Network Segmentation

ACE Team
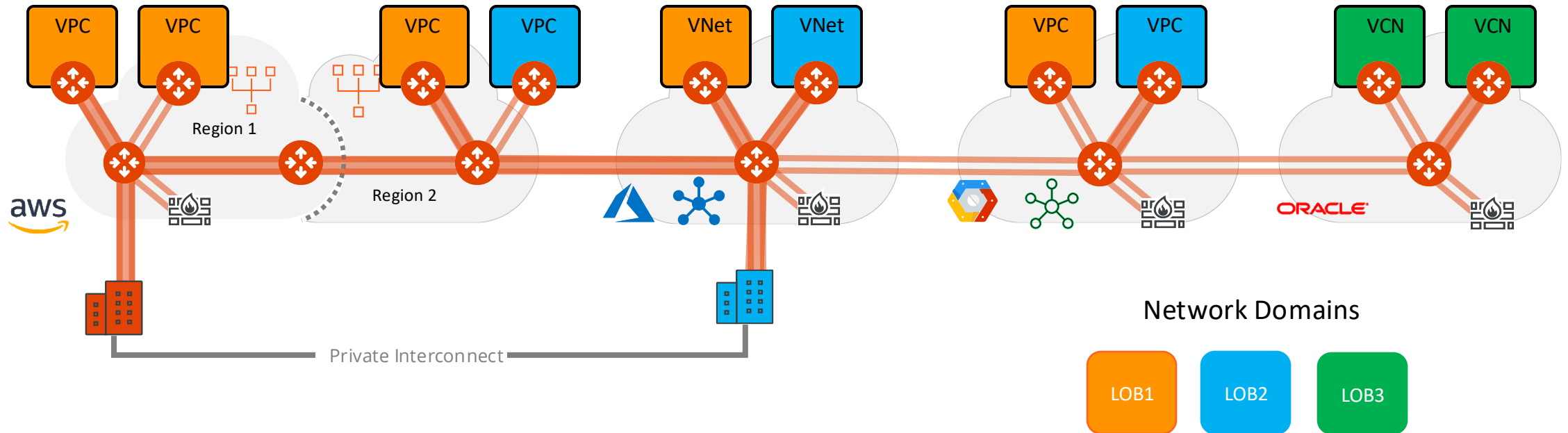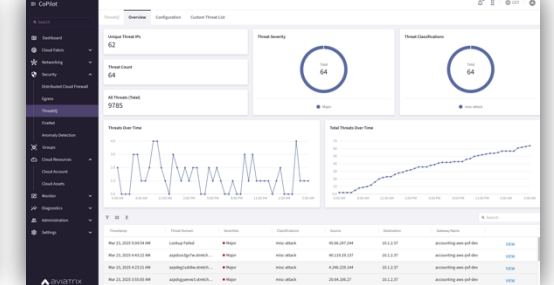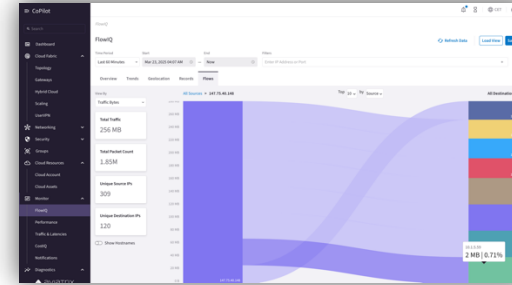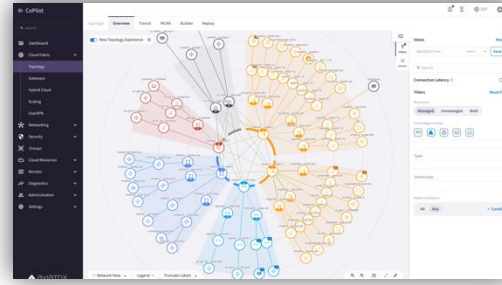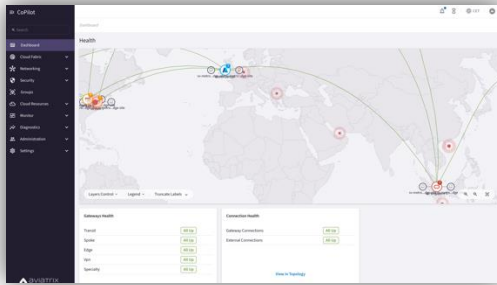
Segmentation

