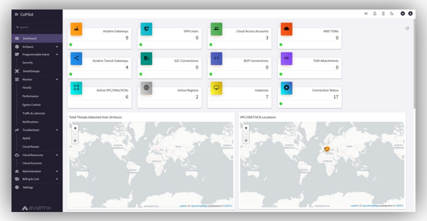
Network Segmentation

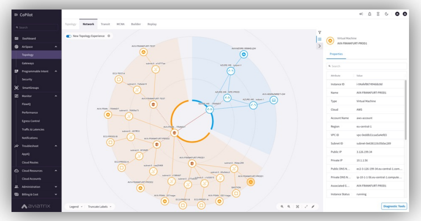
Segmentation

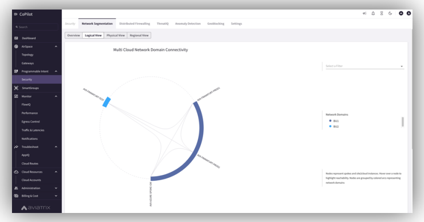
- Enables ZTNA across multi-region and multicloud, including on-premises environment
- Group VNets/VPCs/VCNs/Apps with similar security policies
- Define your own domains
- Use Cases
  - Compliance
  - Governance
  - Audits

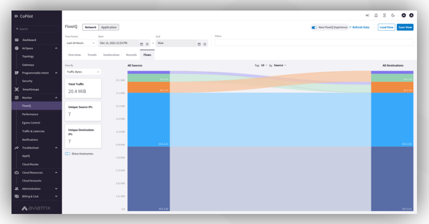
Cloud and Multicloud Network Segmentation

