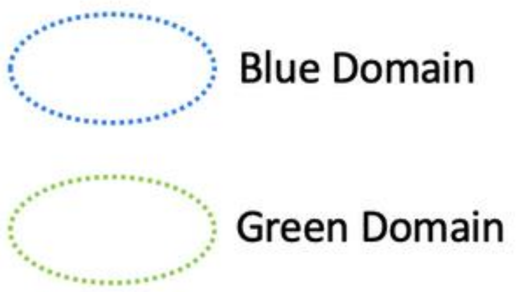
Network Segmentation

ACE Team

Network Segmentation - Overview

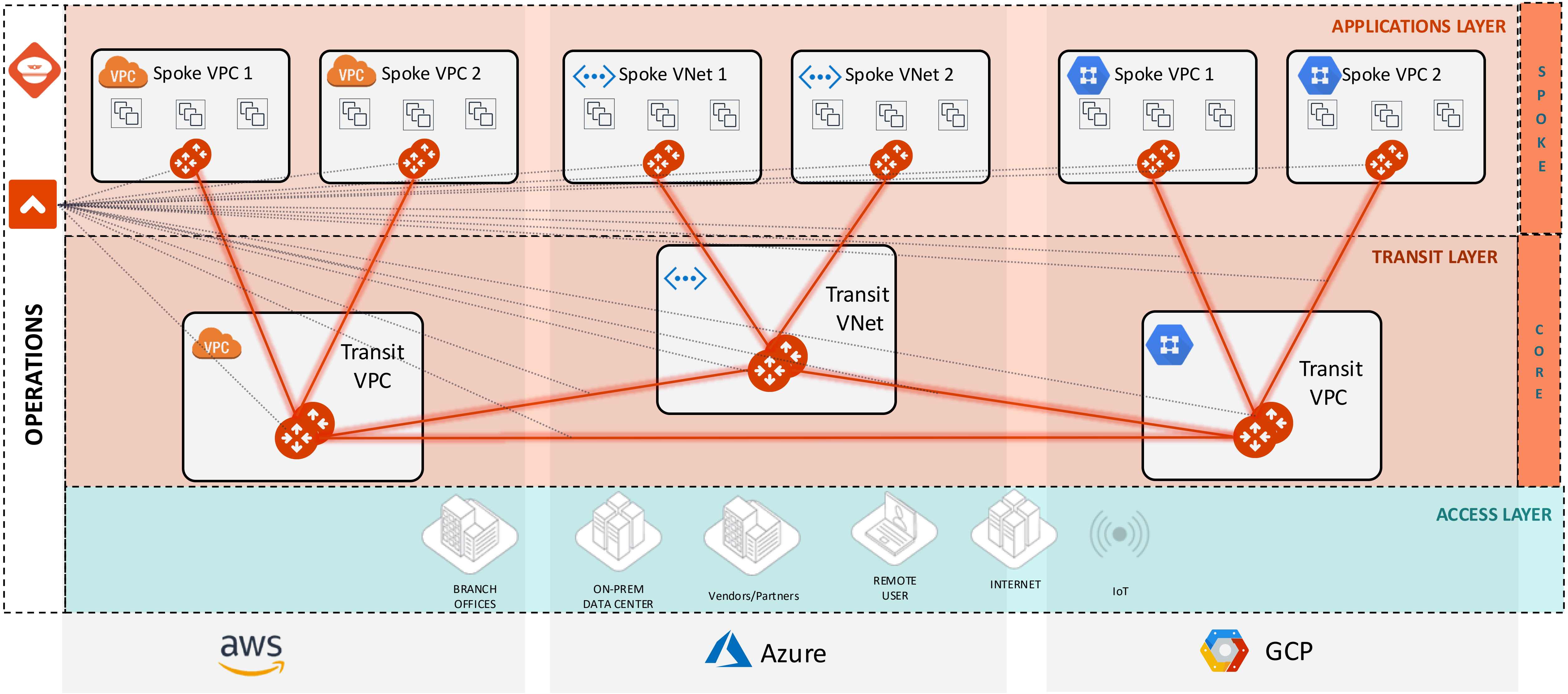
- When you identify groups of spoke and edge VPC/VNets in your infrastructure with the same requirements from a networking point of view (network reachability), you may want to group them in what Aviatrix calls “network domains”.
- A *network domain* is an Aviatrix enforced network of one or more spoke 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.



Implementing Network Segmentation in an Aviatrix-Managed Network (official documentation link):

