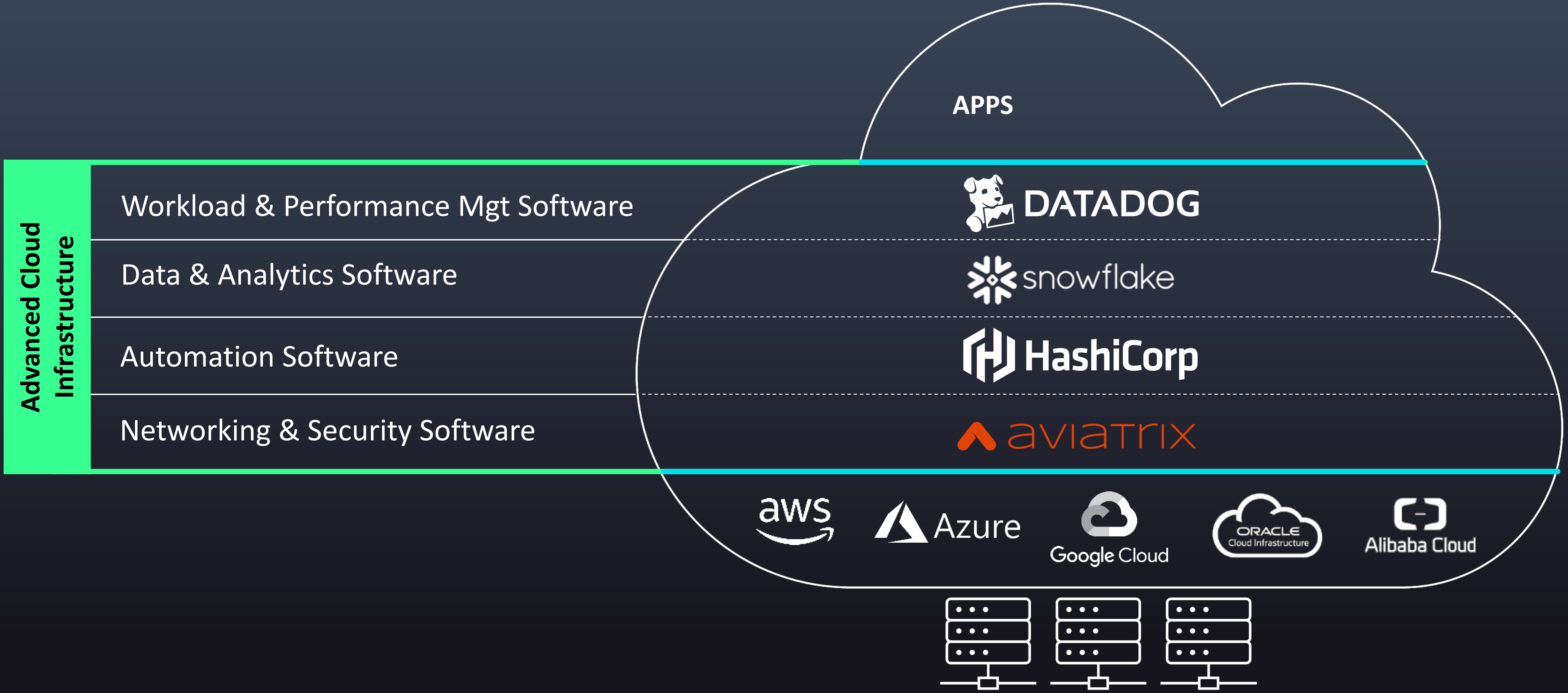
Overview of the Aviatrix Solution

Business-Critical Applications
Require Business-Critical Infrastructure



Advanced Cloud Infrastructure

APPS

Workload & Performance Mgt Software

Data & Analytics Software

Automation Software

Networking & Security Software

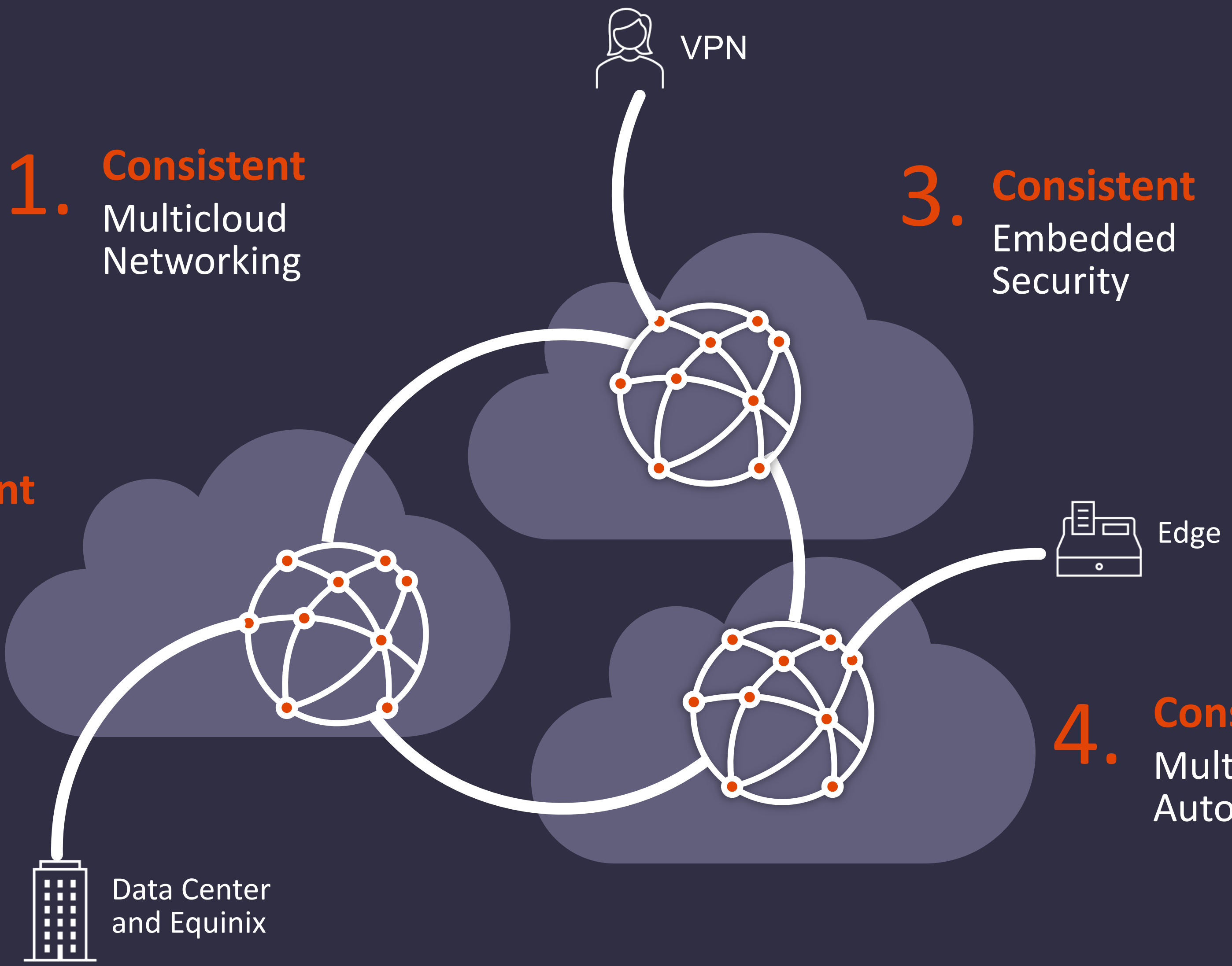
aviatrix

Secure Cloud Networking™

What is it?

Aviatrix Upgrades
Native Cloud
Networking

aws
ORACLE Cloud Infrastructure
Azure
Alibaba Cloud
Google Cloud



1. **Consistent** Multicloud Networking

2. **Consistent** Visibility & Control

3. **Consistent** Embedded Security

4. **Consistent** Multicloud Automation

Top Pains Aviatrix Relieves – What's Yours?

