Egress FQDN Filtering

Problem Statement

Private workloads need internet access

- **SaaS integration**
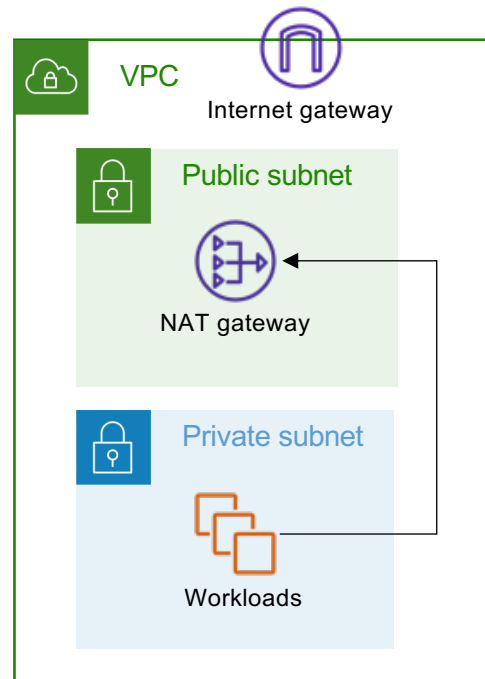
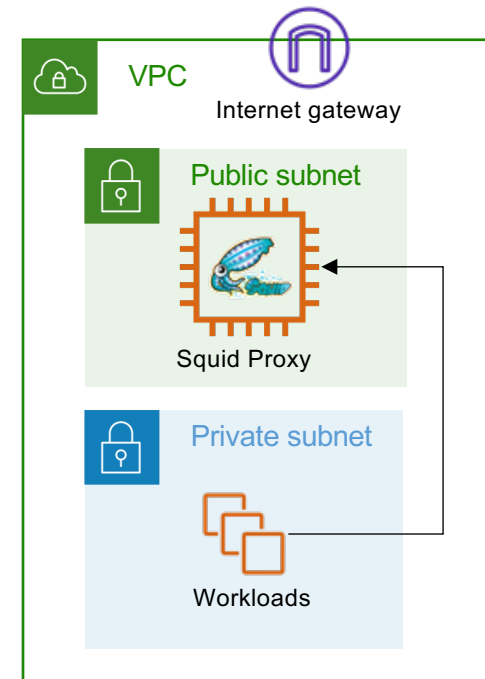- **Patching**