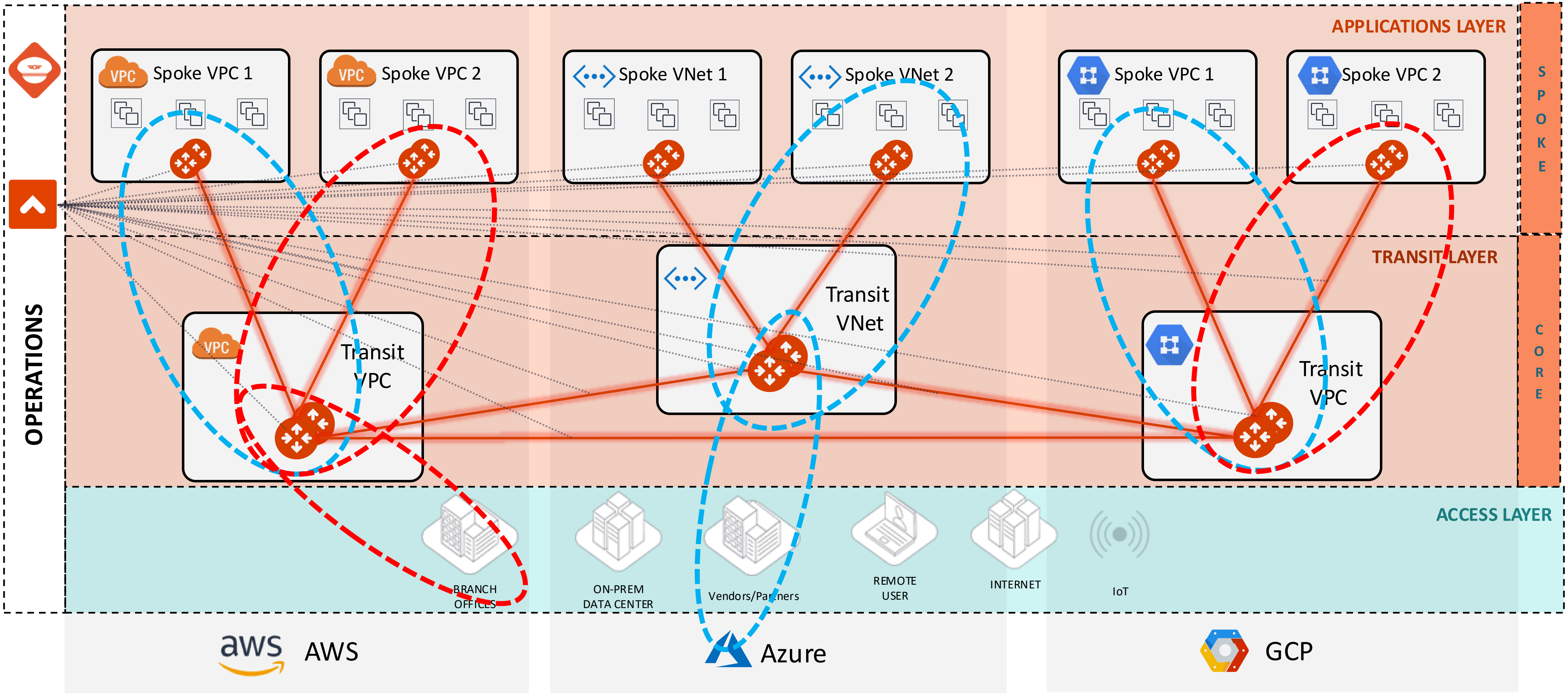
https://docs.aviatrix.com/copilot/latest/network-security/network-segmentation-secured.html?expand=true

CNSF: the Foundations



AVIATRIX

Global Segmentation with Network Domains



AVIATRIX

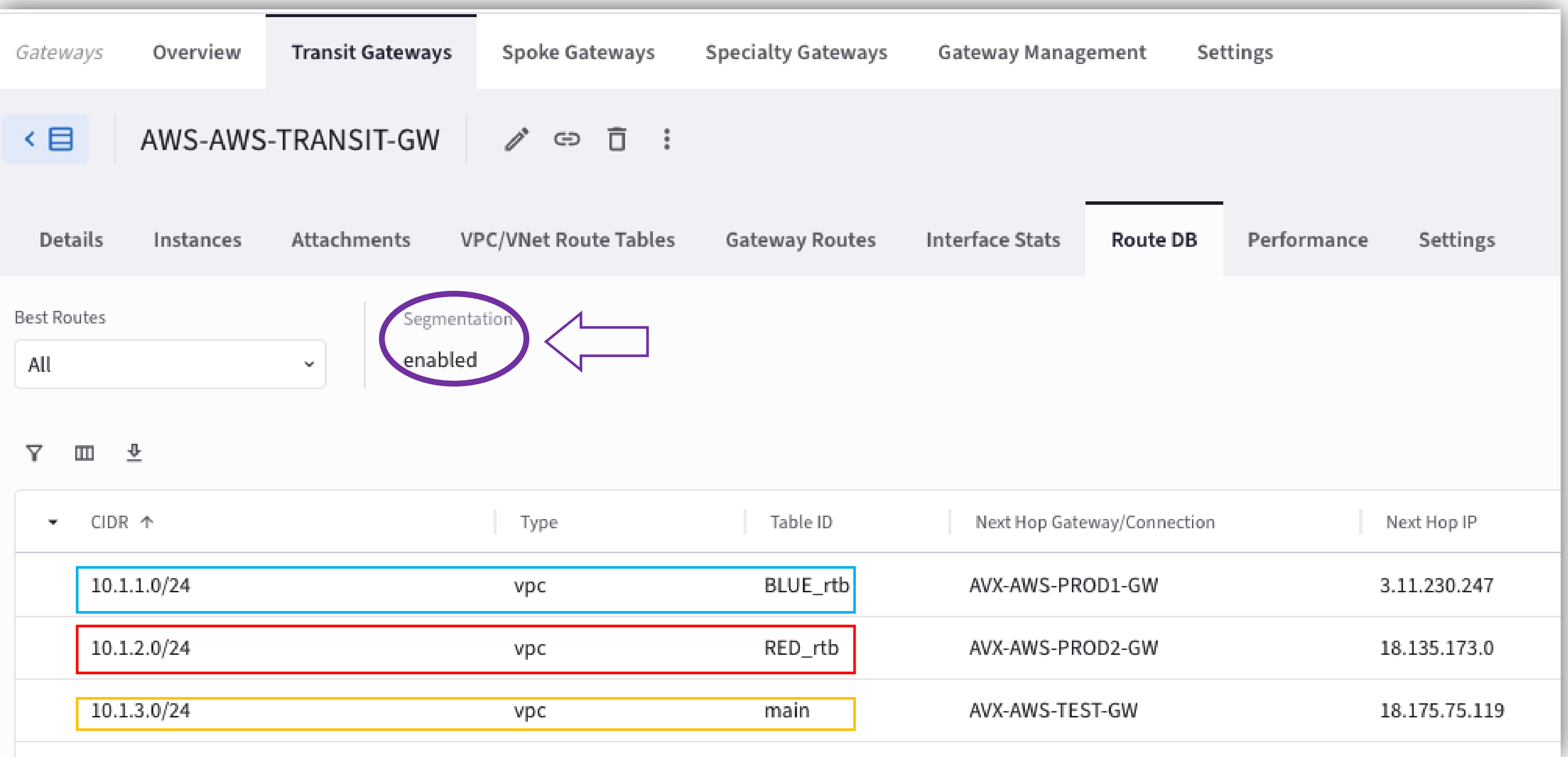
Order of Operations for activating the Network Segmentation