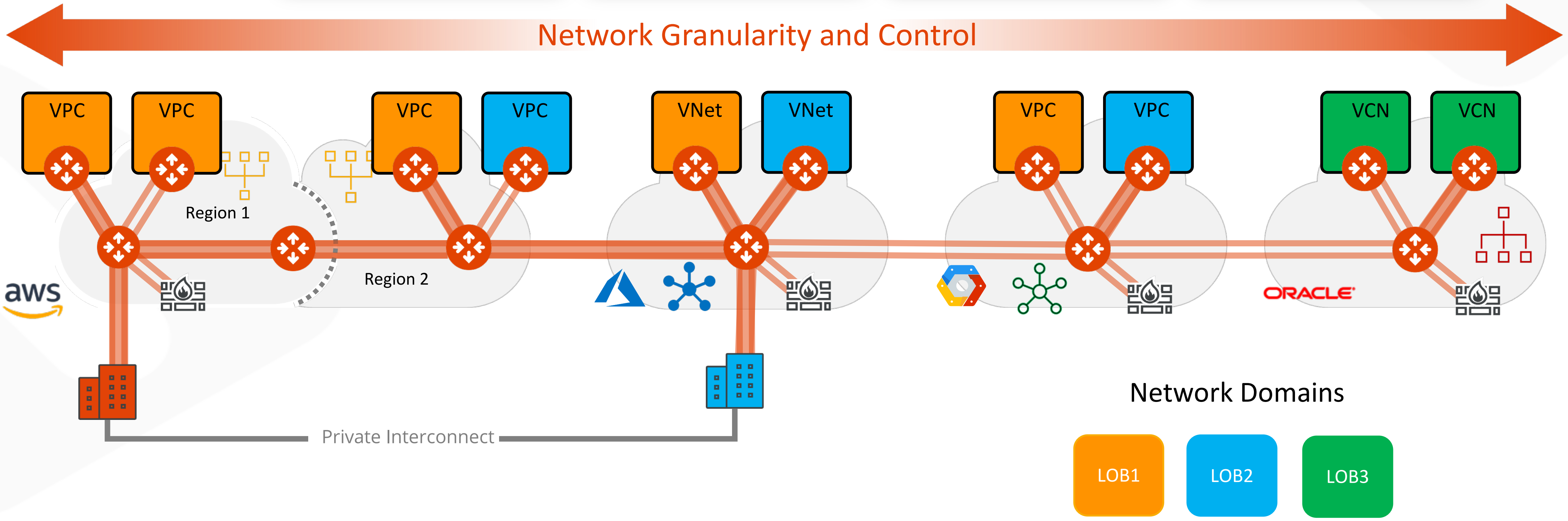
Aviatrix
CoPilot











Network Granularity and Control

VPC

VPC

Region 1

VPC

VPC

Region 2

VNet

VNet

VPC

VPC

VCN

VCN

aws

ORACLE

Private Interconnect

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

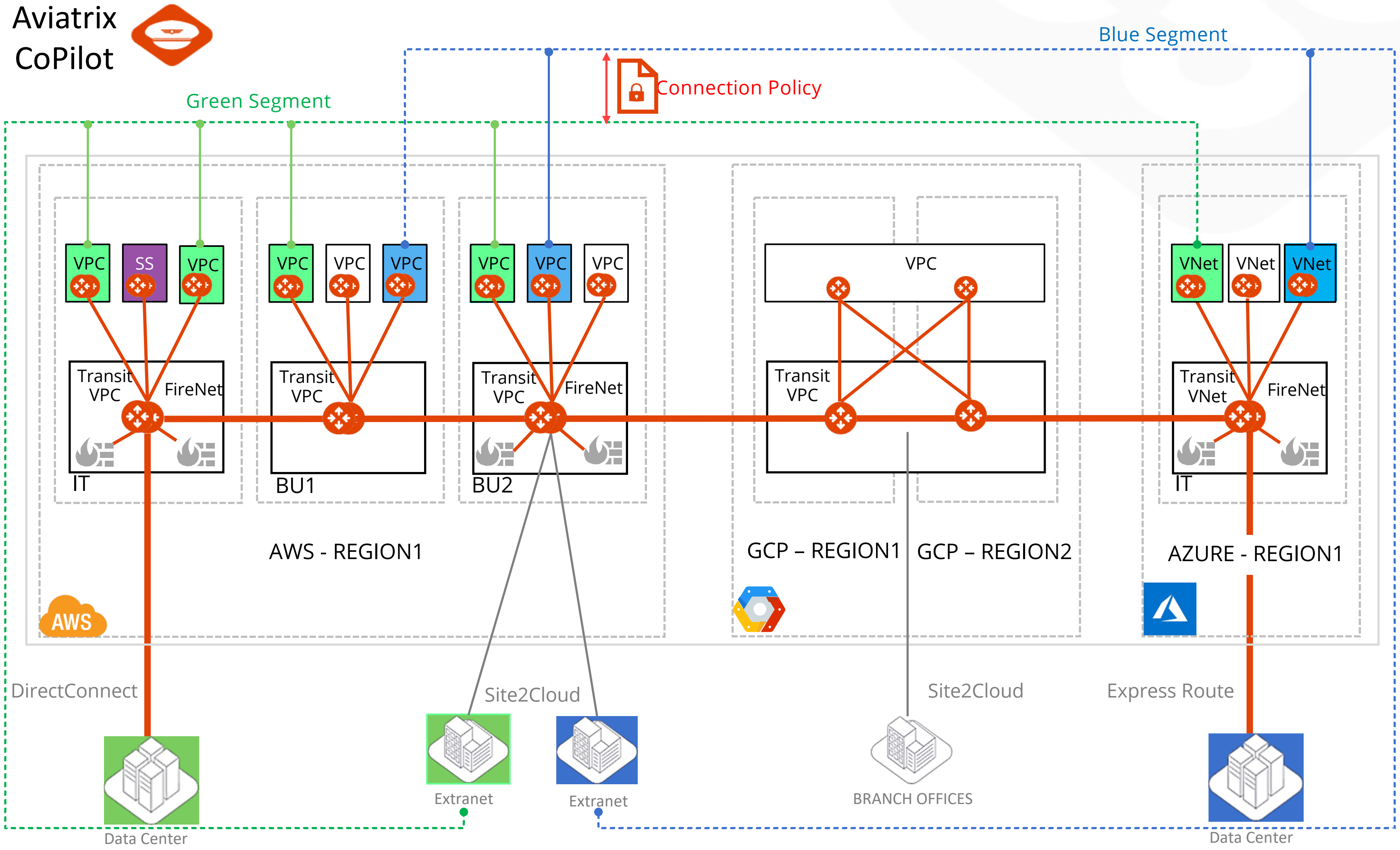
- Single cloud
- Intra-region or inter-region
- Multiple clouds

