AVIATRIX

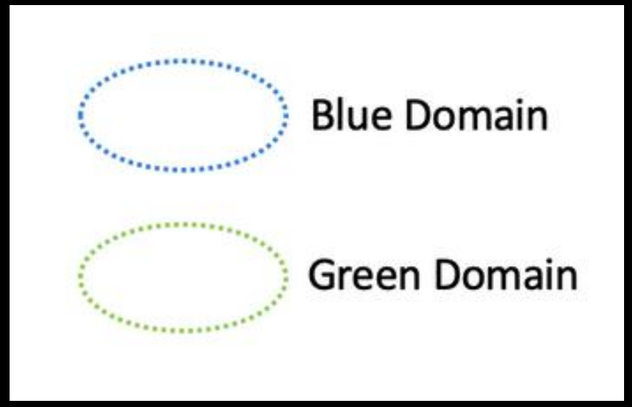
AVIATRIX ACE
AVIATRIX CERTIFIED ENGINEER

# Network Segmentation

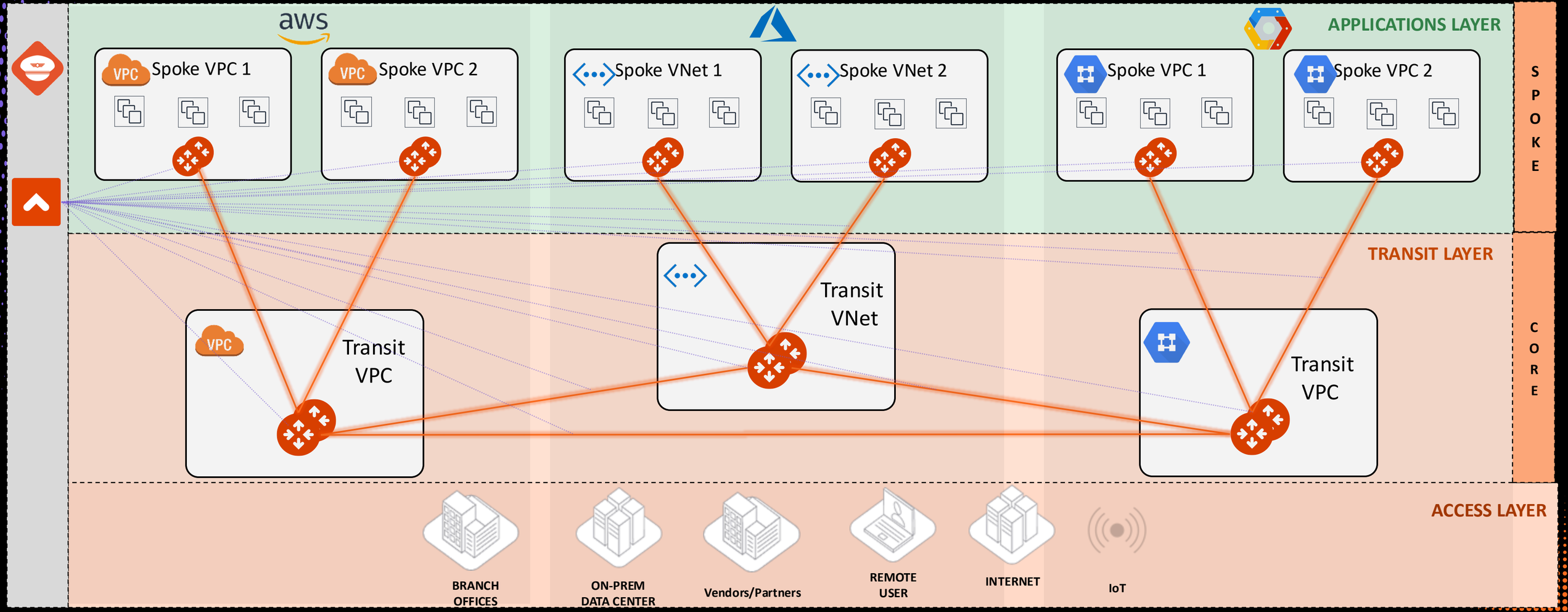

ACE Team

# Definition

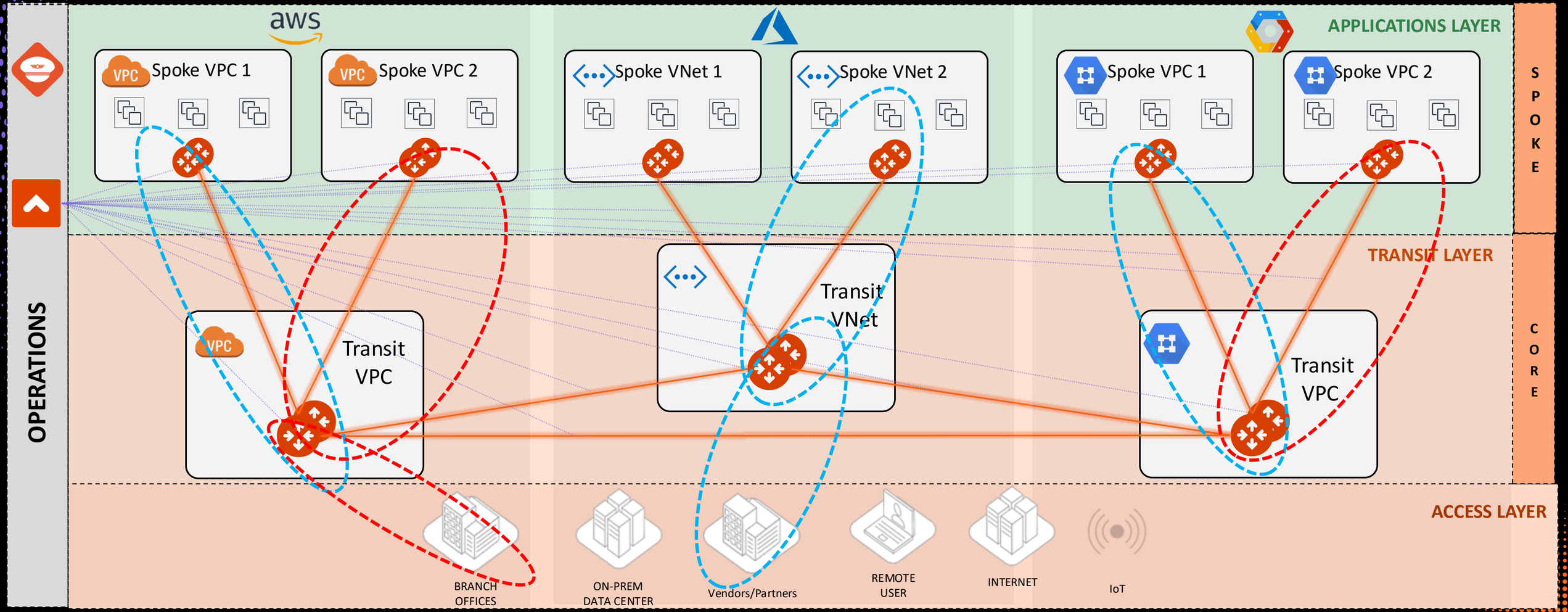
- When you identify groups of spoke and edge VPC/VNets in your infrastructure with the same requirements from a networking point of view (network reachability), you may want to group them in what Aviatrix calls “network domains”.
- A ***network domain*** is an Aviatrix enforced network of one or more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