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

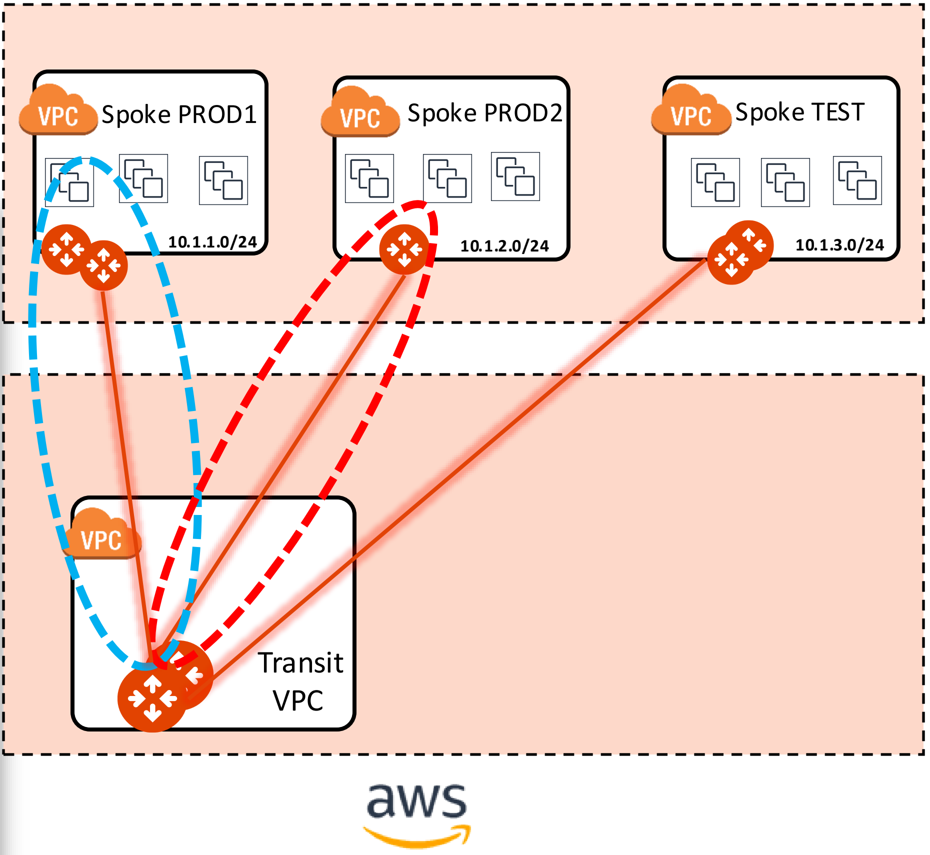
4) Apply the Connection Policy (*optional*)



