Internet Egress close to the Applications

Aviatrix DCF for Secure Egress

Problem Statement

Private workloads need internet access

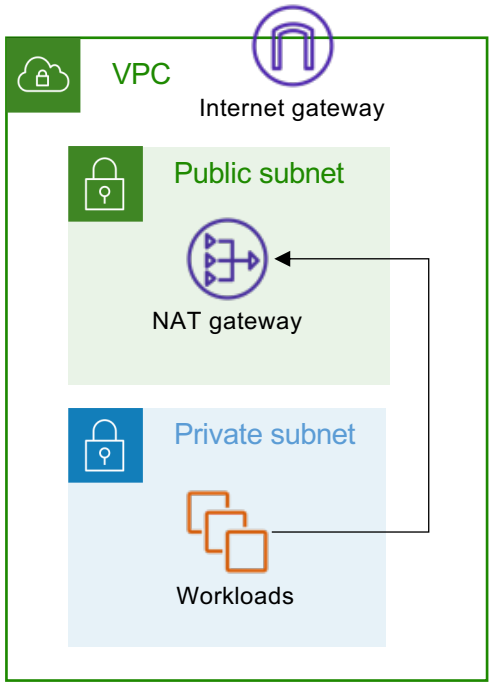
- **SaaS integration**

- **Patching**

- **Updates**

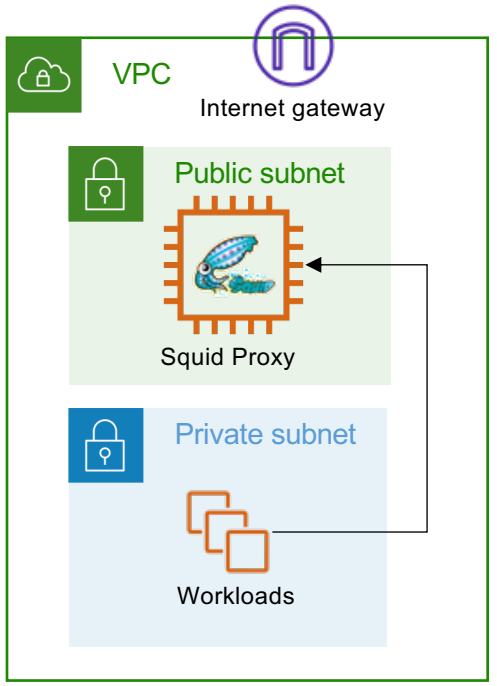
NAT Gateway

- NACLs are necessary