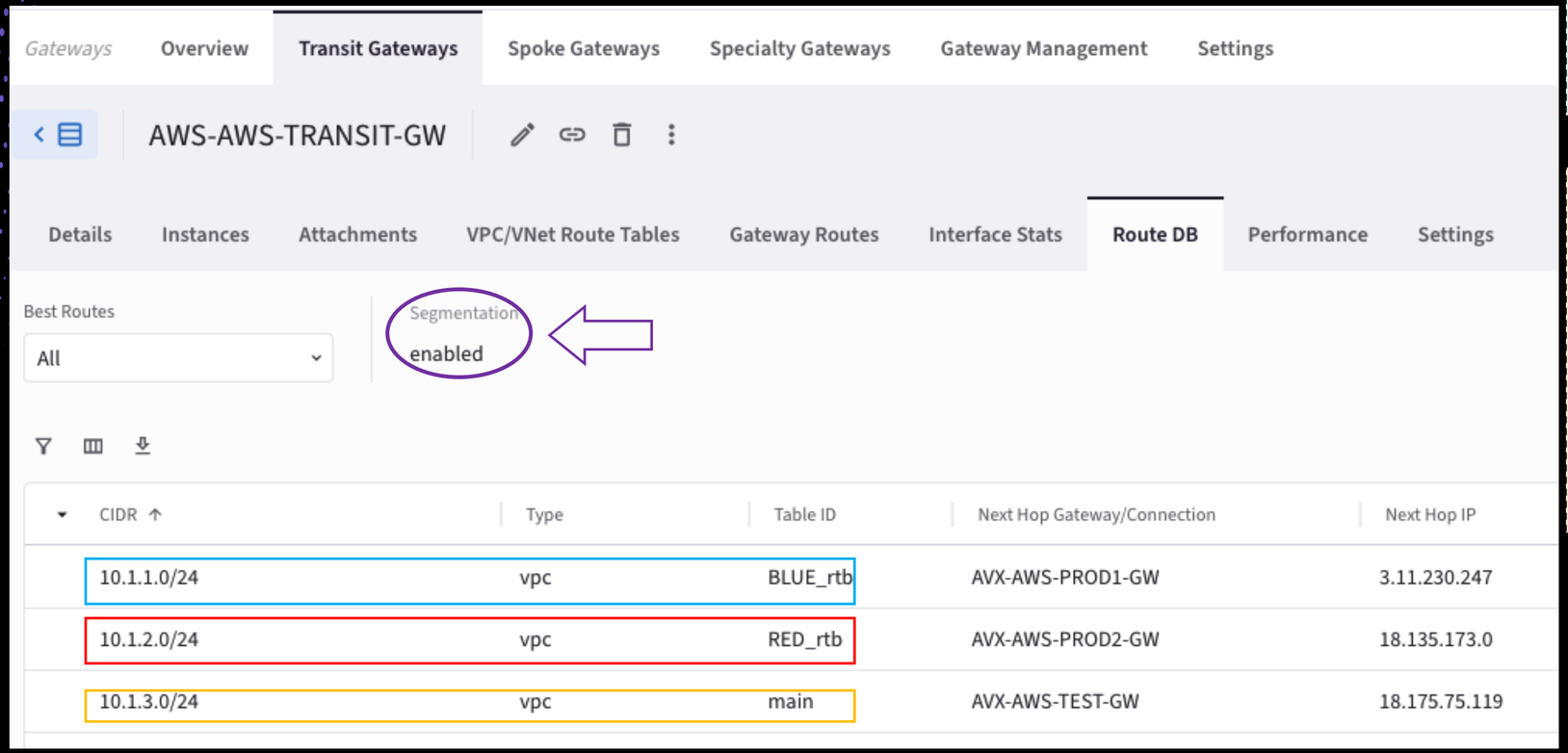


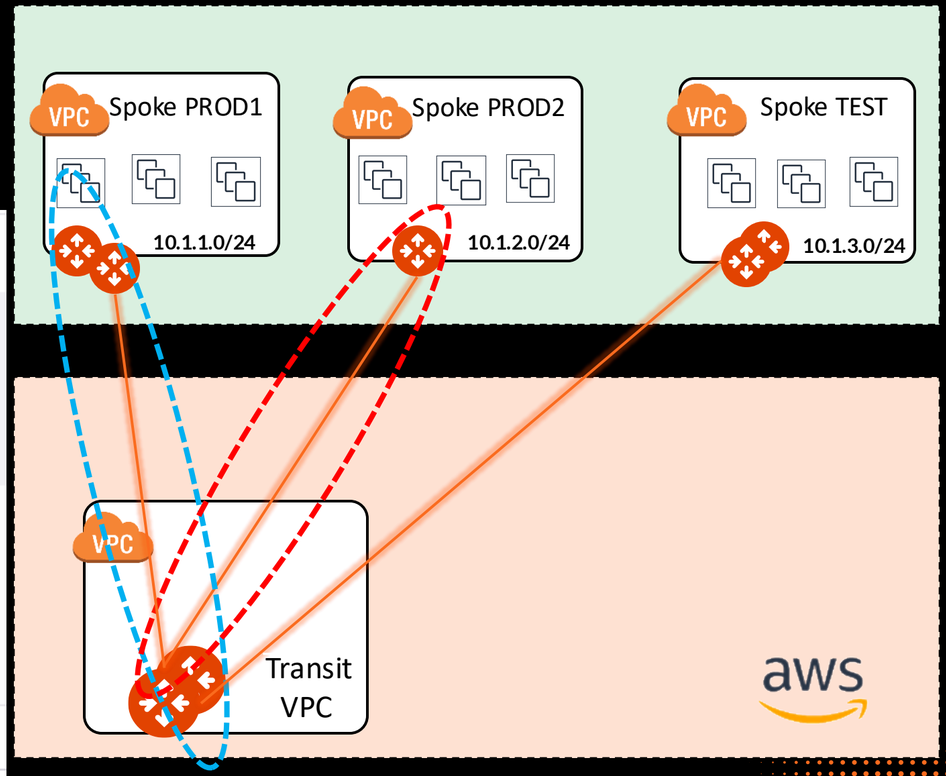
# Macro Segmentation with the Aviatrix Network Domains