- **Main Purpose:** Enables ZTNA across multi-region and multicloud, including on-premises environment
- Group VNets/VPCs/VCNs/Apps with similar security policies
- Define your own domains
- Use Cases
  - Compliance
  - Governance
  - Audits
- The Network Segmentation is also called **Macro-Segmentation**
  - A Network Domain can encompass one or multiple VPCs as a unique logical container (i.e. **Routing Domain**)

Multicloud Network Segmentation

Multicloud Network Segmentation

Policy Based Network Segmentation

- Global
- Consistent / Repeatable
- Across accounts, subscriptions & projects
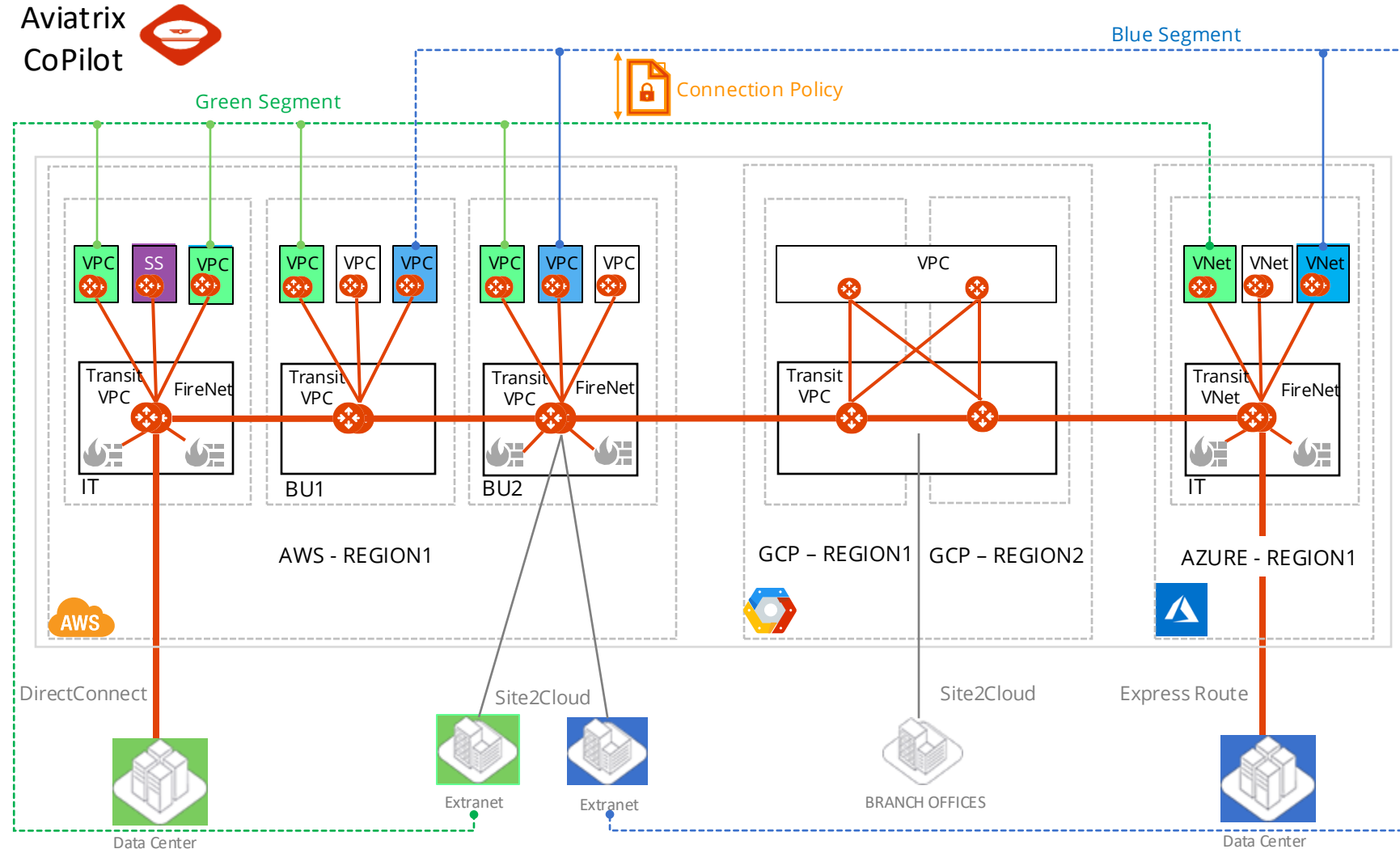
Cloud and Connection Agnostic