- Unrestricted access



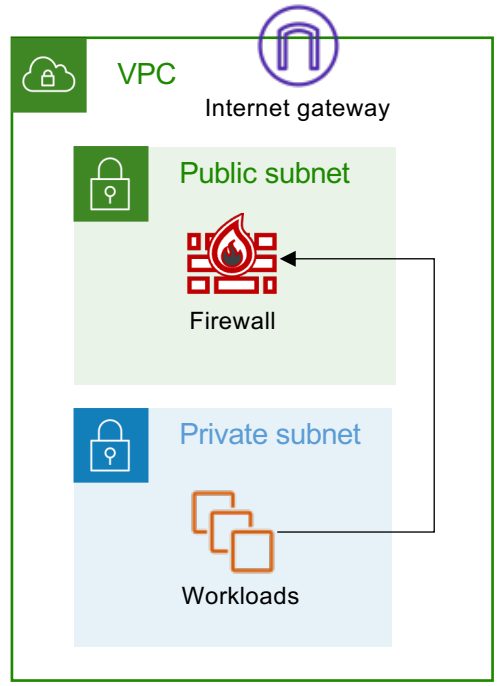
Squid Proxy

- Hard to manage
- Scale and HA issues

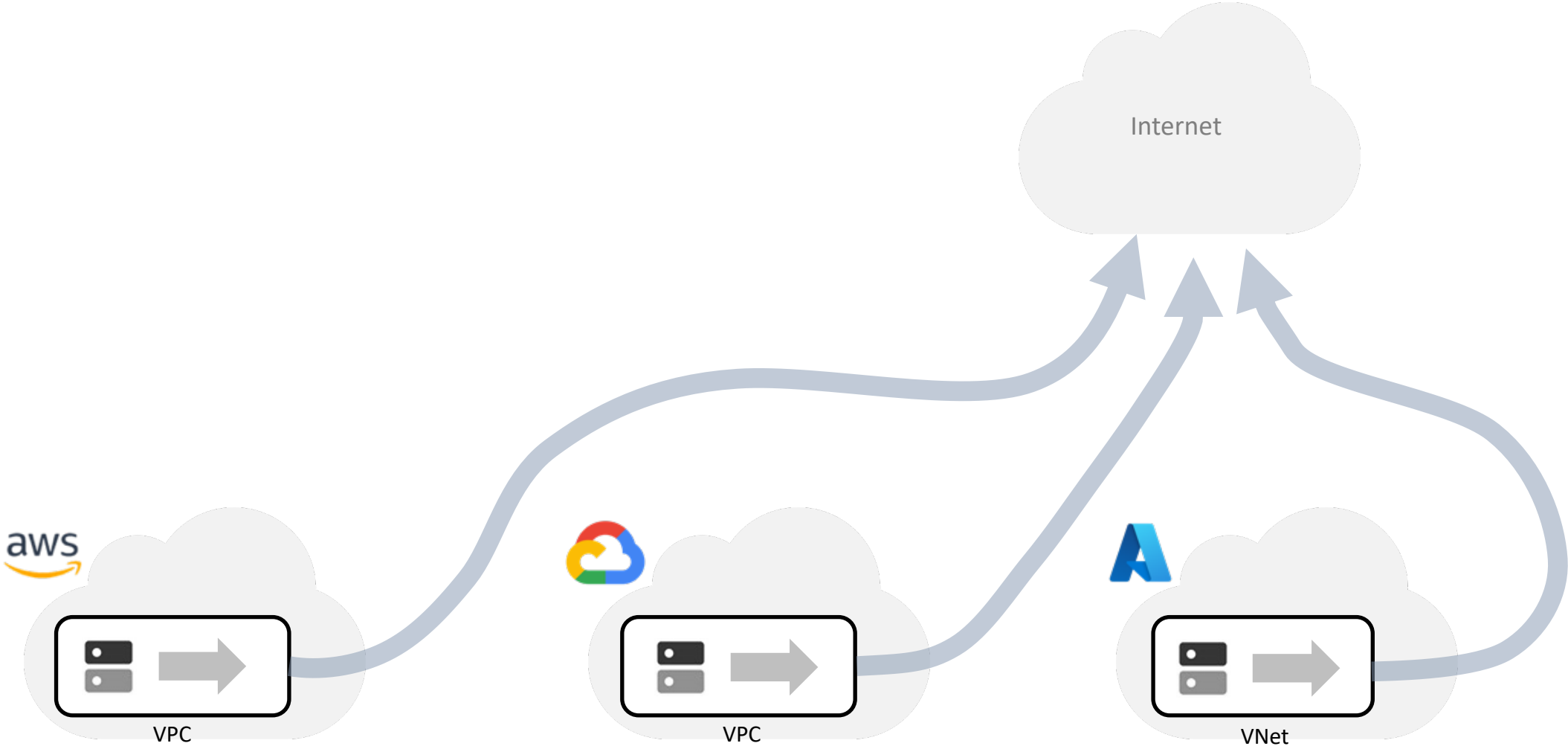


Layer-7 Firewall

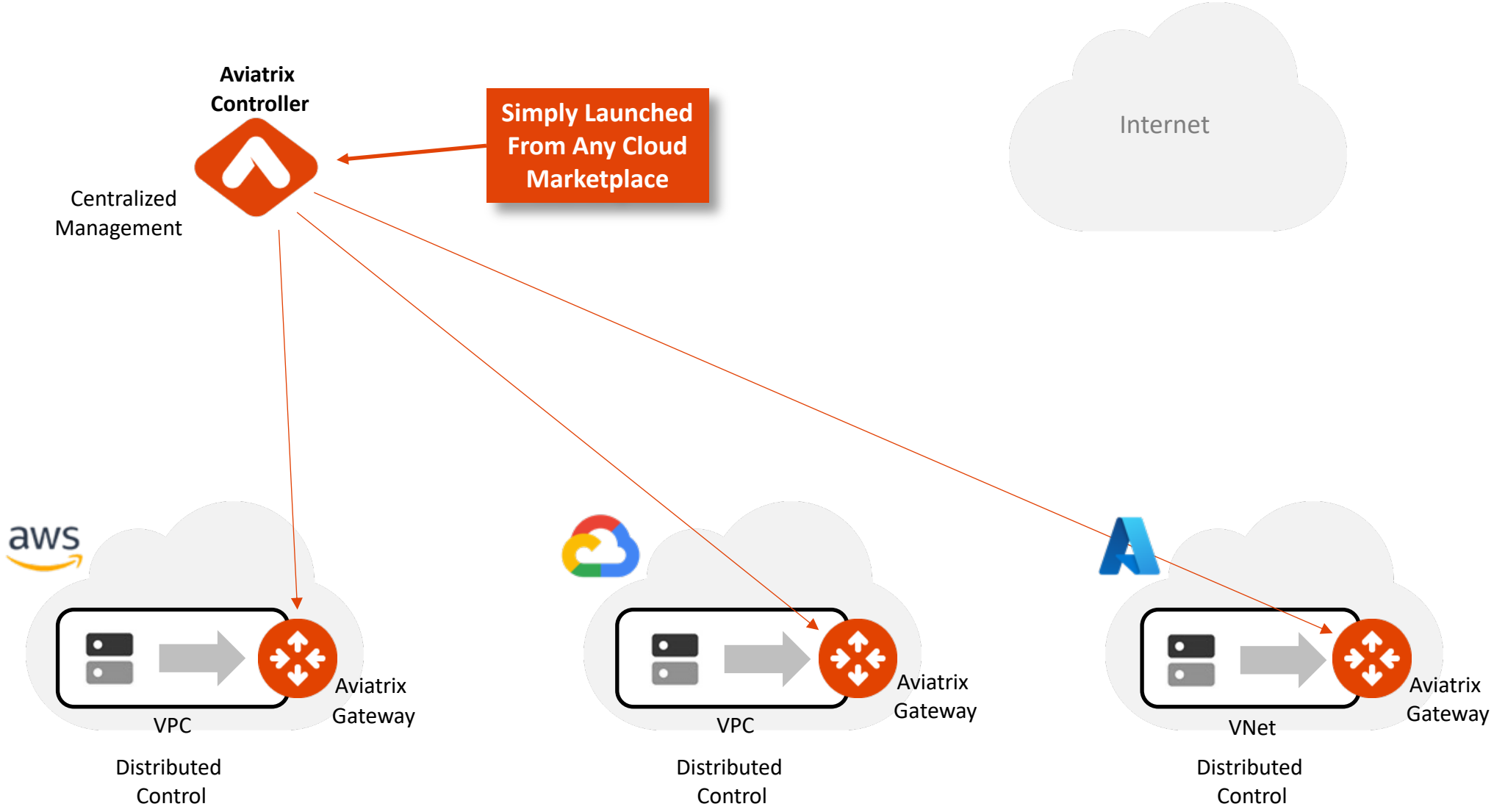
- Overkill
- Expensive

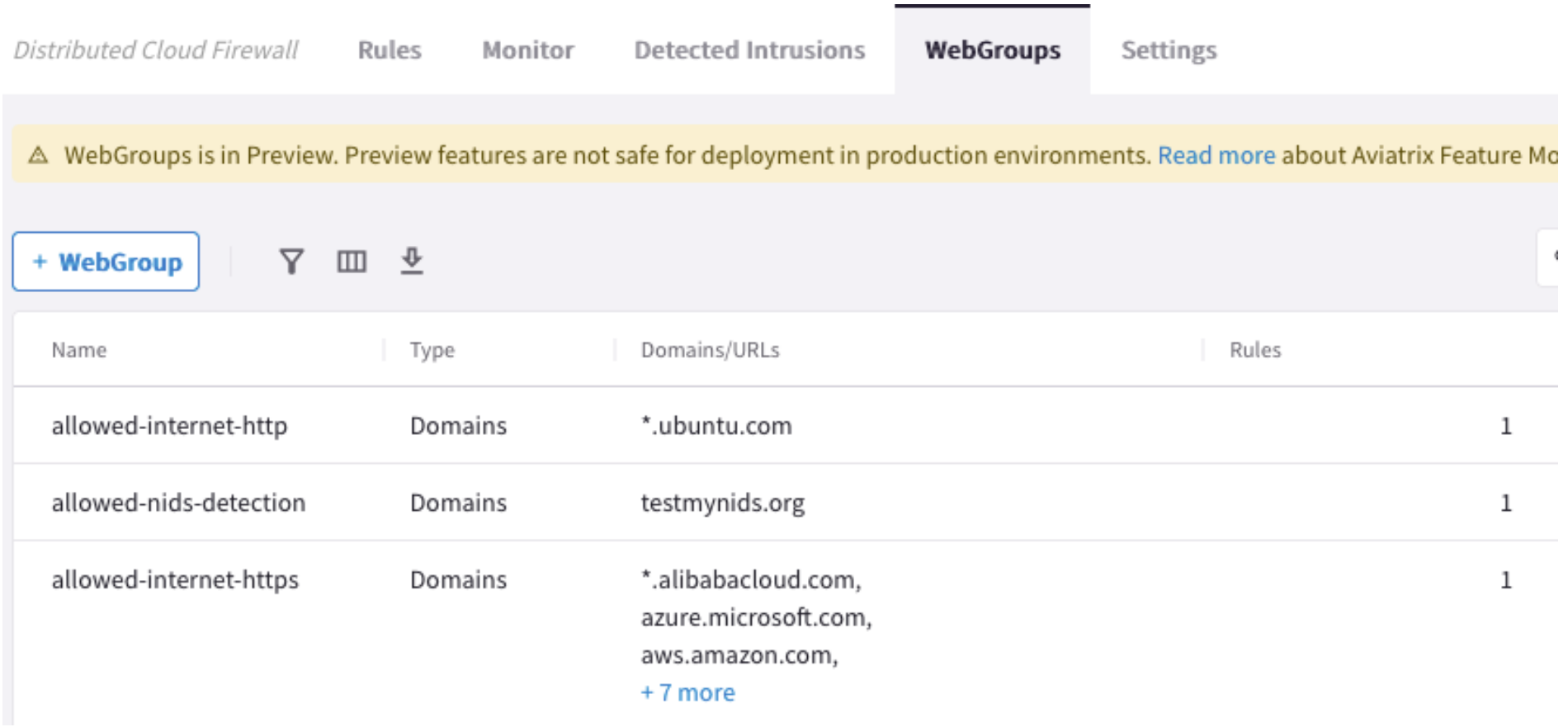


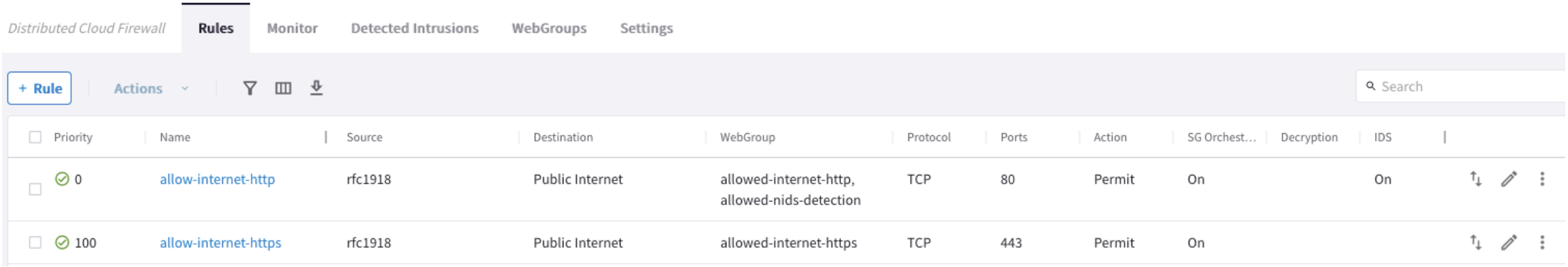
