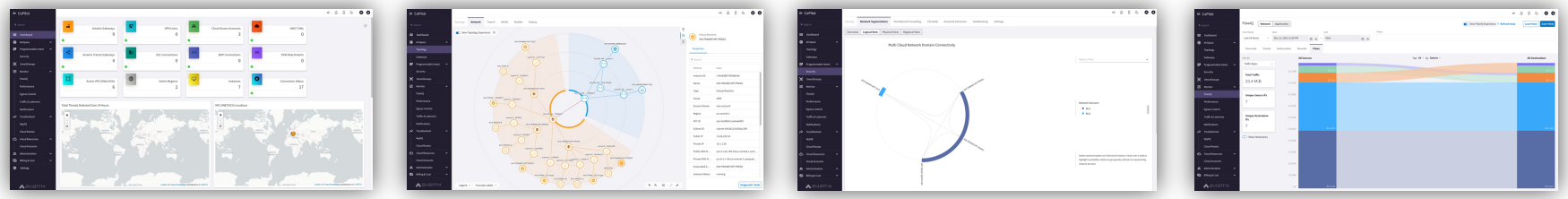
Network Segmentation

Segmentation

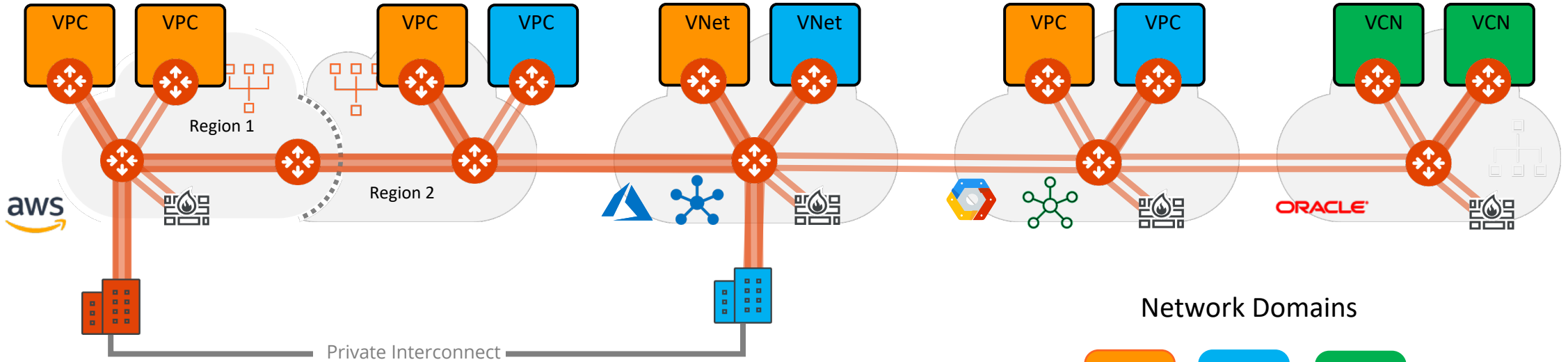
- Enables ZTNA across multi-region and multicloud, including on-premises environment
- Group VNets/VPCs/VCNs/Apps with similar security policies
- Define your own domains
- Use Cases
  - Compliance
  - Governance
  - Audits