Edge/Access Segmentation

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

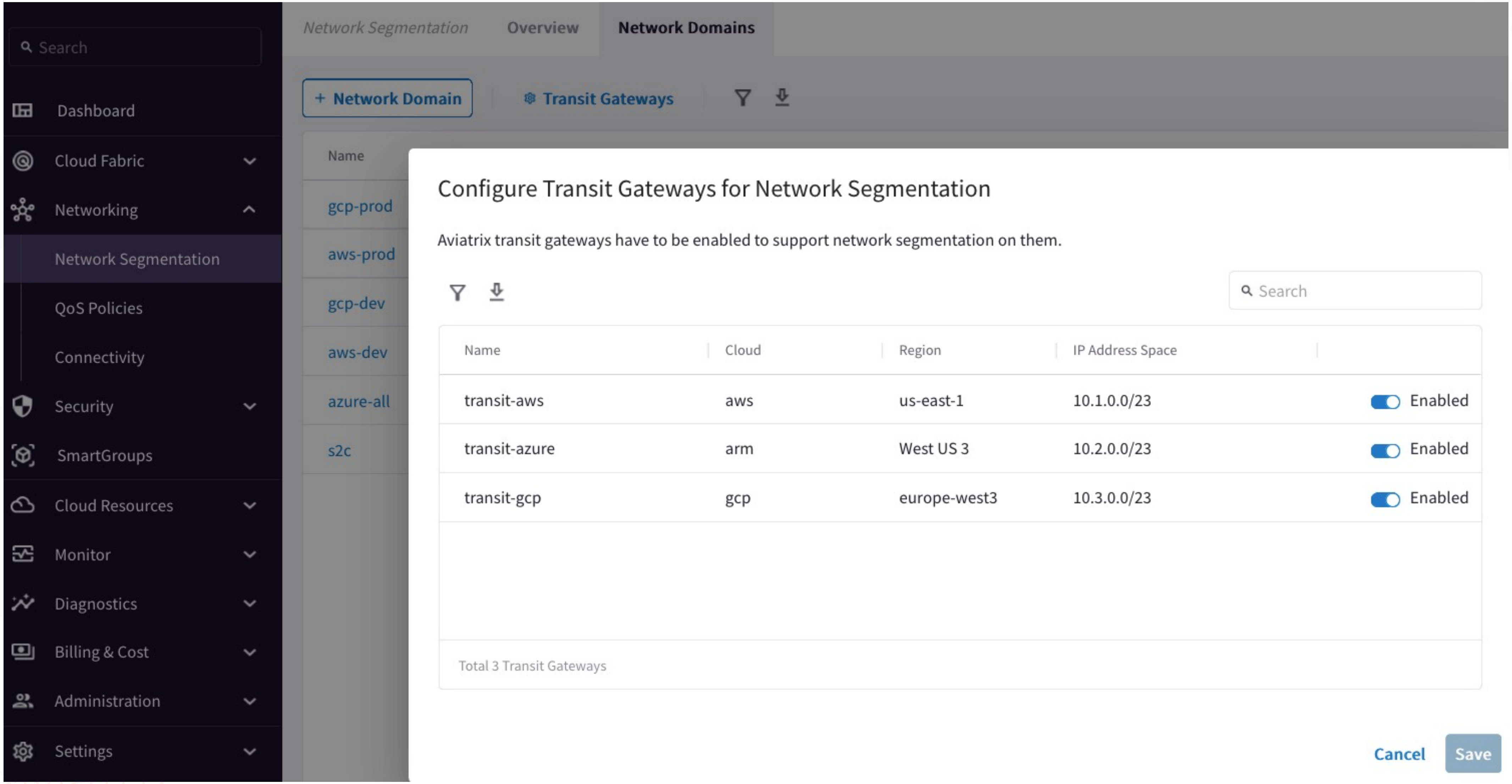
On-Demand Compliance/Governance

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



Network Segmentation

1- Enable Transit Gateway for Segmentation



Configure Transit Gateways for Network Segmentation

