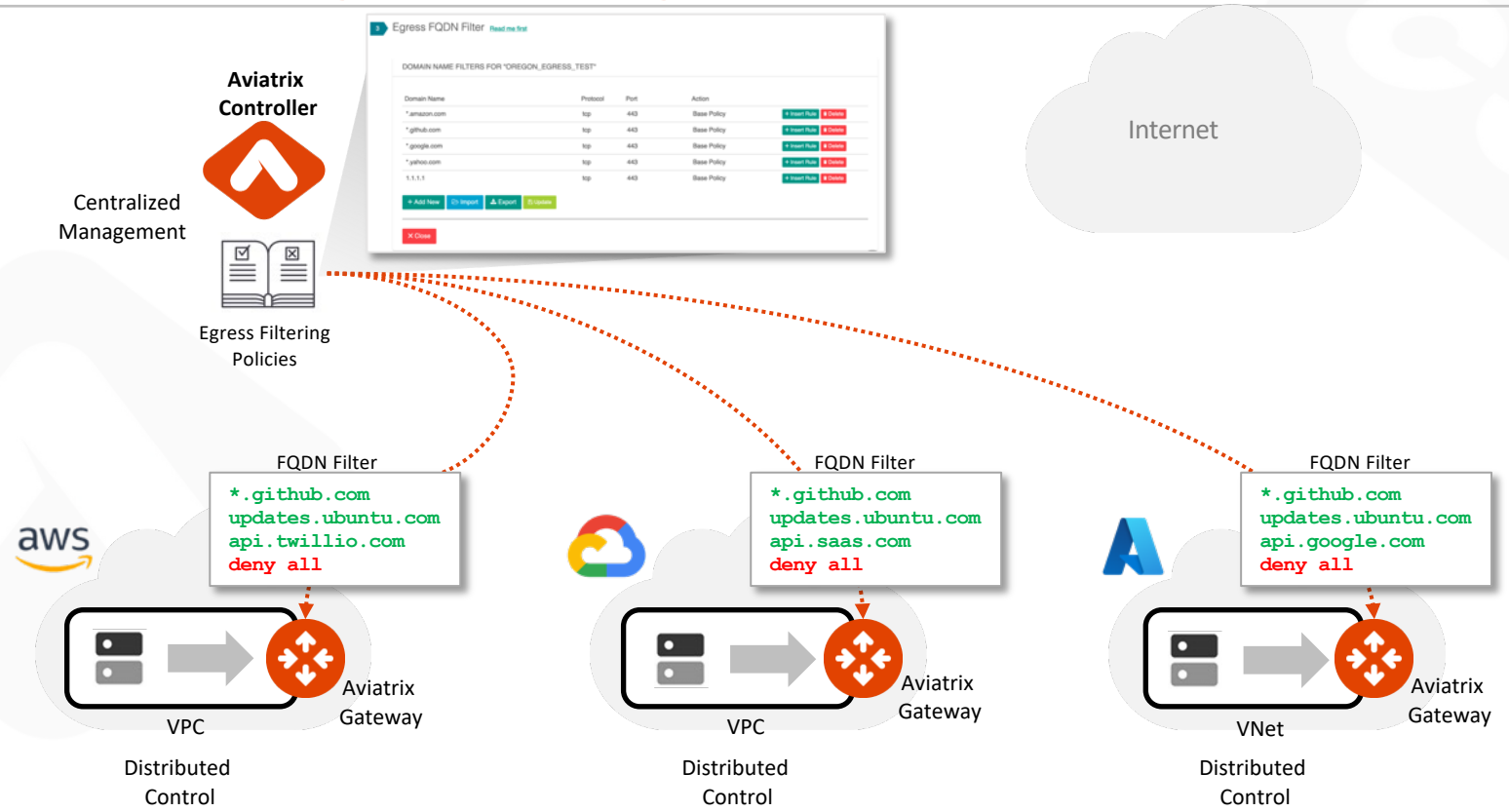
Aviatrix Egress Feature



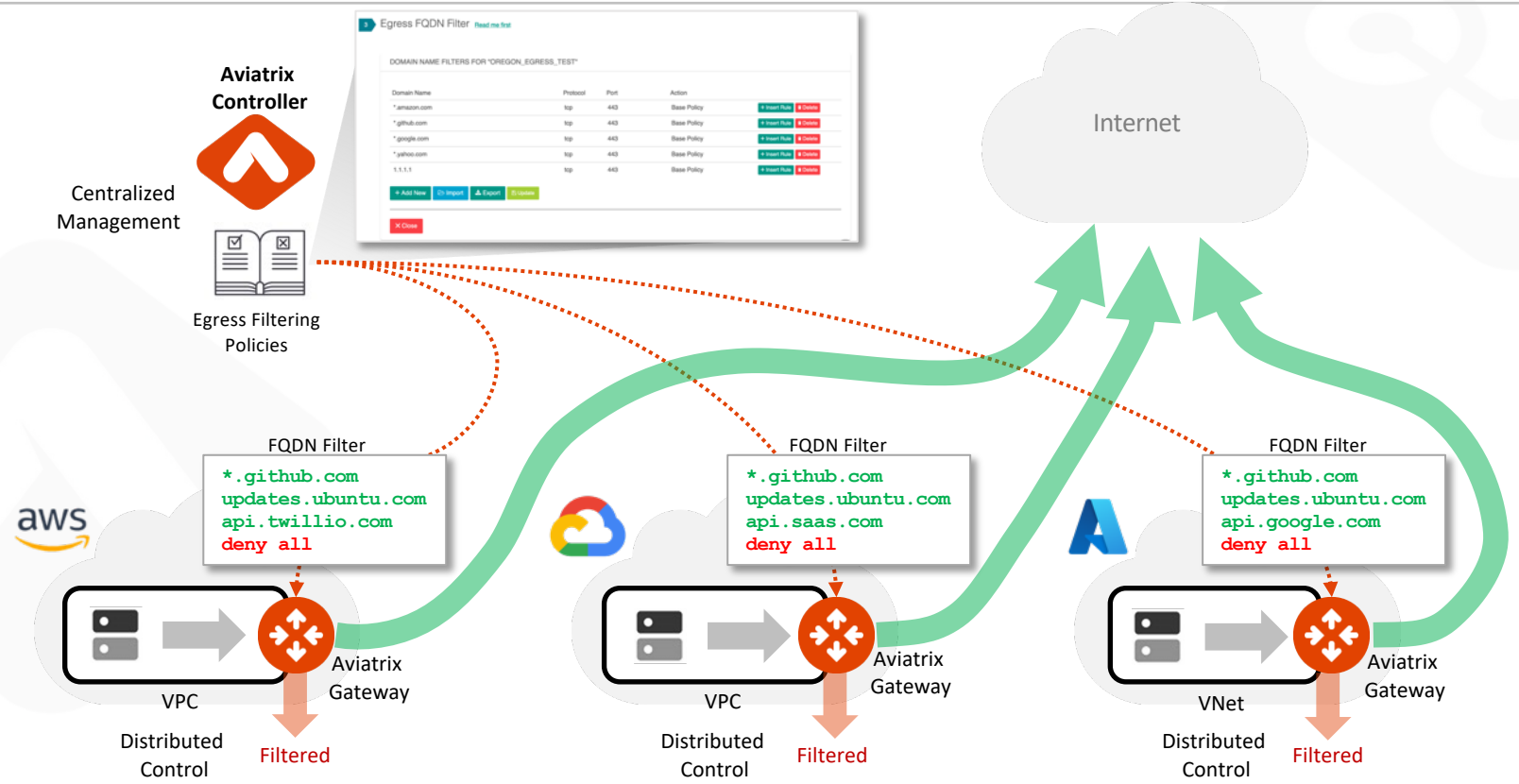
Aviatrix FQDN Egress Filtering



Aviatrix FQDN Egress Filtering