1. Multicloud Networking

- Overlapping IP CIDRs, Overlay IP (SAP/AWS)
- Multicloud Automated Route Propagation
- BGP Into Cloud / Traffic Engineering
- Extending Cloud Ops Model to Edge / Equinix

2. Operational Visibility & Control

- Network Flow Analytics
- Dynamic Topology Mapping
- Packet Capture, Ping, Traceroute
- CostIQ Shared Services Cost Allocation

3. Security Risks and Costs

- Distributed Firewalling IN the network
- High-Performance Encryption (up to 100 Gbps)
- NGFW Service Insertion
- Automated Threat Detection and Mitigation

4. Multicloud Simplicity, Agility, Speed

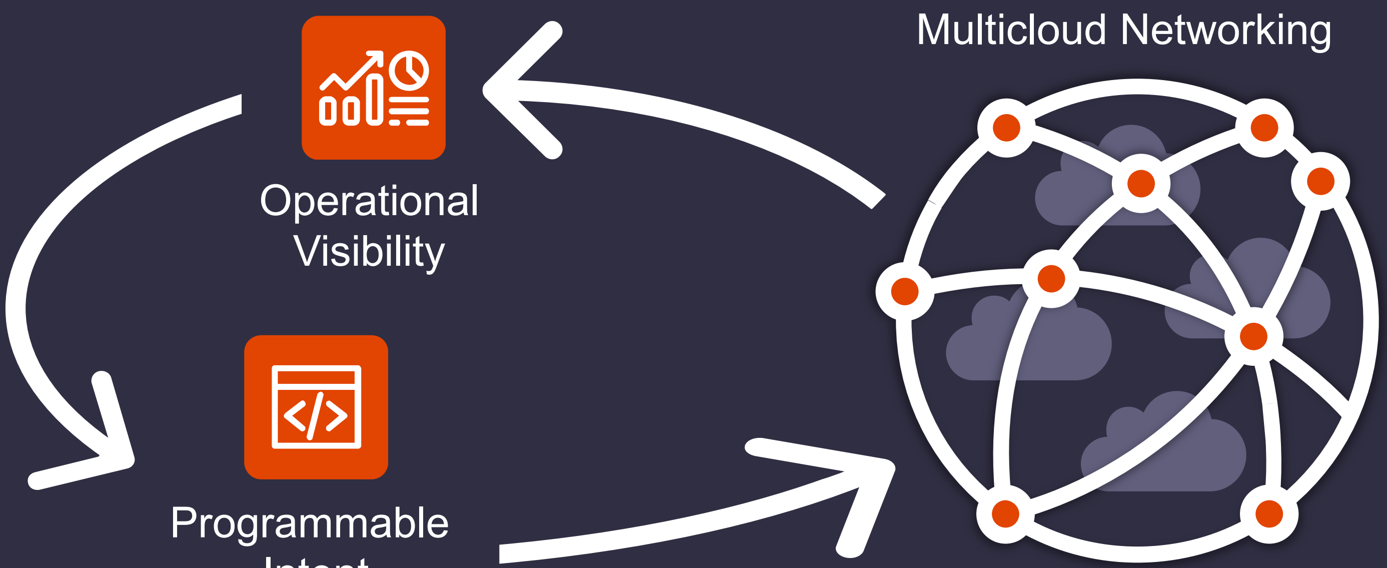
- Beyond Native Cloud Connectivity
- IN the cloud, not just TO the cloud
- Multicloud Terraform Provider
- Self-Service Portal e.g. ServiceNow

SAP Migrations | Customer Onboarding | Acquisition Integrations | Skills Shortage | Resource Efficiency

What Makes Aviatrix Unique?

Aviatrix Cloud Networking Platform

Secure Cloud Networking optimizes business-critical application availability, performance, security, and cost.



Multicloud Networking

Operational Visibility

Programmable Intent

Embedded Telemetry and Distributed Control

Aviatrix CoPilot™

Aviatrix Cloud Fabric

Aviatrix AirSpace | Distributed Data Plane

Embedded Telemetry

See Everything

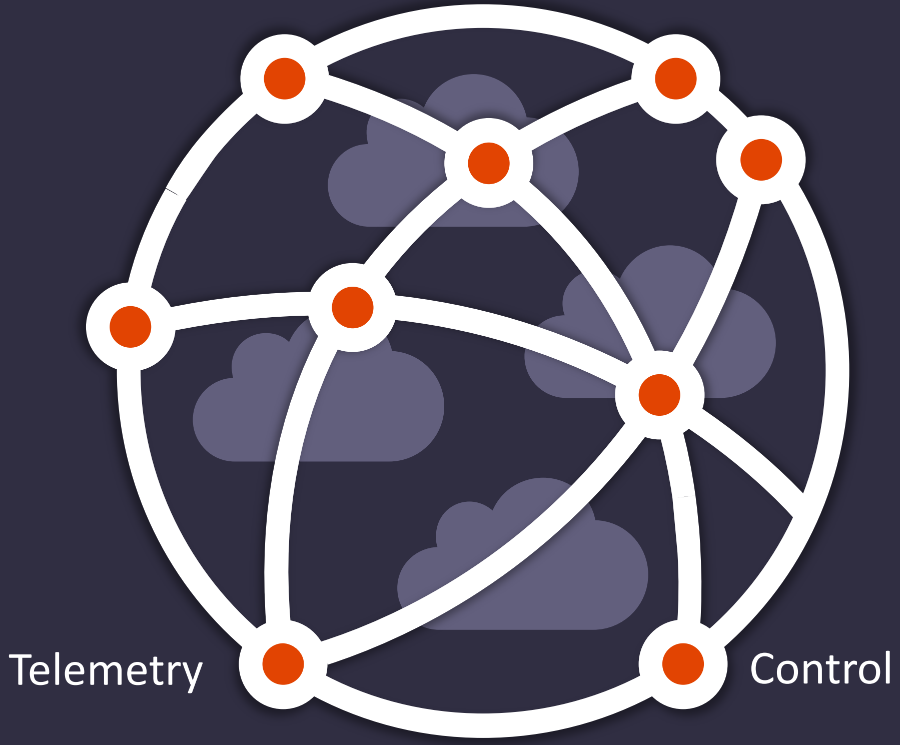
- Network Traffic Telemetry
- Security Telemetry
- Cost Telemetry
- Application Telemetry

Distributed Control

Control Everything

- Distributed Firewalling
- Intelligent Traffic Control

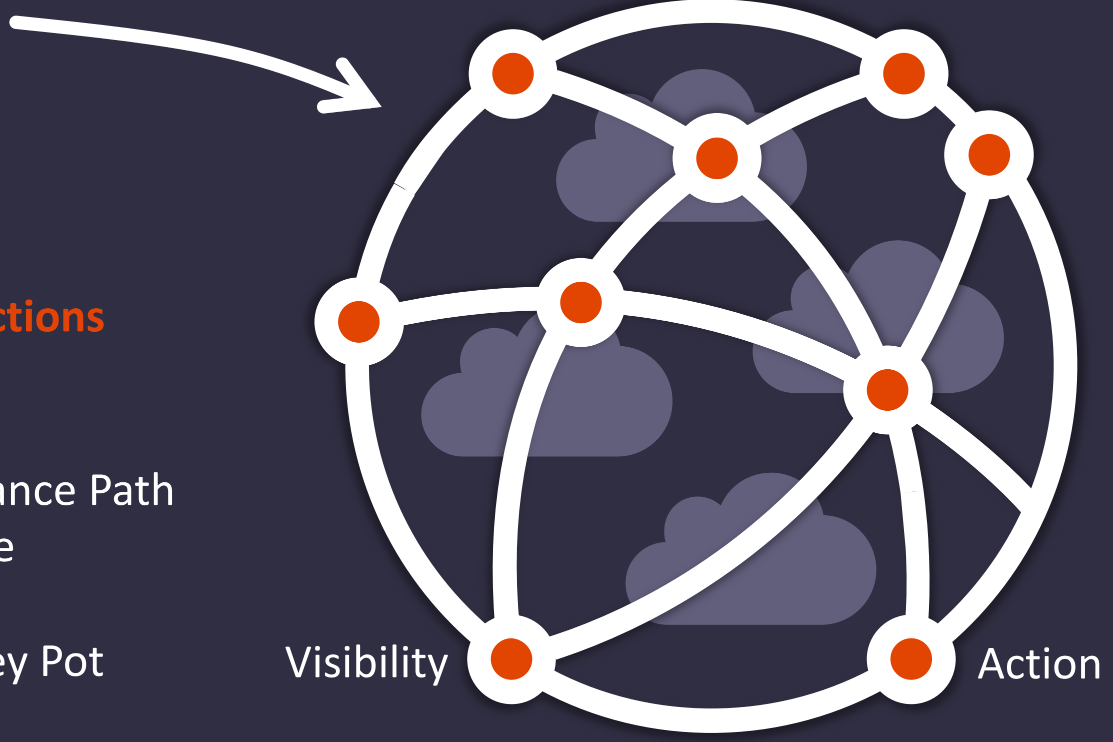
Aviatrix Cloud Fabric



Aviatrix CoPilot | Programmable Intent

IF < DEFINED TRAFFIC IS SEEN >
THEN < EXECUTE INTENDED ACTION >

Aviatrix Cloud Fabric



Security Actions

- Block or Allow
- Network Segmentation
- Micro Segmentation
- Domain Name Filtering
- Threat Detection and Mitigation
- Anomaly Detection