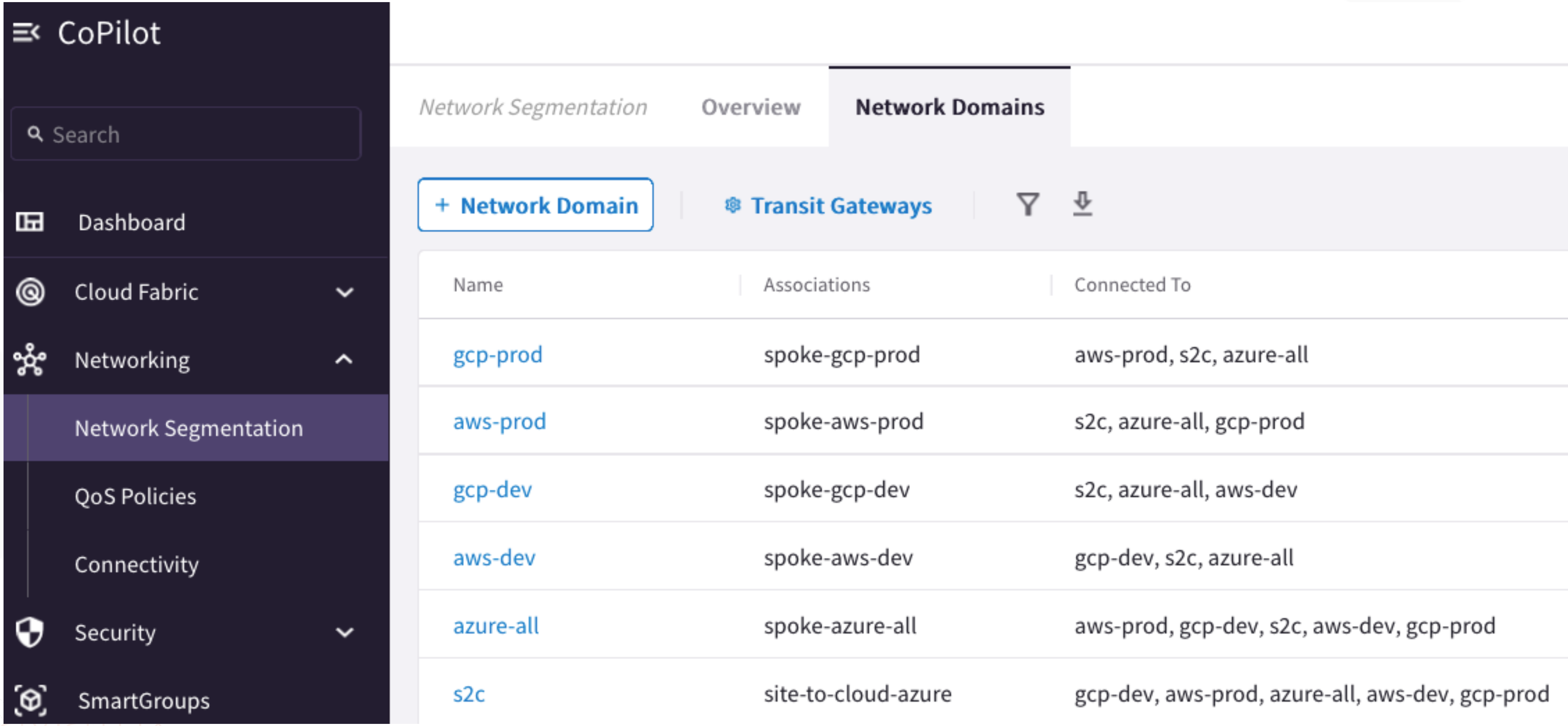
Aviatrix transit gateways have to be enabled to support network segmentation on them.

Name	Cloud	Region	IP Address Space	
transit-aws	aws	us-east-1	10.1.0.0/23	Enabled
transit-azure	arm	West US 3	10.2.0.0/23	Enabled
transit-gcp	gcp	europe-west3	10.3.0.0/23	Enabled