Best Routes: All

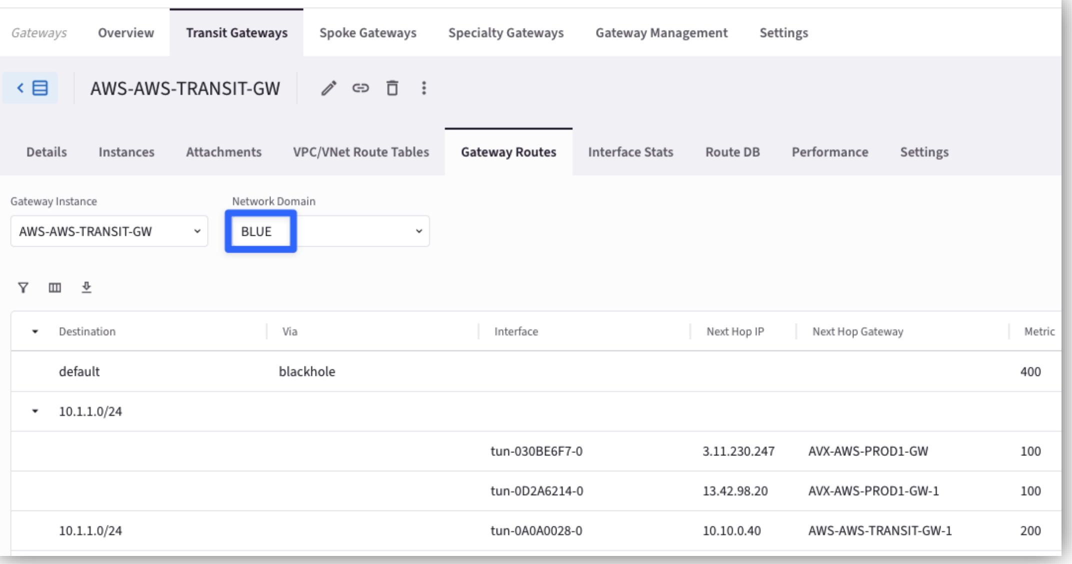
Segmentation: enabled

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)

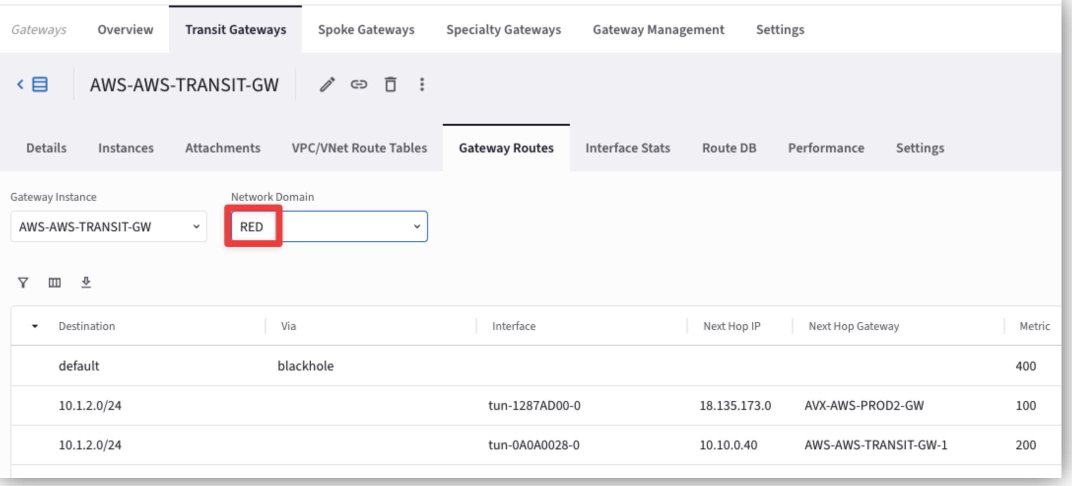
Multiple Routing Domains on the Transit GW



Gateway Instance: AWS-AWS-TRANSIT-GW

Network Domain: BLUE

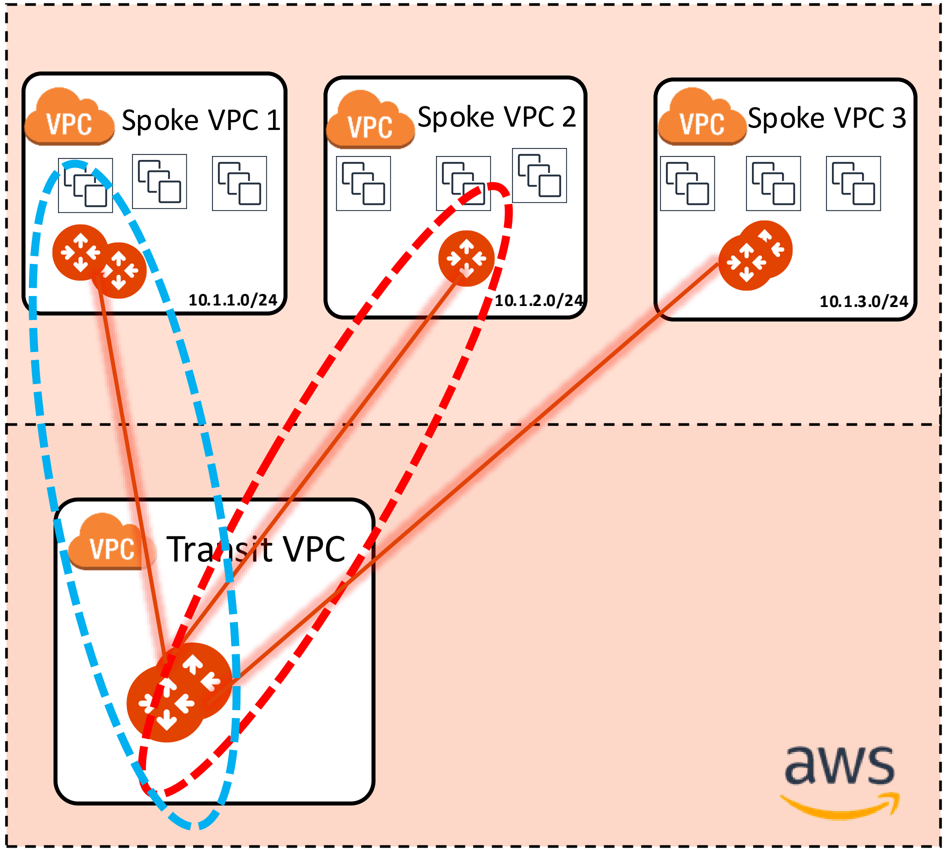
Destination	Via	Interface	Next Hop IP	Next Hop Gateway	Metric
default	blackhole				400
10.1.1.0/24					
		tun-030BE6F7-0	3.11.230.247	AVX-AWS-PROD1-GW	100
		tun-0D2A6214-0	13.42.98.20	AVX-AWS-PROD1-GW-1	100
10.1.1.0/24		tun-0A0A0028-0	10.10.0.40	AWS-AWS-TRANSIT-GW-1	200



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).

