AVIATRIX®

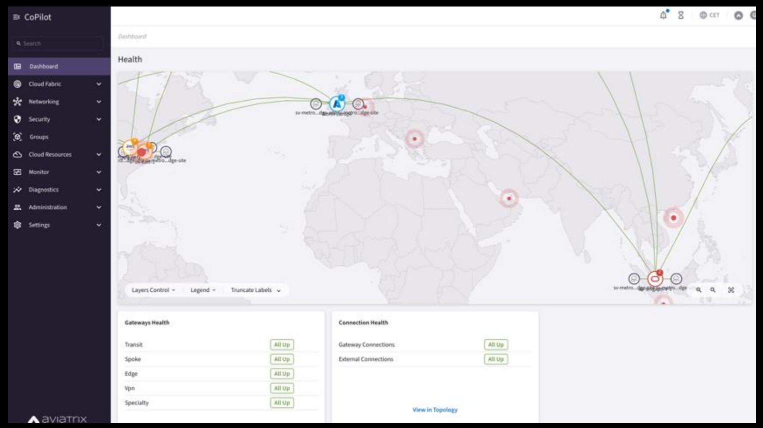
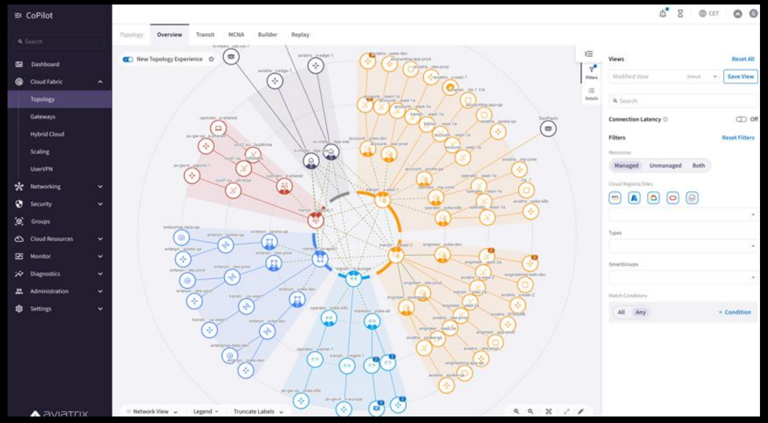
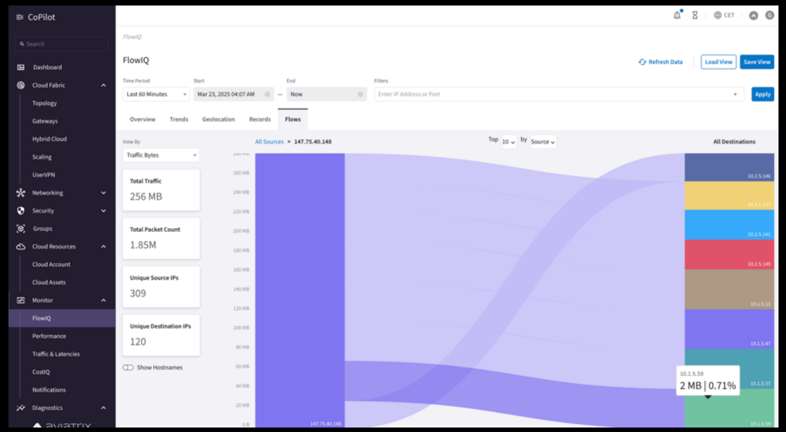
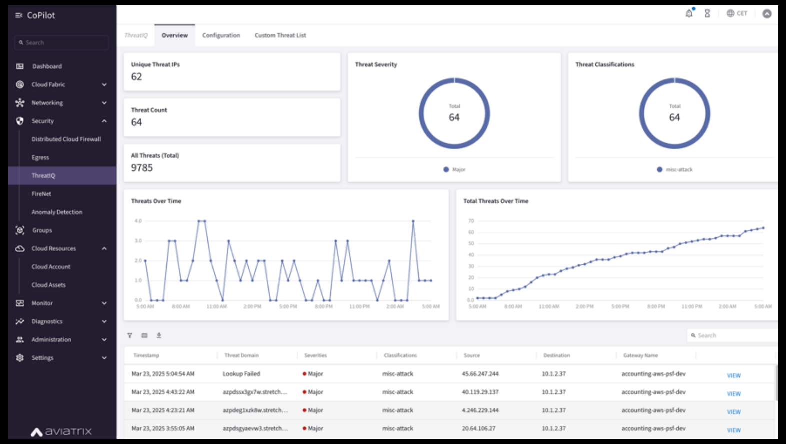
Network Segmentation

Segmentation

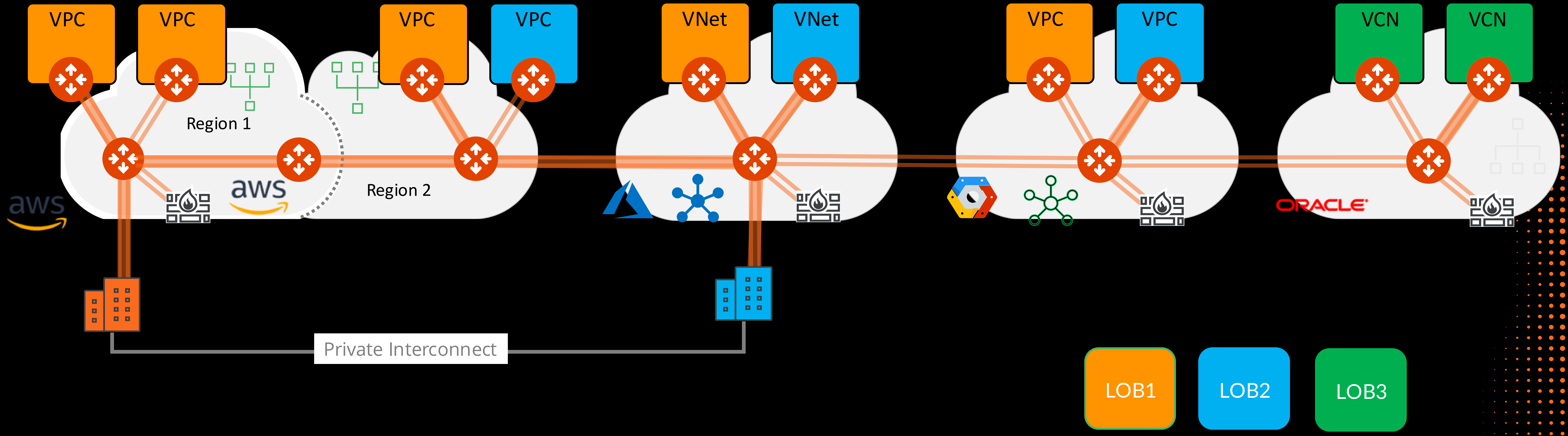
- Main Purpose: Enable ZTNA across multi-region and multi-cloud environments, including on-premises.
- Group VNets/VPCs/VCNs/Apps that share similar security policies.
- Define your own domains.
- Use Cases: Compliance, Governance, Audits.
- Network Segmentation is also referred to as Macro-Segmentation.
- A Network Domain can encompass one or more VPCs as a single logical container (i.e., Routing Domain).

