



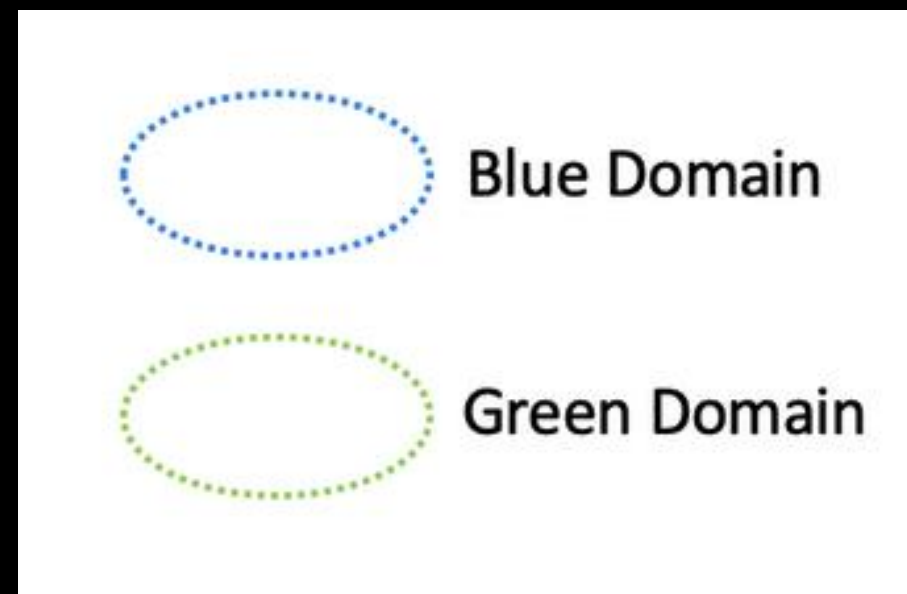
Network Segmentation

ACE Team

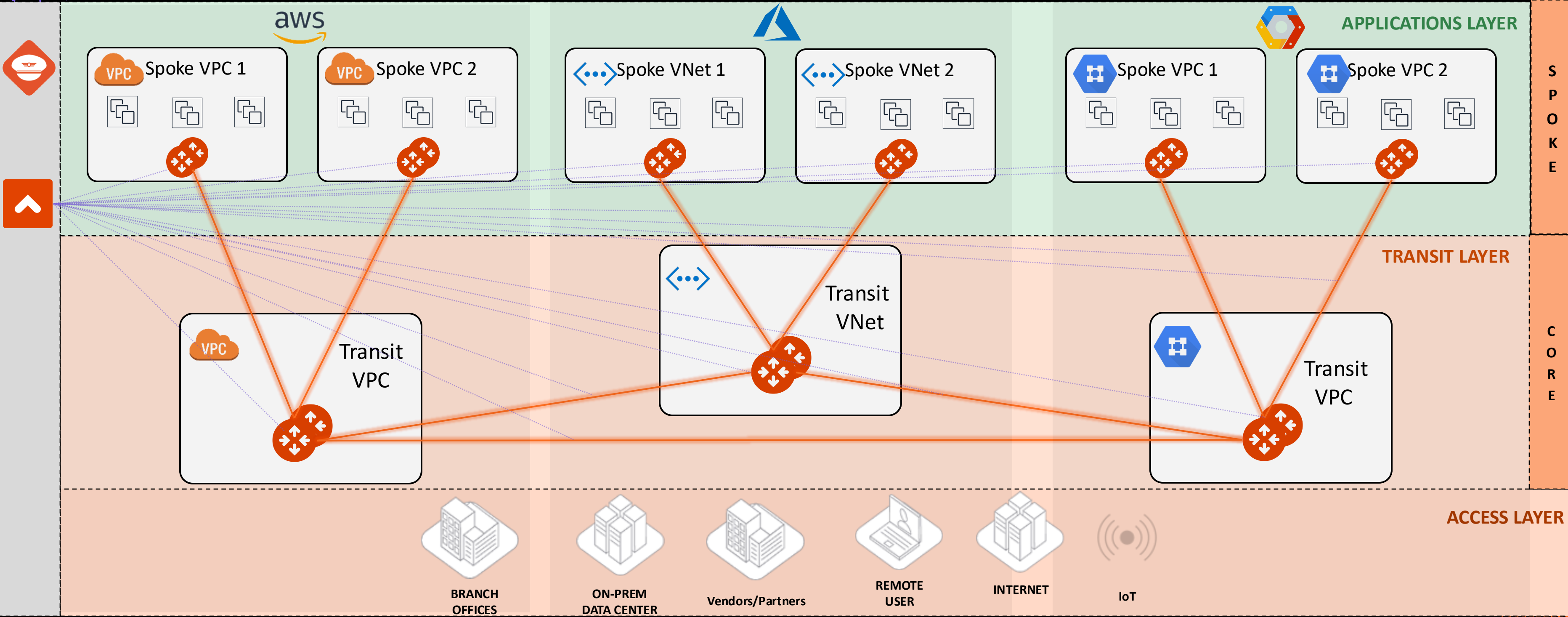


Definition

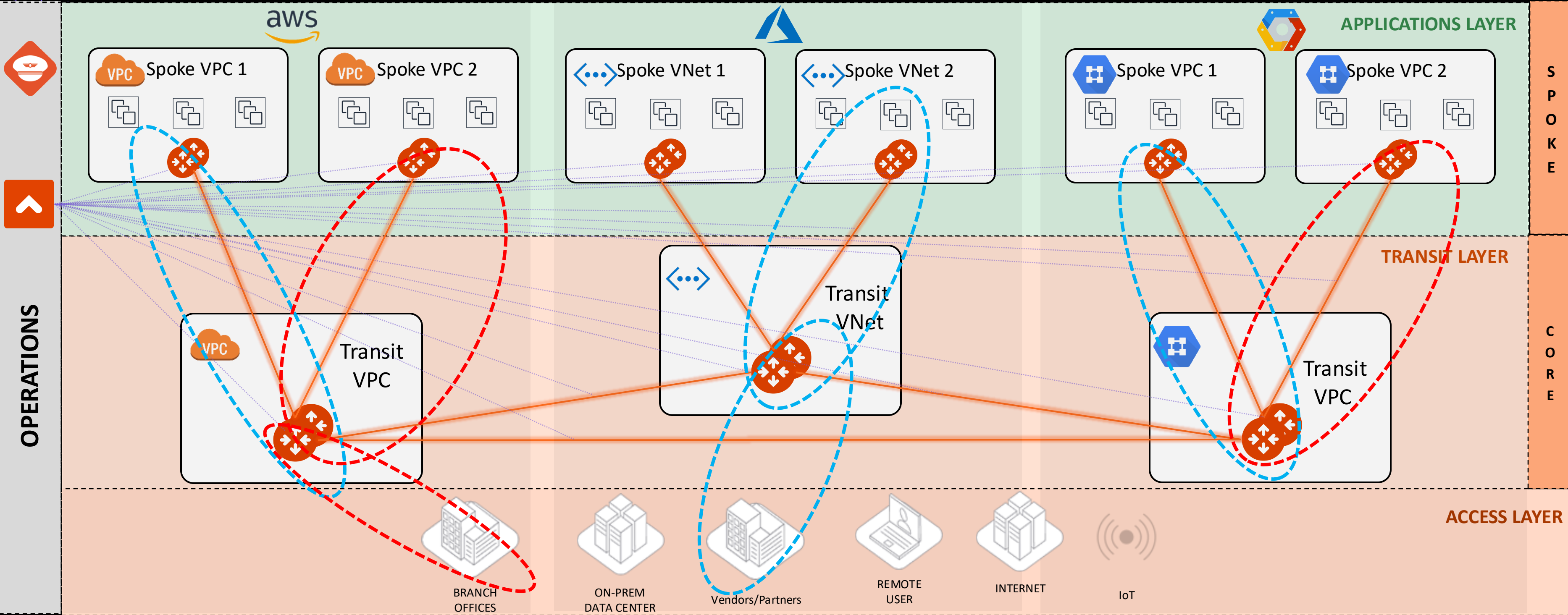
- When you identify groups of spoke and edge VPC/VNets in your infrastructure with the same requirements from a networking point of view (network reachability), you may want to group them in what Aviatrix calls “network domains”.
- A **network domain** is an Aviatrix enforced network of one or more spoke VPC/VCN/VNets.
- The key use case for building network domains is to segment traffic for an enhanced security posture. You use them, in conjunction with *connection policies*, to achieve the network isolation for inter-VPC/VNC/VNets connectivity that you want for your network.