Aviatrix Secure Egress Filtering



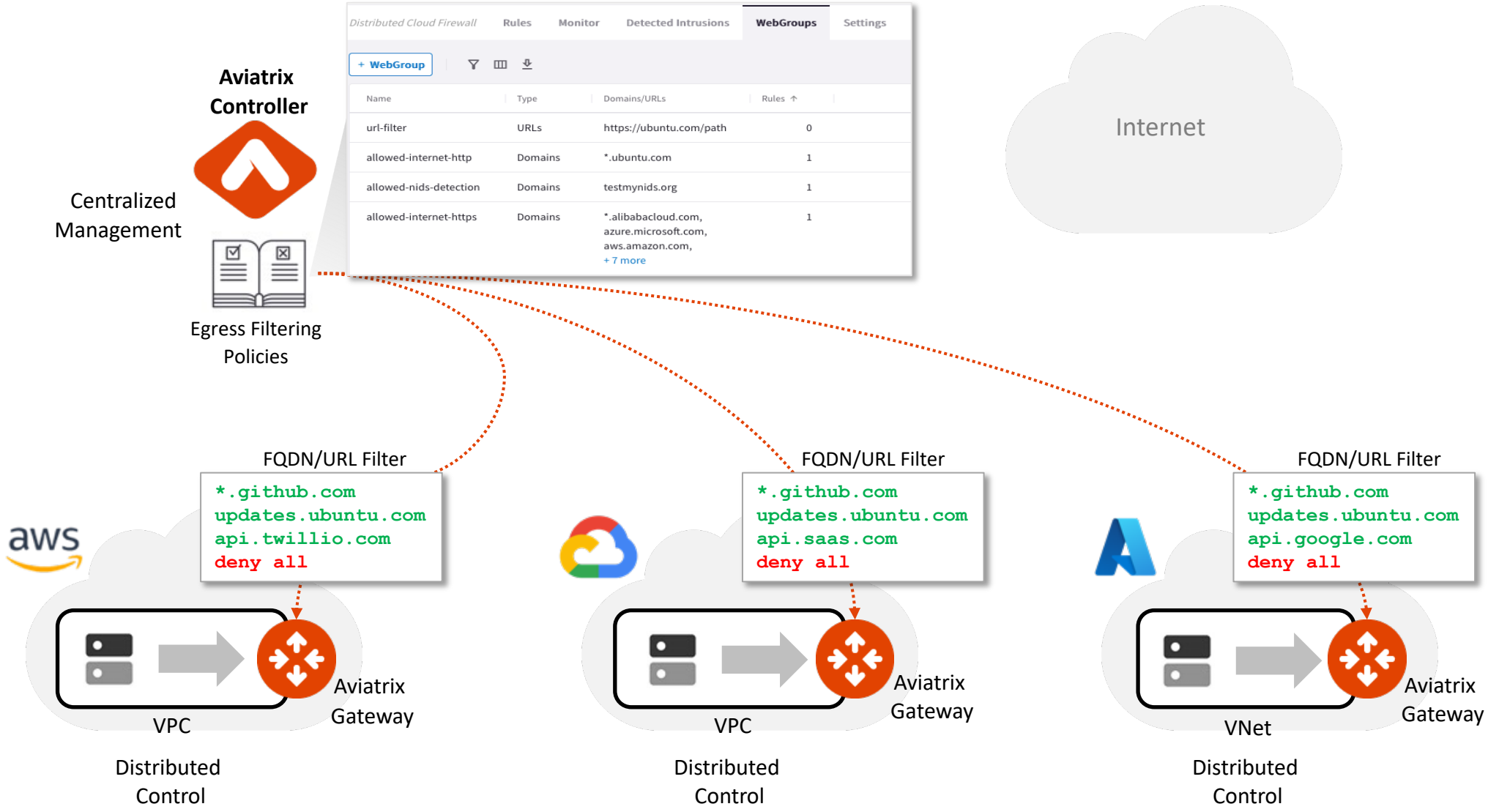
Aviatrix Secure Egress Filtering



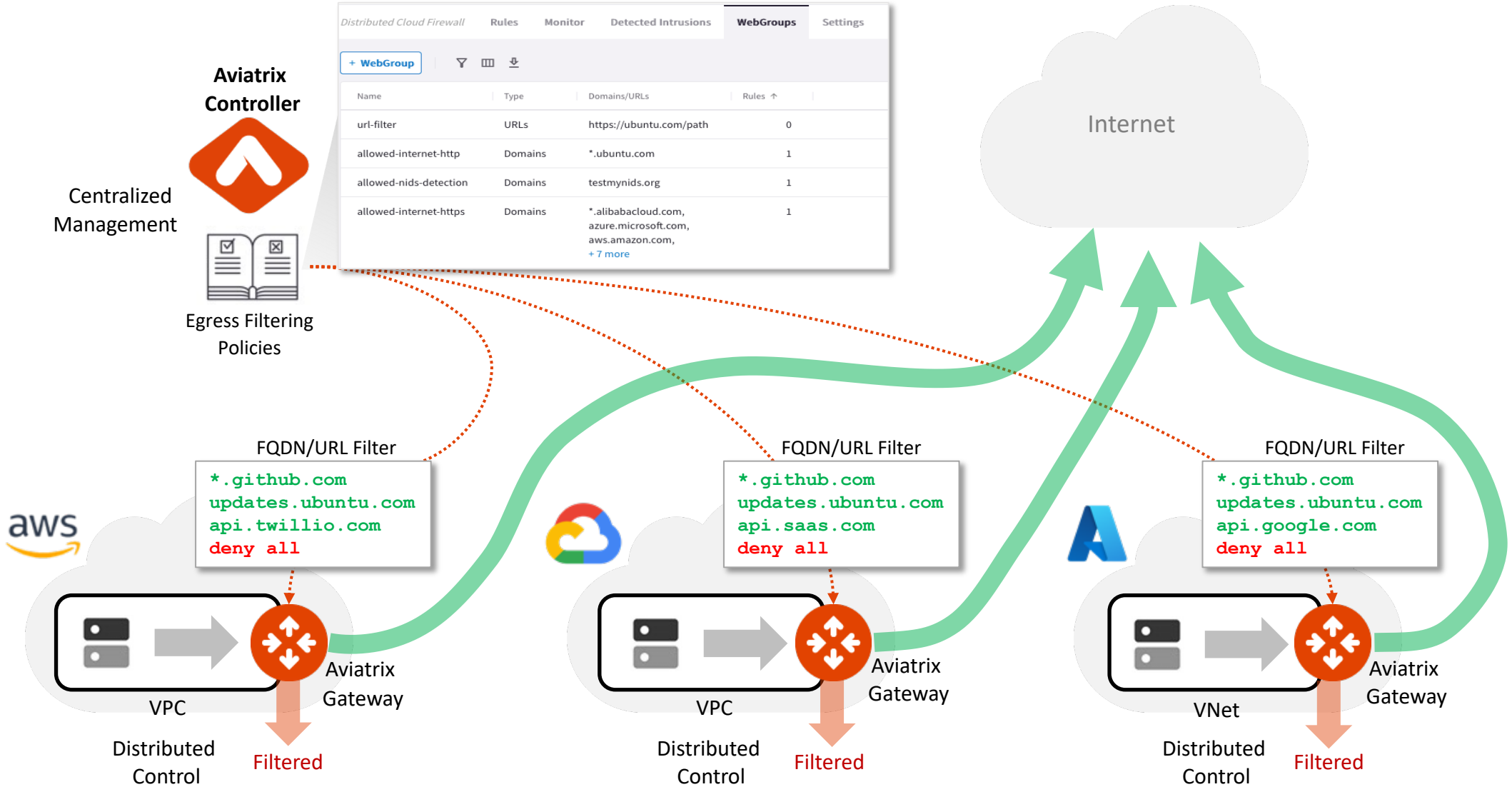

Distributed Cloud Firewall
Rules
Monitor
Detected Intrusions
WebGroups
Settings
WebGroups is in Preview. Preview features are not safe for deployment in production environments. Read more about Aviatrix Feature Mo
+ WebGroup
Name
Type
Domains/URLs
Rules
allowed-internet-http
Domains
*.ubuntu.com
1
allowed-nids-detection
Domains
testmynids.org
1
allowed-internet-https
Domains
*.alibabacloud.com,
azure.microsoft.com,
aws.amazon.com,
+ 7 more
1