Hybrid-Cloud Network Segmentation

Aviatrix CoPilot

Network Granularity and Control



Hybrid-Cloud Network Segmentation

Policy Based Network Segmentation

- Global
- Consistent / Repeatable
- Across accounts, subscriptions & projects

Cloud and Connection Agnostic

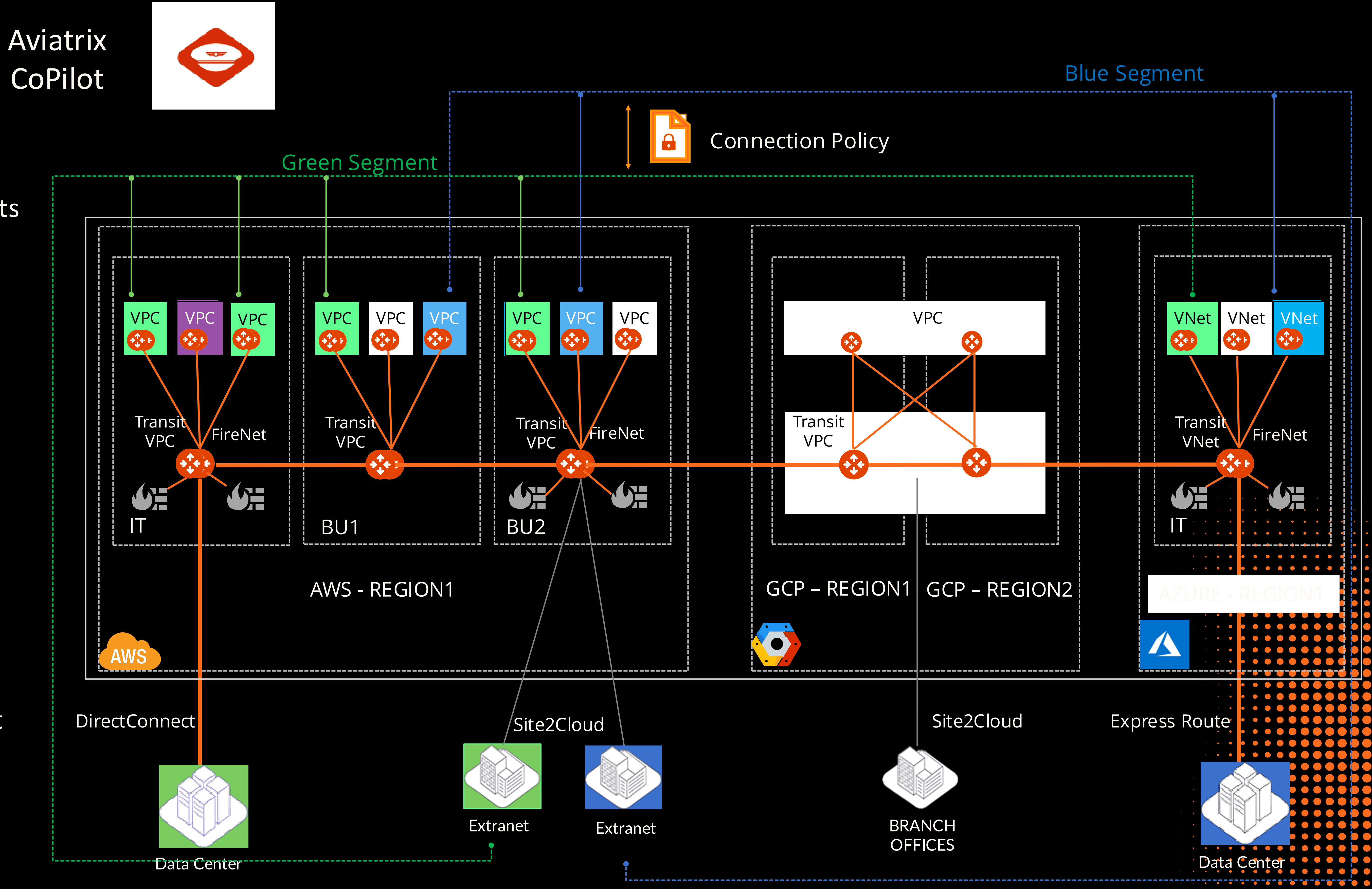
- Single cloud
- Intra-region or inter-region
- Multiple clouds