Cloud and Multicloud Network Segmentation

Aviatrix CoPilot



Network Granularity and Control



Network Domains

LOB1 LOB2 LOB3

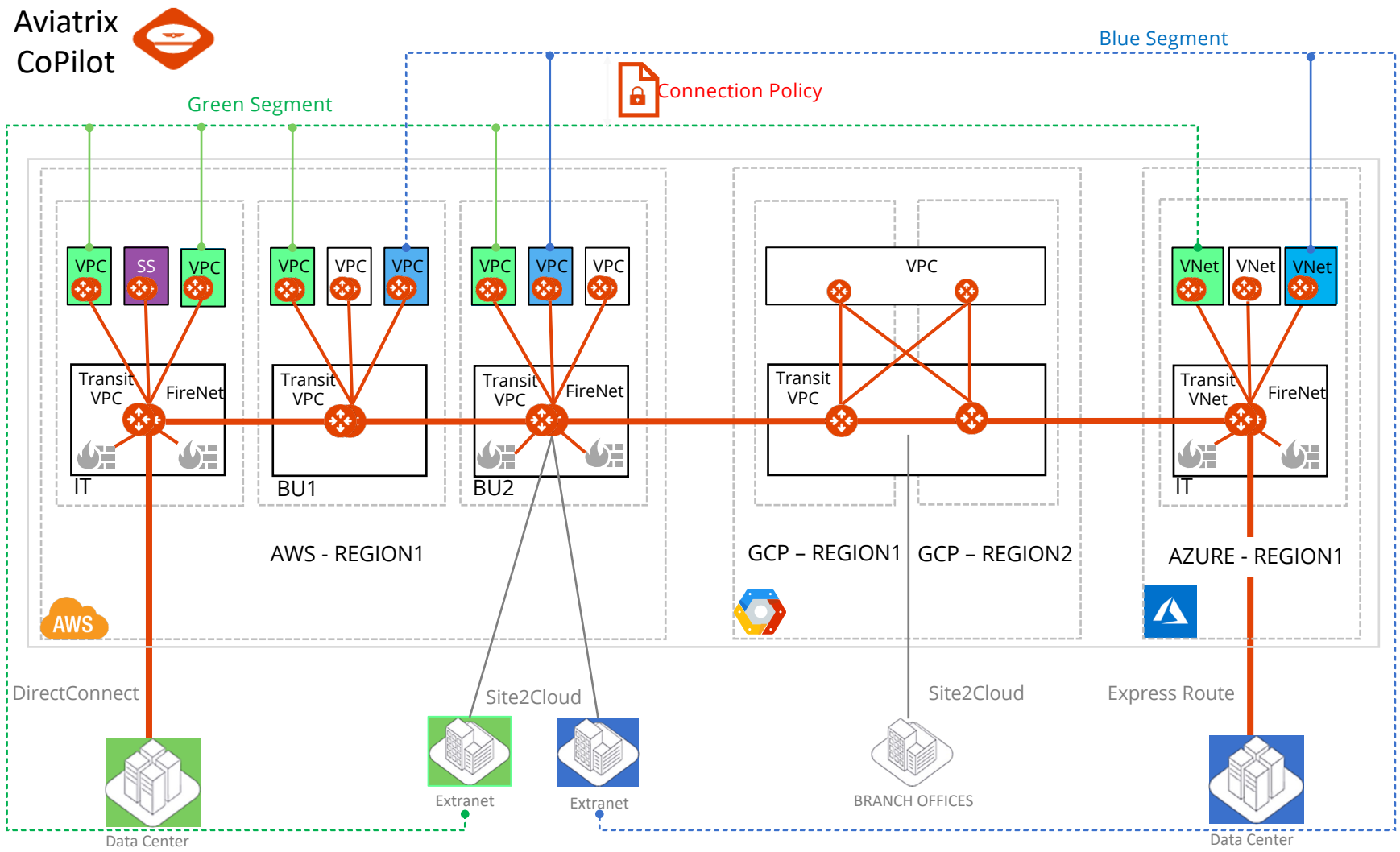
Cloud and Multicloud Network Segmentation

Policy Based Network Segmentation
- Global
- Consistent / Repeatable
- Across accounts, subscriptions & projects

Cloud and Connection Agnostic
- Single cloud
- Intra-region or inter-region
- Multiple clouds