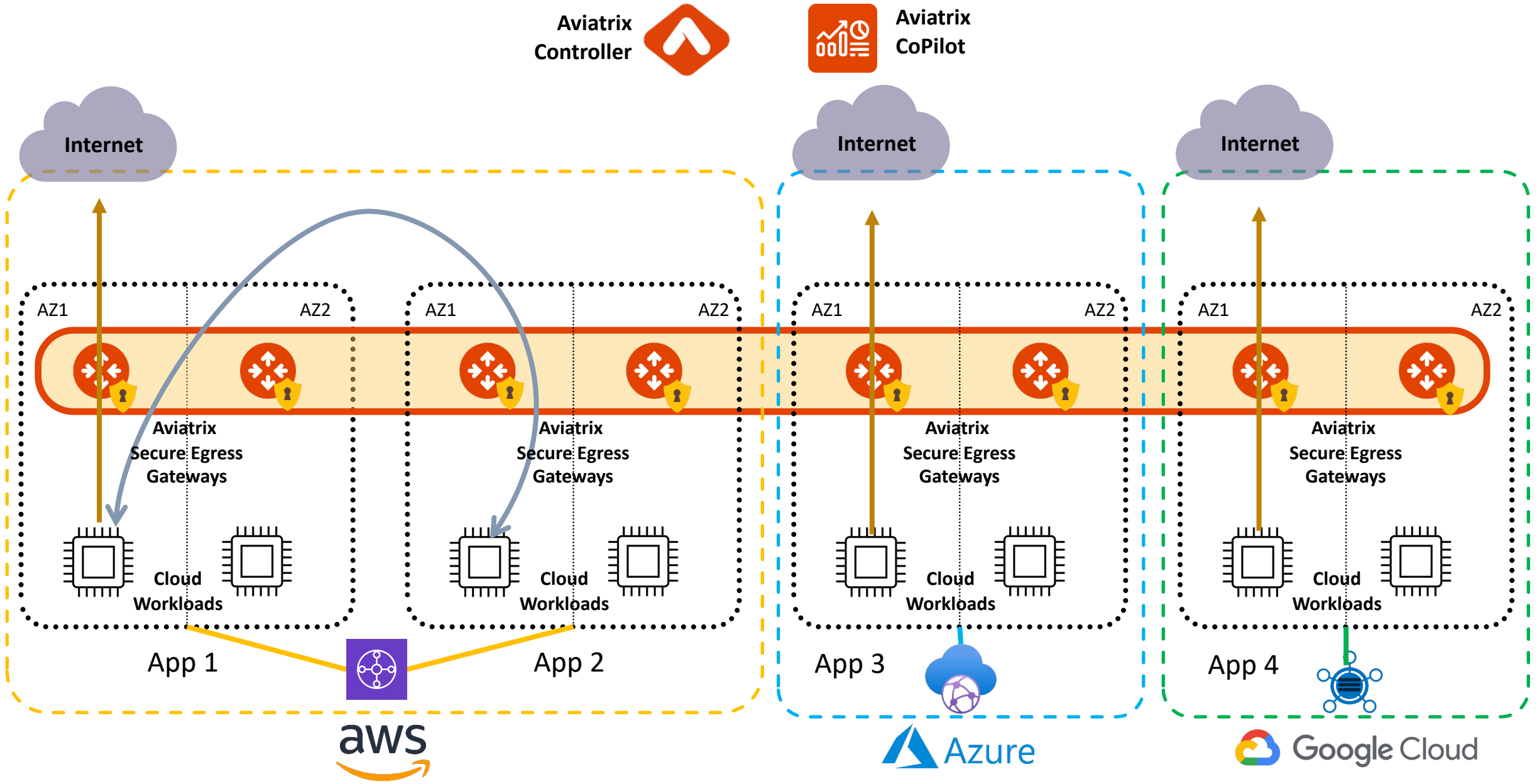

Distributed Cloud Firewall
Rules
Monitor
Detected Intrusions
WebGroups
Settings
+ Rule
Actions
Search
Priority
Name
Source
Destination
WebGroup
Protocol
Ports
Action
SG Orchest...
Decryption
IDS
0
allow-internet-http
rfc1918
Public Internet
allowed-internet-http,
allowed-nids-detection
TCP
80
Permit
On
On
100
allow-internet-https
rfc1918
Public Internet
allowed-internet-https
TCP
443
Permit
On

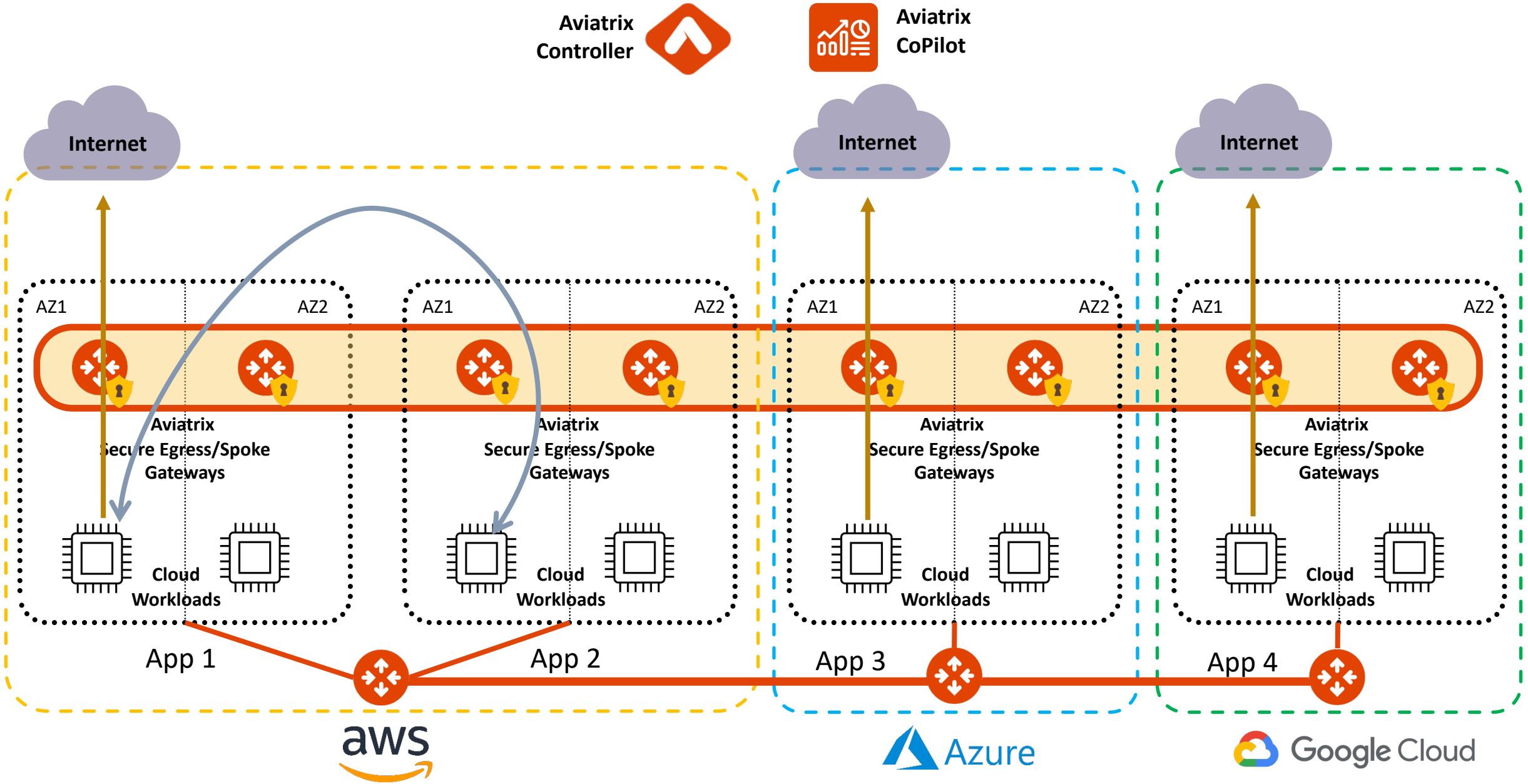