CNSF – The Foundations

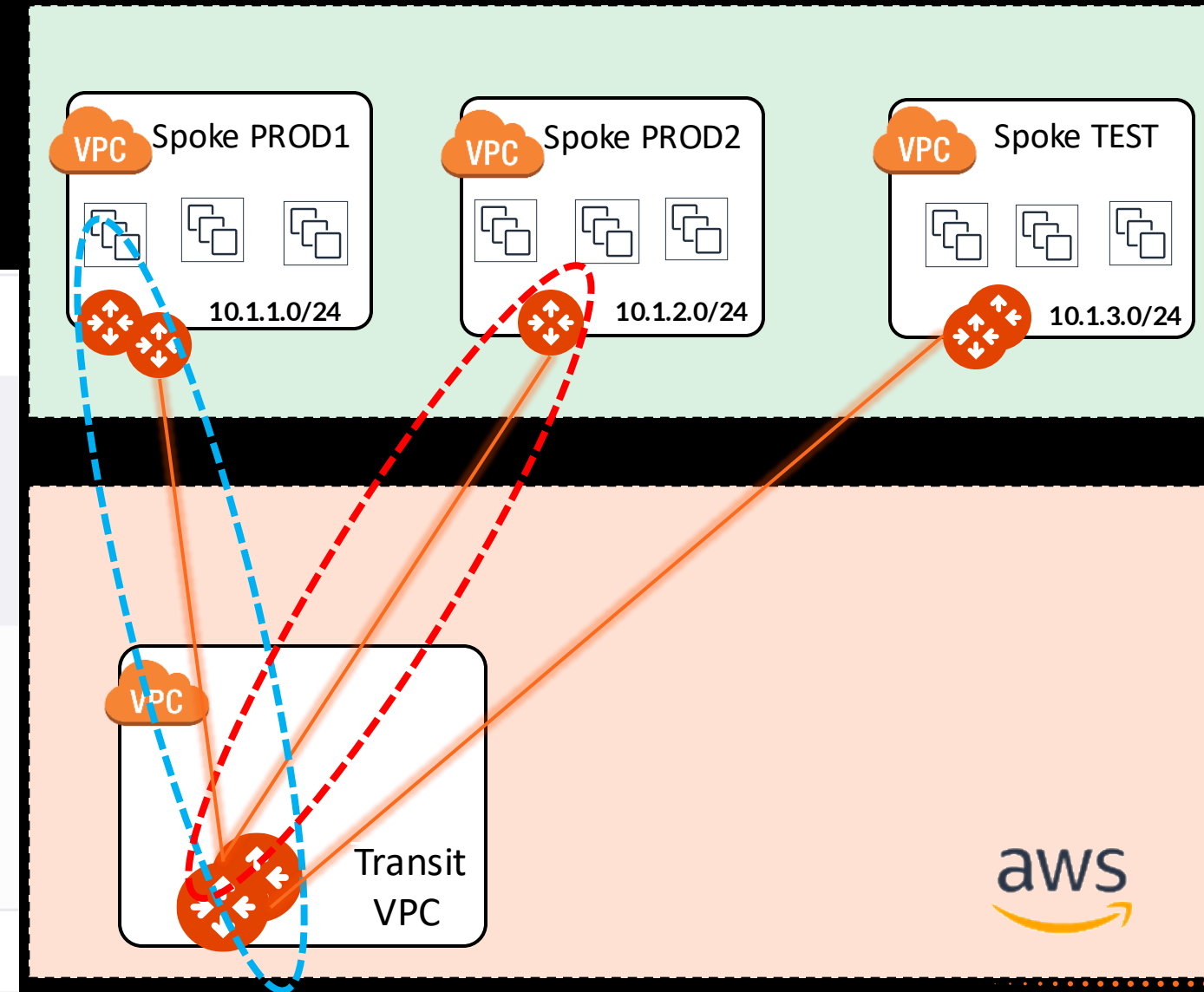


Macro Segmentation with the Aviatrix Network Domains



Network Segmentation: Order of operations

- 1) Enable Network Segmentation on the relevant Transit Gateway(s)
- 2) Create Network Domains (aka *Segments*)
- 3) Associate Spoke Gateways and/or Site2Cloud connections to the Network Domains
- 4) Apply the Connection Policy (*optional*)