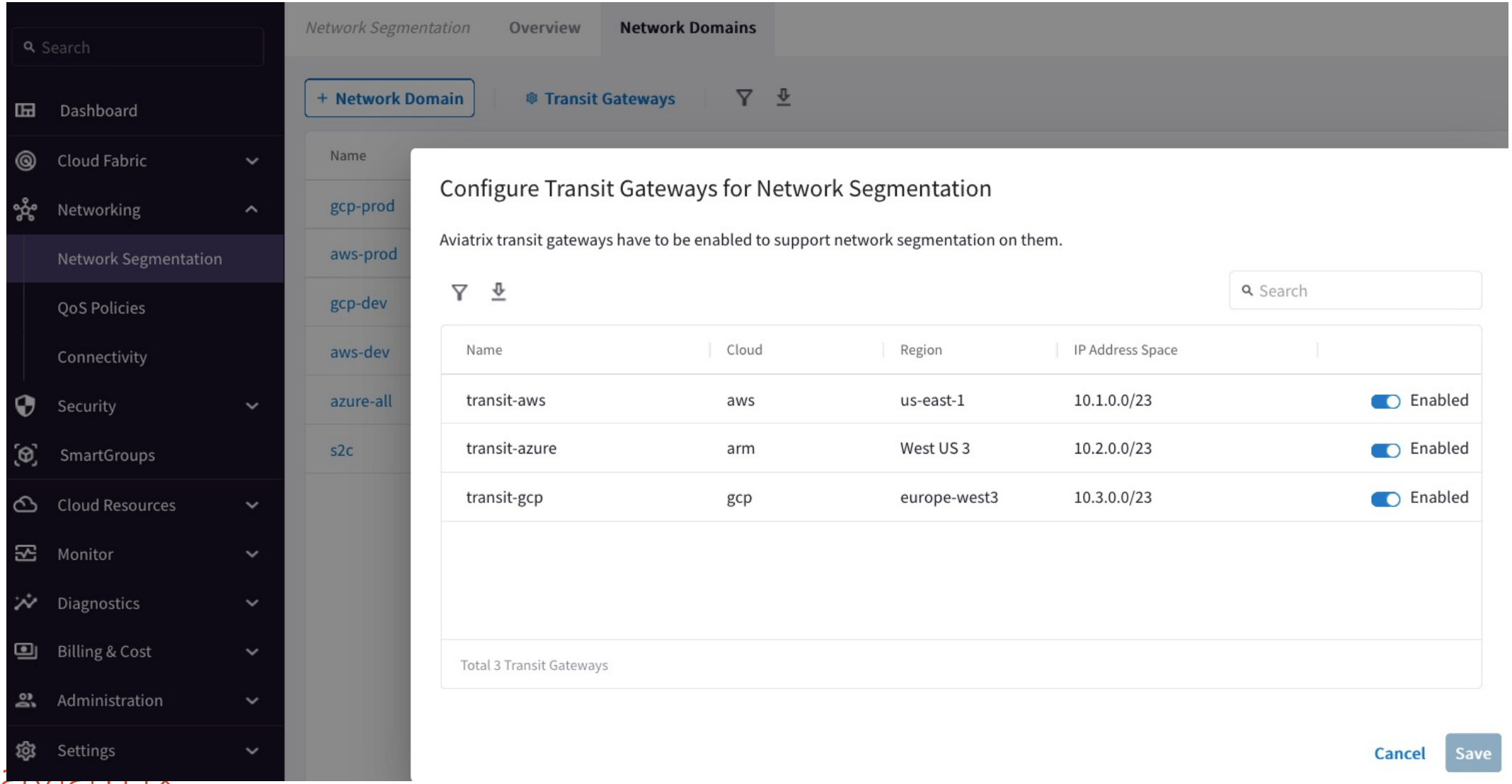
Edge/Access Segmentation
- On-Prem DCs
- Branches
- Extranets
- Cloud Peering

On-Demand Compliance/Governance
- Security Posture within minutes
- Aviatrix control plane realizes the intent
- Zero-Trust
- Flexible
- Automated