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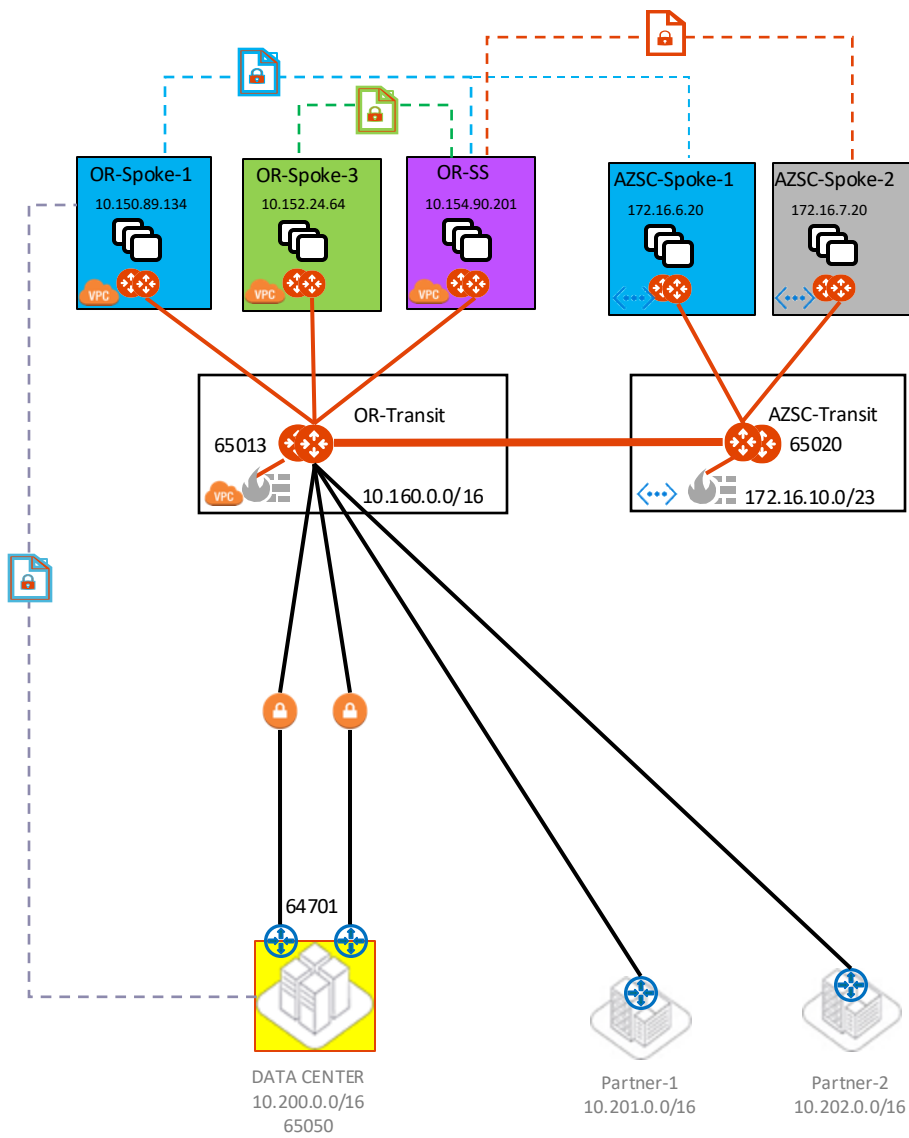- Multiple clouds