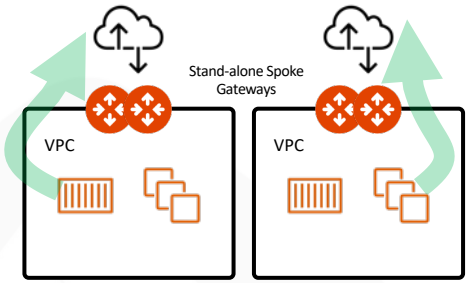


Aviatrix FQDN Egress Filtering

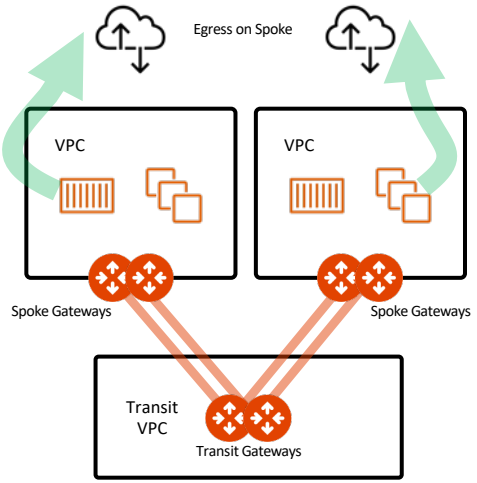


Aviatrix Egress Design Patterns