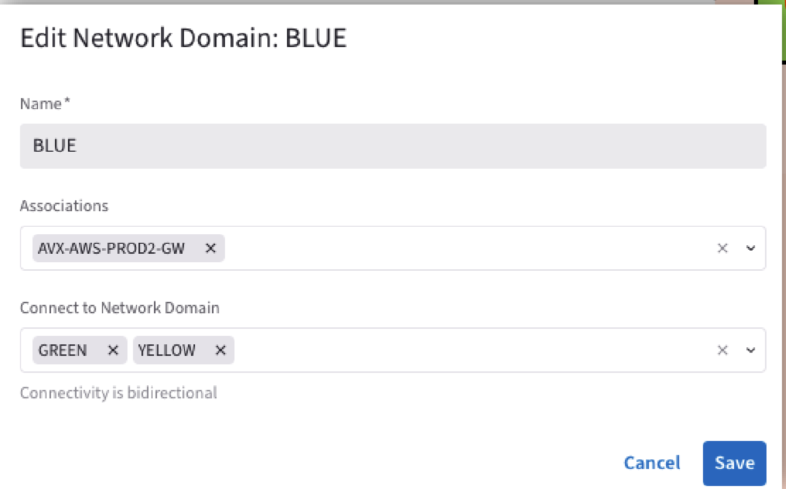
Connection Policy

- 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

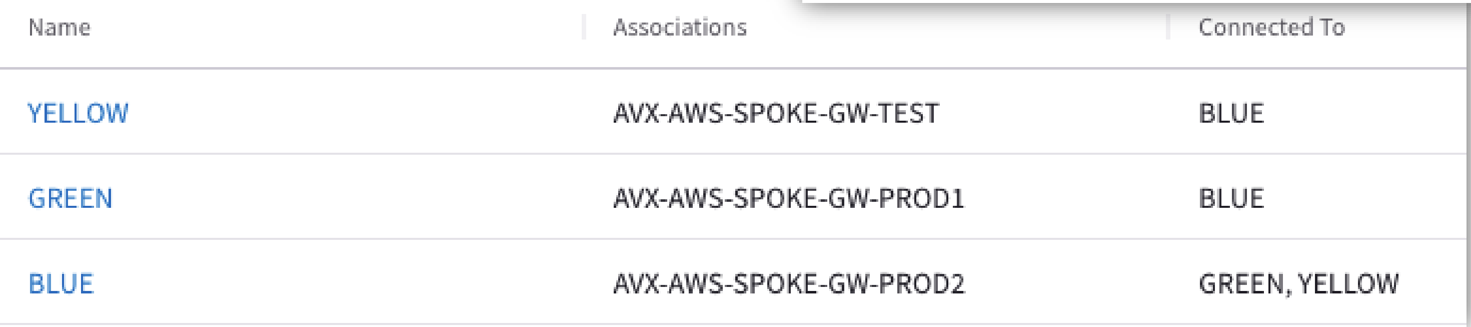
Associations

AVX-AWS-PROD2-GW ×

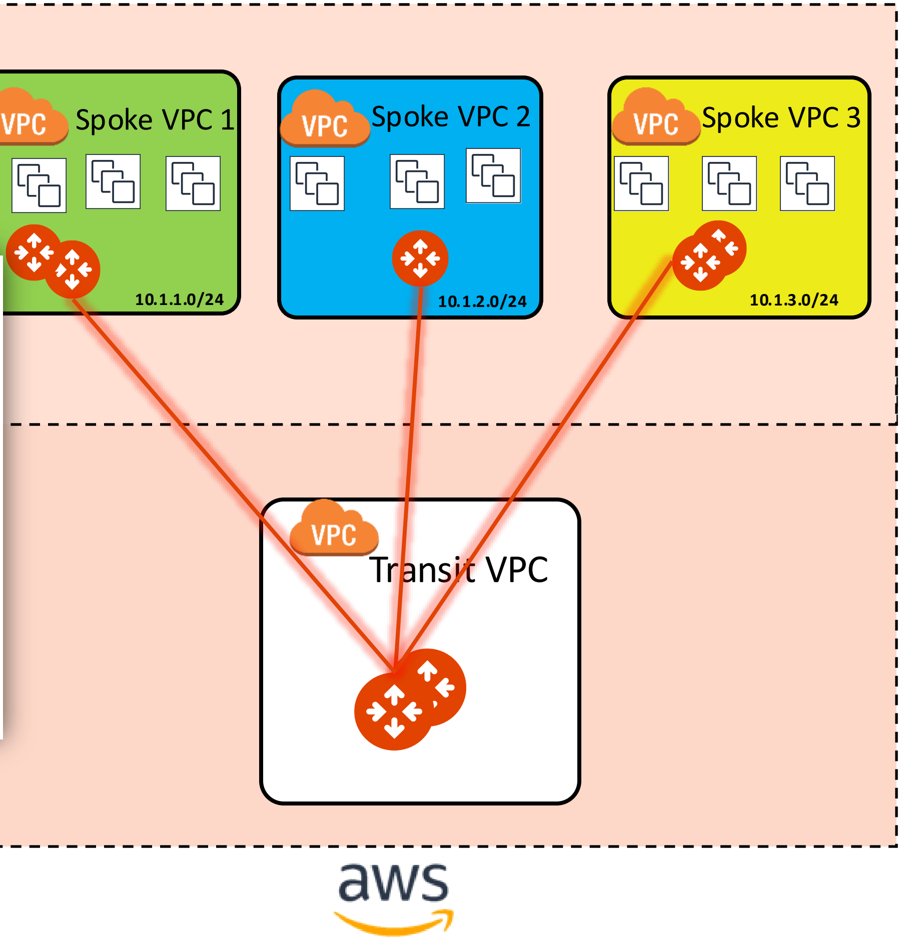
Connect to Network Domain

GREEN × YELLOW ×

Connectivity is bidirectional