# Network Segmentation: Order of operations

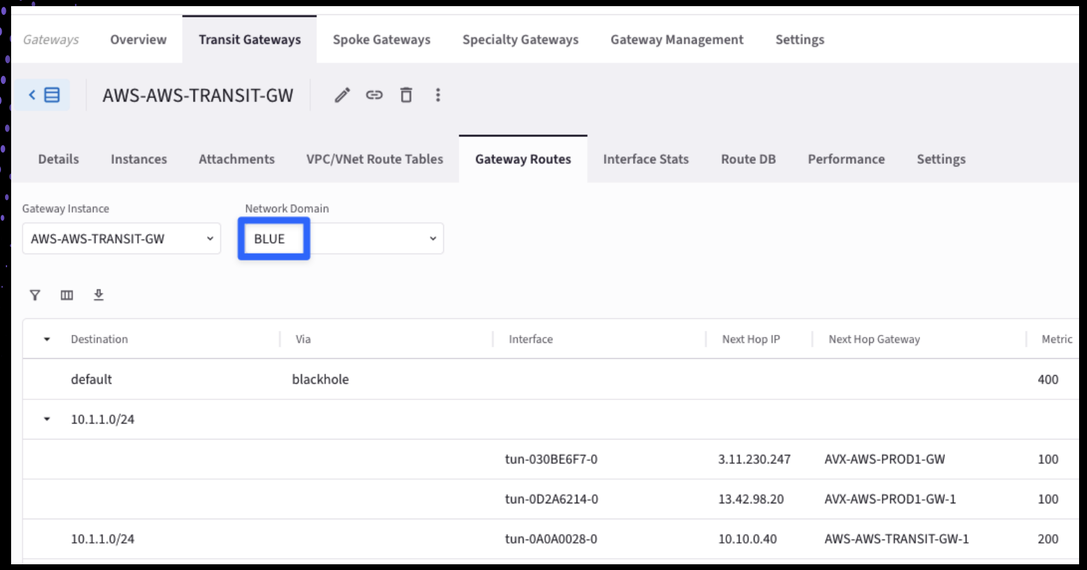
1) Enable Network Segmentation on the relevant Transit Gateway(s)
2) Create Network Domains (aka *Segments*)
3) Associate Spoke Gateways and/or Site2Cloud connections to the Network Domains
4) Apply the Connection Policy (*optional*)