Edge/Access Segmentation

- On-Prem DCs
- Branches
- Extranets
- Cloud Peering

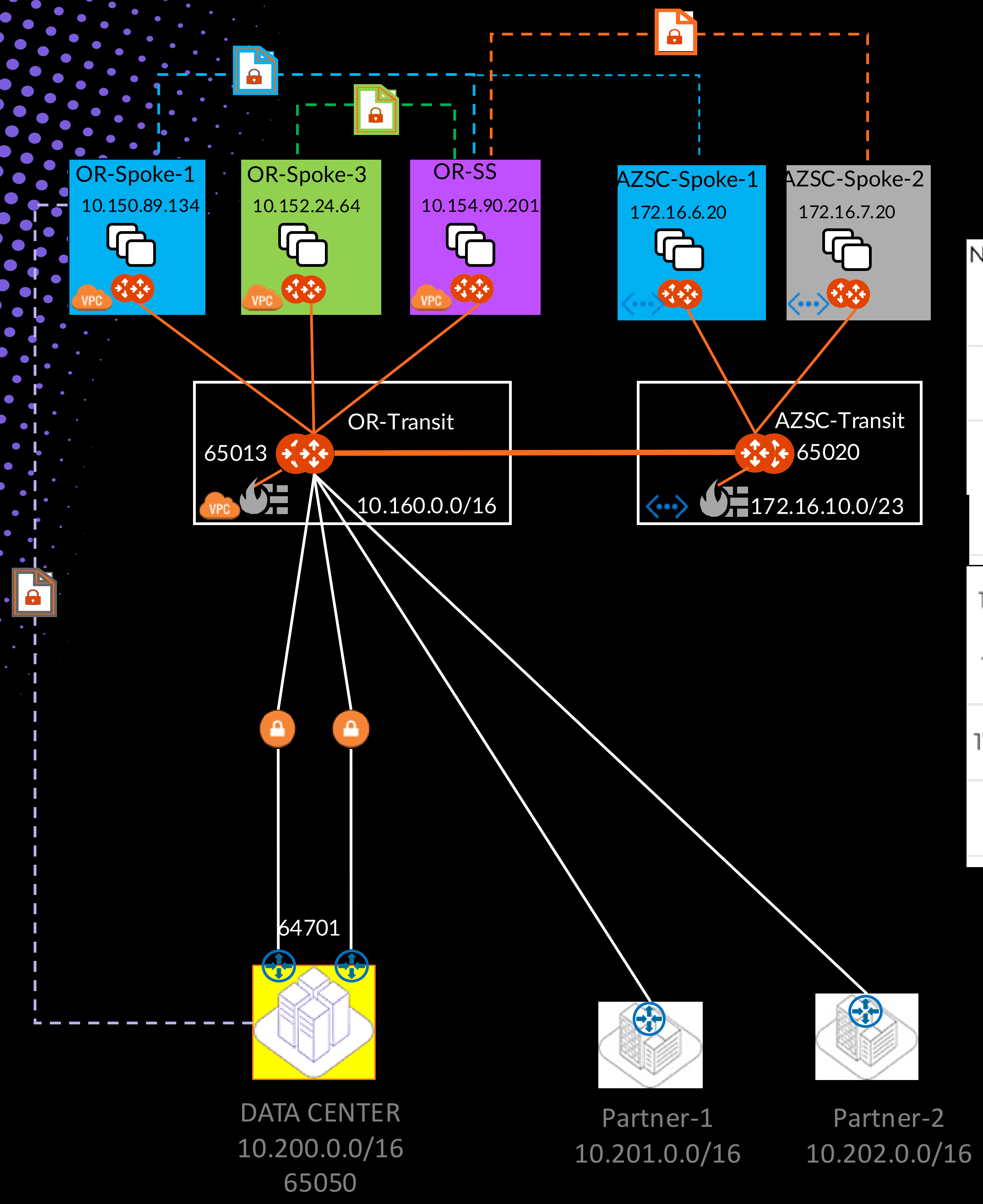
On-Demand Compliance/Governance

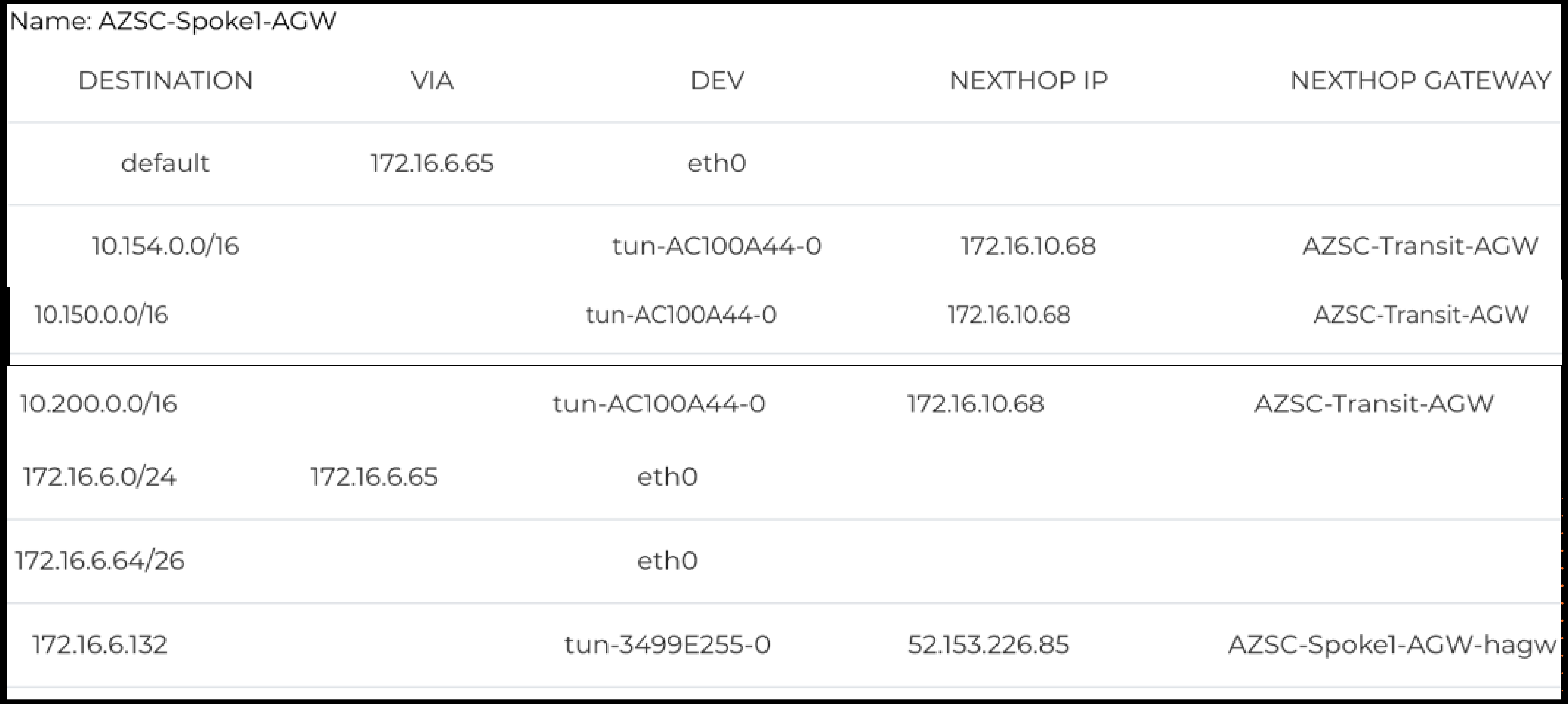
- Security Posture within minutes
- Aviatrix control plane realizes the intent
- Zero-Trust
- Flexible
- Automated