Aviatrix Secure Egress Filtering



Aviatrix Secure Egress Filtering

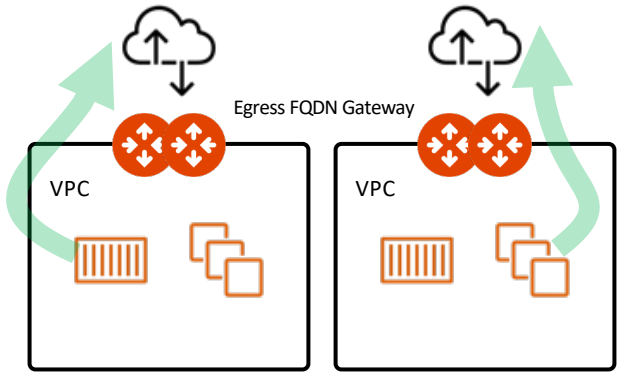



Aviatrix Controller
Aviatrix CoPilot
Internet
Internet
Internet
AZ1
AZ2
AZ1
AZ2
AZ1
AZ2
AZ1
AZ2
Aviatrix Secure Egress Gateways
Aviatrix Secure Egress Gateways
Aviatrix Secure Egress Gateways
Aviatrix Secure Egress Gateways
Cloud Workloads
Cloud Workloads
Cloud Workloads
Cloud Workloads
App 1
App 2
App 3
App 4
aws
Azure
Google Cloud