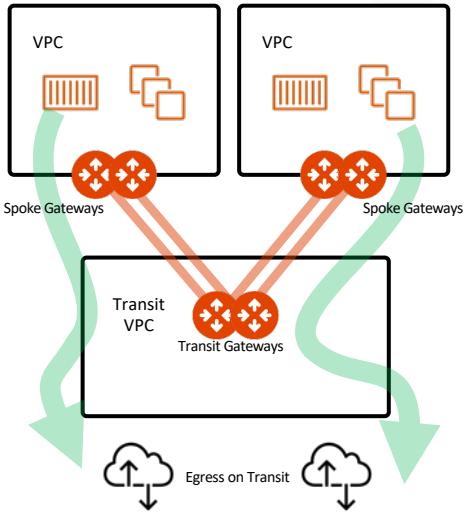
Stand-alone Spoke GW (Distributed)



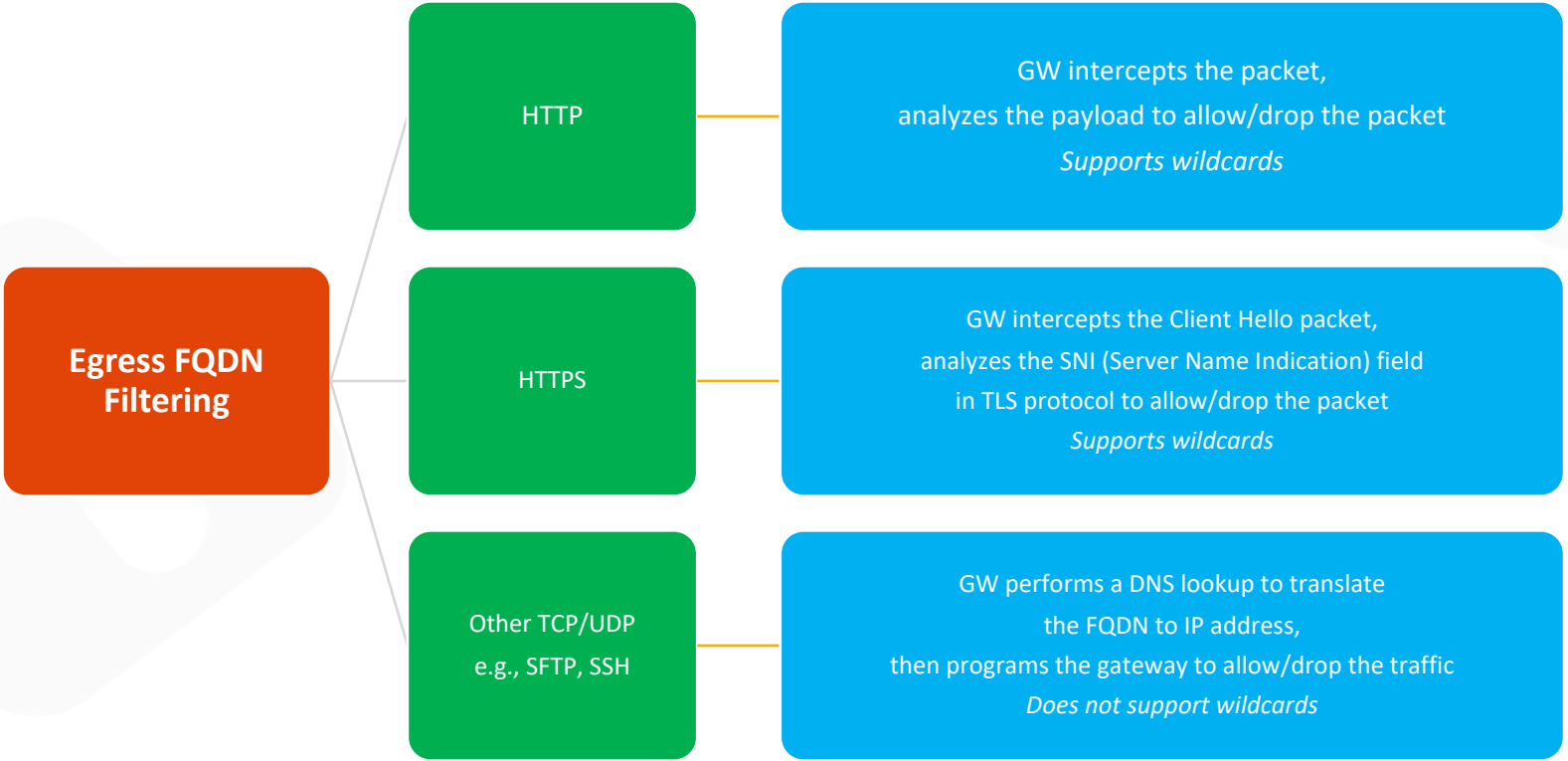
Local Egress (Distributed) with Aviatrix Spoke