AVIATRIX

Hybrid-Cloud Network Segmentation





Name: AZSC-Spoke1-AGW

DESTINATION	VIA	DEV	NEXTHOP IP	NEXTHOP GATEWAY
default	172.16.6.65	eth0		
10.154.0.0/16		tun-AC100A44-0	172.16.10.68	AZSC-Transit-AGW
10.150.0.0/16		tun-AC100A44-0	172.16.10.68	AZSC-Transit-AGW
10.200.0.0/16		tun-AC100A44-0	172.16.10.68	AZSC-Transit-AGW
172.16.6.0/24	172.16.6.65	eth0		
172.16.6.64/26		eth0		
172.16.6.132		tun-3499E255-0	52.153.226.85	AZSC-Spoke1-AGW-hagw

Purple

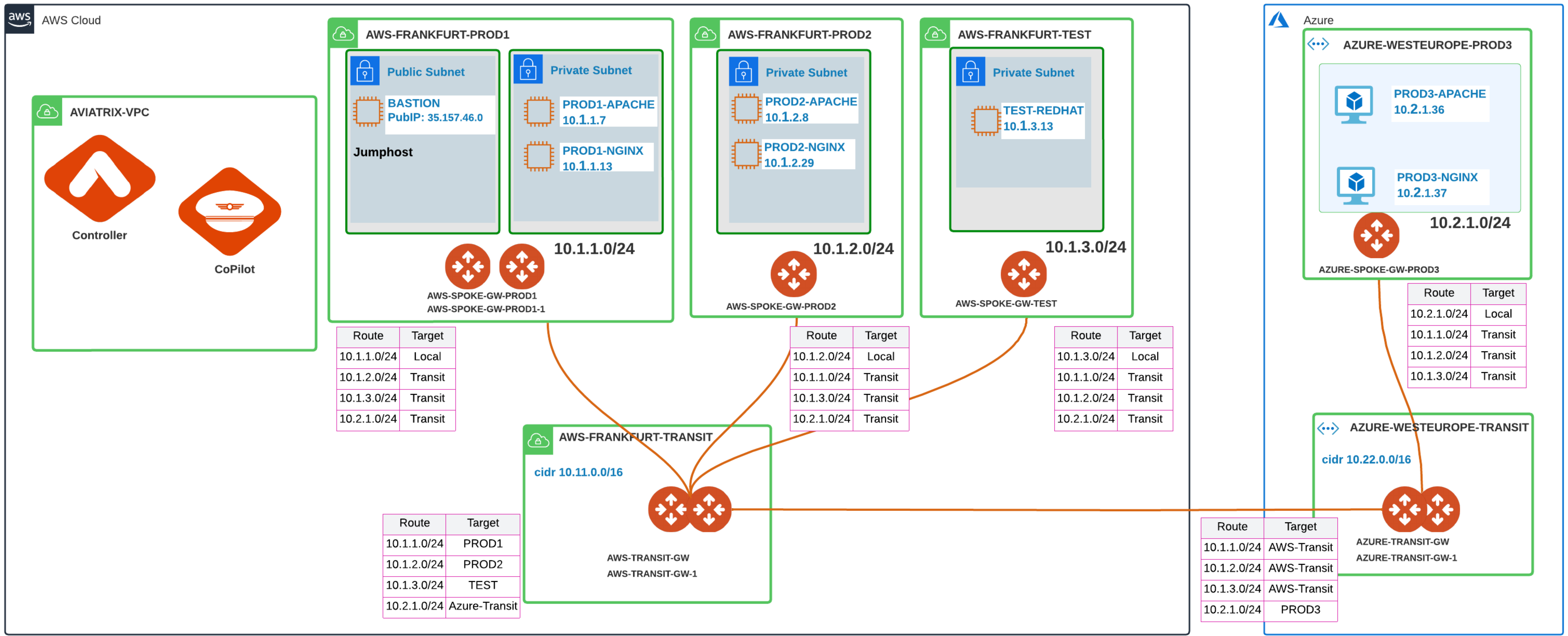
Remote-Blue

Yellow

Local-Blue

AVIATRIX

Enable Network Segmentation on the Transit Gateways



Route	Target
10.1.1.0/24	Local
10.1.2.0/24	Transit
10.1.3.0/24	Transit
10.2.1.0/24	Transit

Route	Target
10.1.2.0/24	Local
10.1.1.0/24	Transit
10.1.3.0/24	Transit
10.2.1.0/24	Transit

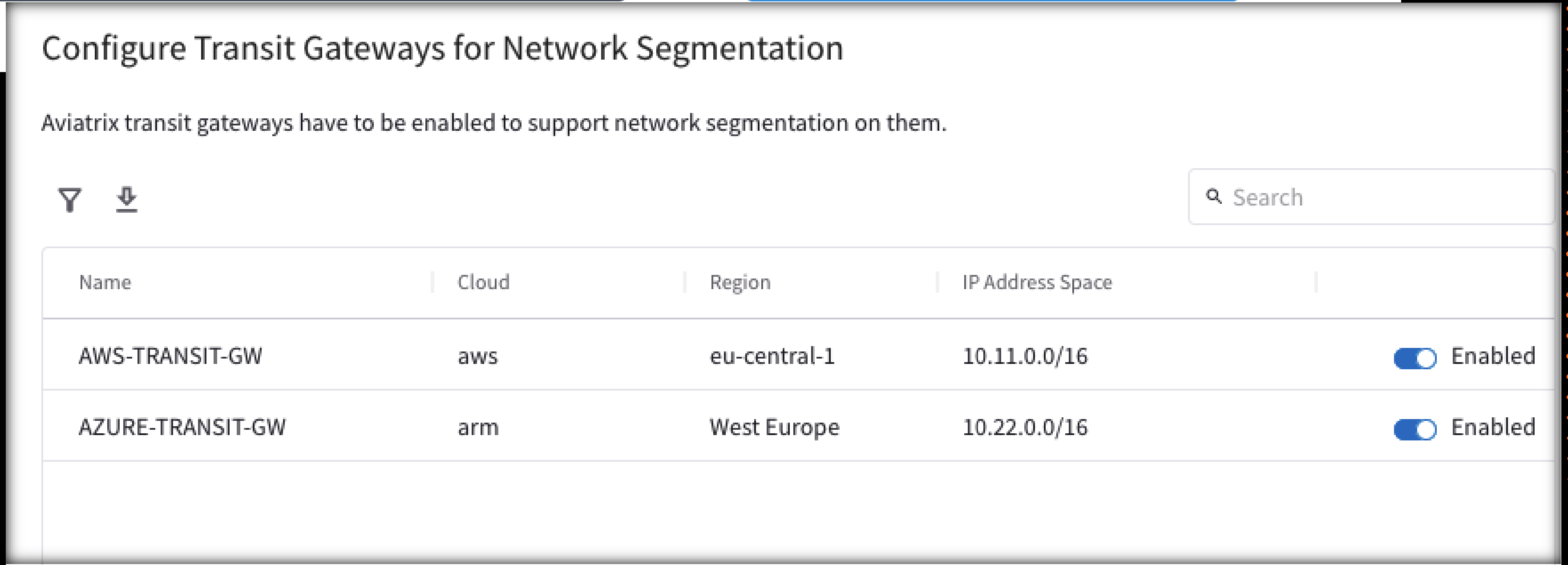
Route	Target
10.1.3.0/24	Local
10.1.1.0/24	Transit
10.1.2.0/24	Transit
10.2.1.0/24	Transit