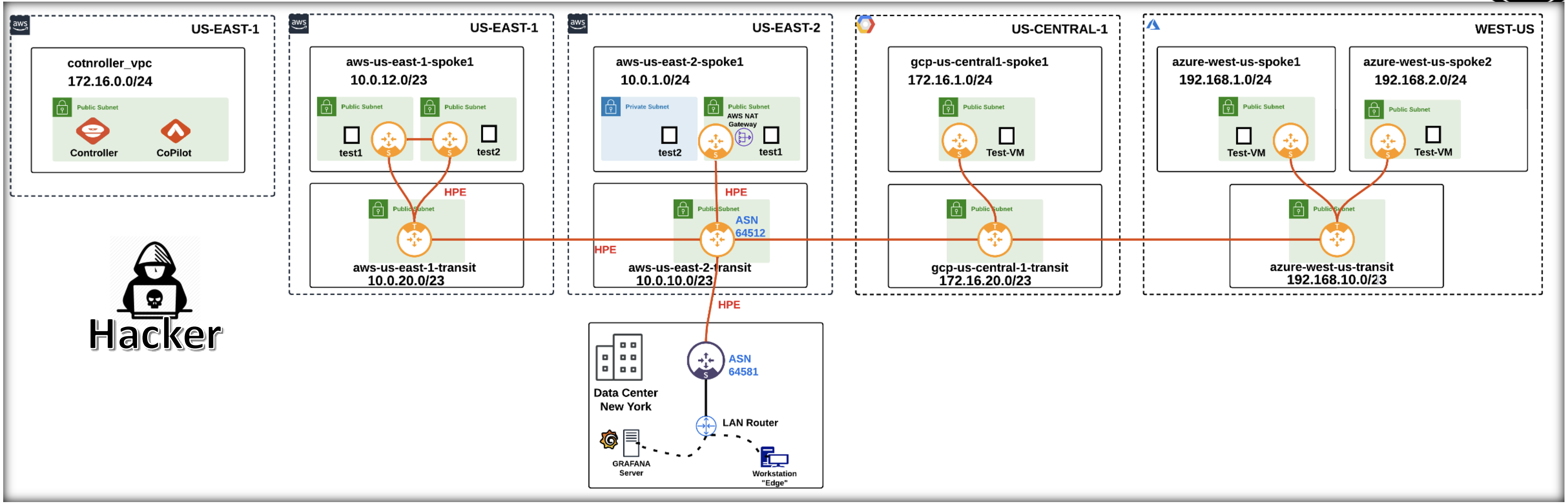


Name	Associations	Connected To
YELLOW	AVX-AWS-SPOKE-GW-TEST	BLUE
GREEN	AVX-AWS-SPOKE-GW-PROD1	BLUE
BLUE	AVX-AWS-SPOKE-GW-PROD2	GREEN, YELLOW



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

Lateral Movement



- An attacker searches for an instance that could serve as a foothold for lateral