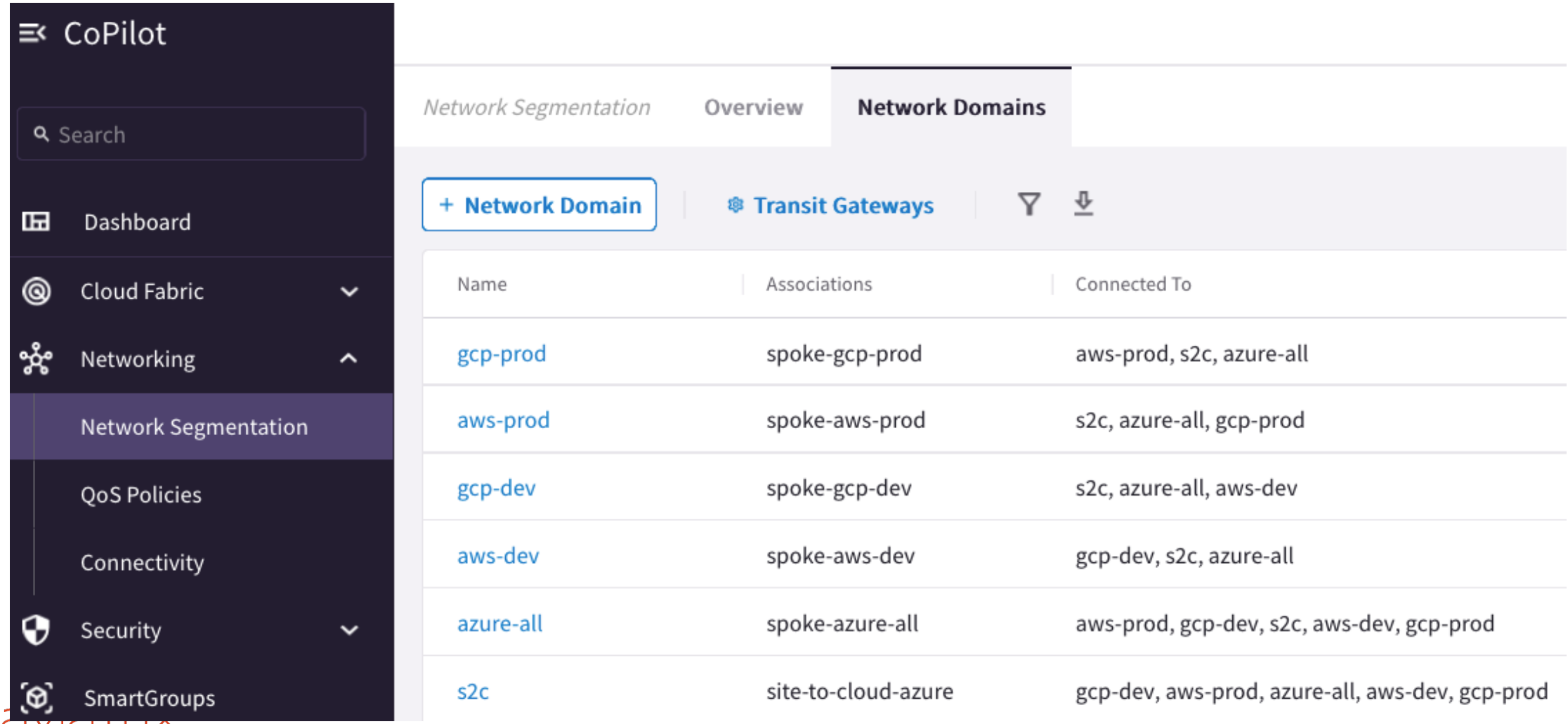
Network Segmentation

1- Enable Transit Gateway for Segmentation

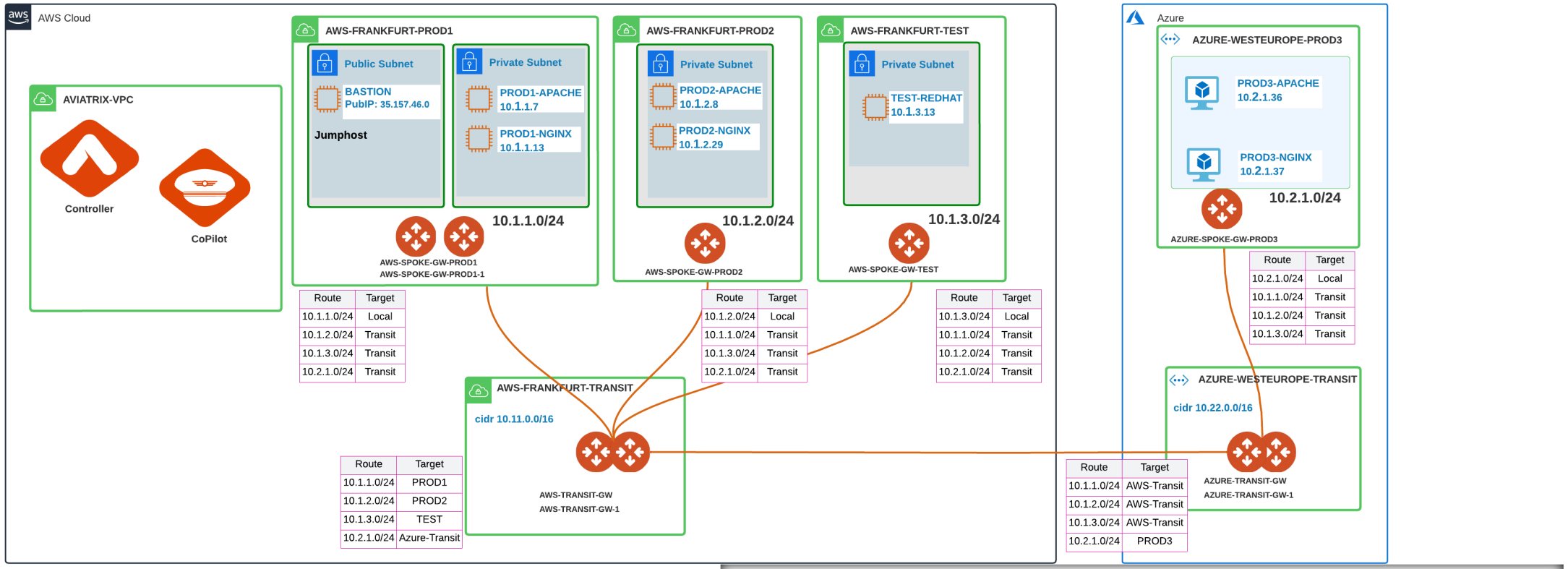


Network Segmentation

2- Create Network Domain (aka Network Segments – think of them as VRFs)
3- Create the association between Network Domains (aka Network Segments)