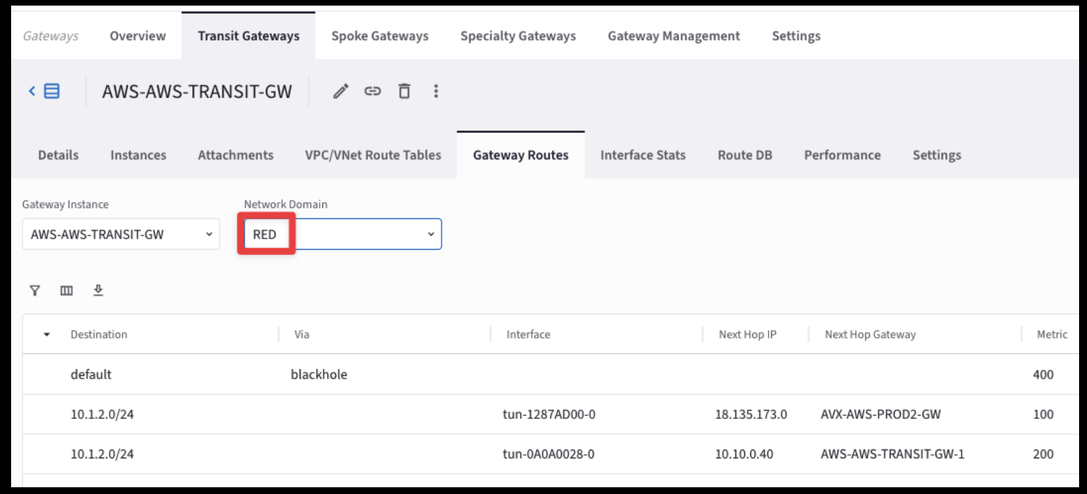


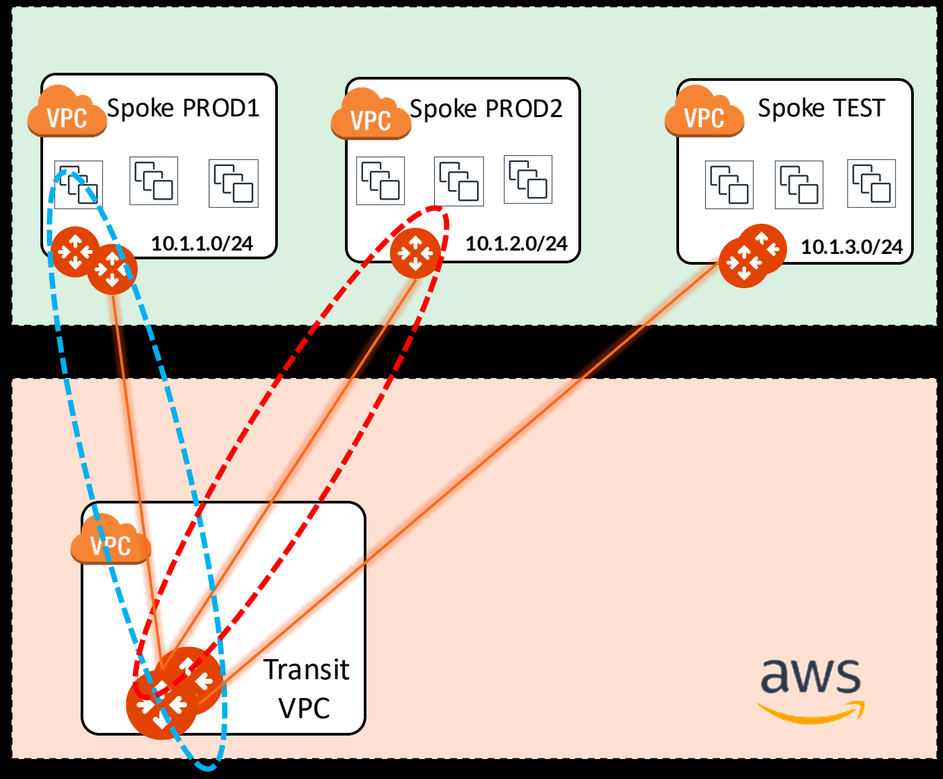




**PATH:** COPILOT > Cloud Fabric > Gateways > Transit Gateways > select the relevant GW > **Route DB** (equivalent of RIB)

# Multiple Routing Domains inside the CNSF




- 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)

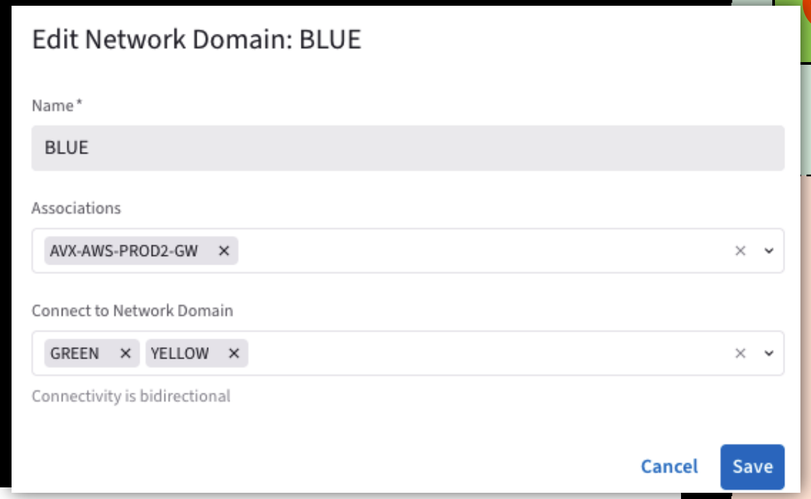
**CAVEAT:** The specific Network Domain view (aka vrf) is only available on the Transit GW. The Spoke GW has only the main routing table (aka GRT).