Route	Target
10.1.1.0/24	PROD1
10.1.2.0/24	PROD2
10.1.3.0/24	TEST
10.2.1.0/24	Azure-Transit

Route	Target
10.2.1.0/24	Local
10.1.1.0/24	Transit
10.1.2.0/24	Transit
10.1.3.0/24	Transit

Route	Target
10.1.1.0/24	AWS-Transit
10.1.2.0/24	AWS-Transit
10.1.3.0/24	AWS-Transit
10.2.1.0/24	PROD3

Caveat: Select the Transit Gateways that will handle traffic for their associated members.



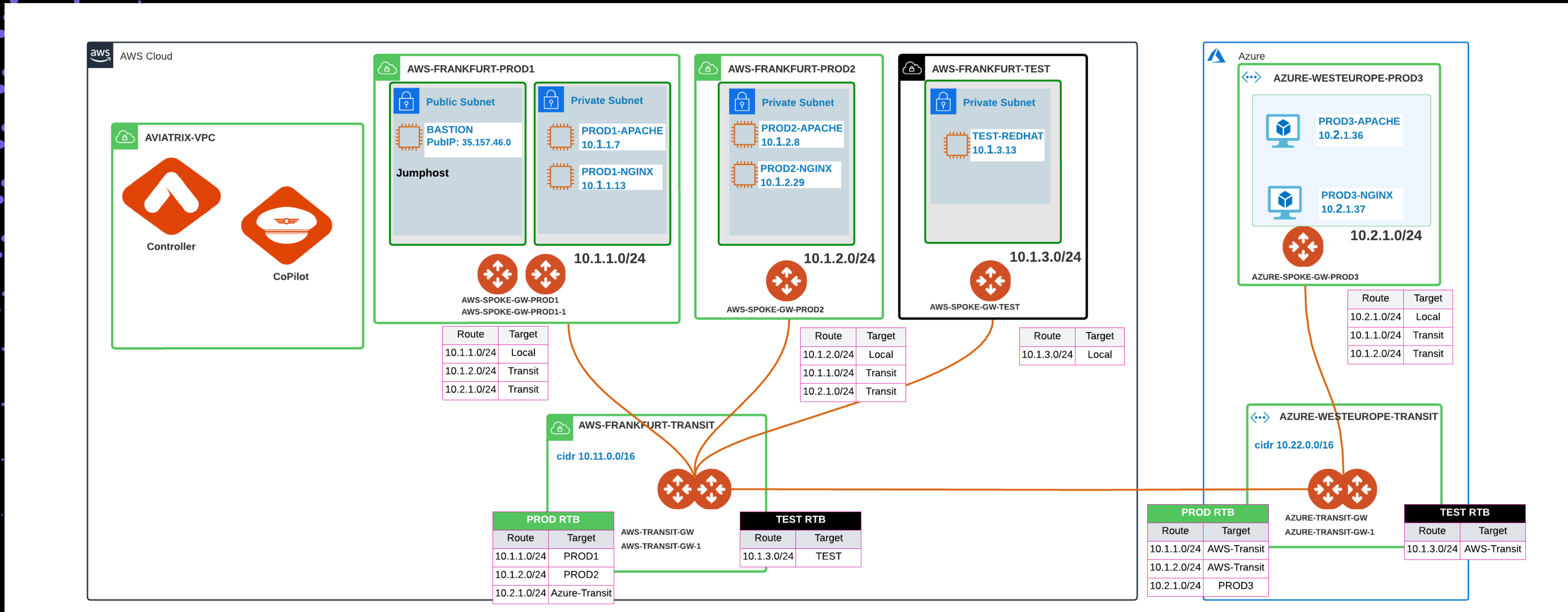
Configure Transit Gateways for Network Segmentation

Aviatrix transit gateways have to be enabled to support network segmentation on them.

Name	Cloud	Region	IP Address Space	
AWS-TRANSIT-GW	aws	eu-central-1	10.11.0.0/16	Enabled
AZURE-TRANSIT-GW	arm	West Europe	10.22.0.0/16	Enabled

AVIATRIX

Creation of Network Domains and VPCs Association



Route	Target
10.1.1.0/24	Local
10.1.2.0/24	Transit
10.2.1.0/24	Transit

Route	Target
10.1.2.0/24	Local
10.1.1.0/24	Transit
10.2.1.0/24	Transit

Route	Target
10.1.3.0/24	Local

Route	Target
10.2.1.0/24	Local
10.1.1.0/24	Transit
10.1.2.0/24	Transit

PROD RTB

Route	Target
10.1.1.0/24	PROD1
10.1.2.0/24	PROD2
10.2.1.0/24	Azure-Transit

TEST RTB

Route	Target
10.1.3.0/24	TEST

PROD RTB

Route	Target
10.1.1.0/24	AWS-Transit
10.1.2.0/24	AWS-Transit
10.2.1.0/24	PROD3

TEST RTB

Route	Target
10.1.3.0/24	AWS-Transit

Transit Gateway

- Multiple RTBs (per each Network Domain)
- Main RTB:
  - ➢ The main RTB will host the ***Transit Routes*** (i.e. the routes of the *backbone layer*) and the routes that belong to *Unmanaged Network Domains* (i.e. VPCs/Vnets not assigned to any Network Domains yet).