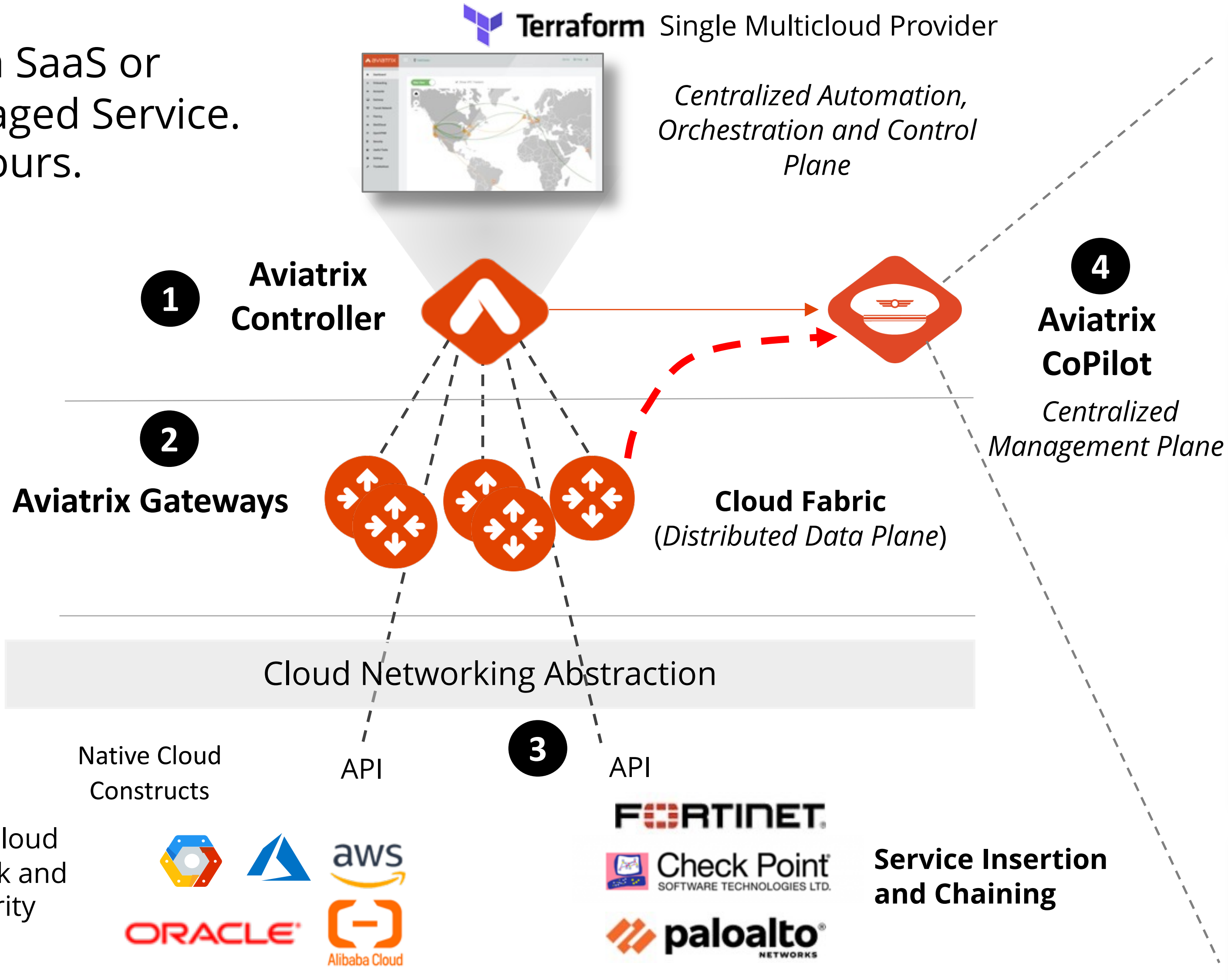
Traffic Control Actions

- Optimize Path
- Low-Cost Path
- High-Performance Path
- Packet Capture
- Log for Audit
- Direct to Honey Pot

Aviatrix Solution Components

Aviatrix Cloud Network Platform Software

Not a SaaS or
Managed Service.
It's Yours.



Terraform Single Multicloud Provider

Centralized Automation, Orchestration and Control Plane

1 **Aviatrix Controller**

2 **Aviatrix Gateways**

Cloud Fabric
(Distributed Data Plane)