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

AVIATRIX

ACE

OPERATIONS

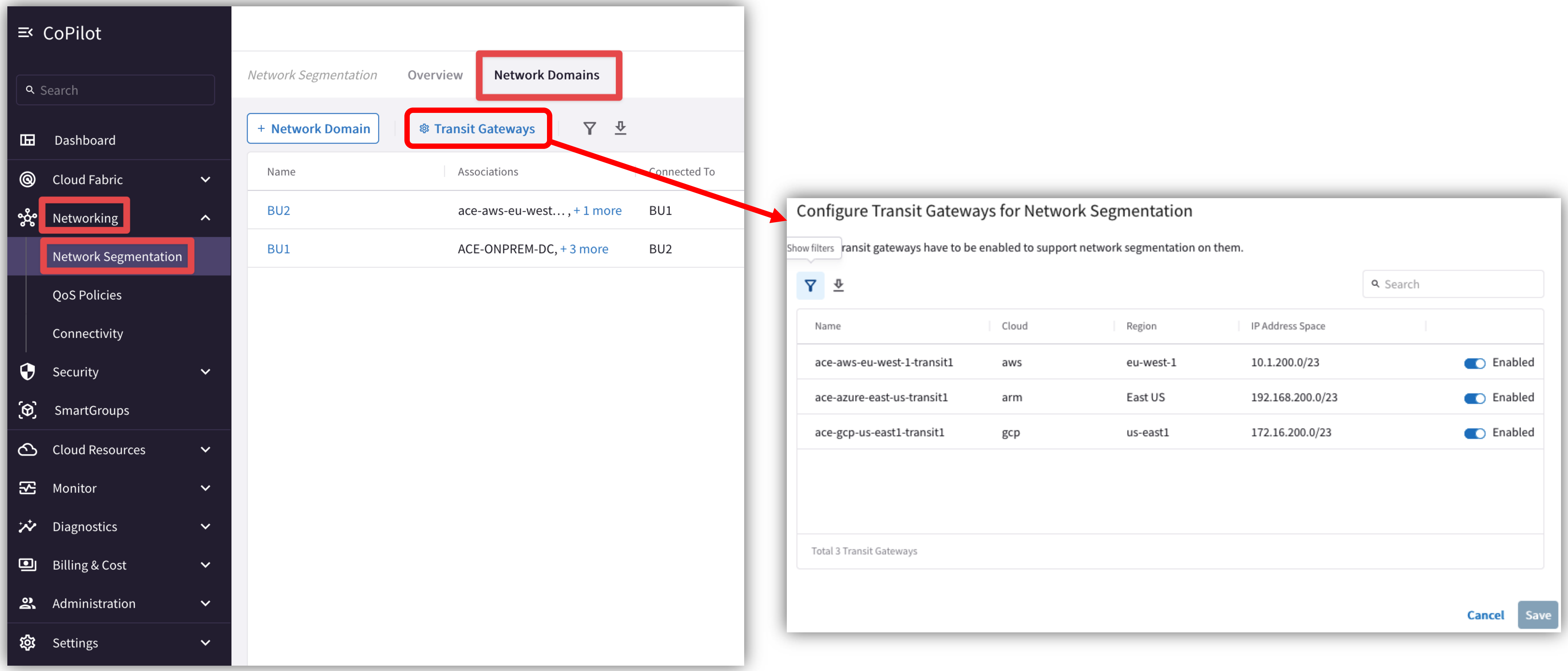
SPECIALTY

Tools for Operating Network Segmentation

Network Segmentation Visibility

- CoPilot: verify the Network Domains

PATH: COPILOT > Networking > Network Segmentation > Network Domains



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

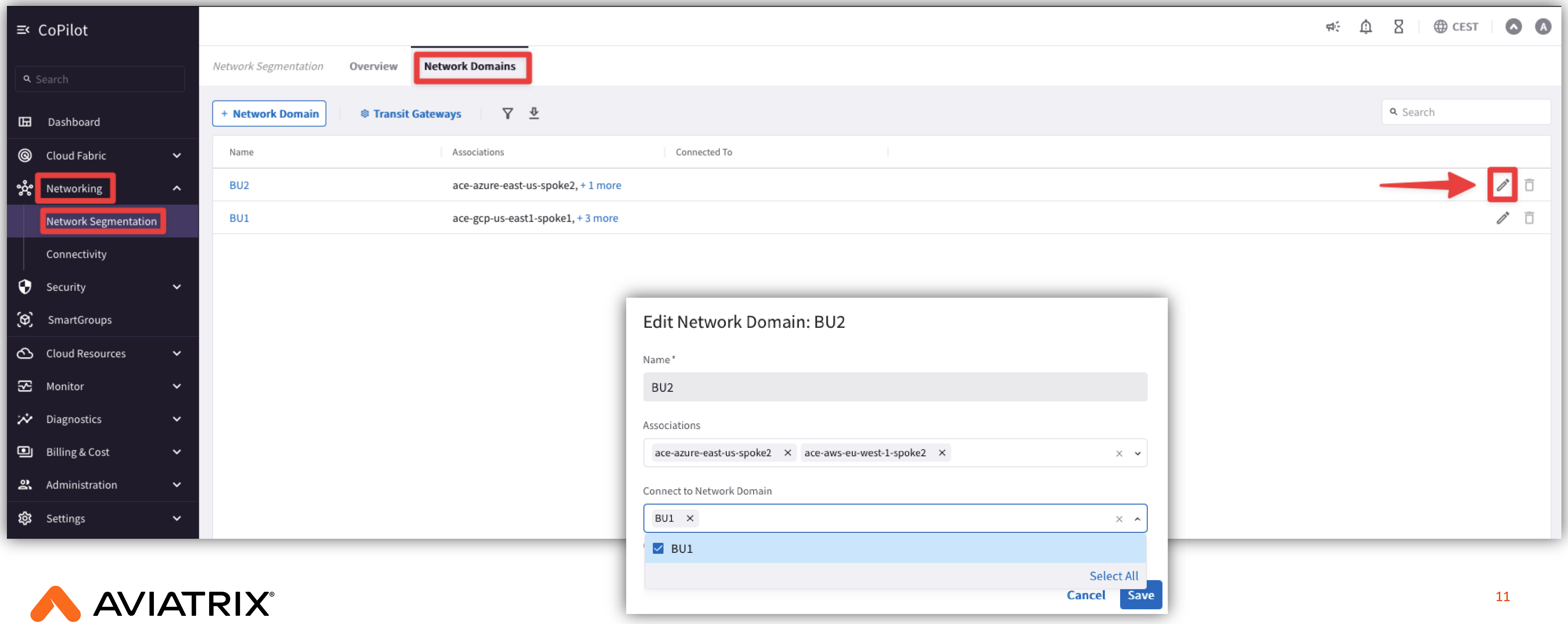
Name	Cloud	Region	IP Address Space	
ace-aws-eu-west-1-transit1	aws	eu-west-1	10.1.200.0/23	Enabled
ace-azure-east-us-transit1	arm	East US	192.168.200.0/23	Enabled
ace-gcp-us-east1-transit1	gcp	us-east1	172.16.200.0/23	Enabled