Centralized Egress with Aviatrix Transit

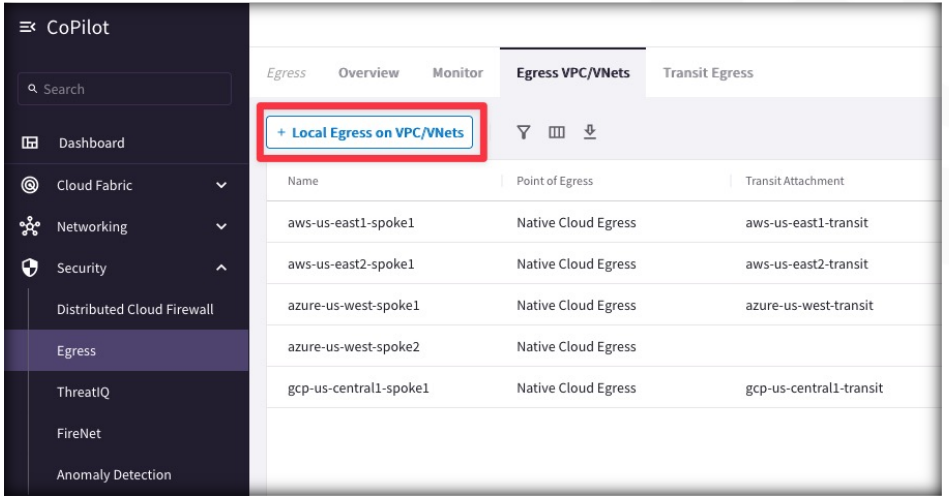


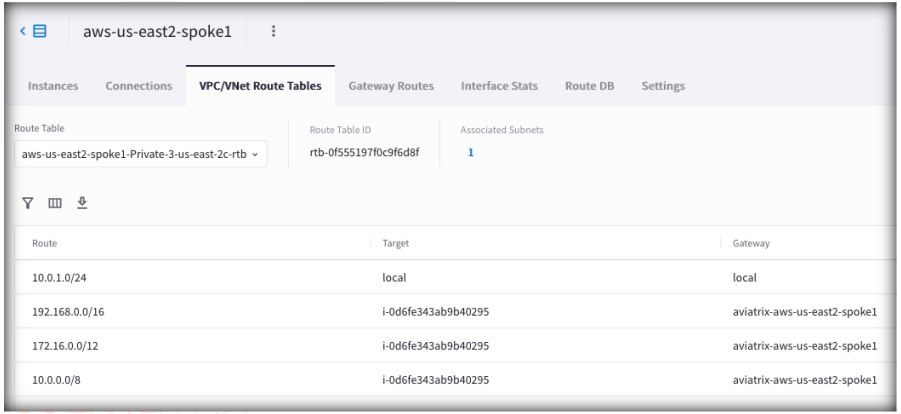
Egress FQDN Filter – Traffic Types

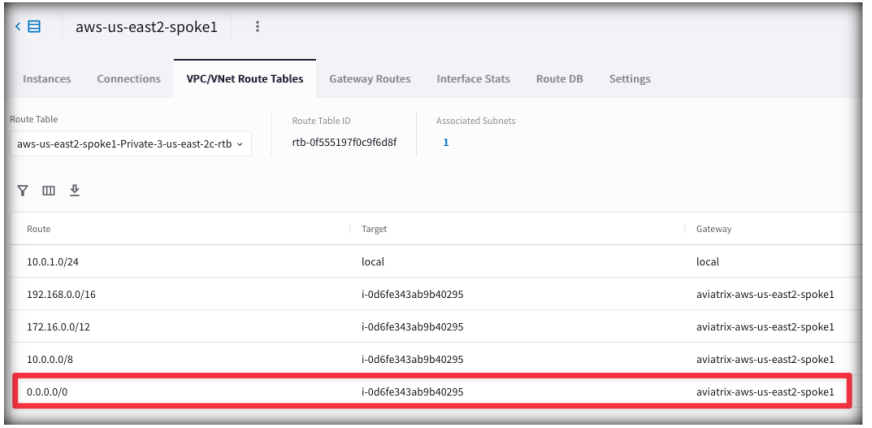


Enable Egress

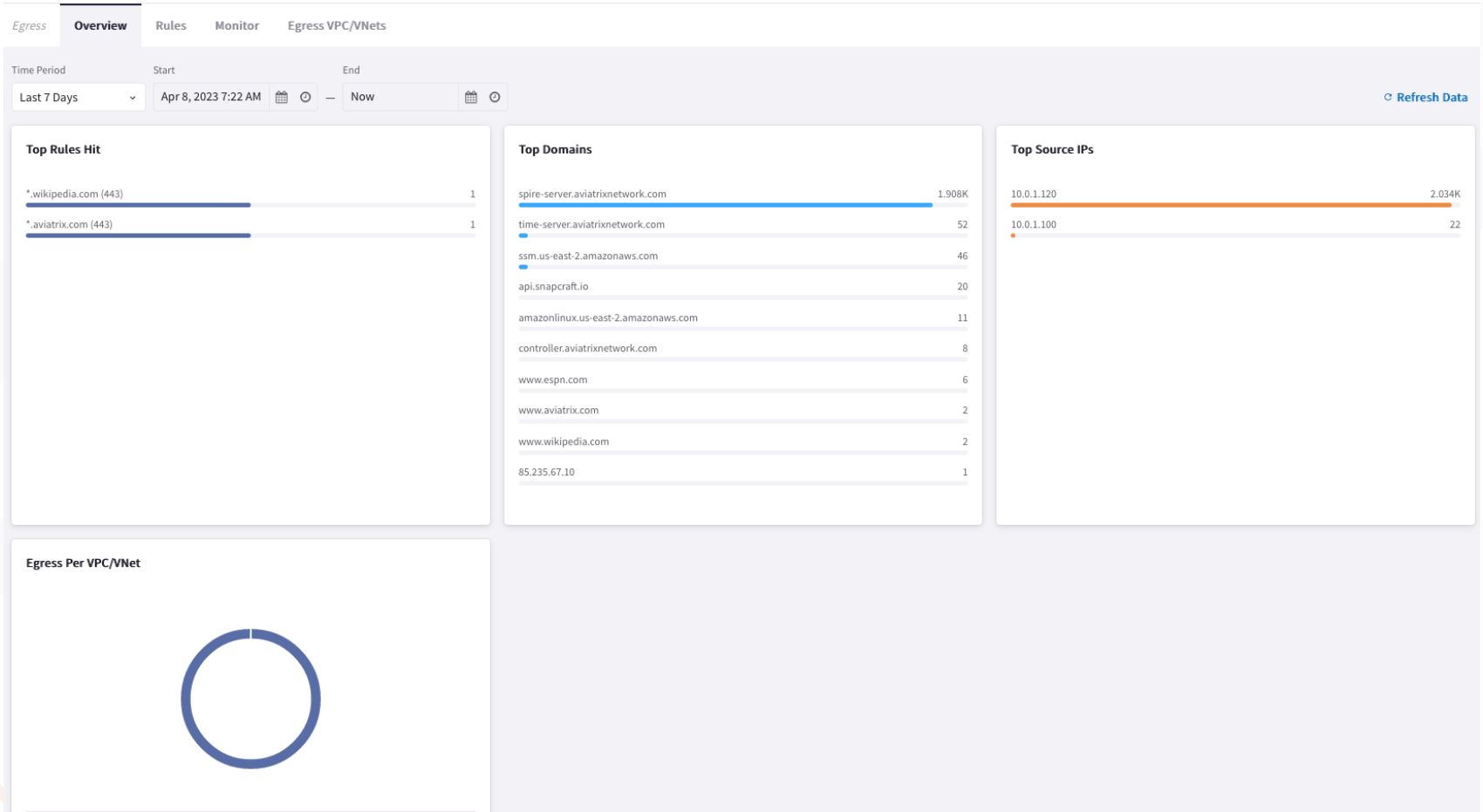
- Adding Egress Control on VPC/VNet changes the default route on VPC/VNet to point to the Spoke Gateway and enables **SNAT**.
- Egress Control also requires additional resources on the Spoke Gateway.
- In addition to the **Local route**, the **three RFC1918 routes**, also a **default route** will be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