# Connection Policy (*optional*)

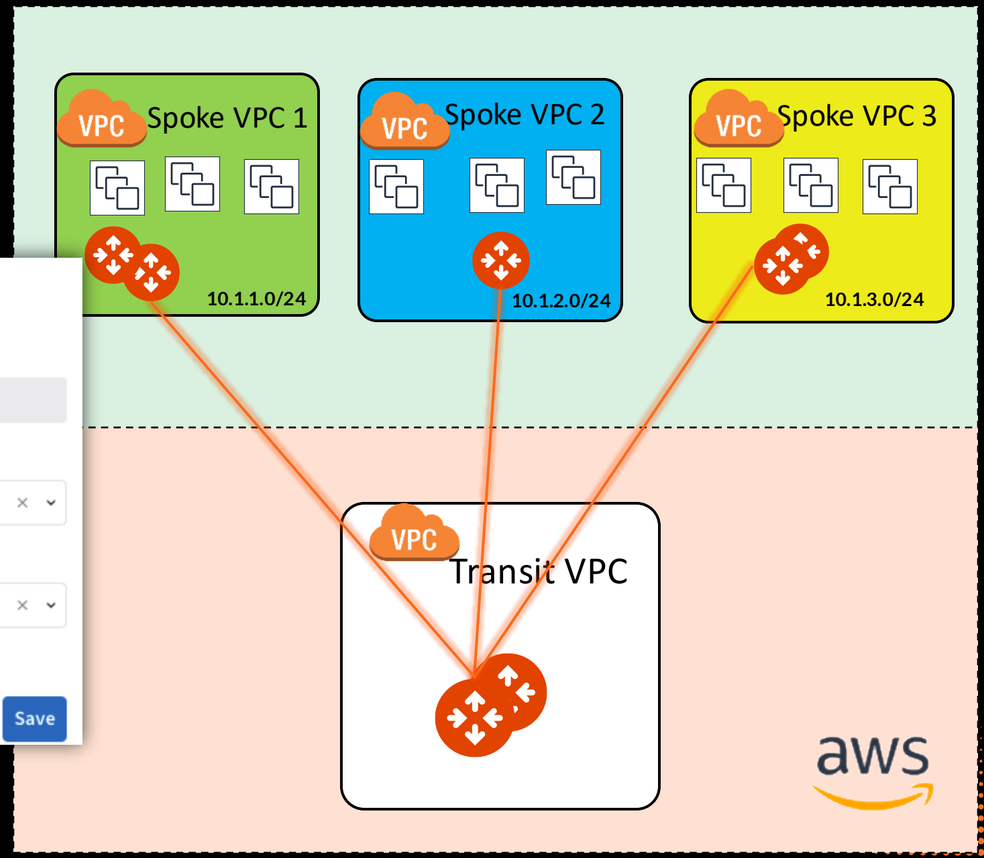
- The Connection policy allows the **inter-domain** communication or **inter-segment** communication (*vrf leaking*).
- The connection policy establishes a bidirectional connectivity (merging the network domains' RTBs).

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.