Total 3 Transit Gateways

Network Segmentation Visibility

- CoPilot: create/modify the Network Domains

PATH: COPILOT > Networking> Network Segmentation > Network Domains > pencil icon (edit)



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

Edit Network Domain: BU2

Name *: BU2

Associations: ace-azure-east-us-spoke2 ✕ ace-aws-eu-west-1-spoke2 ✕

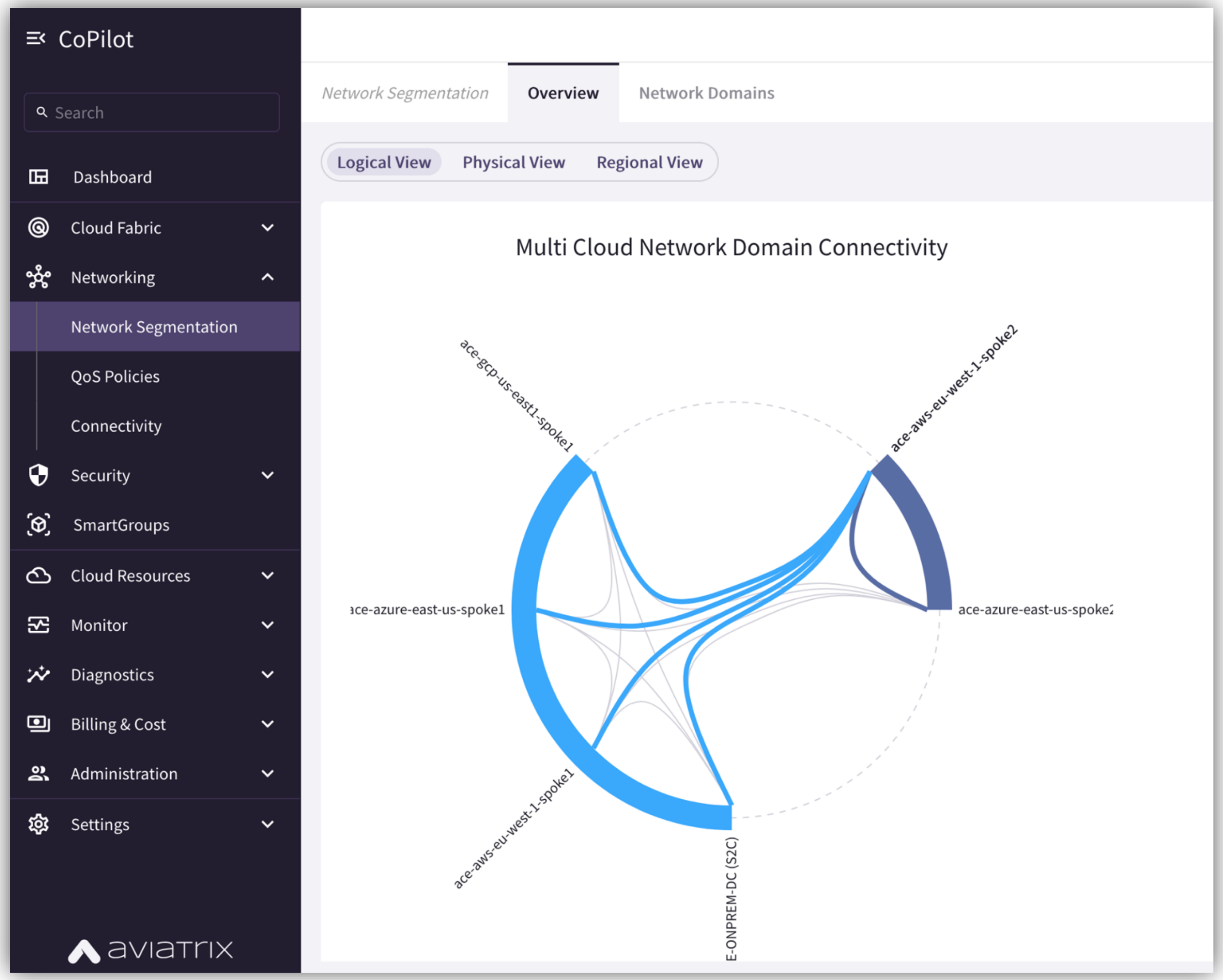
Connect to Network Domain: BU1 ✕

☑ BU1

Network Segmentation Visibility

- CoPilot: verify the Network Relationships

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



AVIATRIX
ACE
★★★
OPERATIONS
SPECIALTY

Next:
Lab 1 Network Domains
&
Lab 2 Connection Policy