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
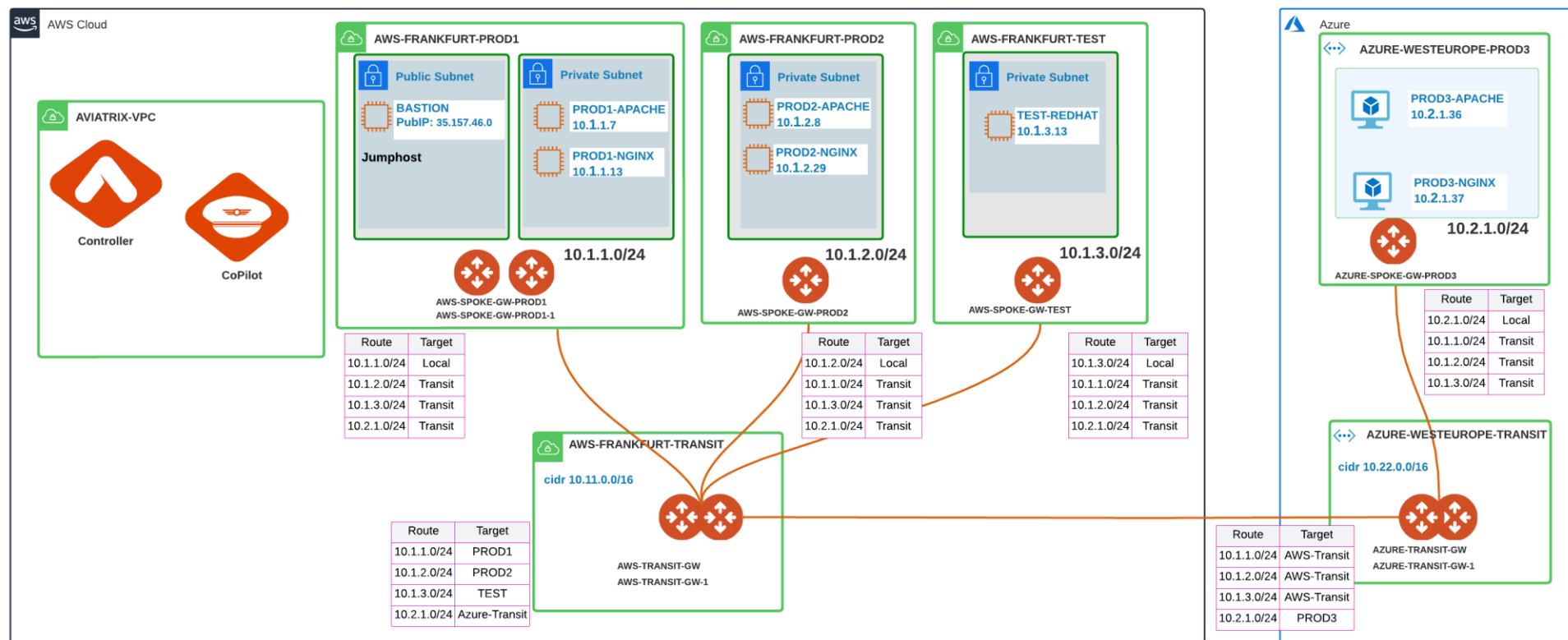- Flexible
- Automated

Multicloud 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

1. Enable Transit Gateways for Network Segmentation

Enable the Network Segmentation:

- Choose the Transit Gateway(s) that will route traffic for its members.
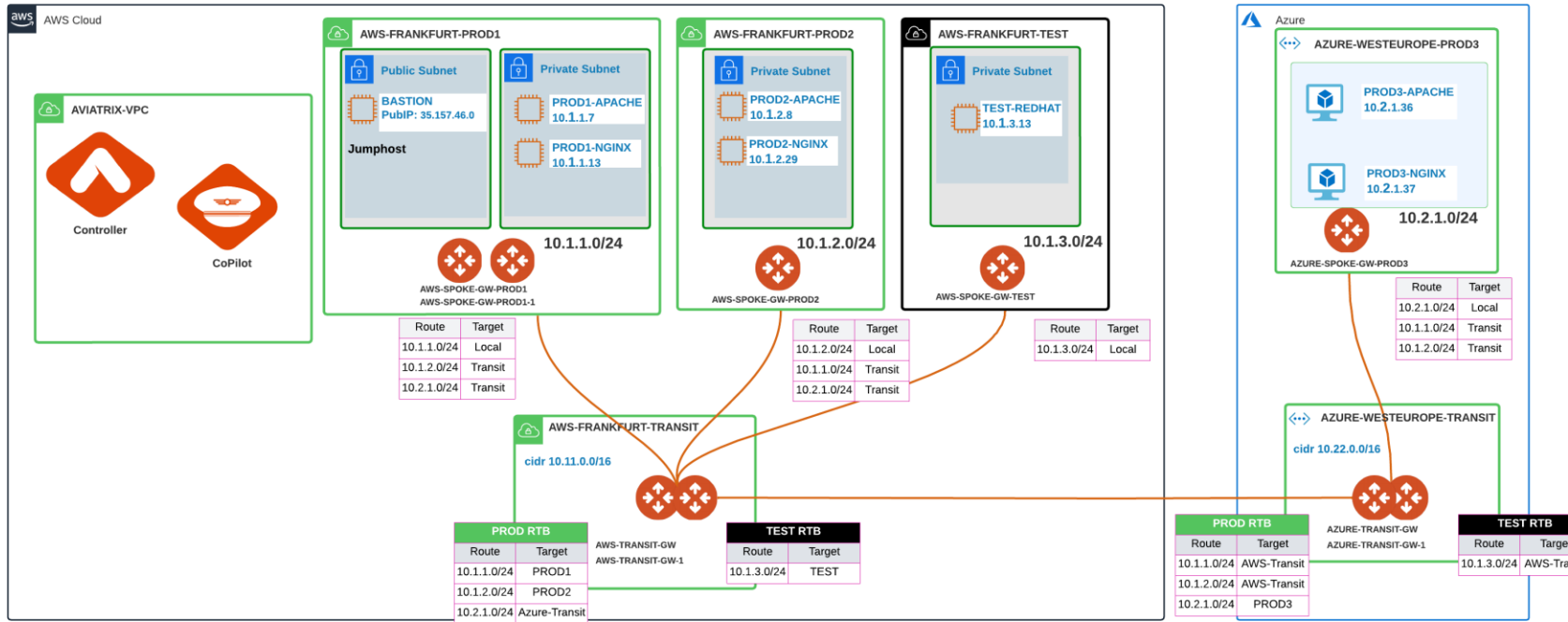
Configure Transit Gateways for Network Segmentation

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

2. Create and Associate a Network Domain

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)