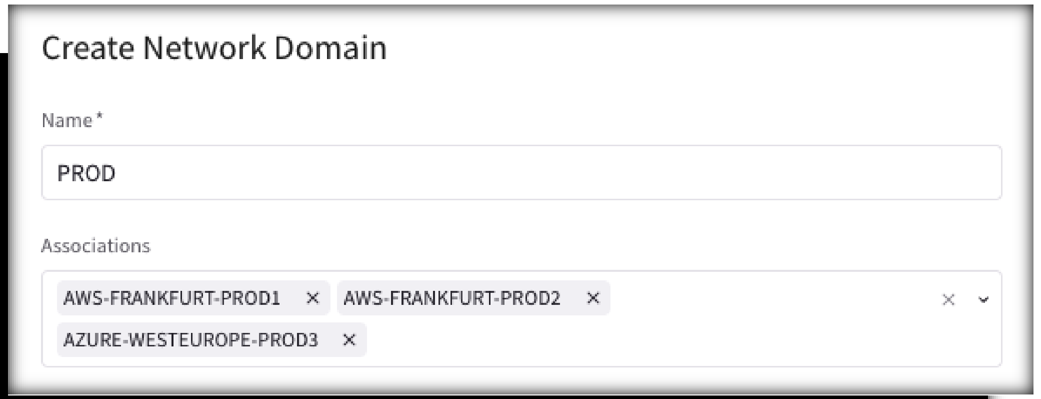
Spoke Gateway

- Single RTB (Main)

➢ Assign a Name to each Network Domain

➢ Associate the Spoke VPCs/Vnets and/or Site2Cloud Connections to the Network Domain