Total 3 Transit Gateways

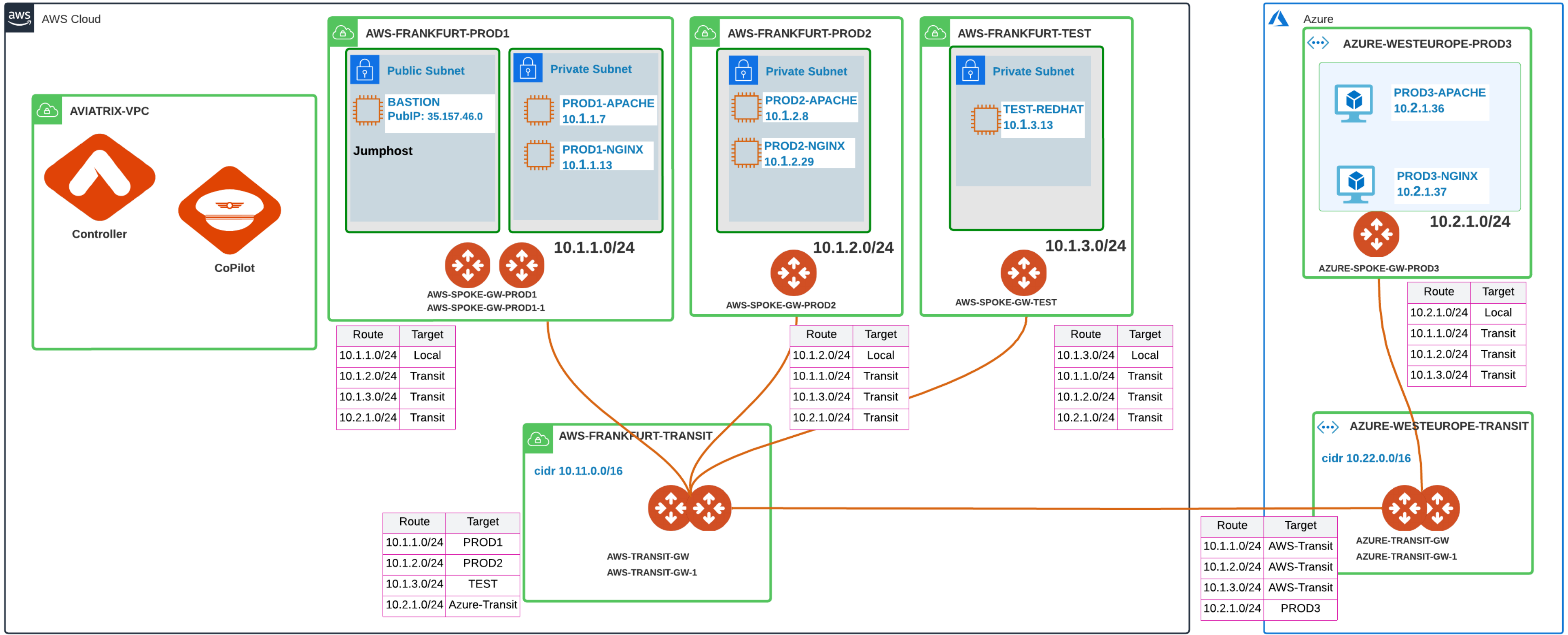
Network Segmentation

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



Name	Associations	Connected To
gcp-prod	spoke-gcp-prod	aws-prod, s2c, azure-all
aws-prod	spoke-aws-prod	s2c, azure-all, gcp-prod
gcp-dev	spoke-gcp-dev	s2c, azure-all, aws-dev
aws-dev	spoke-aws-dev	gcp-dev, s2c, azure-all
azure-all	spoke-azure-all	aws-prod, gcp-dev, s2c, aws-dev, gcp-prod
s2c	site-to-cloud-azure	gcp-dev, aws-prod, azure-all, aws-dev, gcp-prod

1. Enabling a Transit Gateway for Network Segmentation



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

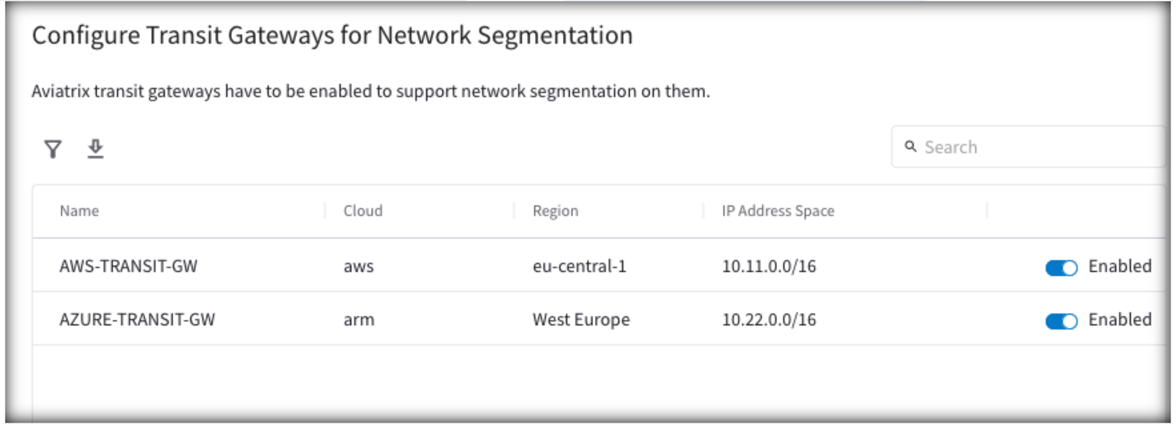
Route	Target
10.2.1.0/24	Local
10.1.1.0/24	Transit
10.1.2.0/24	Transit
10.1.3.0/24	Transit

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

Enable the Network Segmentation:

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

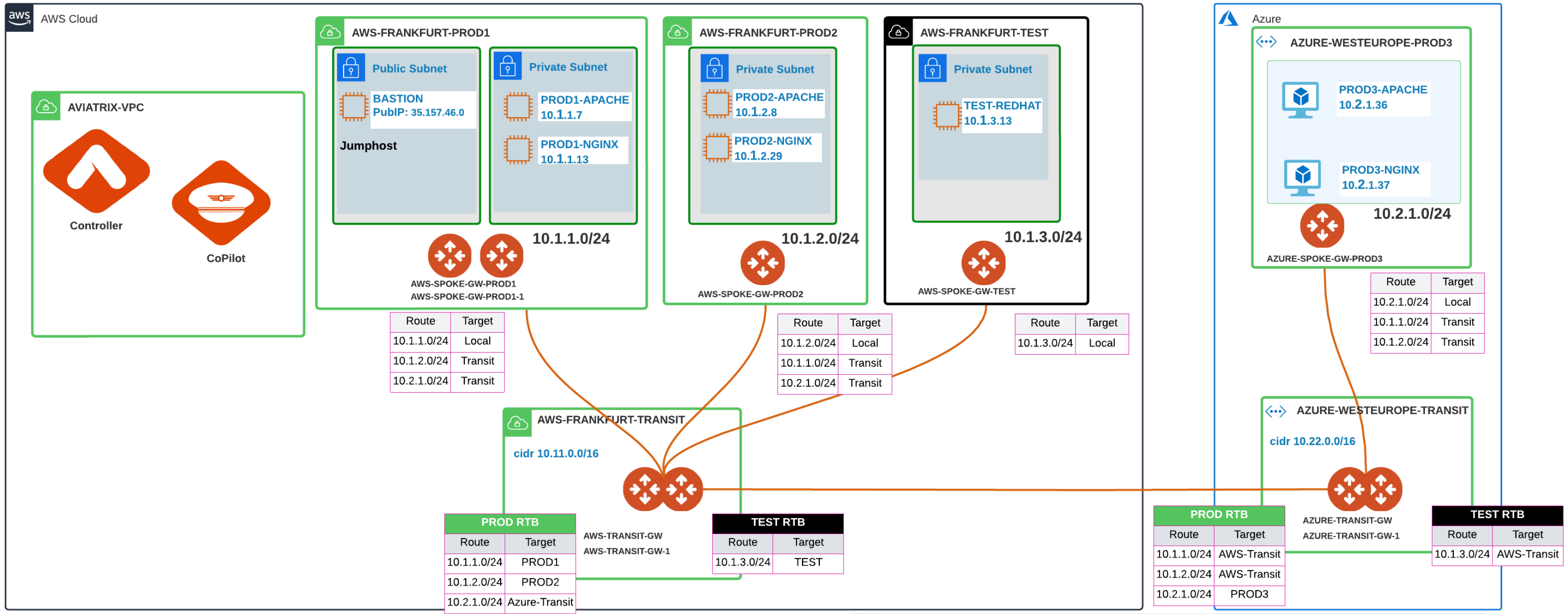


Configure Transit Gateways for Network Segmentation

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. Creating, Connecting, and Associating a Network Domain



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).

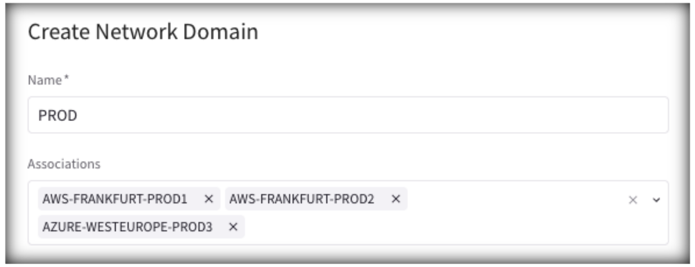
Spoke Gateway

- 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: 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**.