4 **Aviatrix CoPilot**
Centralized Management Plane

Cloud Networking Abstraction

Native Cloud Constructs

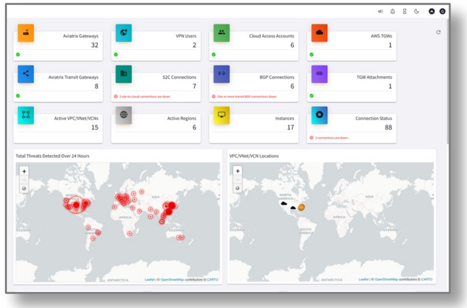
API

3

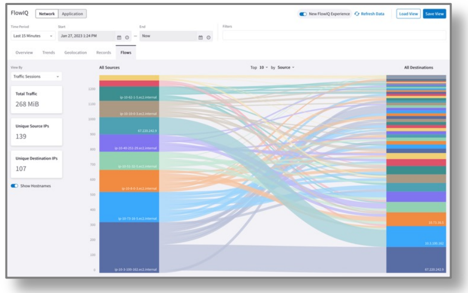
API

Basic Cloud Network and Security

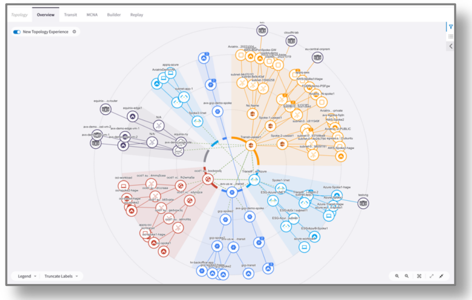
Service Insertion and Chaining



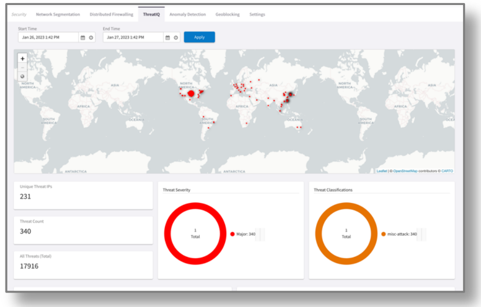
Multicloud Operational Visibility



FlowIQ Multicloud Traffic Flow Analysis

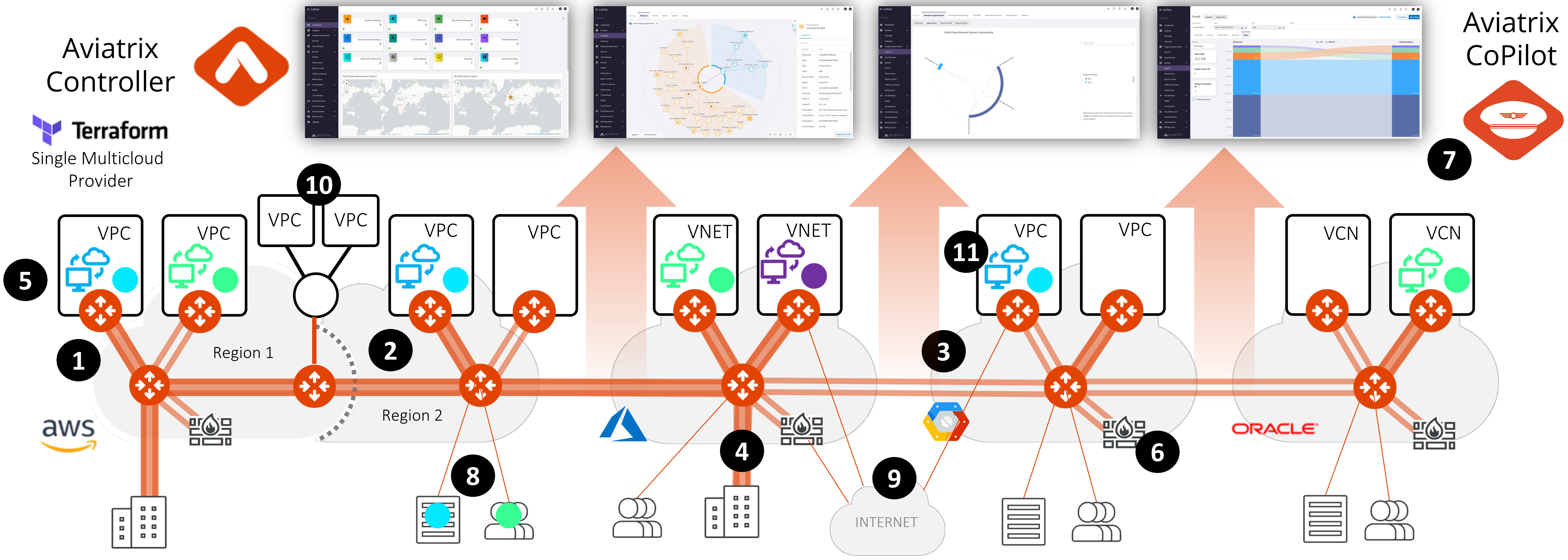


Multicloud Dynamic Topology Mapping



ThreatIQ with ThreatGuard Distributed Threat Visibility and Control

Aviatrix – Foundation of Your Multicloud Networking and Security



Aviatrix Controller

Terraform

Single Multicloud Provider

Aviatrix CoPilot

1. Single Cloud
   Multi-Account
   High-Availability (Active-Active)
   End-to-End Encryption
   Network Correctness

2. Multi-Region

3. Multicloud Repeatable Design

4. High-Performance Encryption

5. Network Segmentation

6. Service Insertion & Chaining

7. Enterprise Operational Visibility

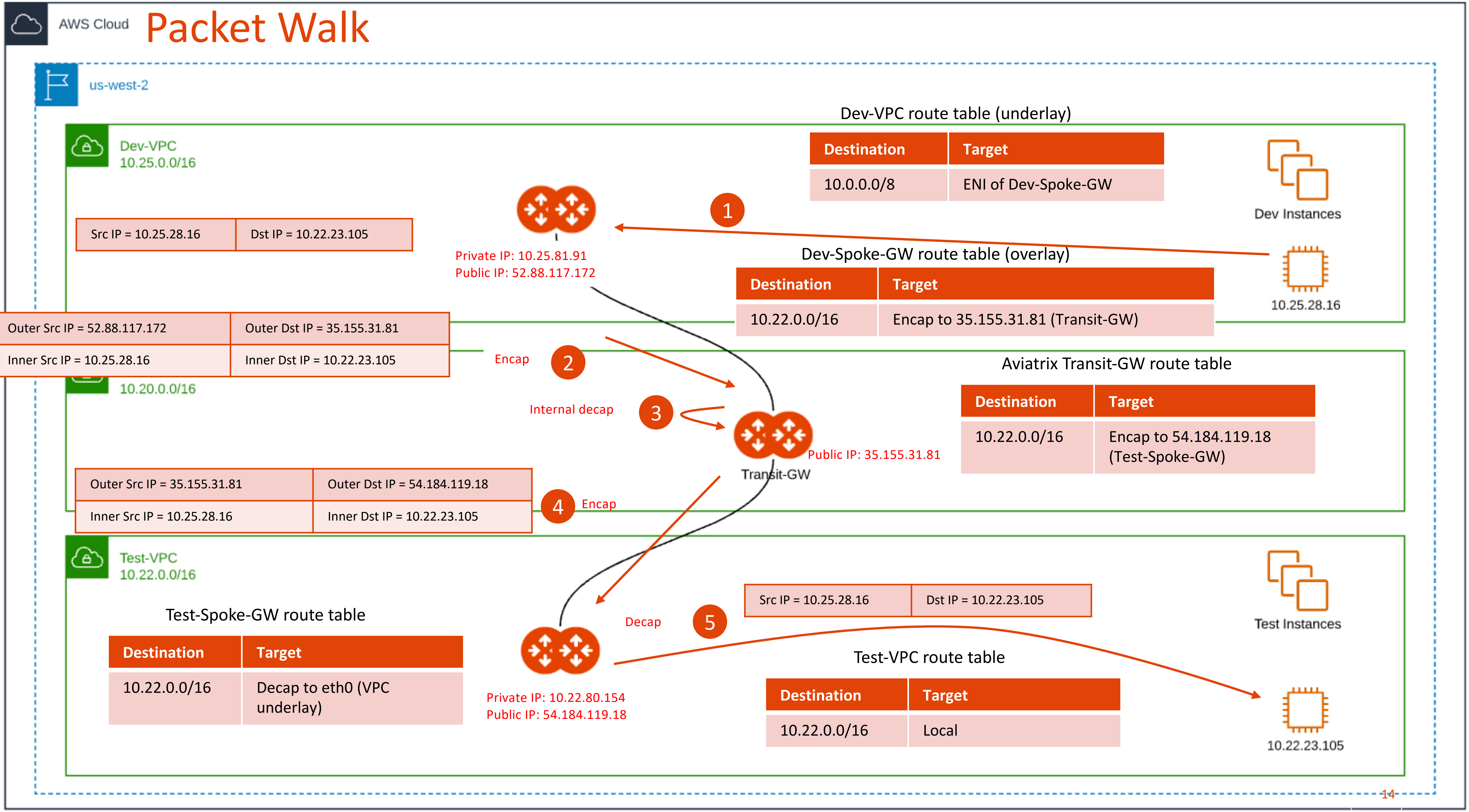
8. Secure Cloud Access

9. Secure Ingress and Egress

10. Cloud-Native

11. Distributed Cloud Firewall

Packet Walk



Dev-VPC route table (underlay)

Destination	Target
10.0.0.0/8	ENI of Dev-Spoke-GW

Src IP = 10.25.28.16	Dst IP = 10.22.23.105

Dev-Spoke-GW route table (overlay)

Destination	Target
10.22.0.0/16	Encap to 35.155.31.81 (Transit-GW)

Outer Src IP = 52.88.117.172	Outer Dst IP = 35.155.31.81
Inner Src IP = 10.25.28.16	Inner Dst IP = 10.22.23.105

Aviatrix Transit-GW route table

Destination	Target
10.22.0.0/16	Encap to 54.184.119.18 (Test-Spoke-GW)

Outer Src IP = 35.155.31.81	Outer Dst IP = 54.184.119.18
Inner Src IP = 10.25.28.16	Inner Dst IP = 10.22.23.105

Test-Spoke-GW route table

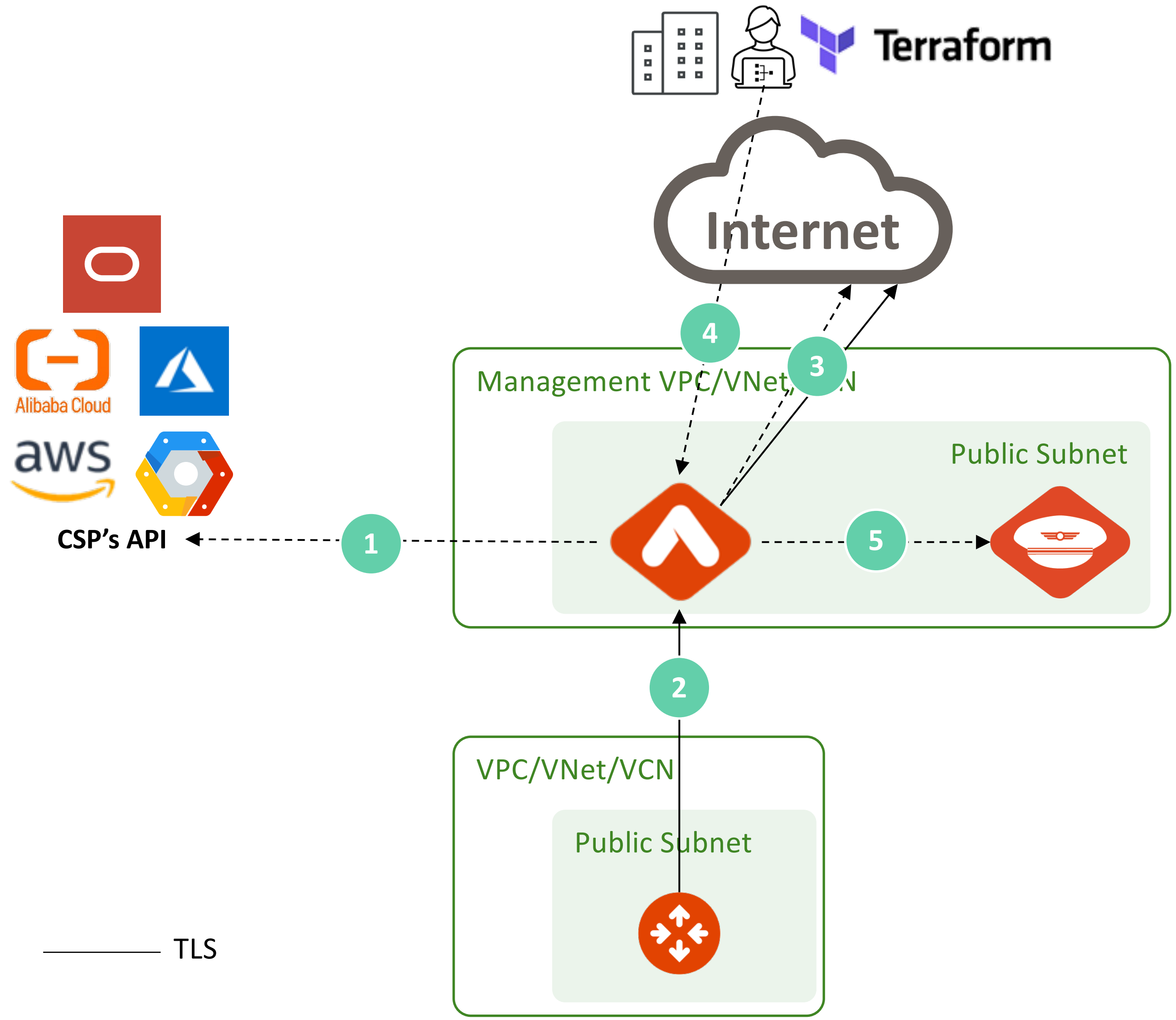
Destination	Target
10.22.0.0/16	Decap to eth0 (VPC underlay)