CAVEAT: You can create maximum **200** Network Domains per each Transit Gateway



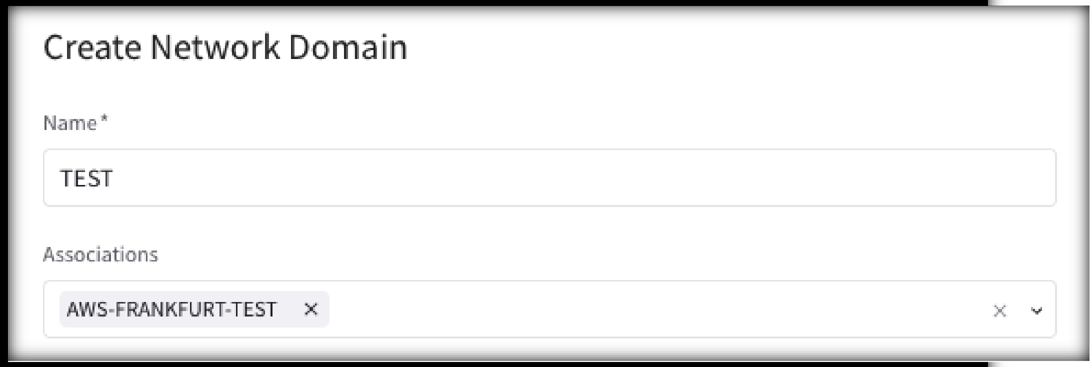
Create Network Domain

Name *

PROD

Associations

AWS-FRANKFURT-PROD1 × AWS-FRANKFURT-PROD2 × AZURE-WESTEUROPE-PROD3 ×



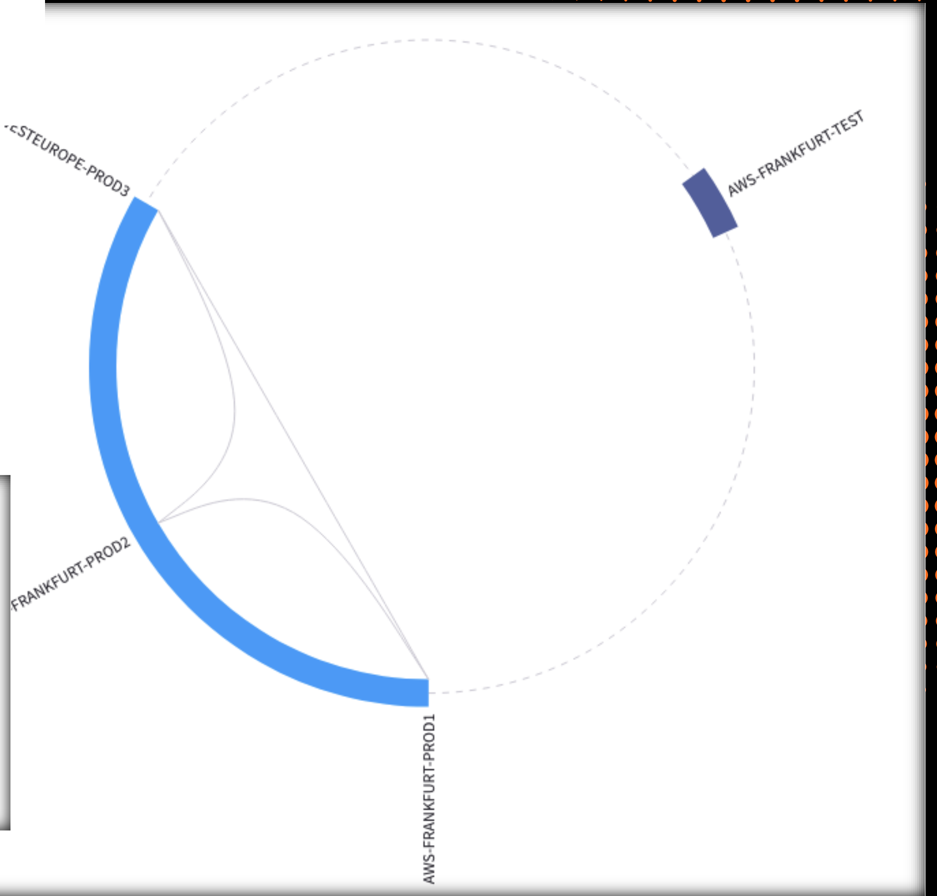
Create Network Domain

Name *

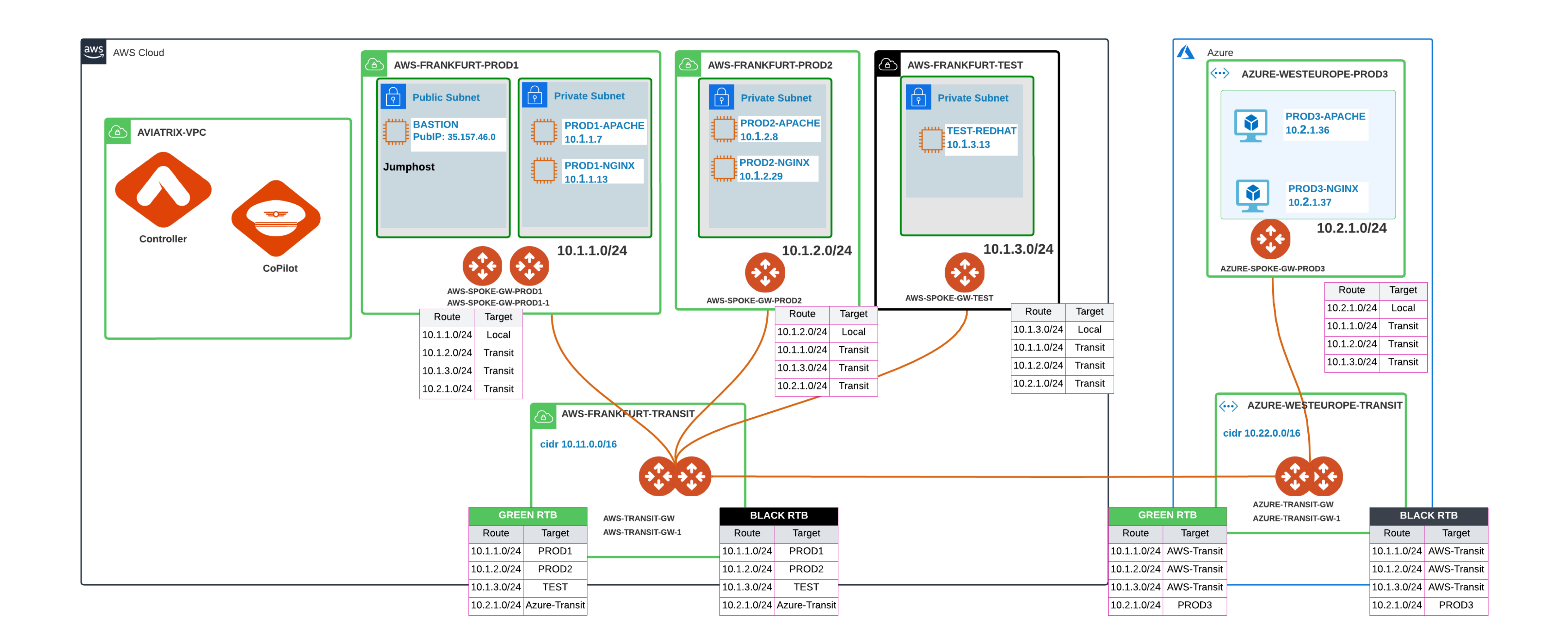
TEST

Associations

AWS-FRANKFURT-TEST ×



Connection Policy



Route	Target
10.1.1.0/24	Local
10.1.2.0/24	Transit
10.1.3.0/24	Transit
10.2.1.0/24	Transit

Route	Target
10.1.2.0/24	Local
10.1.1.0/24	Transit
10.1.3.0/24	Transit
10.2.1.0/24	Transit

Route	Target
10.1.3.0/24	Local
10.1.1.0/24	Transit
10.1.2.0/24	Transit
10.2.1.0/24	Transit

Route	Target
10.2.1.0/24	Local
10.1.1.0/24	Transit
10.1.2.0/24	Transit
10.1.3.0/24	Transit

GREEN RTB

Route	Target
10.1.1.0/24	PROD1
10.1.2.0/24	PROD2
10.1.3.0/24	TEST
10.2.1.0/24	Azure-Transit

BLACK RTB

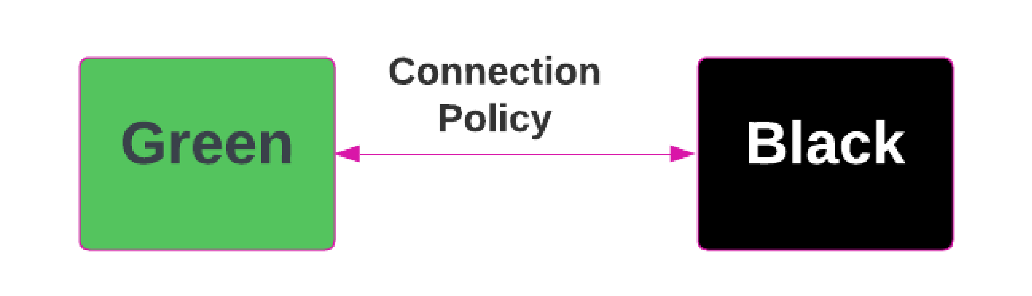
Route	Target
10.1.1.0/24	PROD1
10.1.2.0/24	PROD2
10.1.3.0/24	TEST
10.2.1.0/24	Azure-Transit