Gateways Overview **Transit Gateways** Spoke Gateways Specialty Gateways Gateway Management Settings

< AWS-AWS-TRANSIT-GW

Details Instances Attachments VPC/VNet Route Tables Gateway Routes Interface Stats **Route DB** Performance Settings

Best Routes
All

Segmentation enabled

CIDR	Type	Table ID	Next Hop Gateway/Connection	Next Hop IP
10.1.1.0/24	vpc	BLUE_rtb	AVX-AWS-PROD1-GW	3.11.230.247
10.1.2.0/24	vpc	RED_rtb	AVX-AWS-PROD2-GW	18.135.173.0
10.1.3.0/24	vpc	main	AVX-AWS-TEST-GW	18.175.75.119

PATH: COPILOT > Cloud Fabric > Gateways > Transit Gateways > select the relevant GW > **Route DB** (equivalent of RIB)

Multiple Routing Domains inside the CNSF

Gateways

Overview

Transit Gateways

Spoke Gateways

Specialty Gateways

Gateway Management

Settings

< ☰

AWS-AWS-TRANSIT-GW

✎ 🔗 🗑 ⋮

Details

Instances

Attachments

VPC/VNet Route Tables

Gateway Routes

Interface Stats

Route DB

Performance

Settings

Gateway Instance

AWS-AWS-TRANSIT-GW

Network Domain

BLUE

▼

Destination

Via

Interface

Next Hop IP

Next Hop Gateway

Metric

default

blackhole

400

▼

10.1.1.0/24

10.1.1.0/24

tun-030BE6F7-0

3.11.230.247

AVX-AWS-PROD1-GW

100

10.1.1.0/24

tun-0D2A6214-0

13.42.98.20

AVX-AWS-PROD1-GW-1

100

10.1.1.0/24

tun-0A0A0028-0

10.10.0.40

AWS-AWS-TRANSIT-GW-1

200

Gateways

Overview

Transit Gateways

Spoke Gateways

Specialty Gateways

Gateway Management