Src IP = 10.25.28.16	Dst IP = 10.22.23.105

Test-VPC route table

Destination	Target
10.22.0.0/16	Local

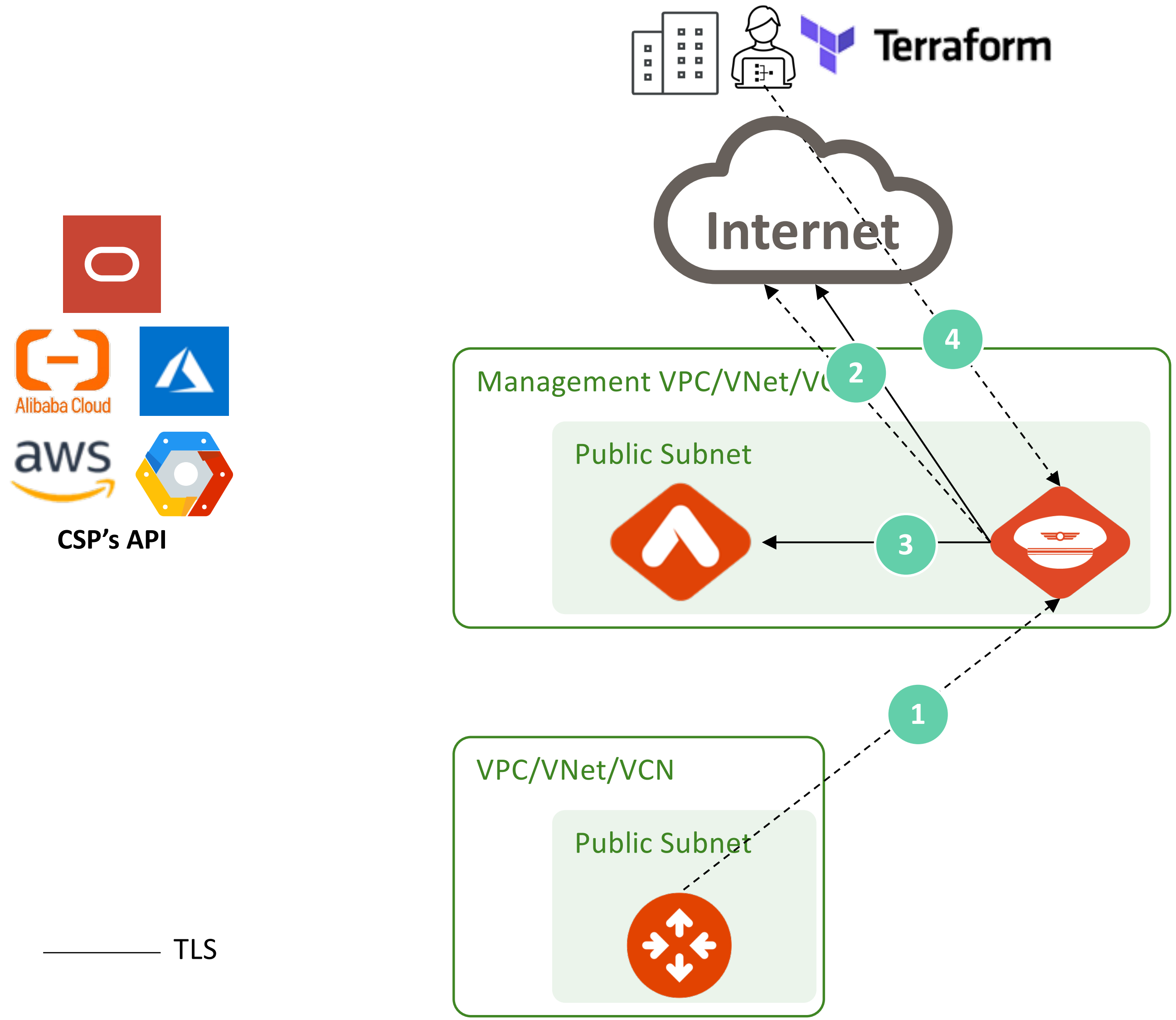
Controller Flows:



Traffic Pattern

1. Controller to CSP's APIs
   - TCP 443
2. Gateway to Controller management traffic
   - Control Plane - TCP 443
3. Controller to Internet
   - DNS, NTP (UDP)
   - Queuing Svc, Updates, Licensing, Diagnostics, Tracelogs, Aviatrix Svcs (TCP 443)
4. Admin to Controller
   - Access locked to customer IP (TCP 443)
5. Controller to CoPilot
   - Syslog - UDP

CoPilot Flows:

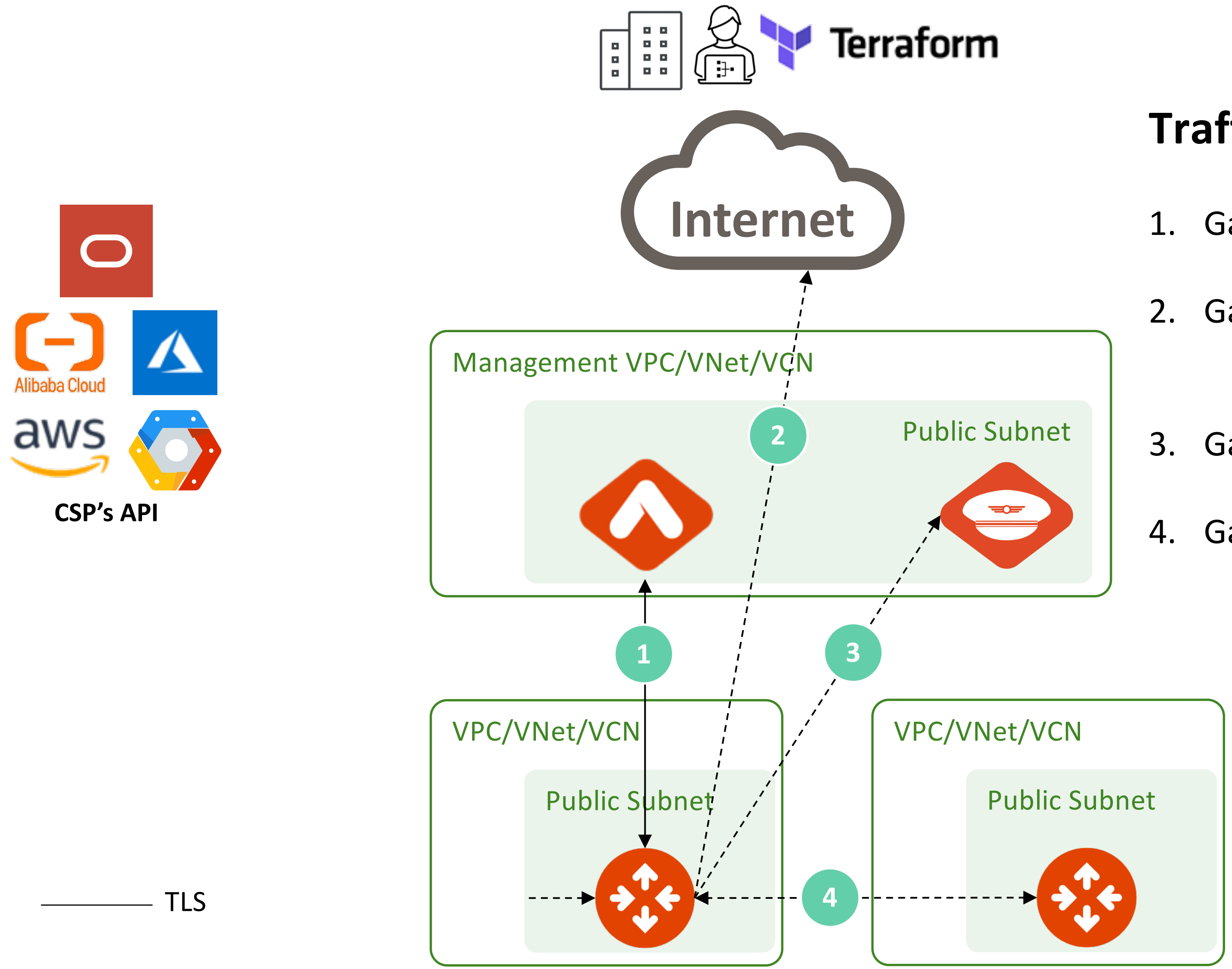


—— TLS

Traffic Pattern

1. Gateways to CoPilot
   - Syslog and NetFlow (UDP, could be over IPSec)
2. CoPilot to Internet
   - NTP, DNS (UDP)
   - Updates, Threat Intelligence, Webhook Srv (TCP 443)
3. CoPilot to Controller
   - TCP 443
4. Admin to CoPilot
   - Access locked to customer IP (TCP 443)

Gateway Flows:



—— TLS

Traffic Pattern

1. Gateway to Controller Heartbeat
   - Control Plane - TCP 443
2. Gateway to Internet
   - DNS (UDP)
   - Google
3. Gateway to CoPilot
   - Syslog, NetFlow (UDP, could be over IPSec)
4. Gateway to Gateway
   - IPSec (UDP 500, 4500)

MCNA in Private Mode:

Multicloud networking by removing the need for public IPs for Aviatrix gateways.

Web proxies are used for the gateways to access the internet.

Underlay communication is done via native cloud constructs such as

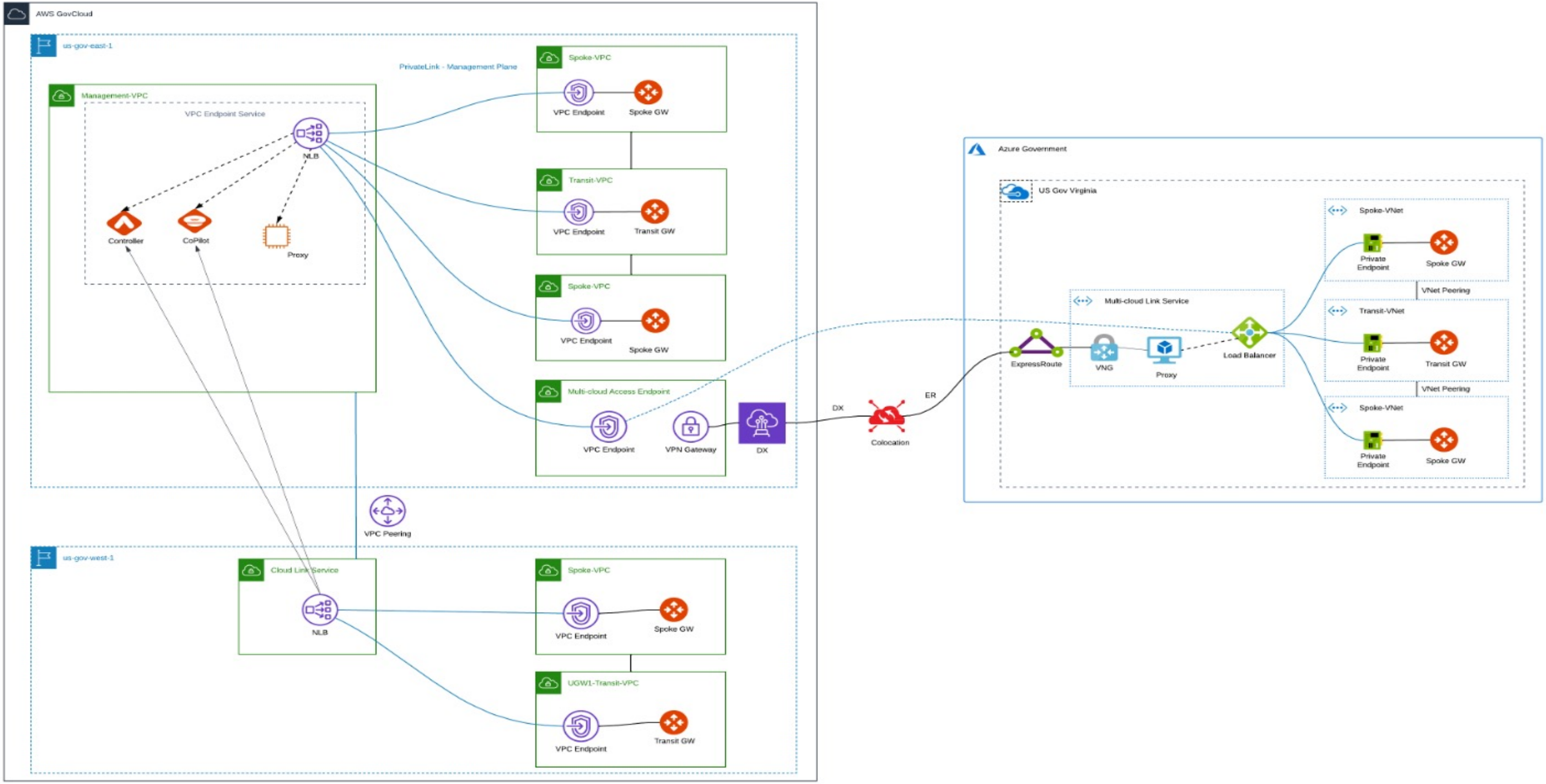
LoadBalancers

Private Link Services

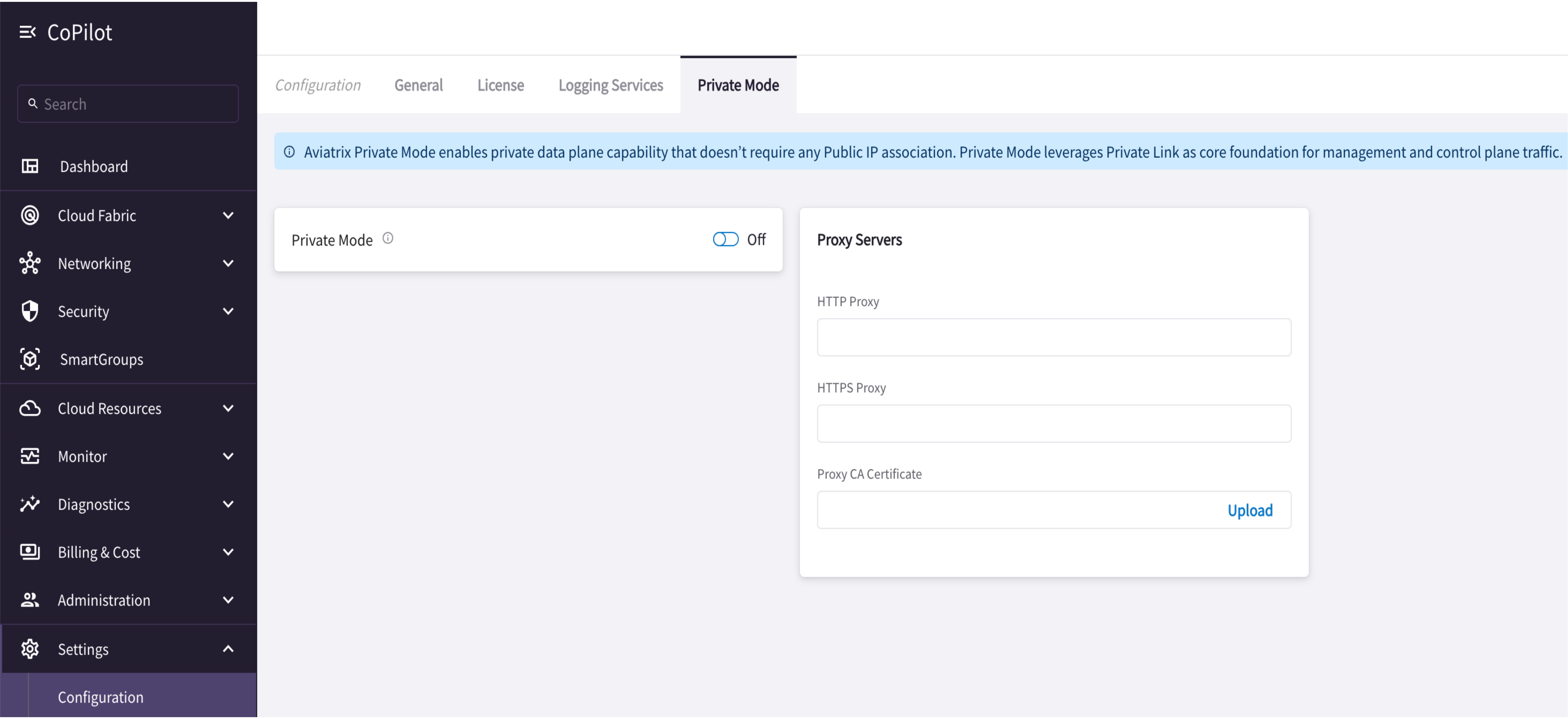
peering connections

Supported in cloud environments such as AWS, AWS GovCloud, Azure, and Azure Government