Visibility from CoPilot

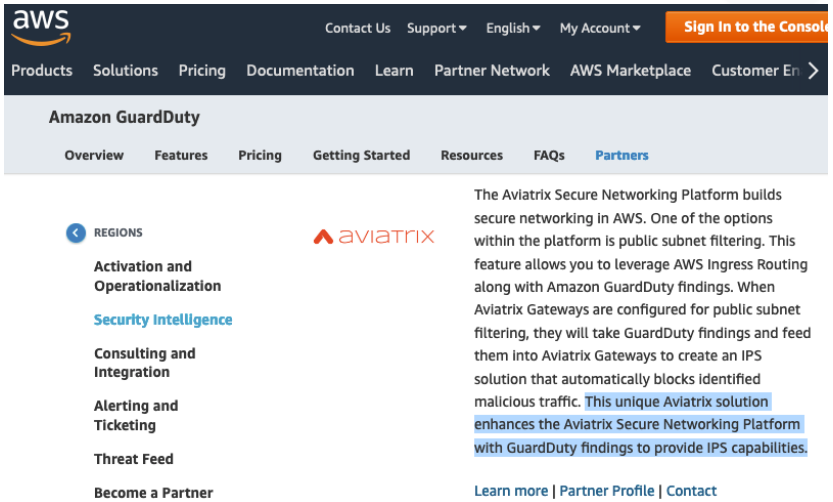


Aviatrix PSF (aka Public Subnet Filtering) with AWS GuardDuty

Problem Statement

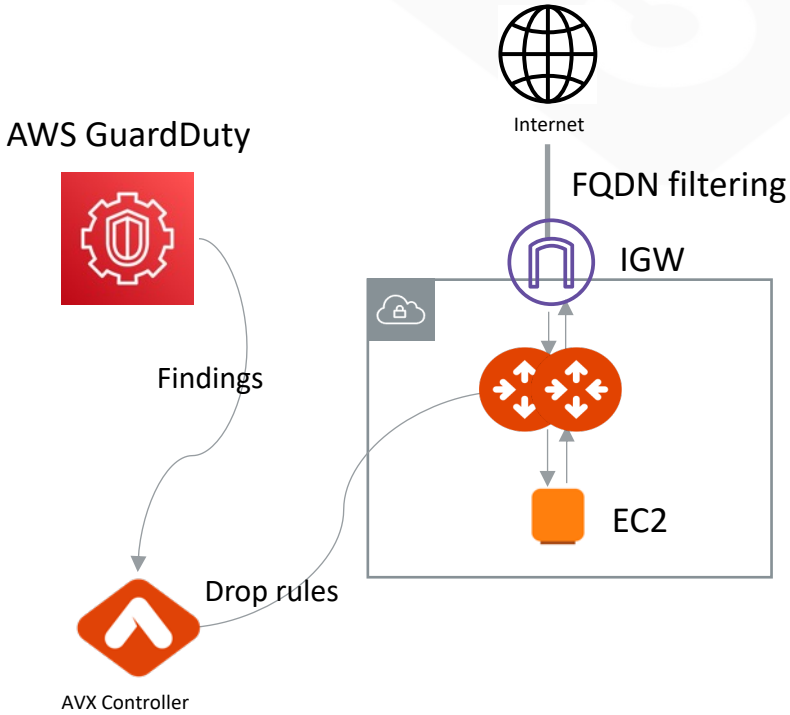
- AWS GuardDuty is a managed service for threat detection (□DS)
  - CrowdStrike and ProofPoint provide information to GuardDuty called □ndicators of Compromise (□oC)
- GuardDuty does not take any action on the malicious activity it finds
  - https://aws.amazon.com/guardduty/resources/partners/

AWS GuardDuty



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 PS GW is also called Public Subnet Filtering (PSF) GW



Lab 6 – Egress