| 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*

**1**

**IDENTITY COMPROMISE**

Initial access through stolen credentials

**2**

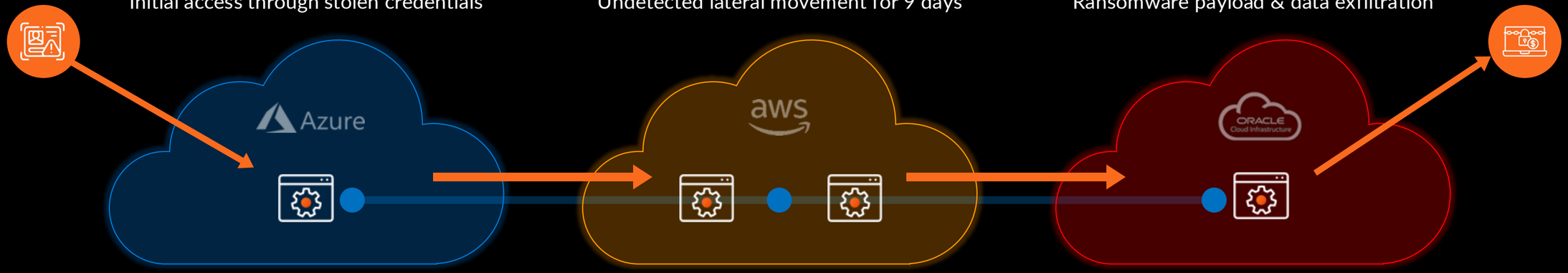
**LATERAL MOVEMENT**

Undetected lateral movement for 9 days