- **Updates**

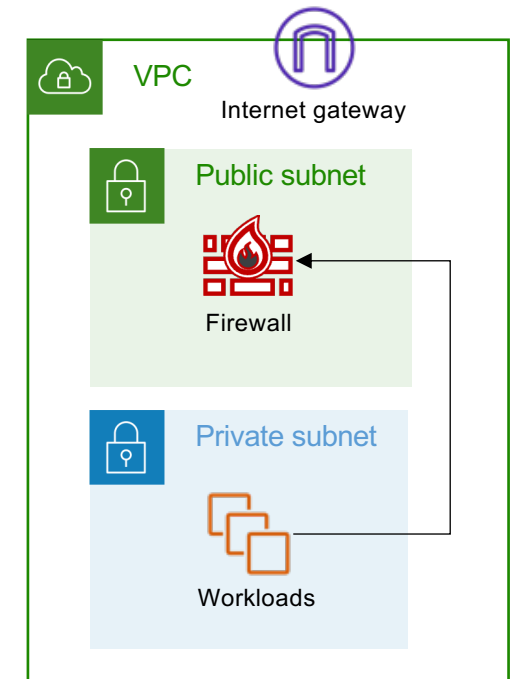### NAT Gateway

- Layer-4 only
- NACLs management

VPC
Internet gateway

Public subnet

NAT gateway

Private subnet

Workloads

Squid Proxy

- Hard to manage
- Scale and HA issues