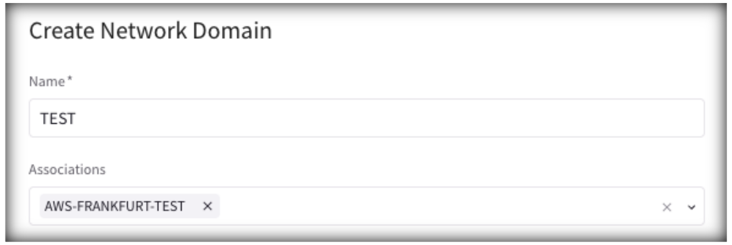
Create Network Domain

Name *

PROD

Associations

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



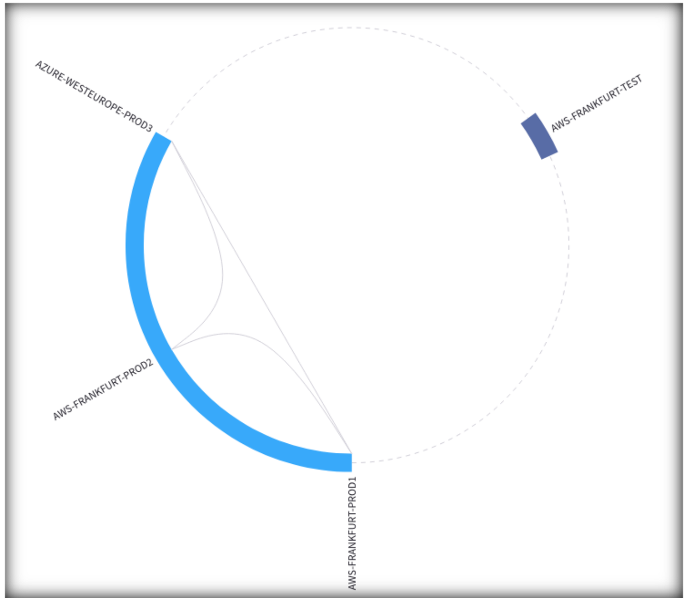
Create Network Domain

Name *

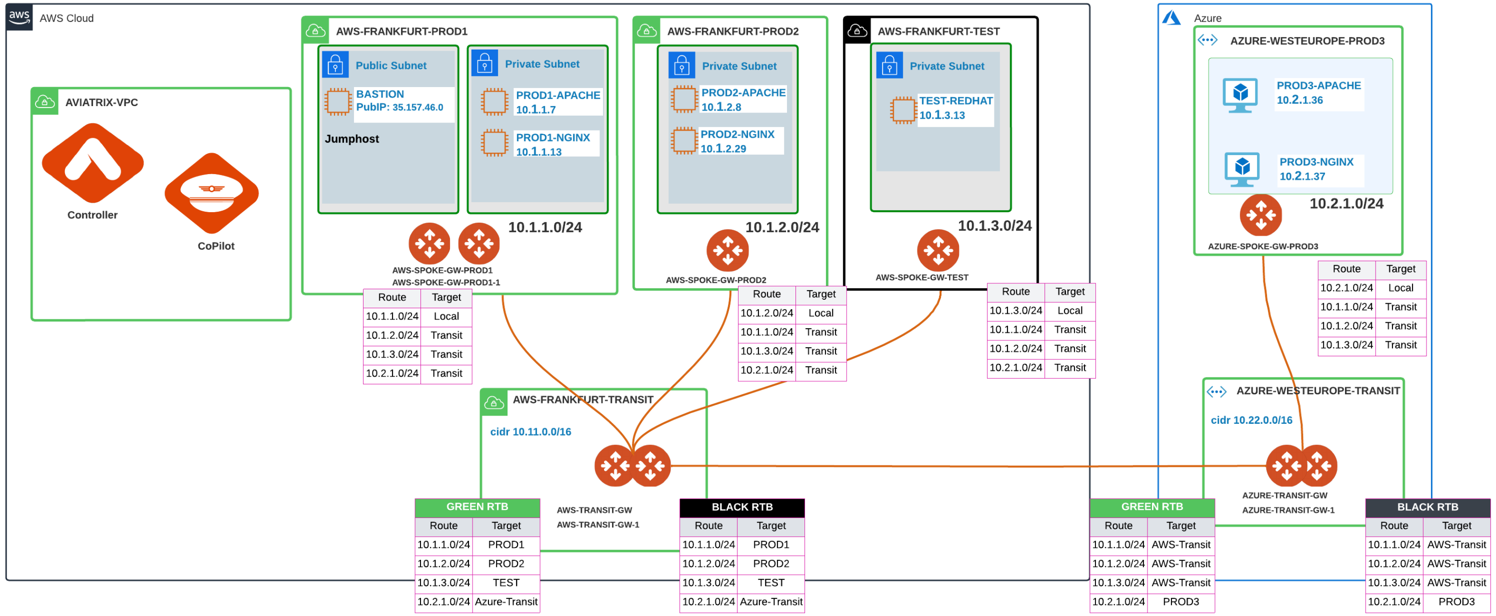
TEST

Associations

AWS-FRANKFURT-TEST ×



3. Apply the Connection Policy



AWS-SPOKE-GW-PROD1

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

AWS-SPOKE-GW-PROD2

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

AWS-SPOKE-GW-TEST

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

AZURE-SPOKE-GW-PROD3

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

AWS-FRANKFURT-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

AWS-FRANKFURT-TRANSIT: BLACK RTB

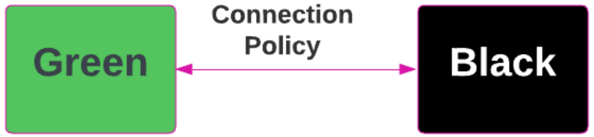
Route	Target
10.1.1.0/24	PROD1
10.1.2.0/24	PROD2
10.1.3.0/24	TEST
10.2.1.0/24	Azure-Transit