Settings

< ☰

AWS-AWS-TRANSIT-GW

✎ 🔗 🗑 ⋮

Details

Instances

Attachments

VPC/VNet Route Tables

Gateway Routes

Interface Stats

Route DB

Performance

Settings

Gateway Instance

AWS-AWS-TRANSIT-GW

Network Domain

RED

▼

Destination

Via

Interface

Next Hop IP

Next Hop Gateway

Metric

default

blackhole

400

10.1.2.0/24

tun-1287AD00-0

18.135.173.0

AVX-AWS-PROD2-GW

100

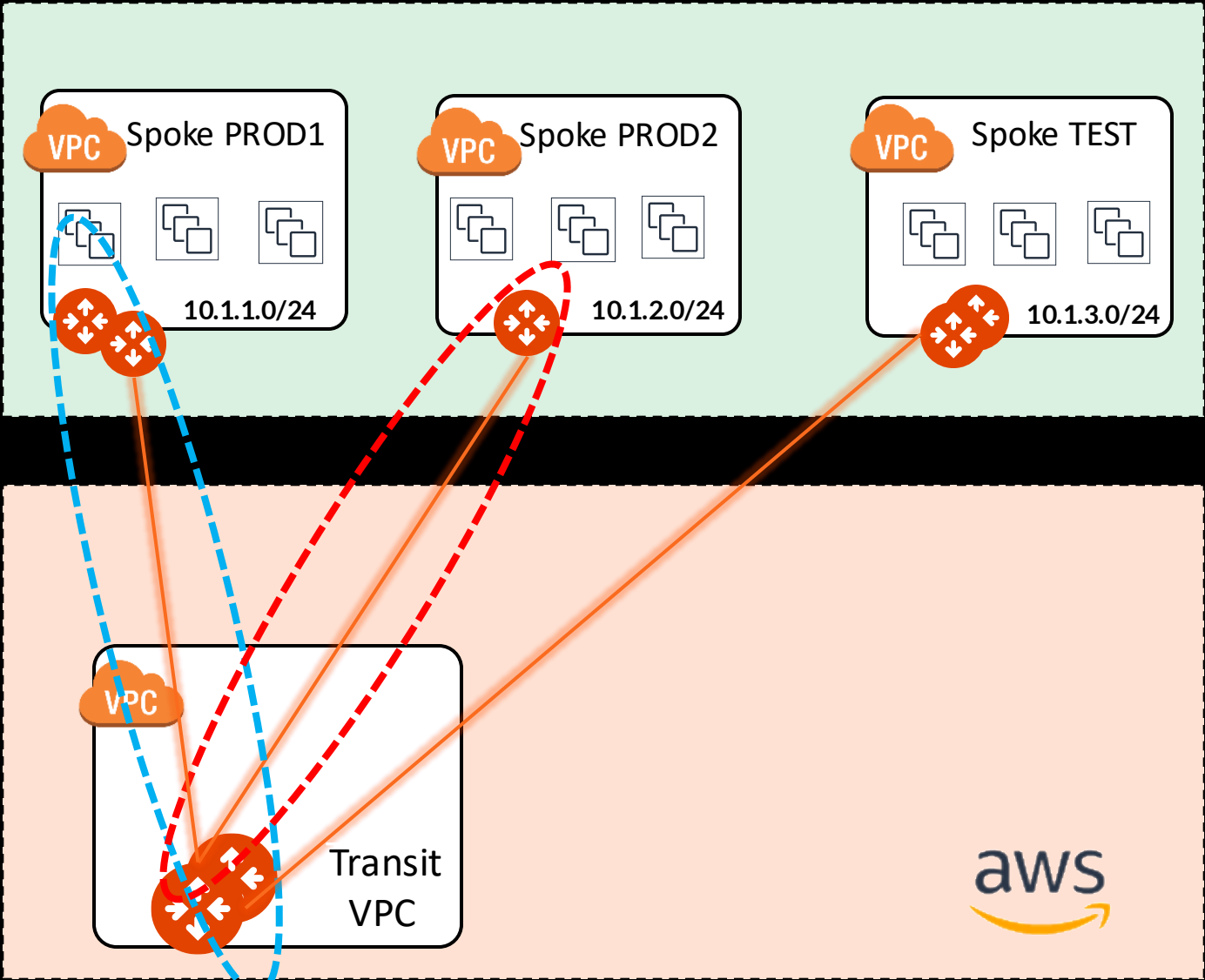
10.1.2.0/24

tun-0A0A0028-0

10.10.0.40

AWS-AWS-TRANSIT-GW-1

200



- A single Spoke gateway or a Cluster of Spoke Gateways can be associated to a unique domain!
- **PATH:** COPILOT > Cloud Fabric > Gateways > Transit Gateways > select the relevant GW > **Gateway Routes** and then filter based on the network domain (i.e. VRF)
- **CAVEAT:** The specific Network Domain view (aka vrf) is only available on the Transit GW. The Spoke GW has only the main routing table (aka GRT).

Connection Policy (*optional*)

- The Connection policy allows the **inter-domain** communication or **inter-segment** communication (*vrf leaking*).
- The connection policy establishes a bidirectional connectivity (merging the network domains' RTBs).

In the example on the right, there are three domains: **Green**, **Blue** & **Yellow**

- If the Blue domain acts as the Shared Services Domain, It will be connected to both the GREEN domain and the YELLOW domain.