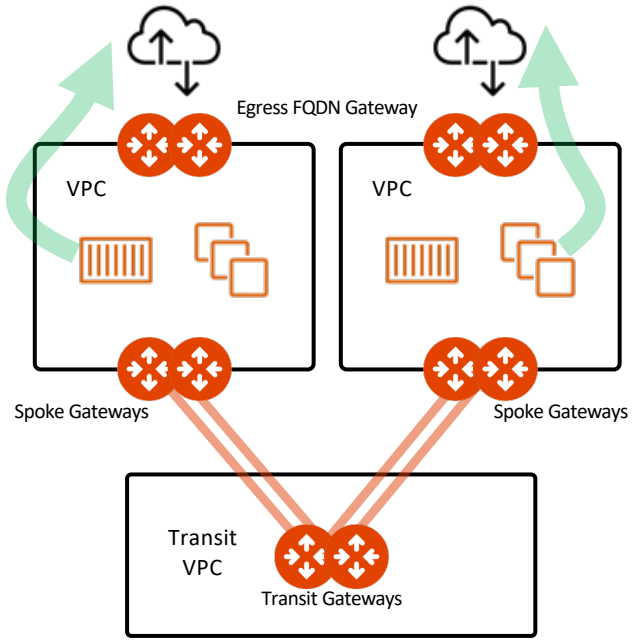

Aviatrix Controller
Aviatrix CoPilot
Internet
Internet
Internet
AZ1
AZ2
AZ1
AZ2
AZ1
AZ2
AZ1
AZ2
Aviatrix Secure Egress/Spoke Gateways
Aviatrix Secure Egress/Spoke Gateways
Aviatrix Secure Egress/Spoke Gateways
Aviatrix Secure Egress/Spoke Gateways
Cloud Workloads
Cloud Workloads
Cloud Workloads
Cloud Workloads
App 1
App 2
App 3
App 4
aws
Azure
Google Cloud

Aviatrix Secure Egress Filtering Design Pattern

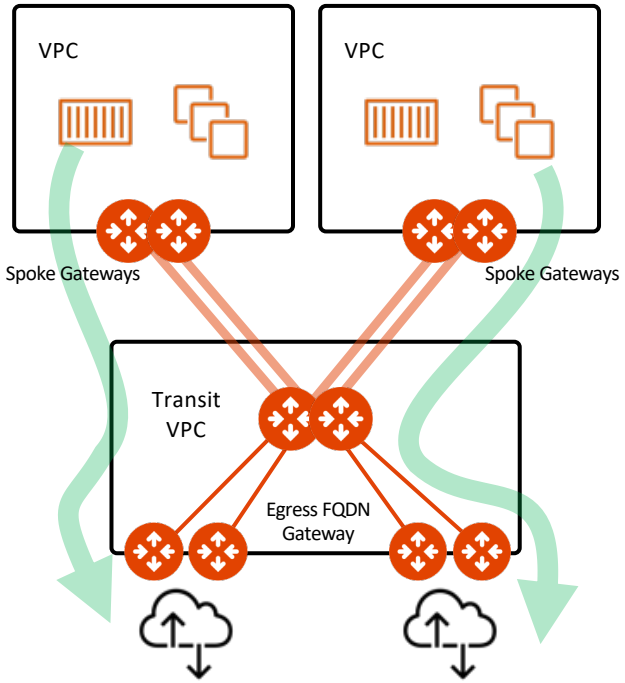
Local Egress FQDN Filtering (Distributed)