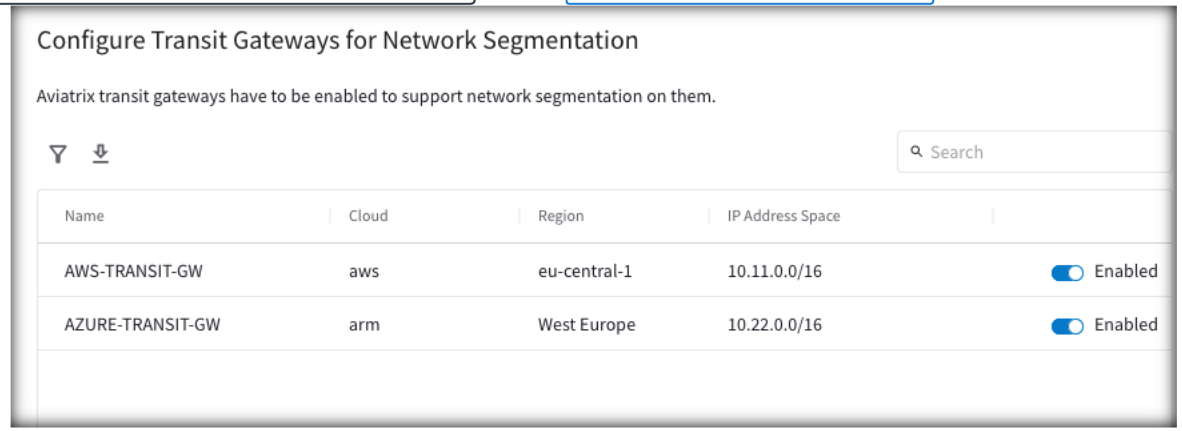


1. Enabling a Transit Gateway for Network Segmentation

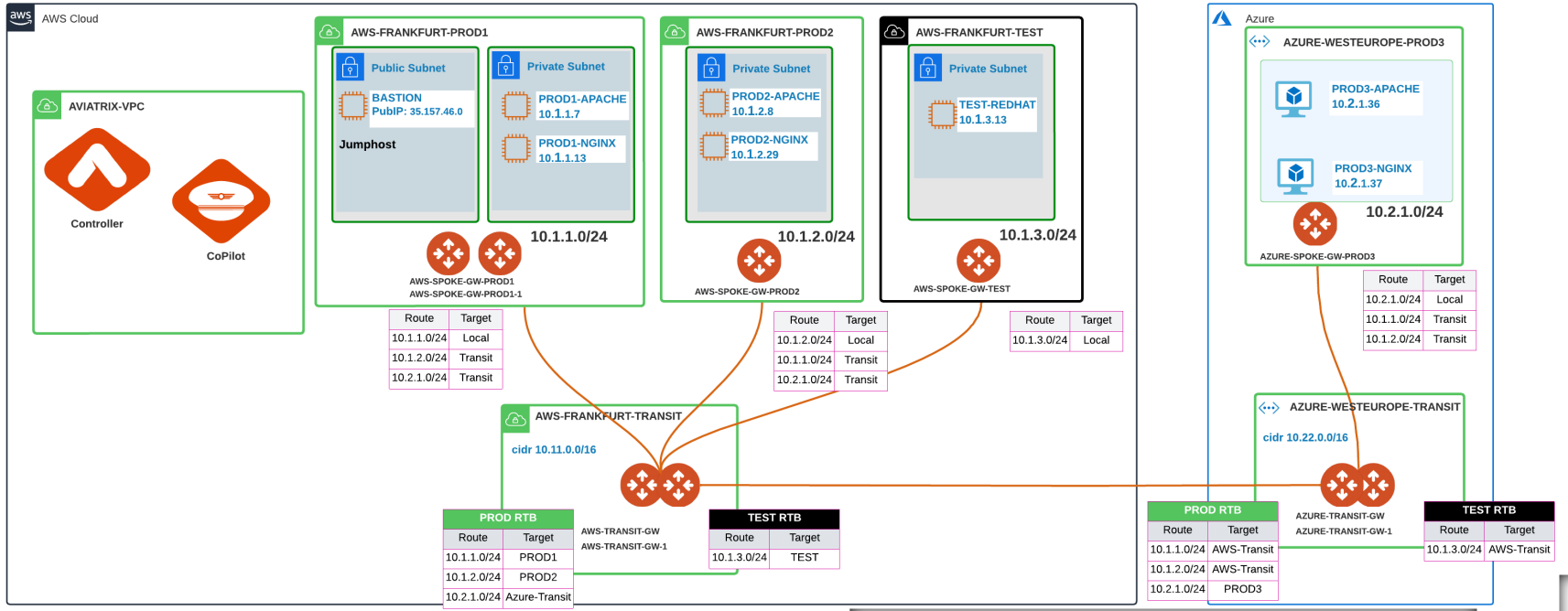


Enable the Network Segmentation:

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



2. Creating, Connecting, and Associating a Network Domain



Create the Network Domains:

- Assign a Name to each Network Domain
- Associate the Spoke VPCs/Vnets and/or Site2Cloud Connections to the Network Domain

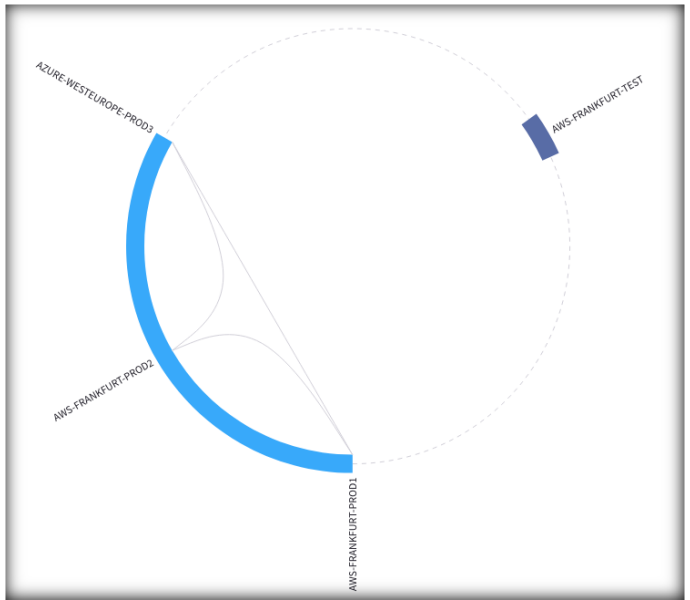
CAVEAT: A network-domain name can only have letters, digits, a hyphen (-), and an underscore (_). The name must start with a letter and must have 2-27 characters. For example, **Dev_Domain**.