Edit Network Domain: BLUE

Name *

BLUE

Associations

AVX-AWS-PROD2-GW

Connect to Network Domain

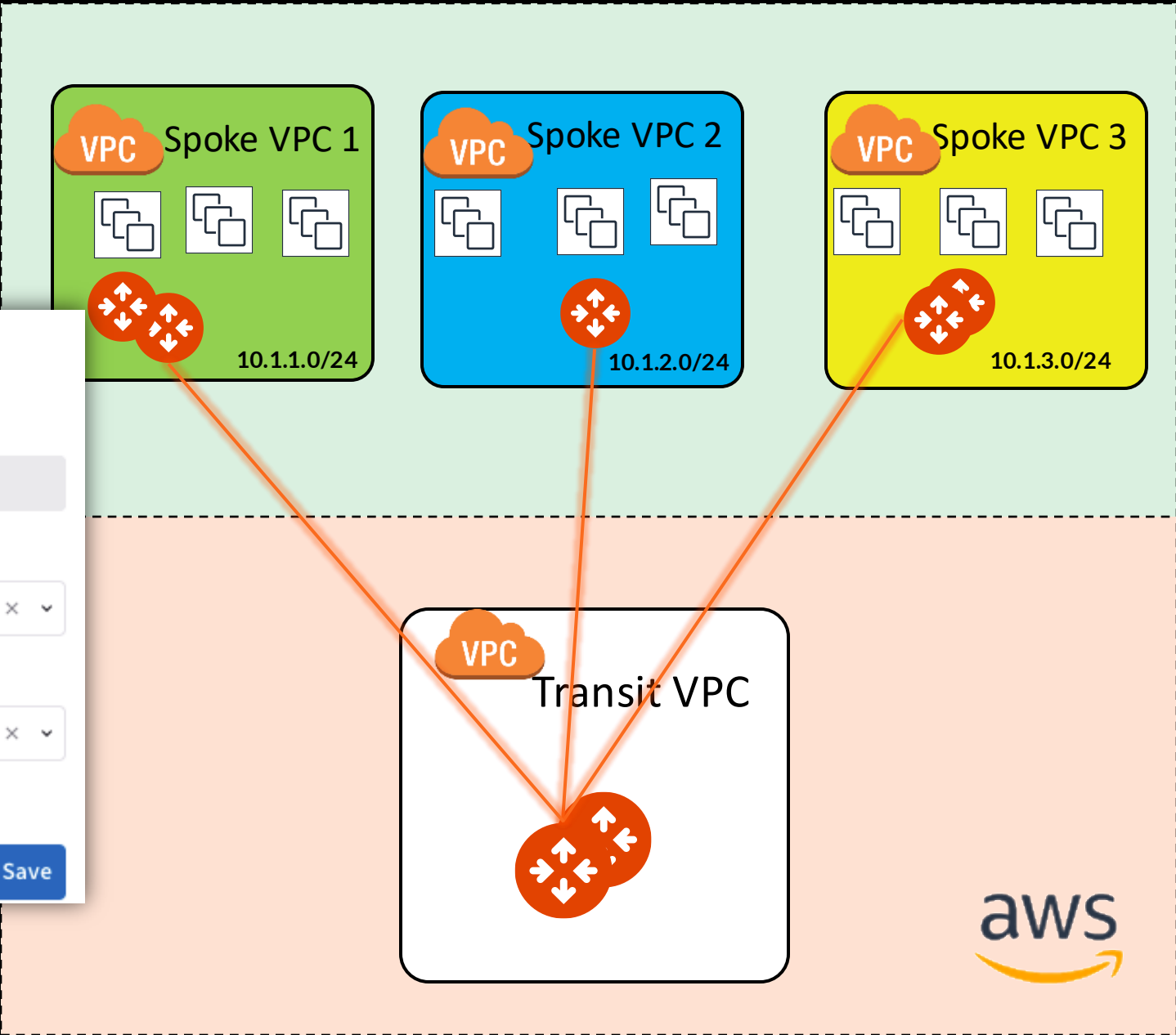
GREENYELLOW

Connectivity is bidirectional

Cancel

Save

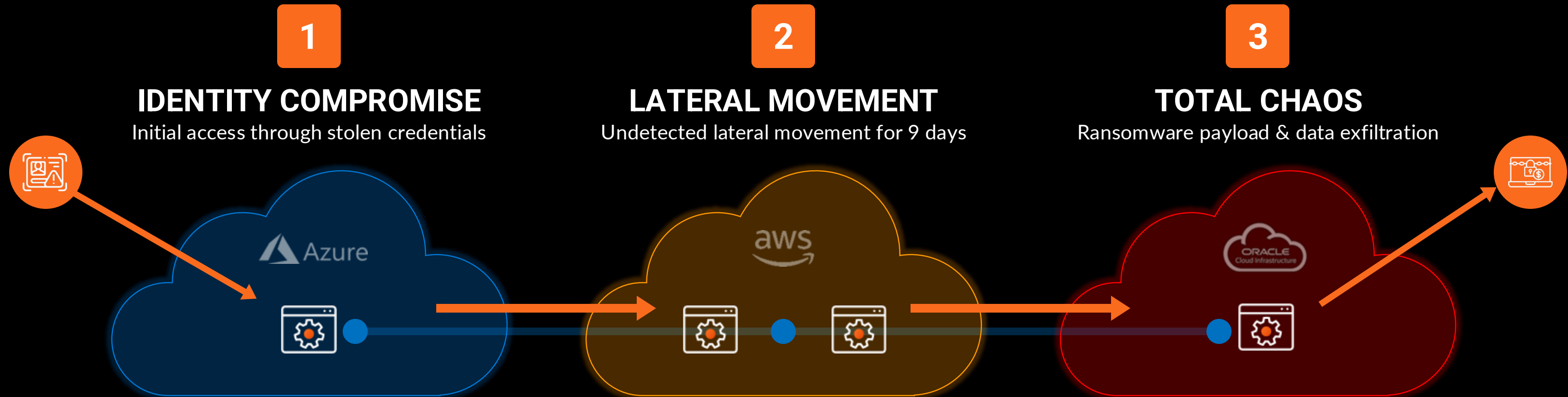
Name	Associations	Connected To
YELLOW	AVX-AWS-SPOKE-GW-TEST	BLUE
GREEN	AVX-AWS-SPOKE-GW-PROD1	BLUE
BLUE	AVX-AWS-SPOKE-GW-PROD2	GREEN, YELLOW



- **CAVEAT:** a connection policy can't be applied on the main RTB (aka Global Routing Table).

Anatomy of Today's Threats: Lateral Movement

RECENT SUCCESSFUL ATTACKS ARE FOLLOWING THE SAME PATTERNS



Tools for Operating Network Segmentation



Network Segmentation Configuration part.1

- CoPilot: Configure and enable the feature
- PATH:** COPILOT > Networking > Network Segmentation > Network Domains > Transit Gateways

CoPilot

Search

Dashboard

Cloud Fabric

Networking

Network Segmentation

QoS Policies

Connectivity

Security

SmartGroups

Cloud Resources

Monitor

Diagnostics

Billing & Cost

Administration

Settings

Network Segmentation

Overview

Network Domains

+ Network Domain

Transit Gateways

Name	Associations	Connected To
BU2	ace-aws-eu-west..., + 1 more	BU1
BU1	ACE-ONPREM-DC, + 3 more	BU2

Configure Transit Gateways for Network Segmentation

Show filters

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

Filter

Download

Search

Name	Cloud	Region	IP Address Space	
ace-aws-eu-west-1-transit1	aws	eu-west-1	10.1.200.0/23	<input checked="" type="checkbox"/> Enabled