**3**

**TOTAL CHAOS**

Ransomware payload & data exfiltration

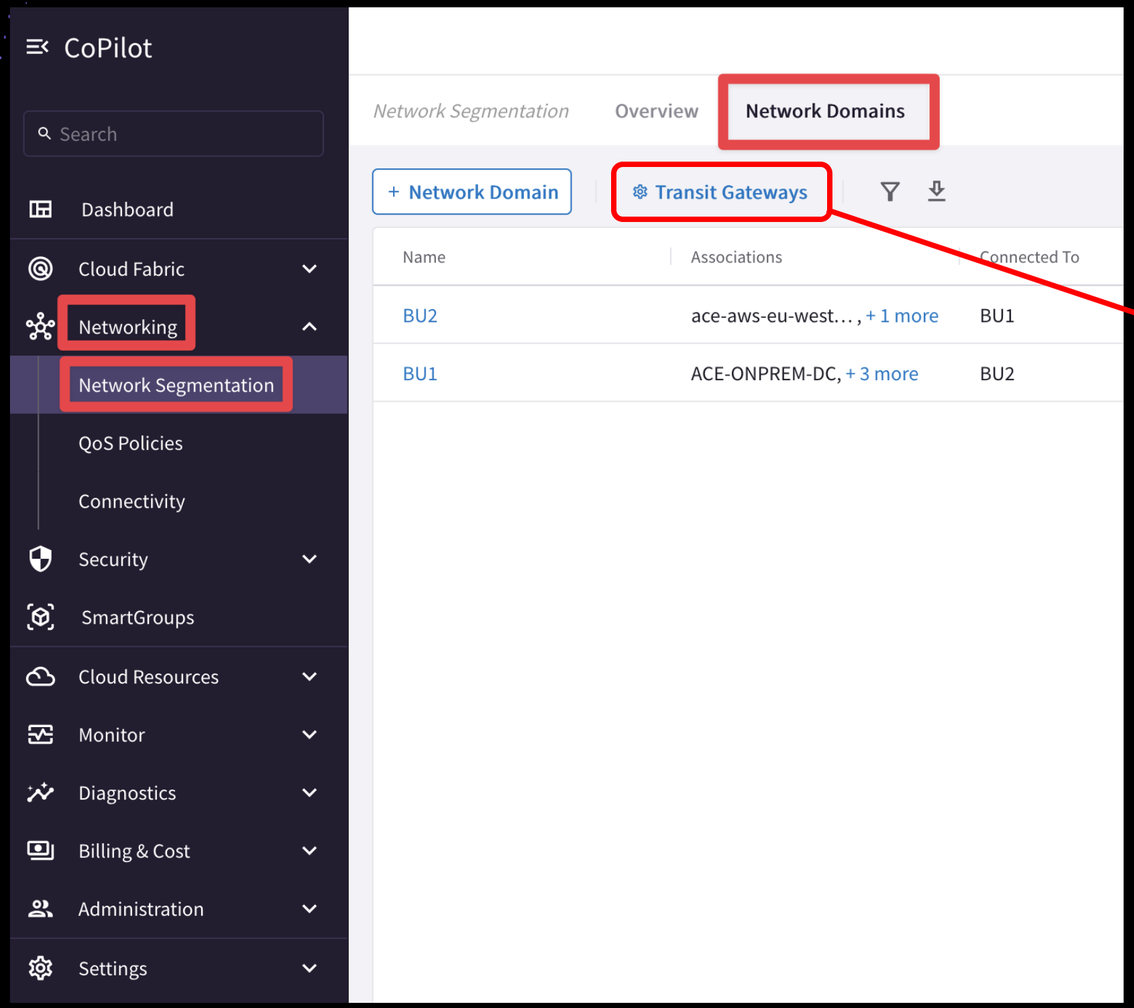


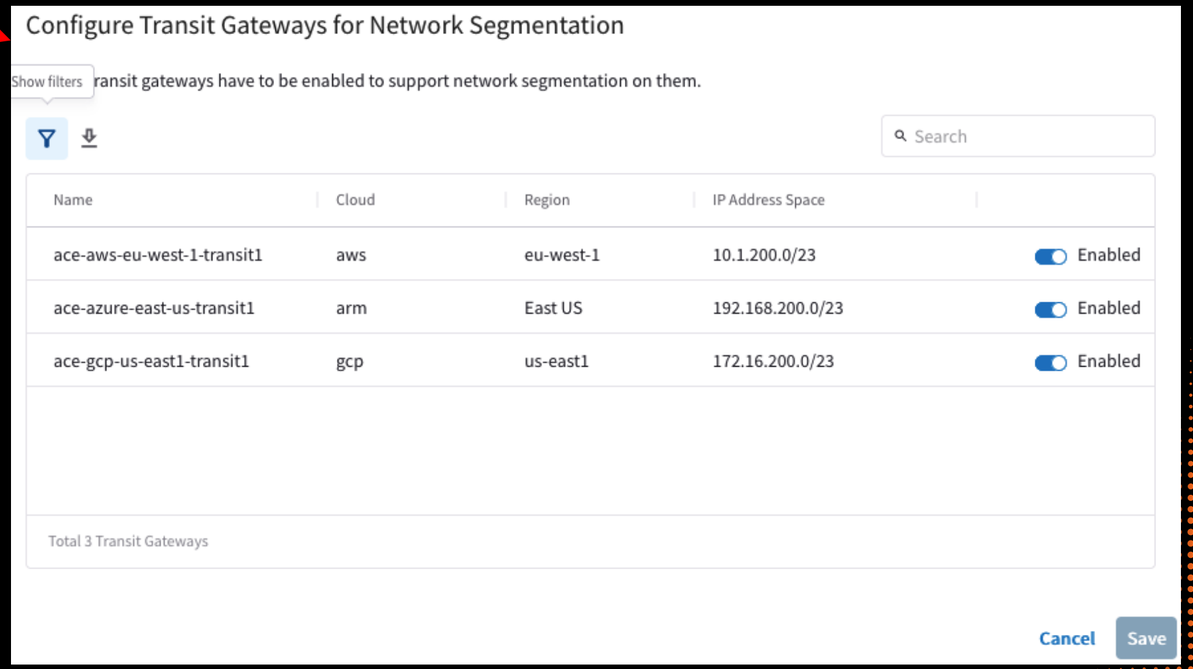
# Tools for Operating Network Segmentation