Transit Gateway

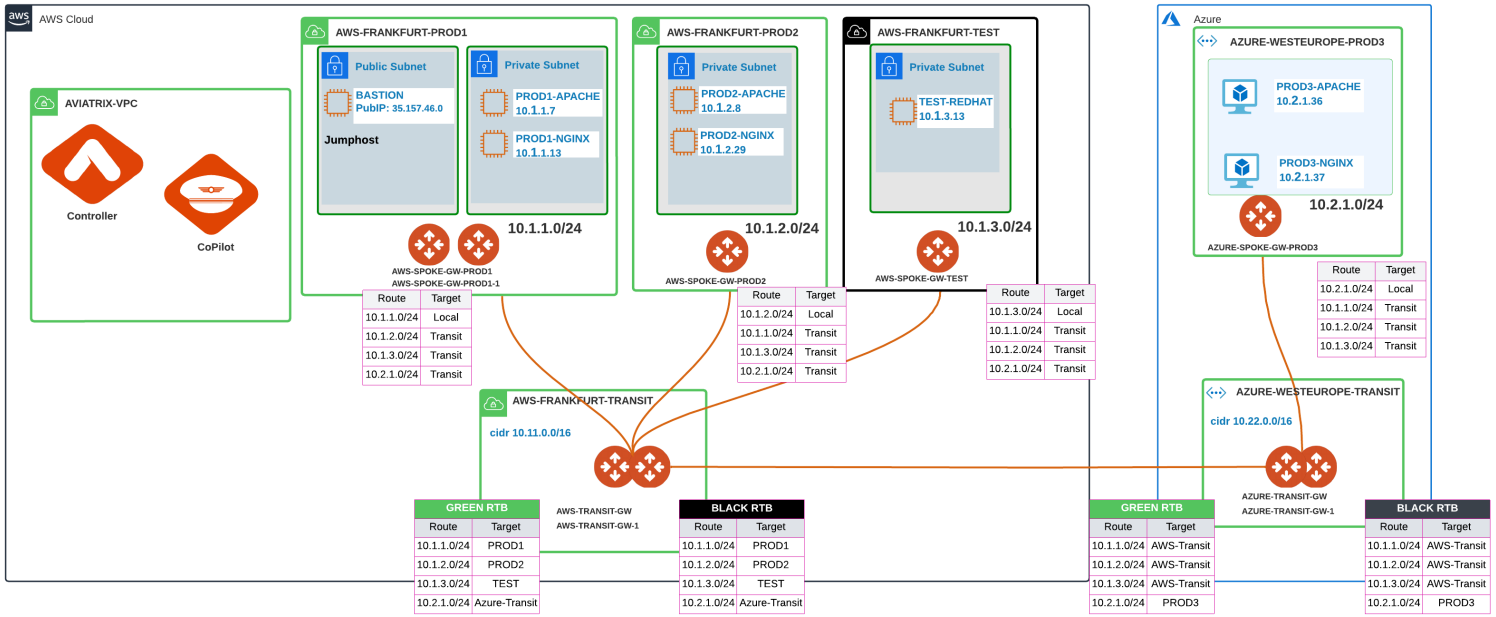
- Multiple RTBs (per each Network Domain)
- Main RTB:
  - ➢ The main RTB will host the Transit Routes (i.e. the routes of the *backbone layer*) and the routes that belong to *Unmanaged Network Domains* (i.e. VPCs/Vnets not assigned to any Network Domains).

Spoke Gateway

- Single RTB (Main)



3. Apply the 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	GREEN RTB 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