ace-azure-east-us-transit1	arm	East US	192.168.200.0/23	<input checked="" type="checkbox"/> Enabled
ace-gcp-us-east1-transit1	gcp	us-east1	172.16.200.0/23	<input checked="" type="checkbox"/> Enabled

Total 3 Transit Gateways

CancelSave

Network Segmentation Configuration part.2

- CoPilot: create/modify the Network Domains

PATH: COPILOT > Networking> Network Segmentation > Network Domains > + Network Domain / pencil icon (*for editing an existing Segment*)

The screenshot displays the Aviatrix CoPilot interface. On the left is a dark sidebar with a search bar and a menu containing: Dashboard, Cloud Fabric, Networking (highlighted with a red box), Network Segmentation (highlighted with a red box), Connectivity, Security, SmartGroups, Cloud Resources, Monitor, Diagnostics, Billing & Cost, Administration, and Settings. The main panel is titled 'Network Segmentation' and has tabs for 'Overview' and 'Network Domains' (the latter is highlighted with a red box). Below the tabs are buttons for '+ Network Domain' and 'Transit Gateways', along with filter and download icons. A search bar is on the right. A table lists network domains:

Name	Associations	Connected To
BU2	ace-azure-east-us-spoke2, + 1 more	
BU1	ace-gcp-us-east1-spoke1, + 3 more	

Red arrows point to the edit (pencil) and delete (trash) icons for the BU2 domain. An 'Edit Network Domain: BU2' modal is open in the foreground, showing:

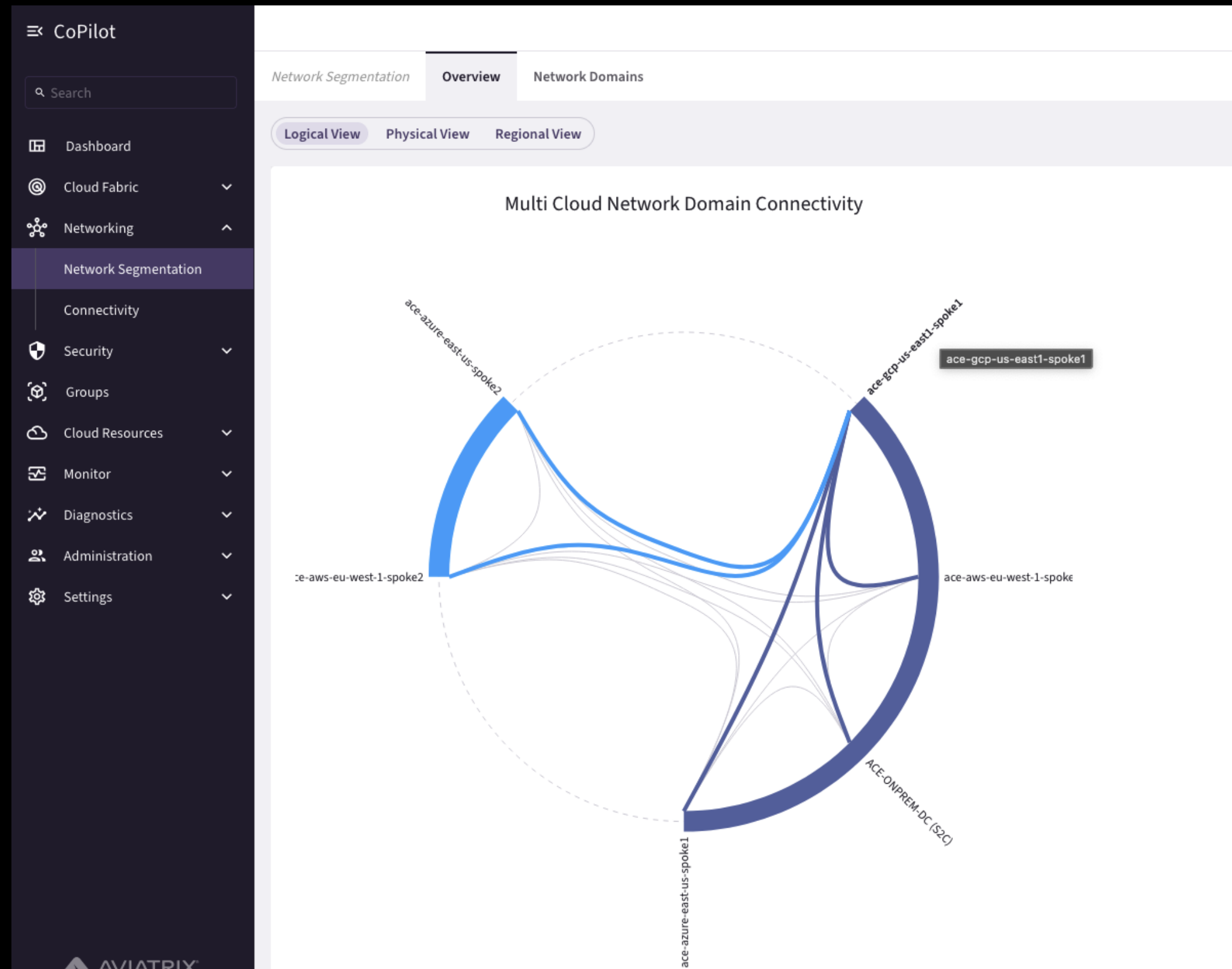
- Name ***: BU2
- Associations**: ace-azure-east-us-spoke2, ace-aws-eu-west-1-spoke2
- Connect to Network Domain**: BU1 (selected with a checkmark)

The modal includes 'Select All', 'Cancel', and 'Save' buttons at the bottom.

Network Segmentation Visibility

- CoPilot: verify the Network Relationships

PATH: COPILOT > Networking > Network Segmentation > Overview > Logical View



Next: Lab 1 Network Domains & Lab 2 Connection Policy