VPC
Internet gateway

Public subnet

Squid Proxy

Private subnet

Workloads

Layer-7 Firewall

- Overkill
- Expensive
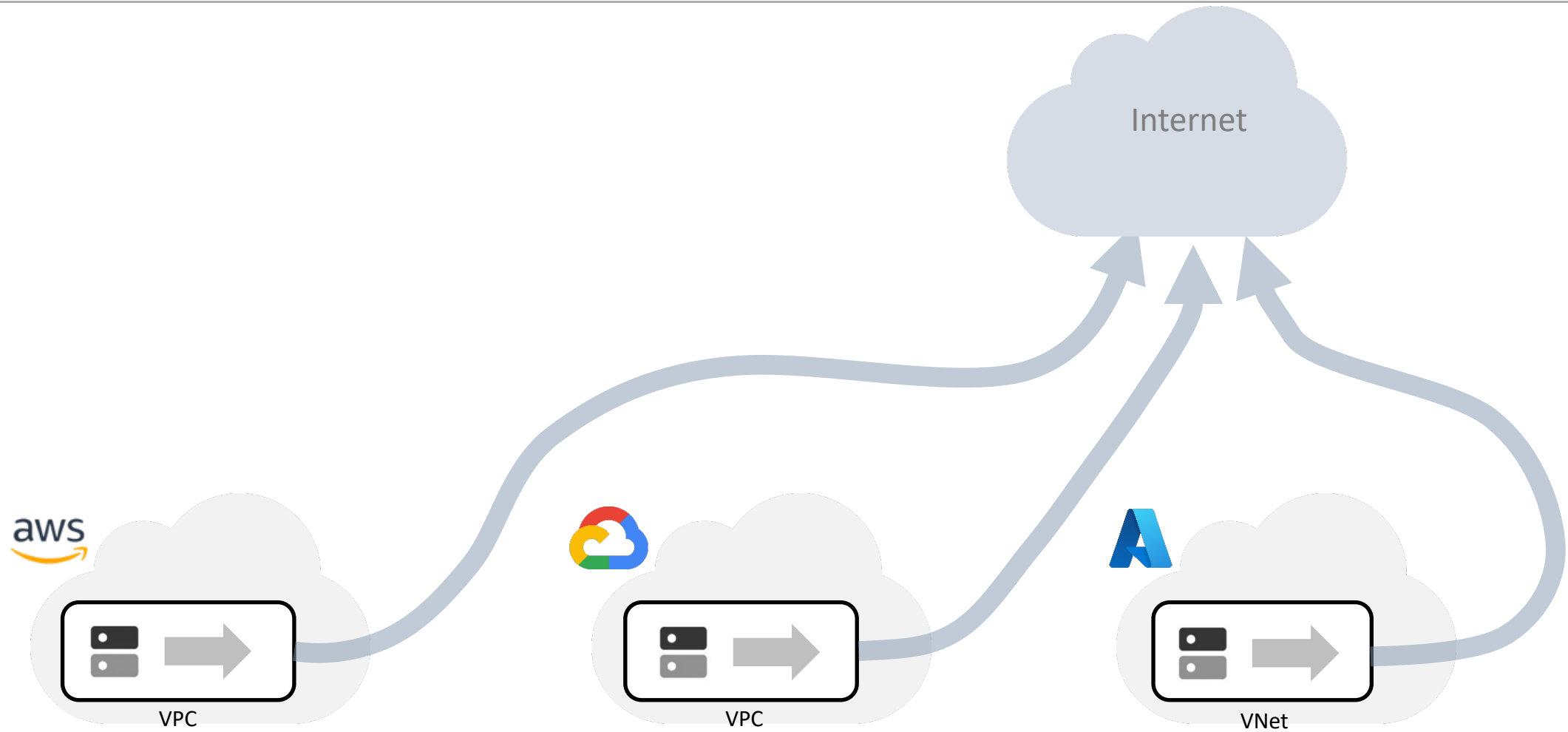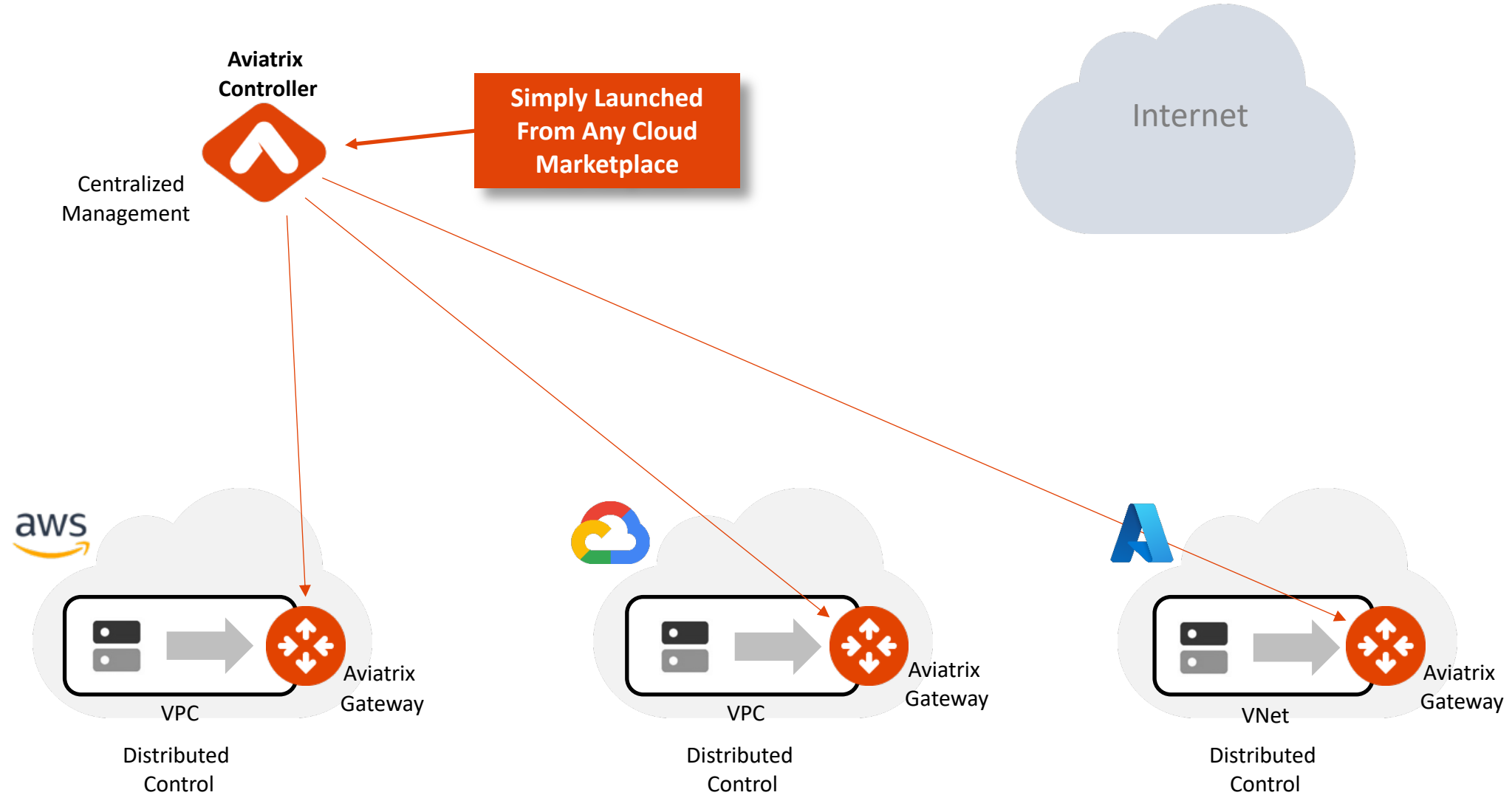
VPC
Internet gateway