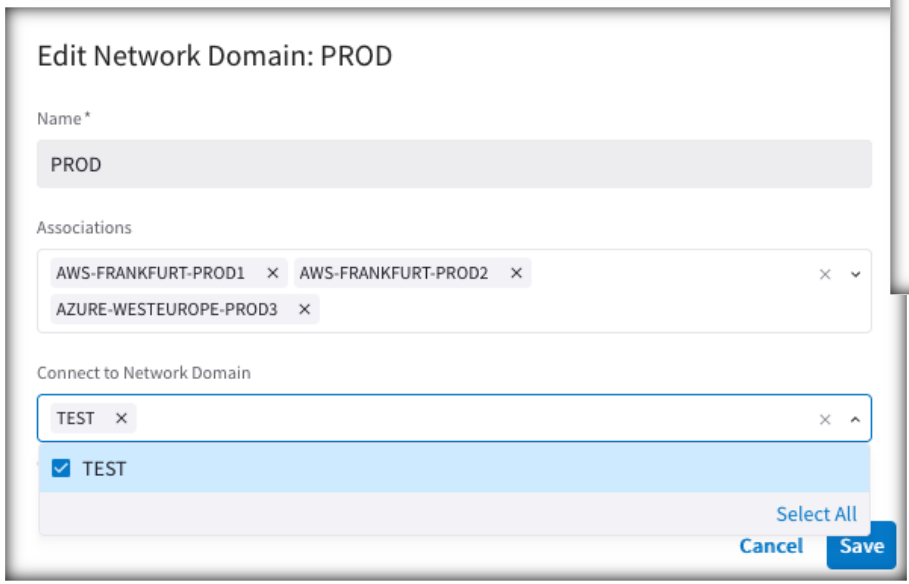
BLACK RTB Route	BLACK RTB Target
10.1.1.0/24	PROD1
10.1.2.0/24	PROD2
10.1.3.0/24	TEST
10.2.1.0/24	Azure-Transit

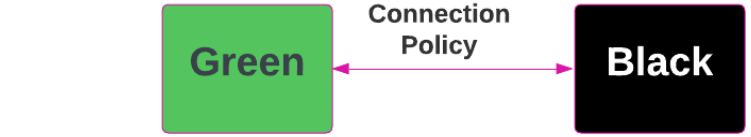
GREEN RTB Route	GREEN RTB Target
10.1.1.0/24	AWS-Transit
10.1.2.0/24	AWS-Transit
10.1.3.0/24	AWS-Transit
10.2.1.0/24	PROD3

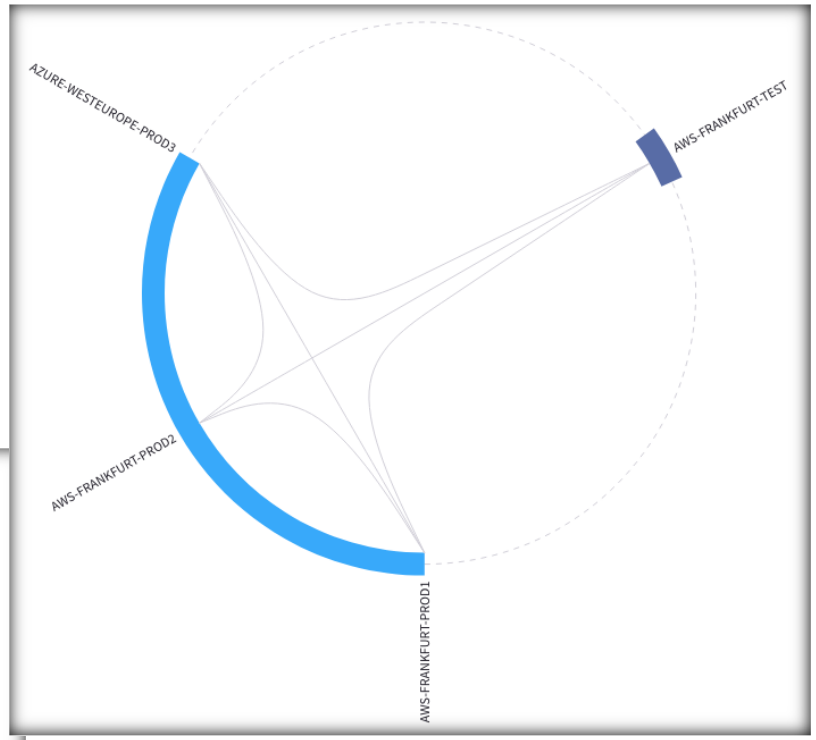
BLACK RTB Route	BLACK RTB Target
10.1.1.0/24	AWS-Transit
10.1.2.0/24	AWS-Transit
10.1.3.0/24	AWS-Transit
10.2.1.0/24	PROD3

Optionally, enable the Connection Policy:

- Network Domains' routing tables are merged (i.e. *vrf leaking*).







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

COMMUNITY
https://community.aviatrix.com