Local Egress FQDN Filtering (Distributed) with Aviatrix Transit

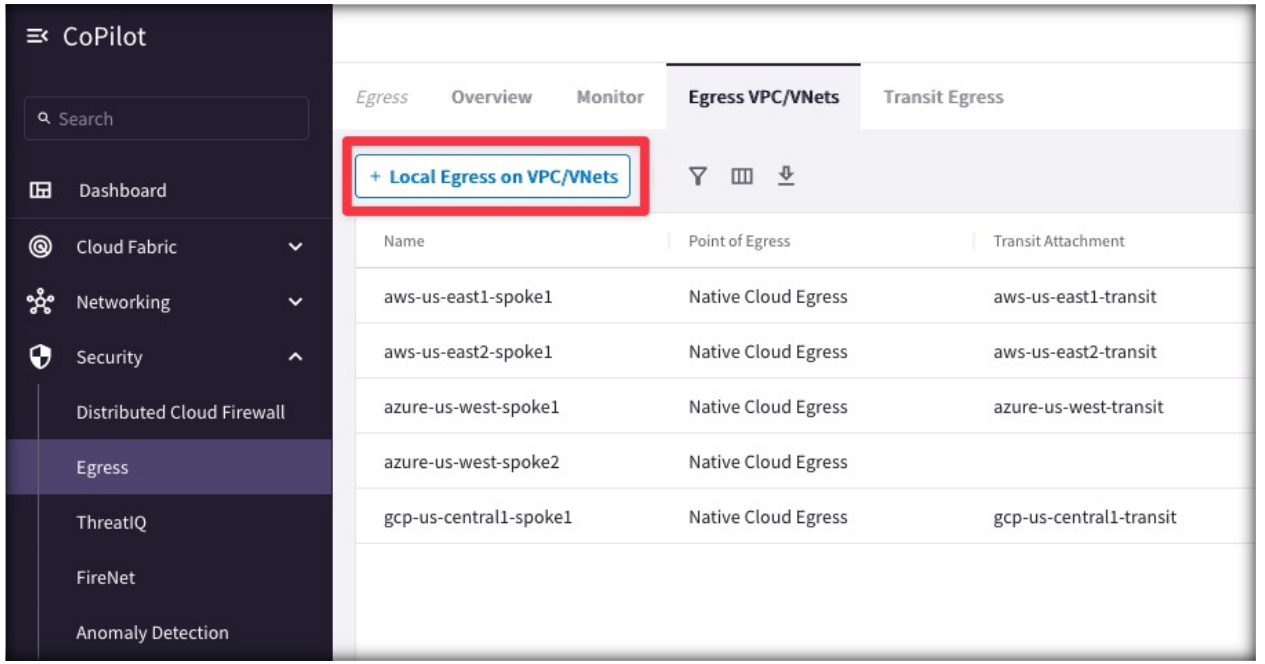


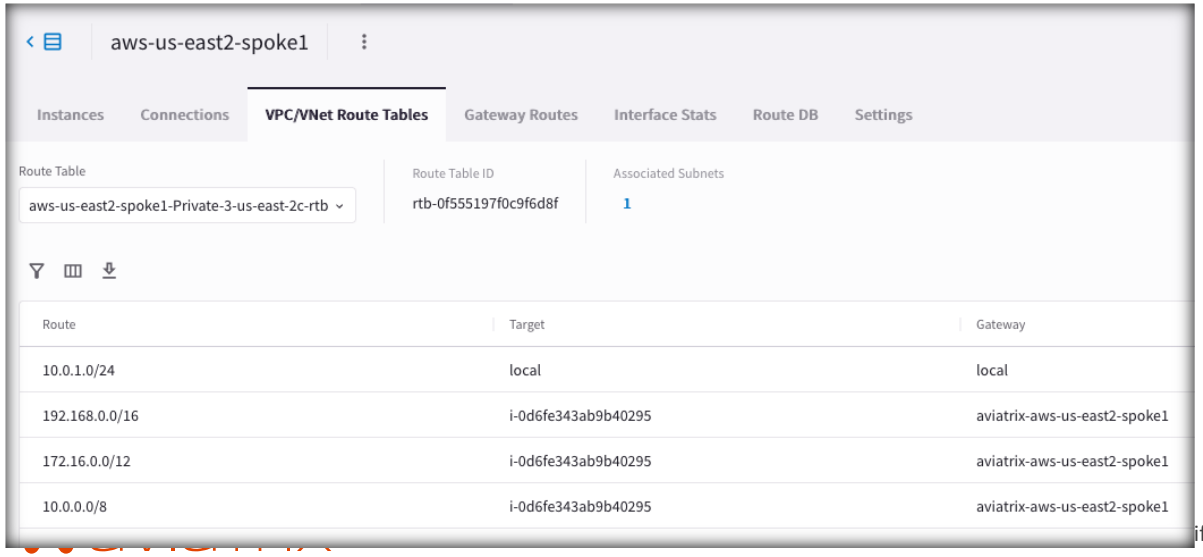
Centralized Egress with Aviatrix Transit

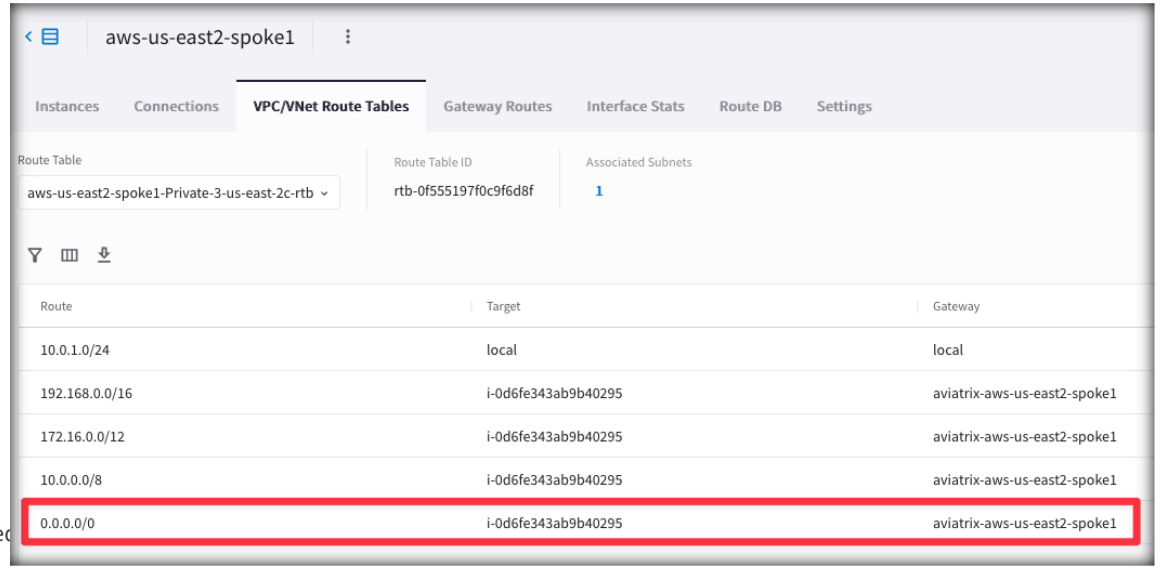


Enable Egress

- 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.







aviatrix

Aviatrix Certified Engineer (ACE)
https://aviatrix.com/ACE

COMMUNITY
https://community.aviatrix.com