Private Mode Architecture



Enabling Private Mode:



ⓘ Aviatrix Private Mode enables private data plane capability that doesn’t require any Public IP association. Private Mode leverages Private Link as core foundation for management and control plane traffic.

Private Mode ⓘ Off

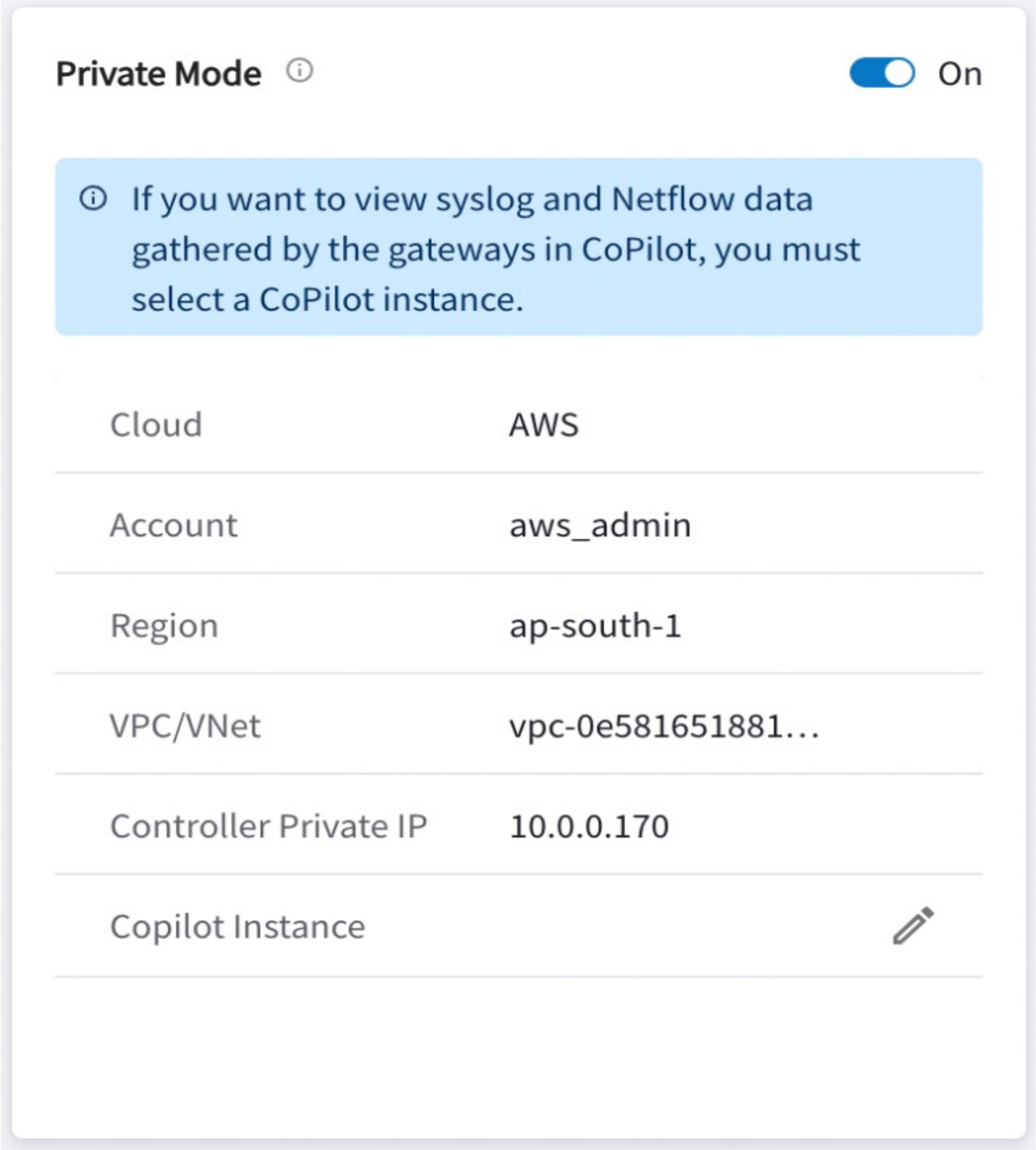
Proxy Servers

HTTP Proxy

HTTPS Proxy

Proxy CA Certificate Upload

After Enabling Private Mode:



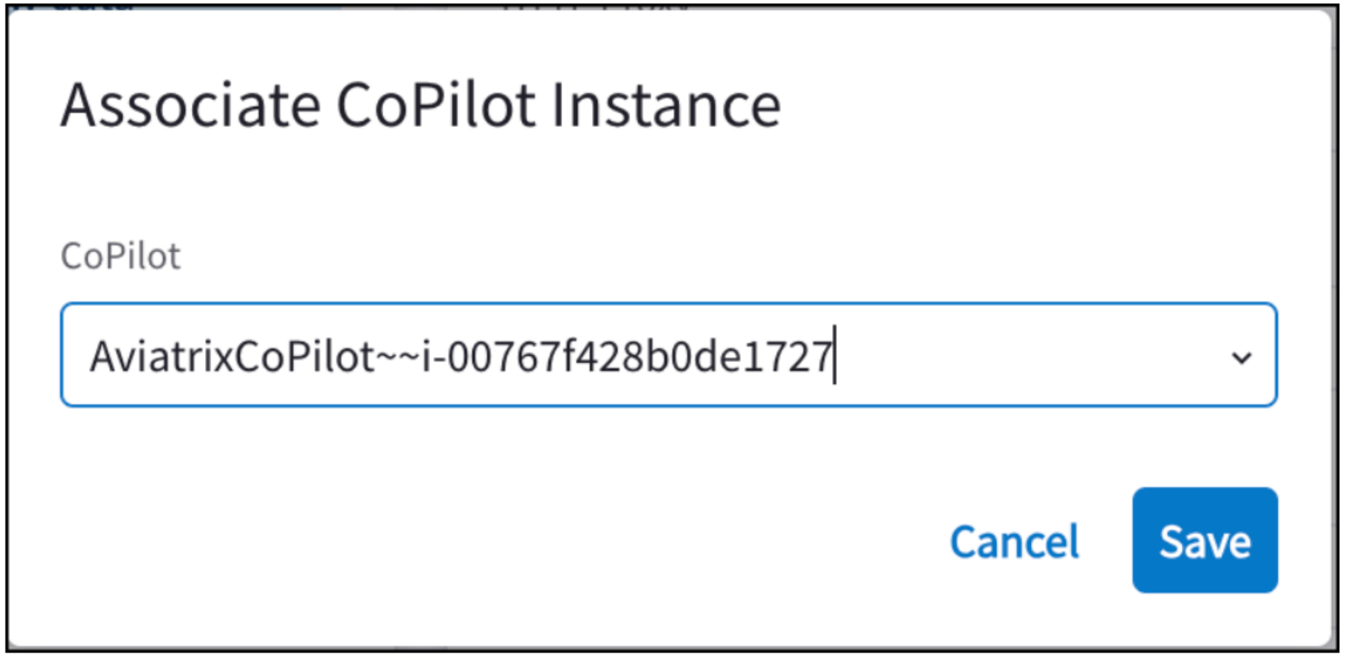
Private Mode ⓘ ● On

ⓘ If you want to view syslog and Netflow data gathered by the gateways in CoPilot, you must select a CoPilot instance.