Public subnet

Firewall

Private subnet

Workloads

aviatrix

Aviatrix FQDN Egress Filtering

Aviatrix FQDN Egress Filtering

Aviatrix Controller

Centralized Management

Simply Launched From Any Cloud Marketplace

Internet

aws

VPC

Aviatrix Gateway

Distributed Control

VPC

Aviatrix Gateway

Distributed Control

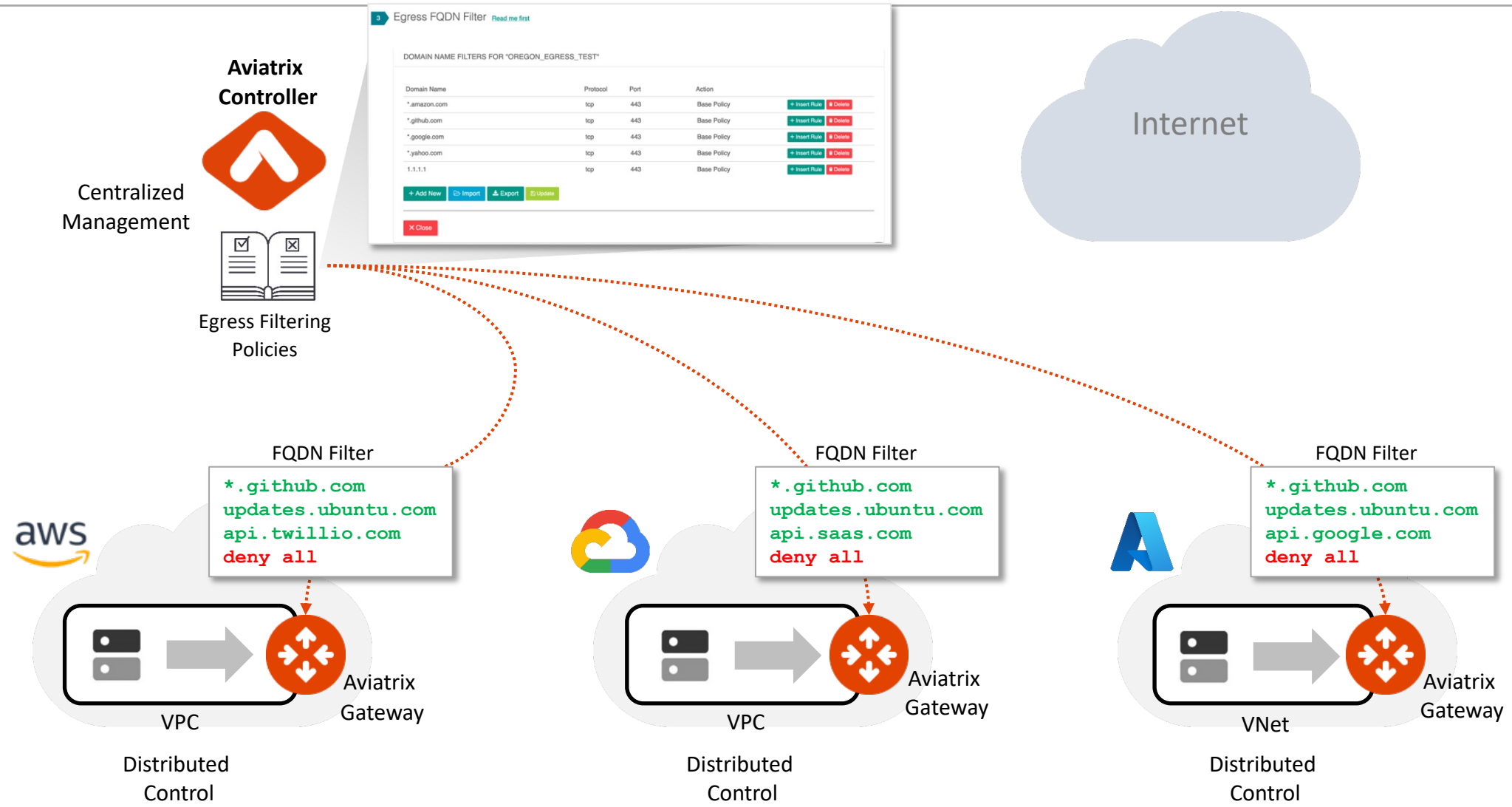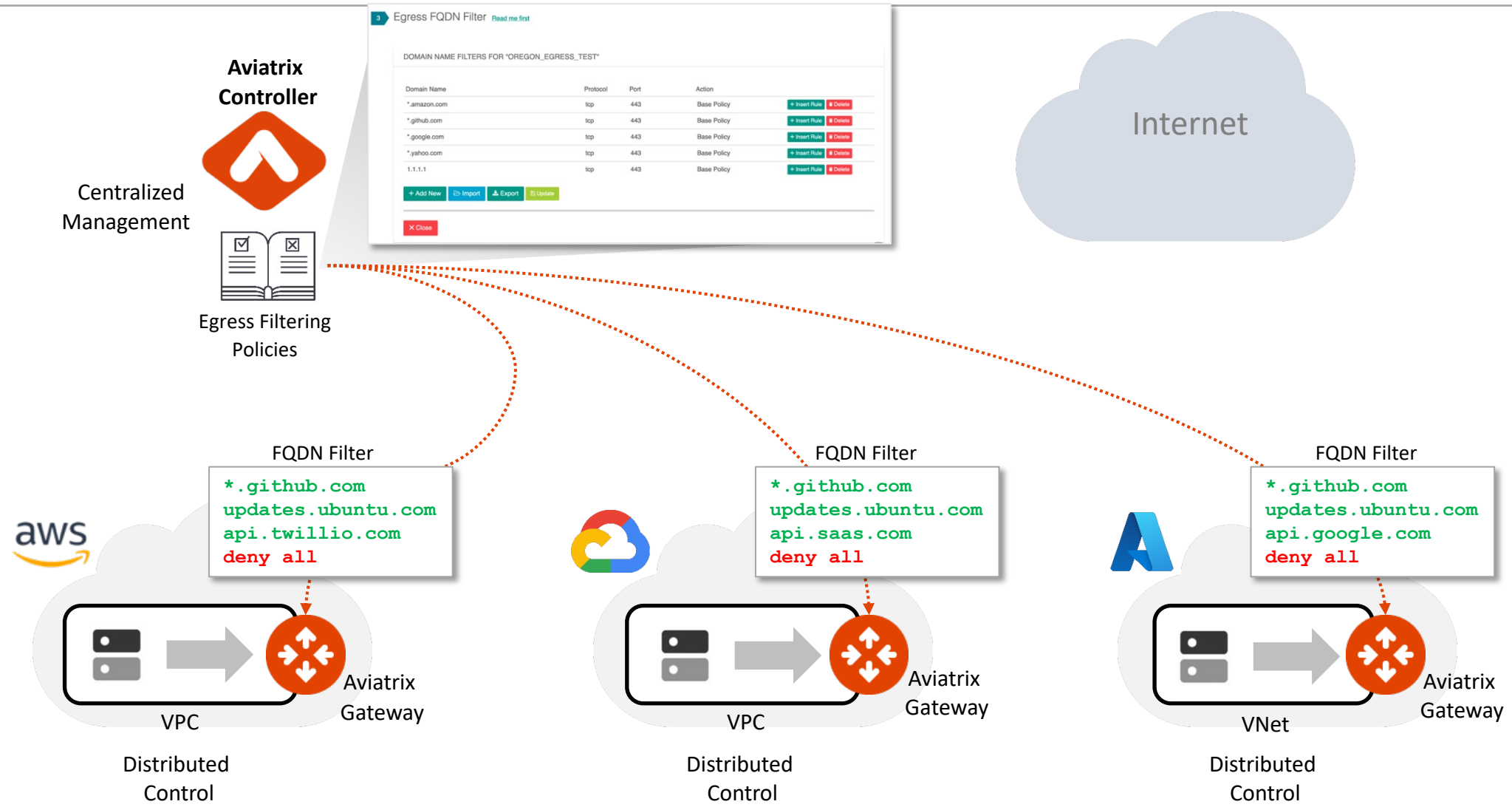VNet