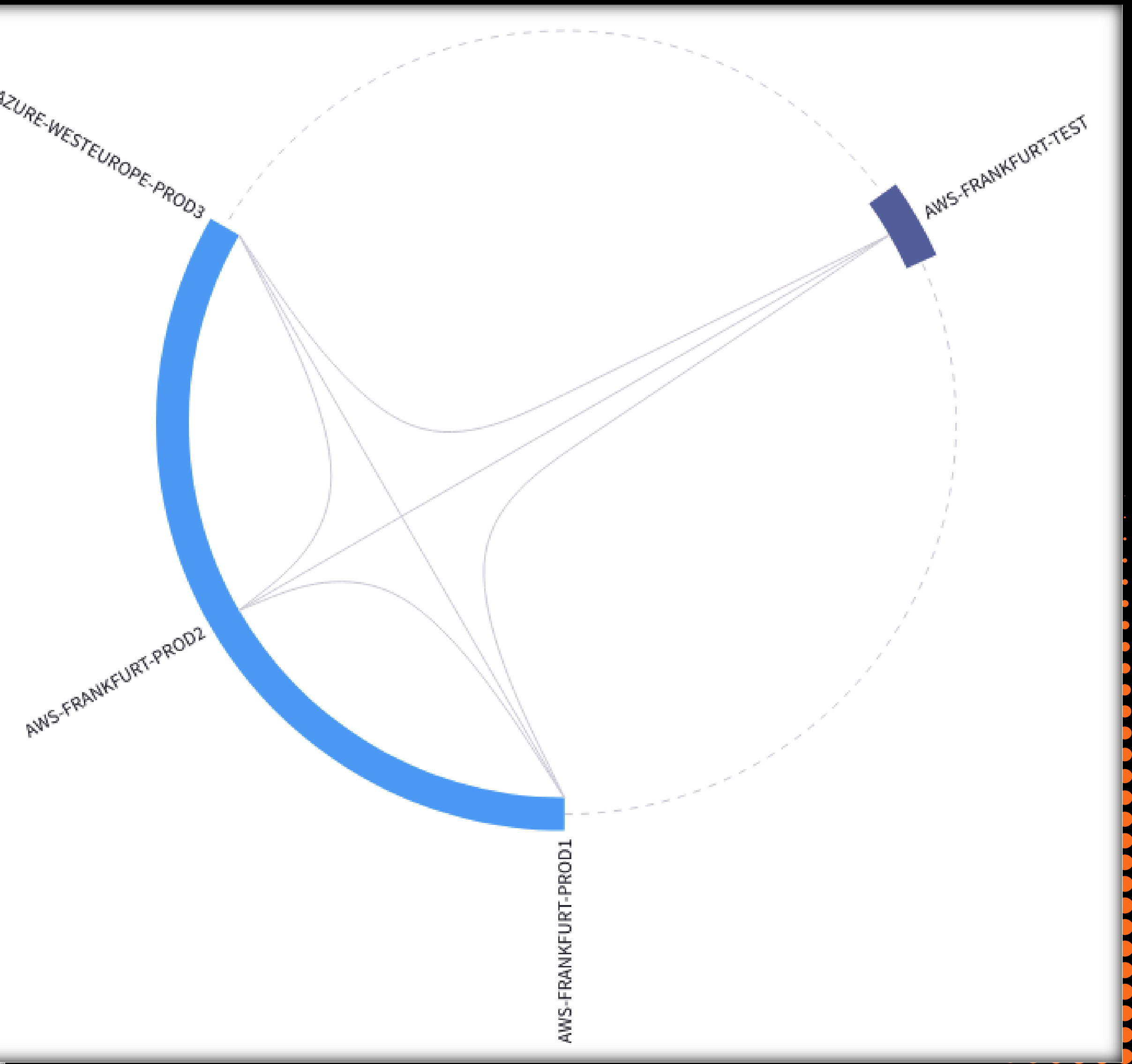
GREEN RTB

Route	Target
10.1.1.0/24	AWS-Transit
10.1.2.0/24	AWS-Transit
10.1.3.0/24	AWS-Transit
10.2.1.0/24	PROD3

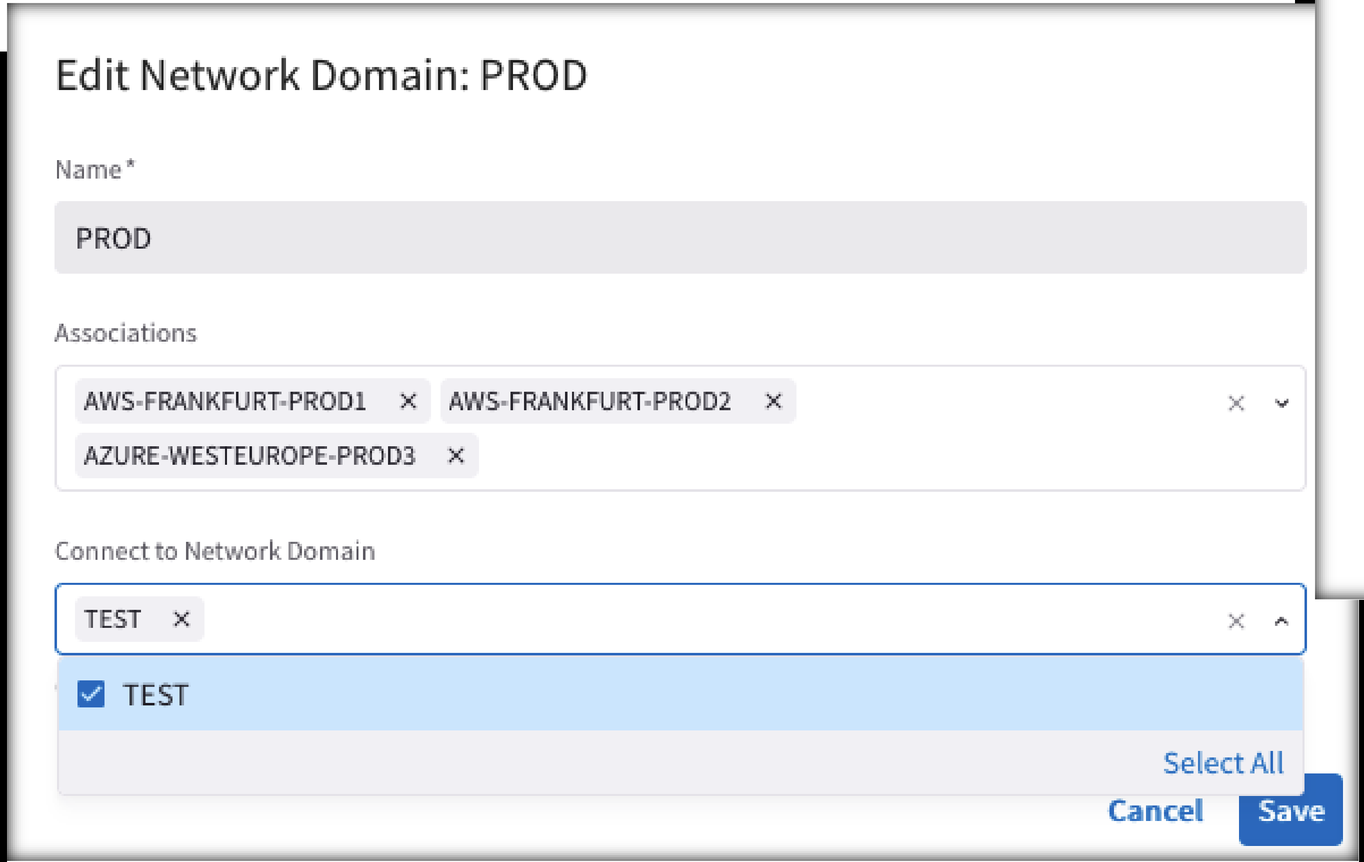
BLACK RTB

Route	Target
10.1.1.0/24	AWS-Transit
10.1.2.0/24	AWS-Transit
10.1.3.0/24	AWS-Transit
10.2.1.0/24	PROD3





- **Optionally enable the Connection Policy**: the different routing tables will be merged (i.e., *VRF Lite Route Leaking*).



Edit Network Domain: PROD

Name*

PROD

Associations

AWS-FRANKFURT-PROD1 ✕ AWS-FRANKFURT-PROD2 ✕ AZURE-WESTEUROPE-PROD3 ✕

Connect to Network Domain

TEST ✕

☑ TEST

AVIATRIX

Next: Lab 3 - Network Segmentation