Cloud	AWS
Account	aws_admin
Region	ap-south-1
VPC/VNet	vpc-0e581651881...
Controller Private IP	10.0.0.170
Copilot Instance	✎

- All gateways you create will use private IPs.
- You will not be able to create or deploy non-private gateways.
- A mixture of public and private IPs is not possible.

To view syslog and NetFlow data gathered by the gateways in CoPilot, you must select a CoPilot instance.

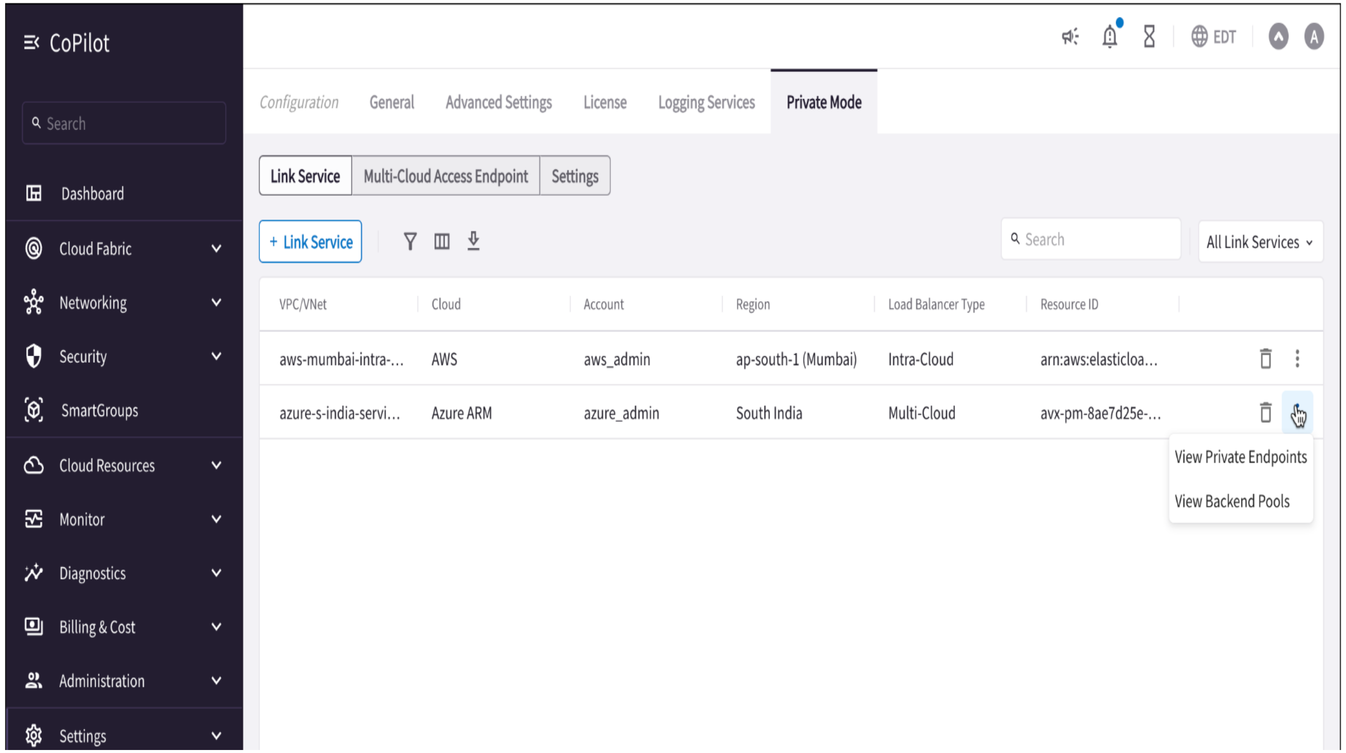


Associate CoPilot Instance

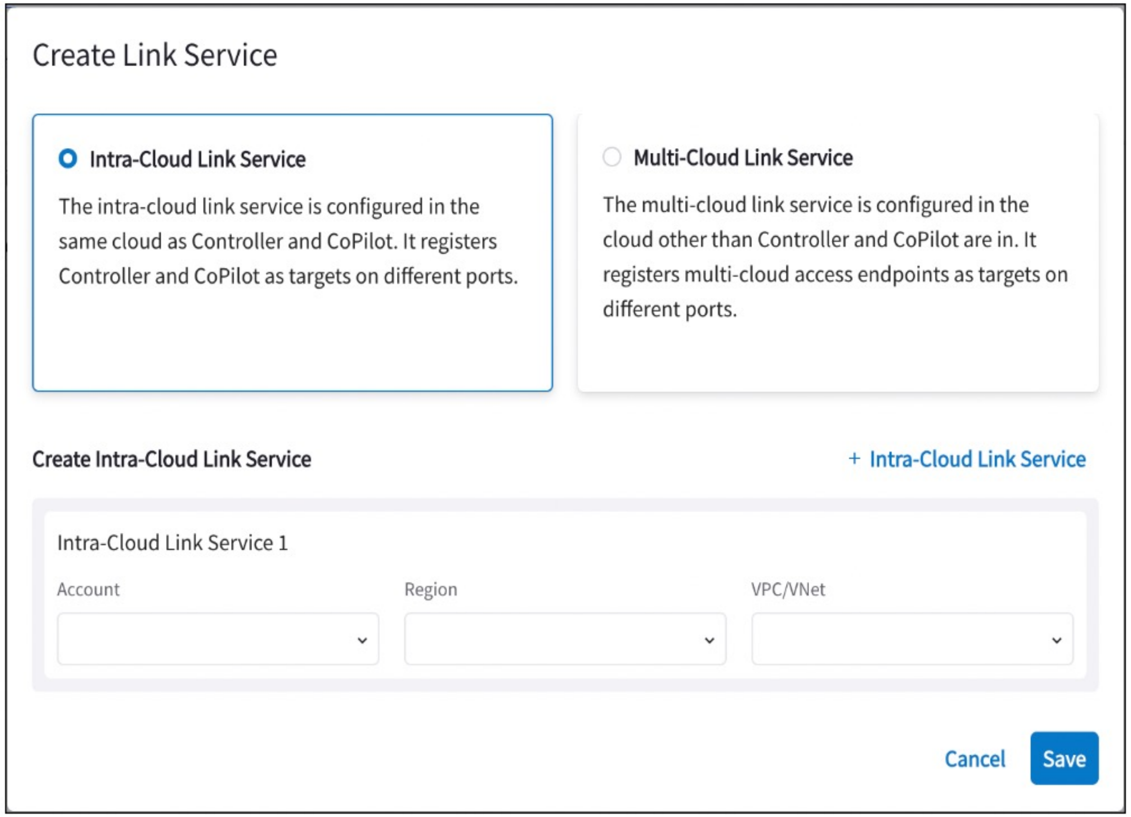
CoPilot: AviatrixCoPilot~~i-00767f428b0de1727

Creation of Link Services for Private Mode:

- For a single cloud Private Mode environment, create an Intra-Cloud Link Service (AWS only).
- For multicloud, create an Intra-Cloud Link Service and a Multicloud Link Service.
- Prior to establishing the Multicloud Link Service, it is essential to set up multi-cloud access endpoints.
- On the Private Mode > Link Service tab, click **+Link Service**.



VPC/VNet	Cloud	Account	Region	Load Balancer Type	Resource ID
aws-mumbai-intra-...	AWS	aws_admin	ap-south-1 (Mumbai)	Intra-Cloud	arn:aws:elasticloa...
azure-s-india-servi...	Azure ARM	azure_admin	South India	Multi-Cloud	avx-pm-8ae7d25e-...



Create Link Service

● **Intra-Cloud Link Service**

The intra-cloud link service is configured in the same cloud as Controller and CoPilot. It registers Controller and CoPilot as targets on different ports.

○ **Multi-Cloud Link Service**

The multi-cloud link service is configured in the cloud other than Controller and CoPilot are in. It registers multi-cloud access endpoints as targets on different ports.

Create Intra-Cloud Link Service

Intra-Cloud Link Service 1

Account

Region

VPC/VNet

Private Mode Limitations

- Site2Cloud can only be created over a private network using a private IP
- Aviatrix TGW Orchestrator not available
- BGP over LAN not available
- Controller Security tab: features on this tab not supported
- High Performance Encryption (HPE) over the internet not supported
- Egress for Transit FireNet not supported
- Creation of VPN, Public Subnet Filtering gateways not supported
- Launching gateways in the same VPC/VNet as the Link Service VPC/VNet not supported
- Egress through Firewall: cannot enable internet-bound egress traffic for inspection
- Software rollback to 6.7 not supported (since Private Mode did not exist prior to 6.8)
- Cross-cloud Spoke-Transit peering is not supported with private IPs