Aviatrix Gateway

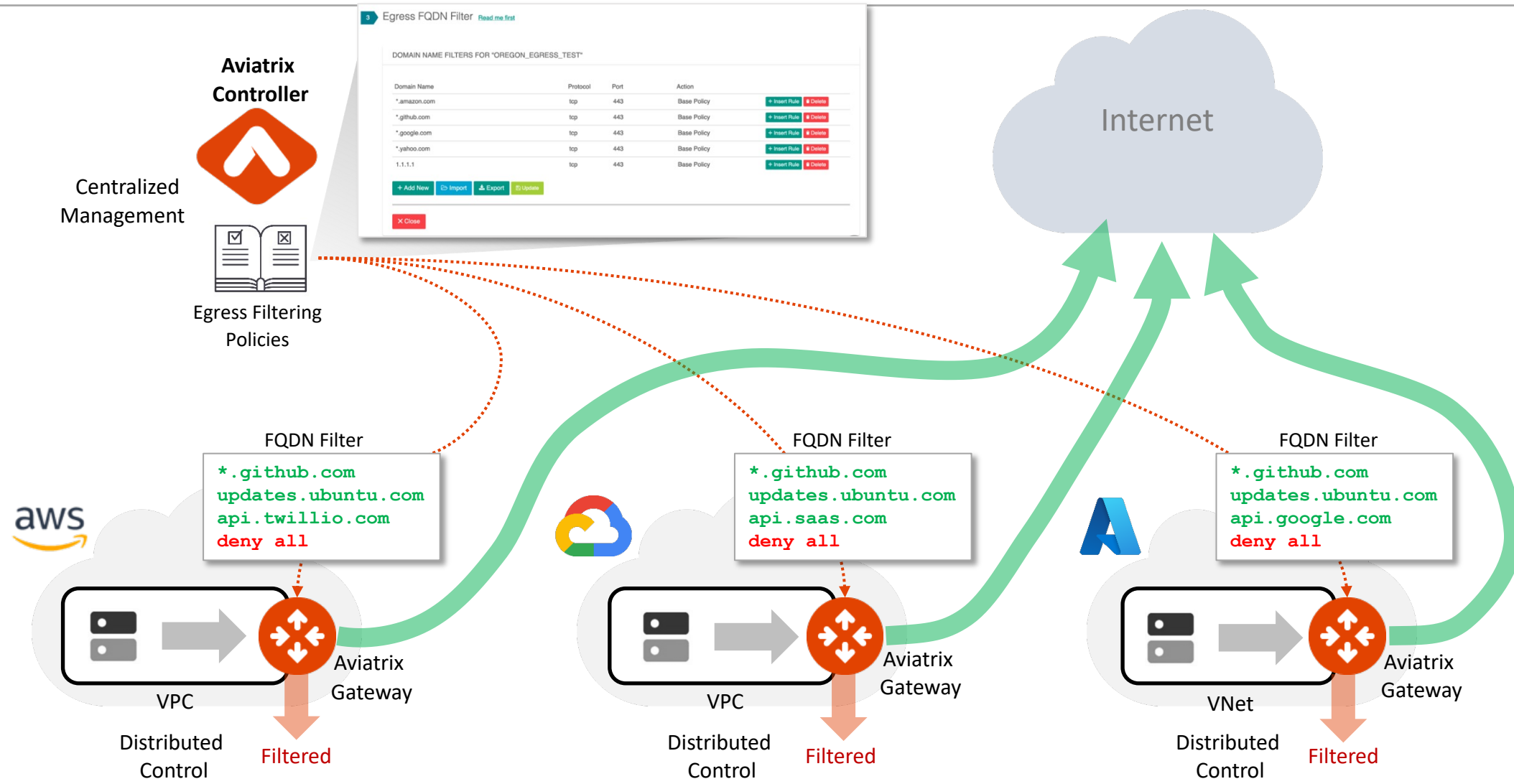Distributed Control

aviatrix

Aviatrix FQDN Egress Filtering

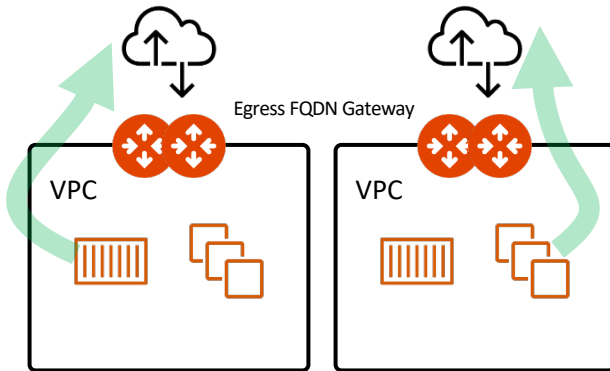# Aviatrix FQDN Egress Filtering
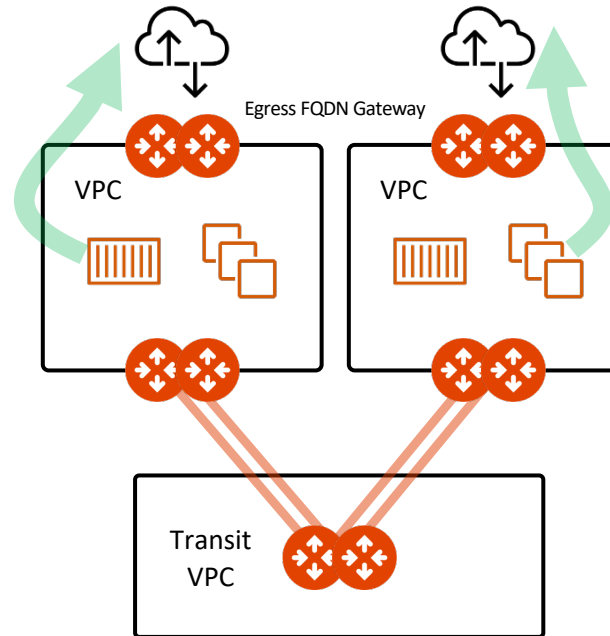
Aviatrix FQDN Egress Filtering

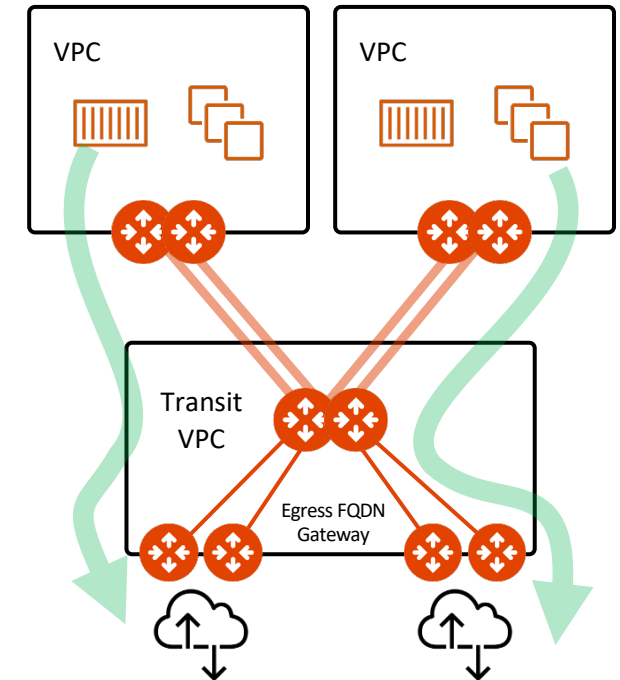# Aviatrix FQDN Egress Filtering Design Pattern

Local Egress FQDN Filtering (Distributed)

Local Egress FQDN Filtering (Distributed) with Aviatrix Transit

Centralized Egress with Aviatrix Transit

Zero Touch Network Access

There are two possible models:

- **DENY LIST MODEL** (THREAT-CENTRIC MODEL):
  - ❏ allow all data to flow, except for exactly what you say should be stopped.

- **ALLOW LIST MODEL** (TRUST-CENTRIC MODEL):
  - ❏ deny everything and only permit what you explicitly allow.

aviatrix

Tools for troubleshooting Egress FQDN Filtering

aviatrix

Egress FQDN Filter & Gateway's state

PATH: CONTROLLER > SECURITY > Egress Control

FQDN Stats

PATH: CONTROLLER > SECURITY > FQDN Stats

aviatrix

Next:

Lab 7 Egress FQDN