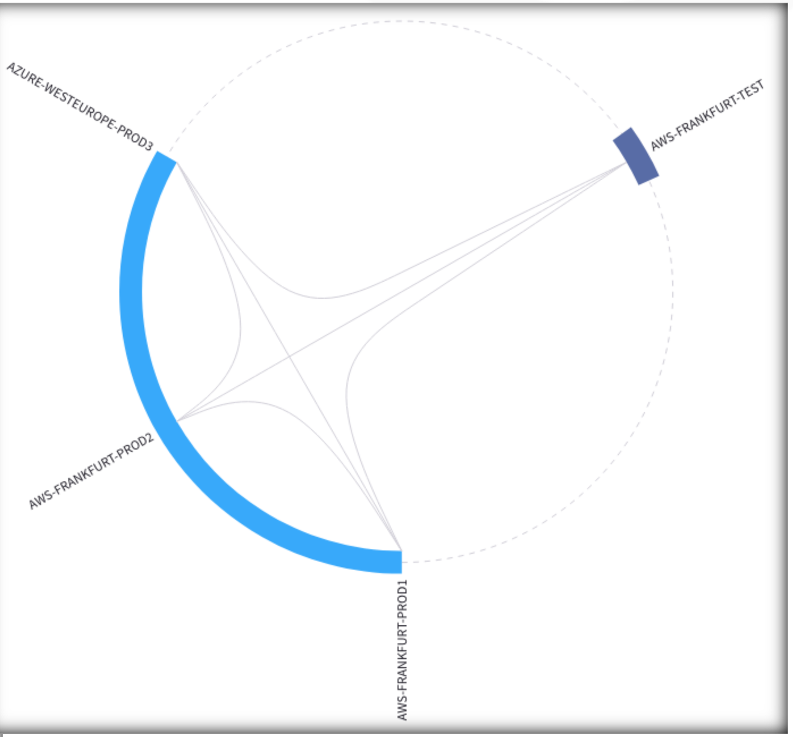
AZURE-WESTEUROPE-TRANSIT: GREEN RTB

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

AZURE-WESTEUROPE-TRANSIT: BLACK RTB

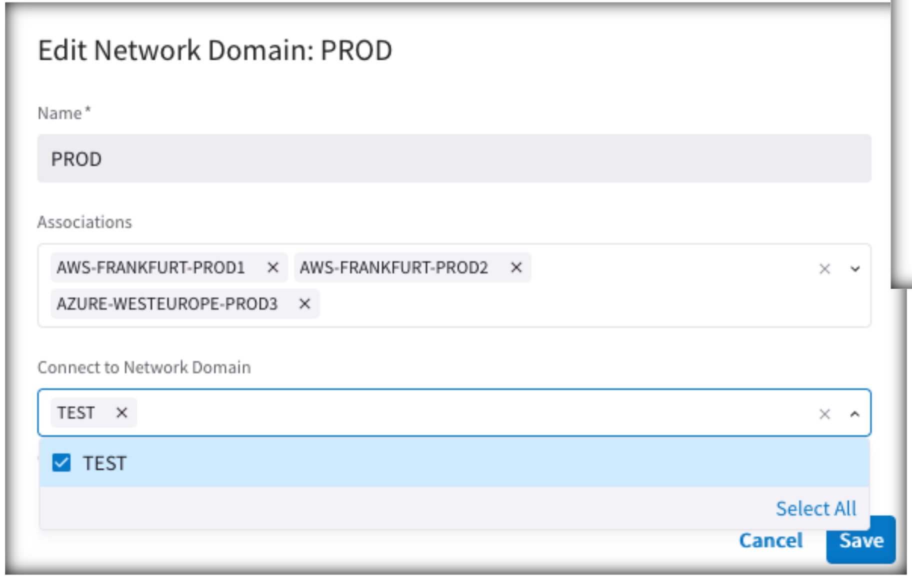
Route	Target
10.1.1.0/24	AWS-Transit
10.1.2.0/24	AWS-Transit
10.1.3.0/24	AWS-Transit
10.2.1.0/24	PROD3





Optionally, enable the Connection Policy:

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



Edit Network Domain: PROD

Name *

PROD

Associations

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

Connect to Network Domain

TEST ×

☑ TEST

aviatrix

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

COMMUNITY
https://community.aviatrix.com