Create the Network Domains:
- 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
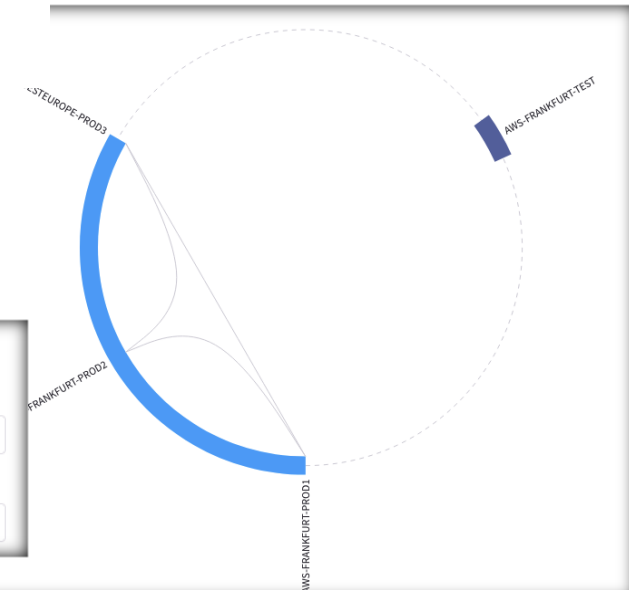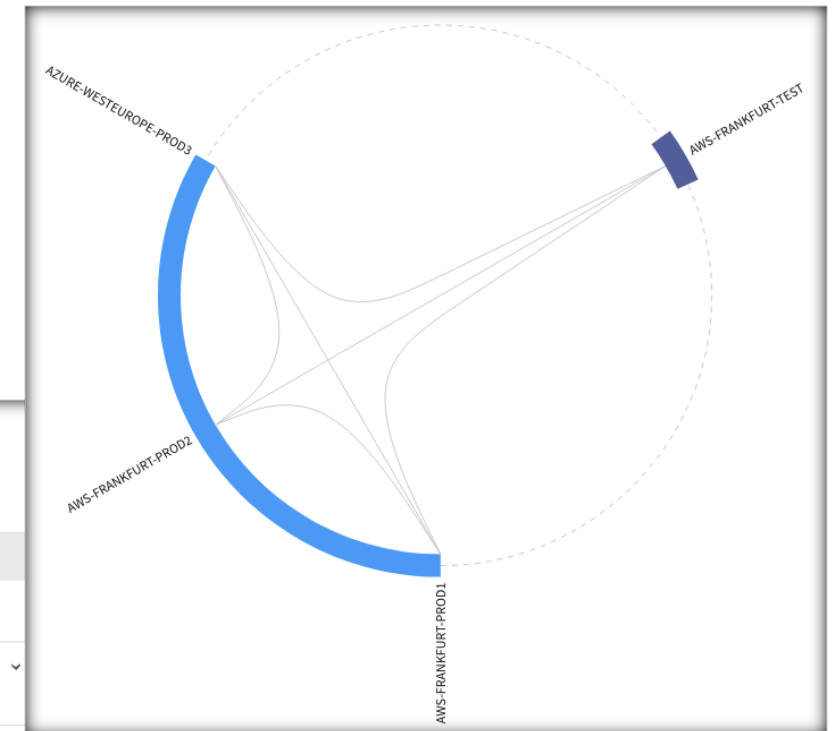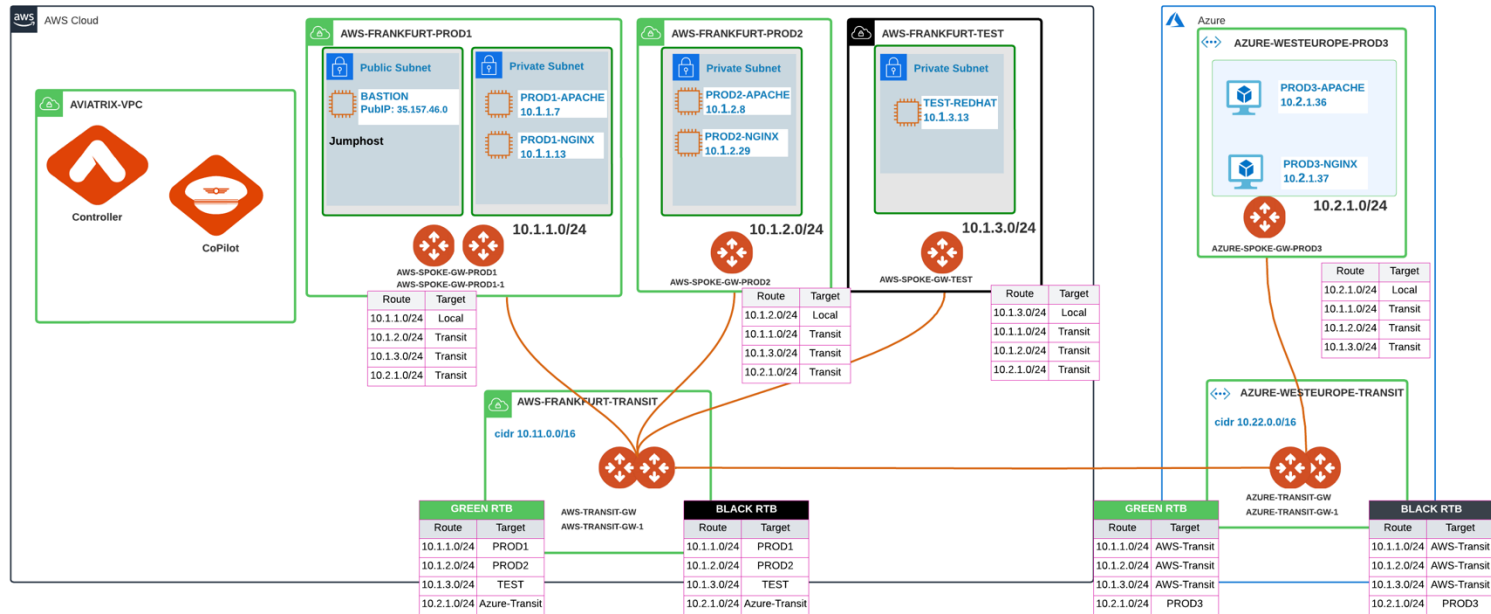
3. Apply the Connection Policy (optional)

Optionally, enable the Connection Policy:
• Network Domains' routing tables are merged (i.e. *vrf leaking*).

Next: Lab 3 - Network Segmentation