# Network Segmentation Configuration part.1

- CoPilot: Configure and enable the feature

**PATH:** COPILOT > Networking > Network Segmentation > Network Domains > Transit Gateways

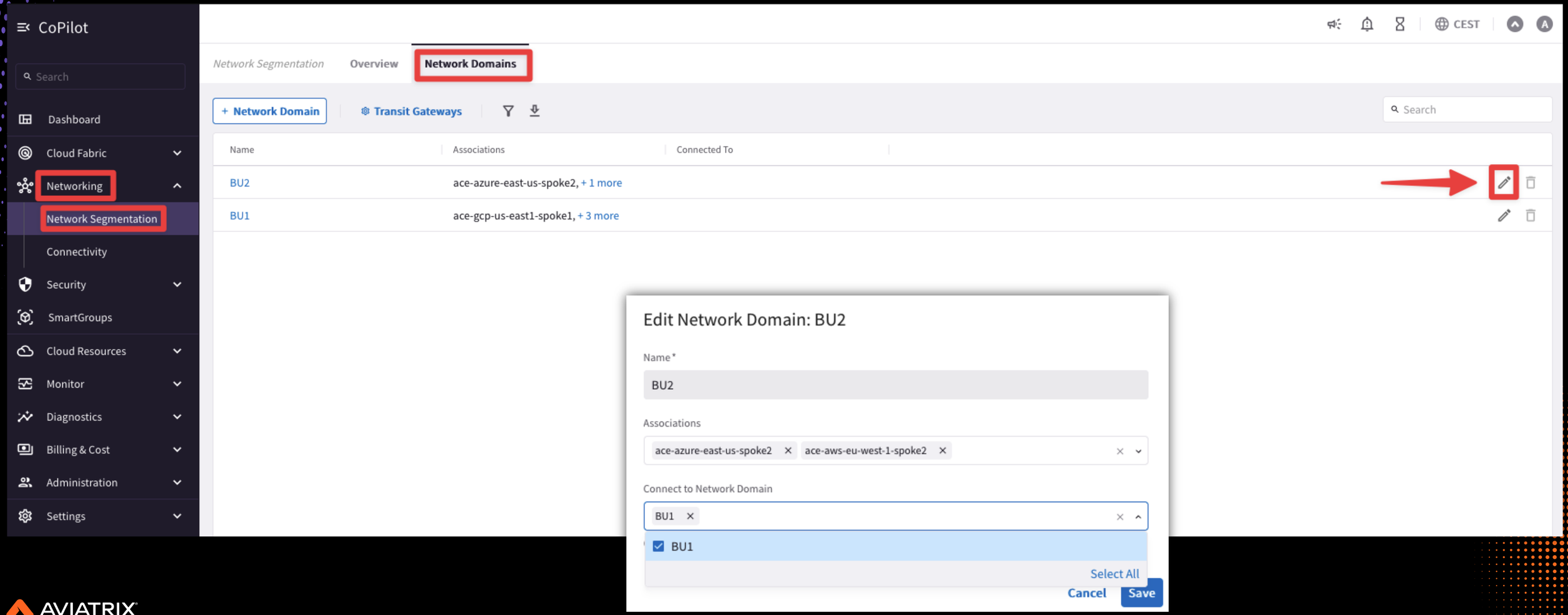


# Network Segmentation Configuration part.2

- CoPilot: create/modify the Network Domains

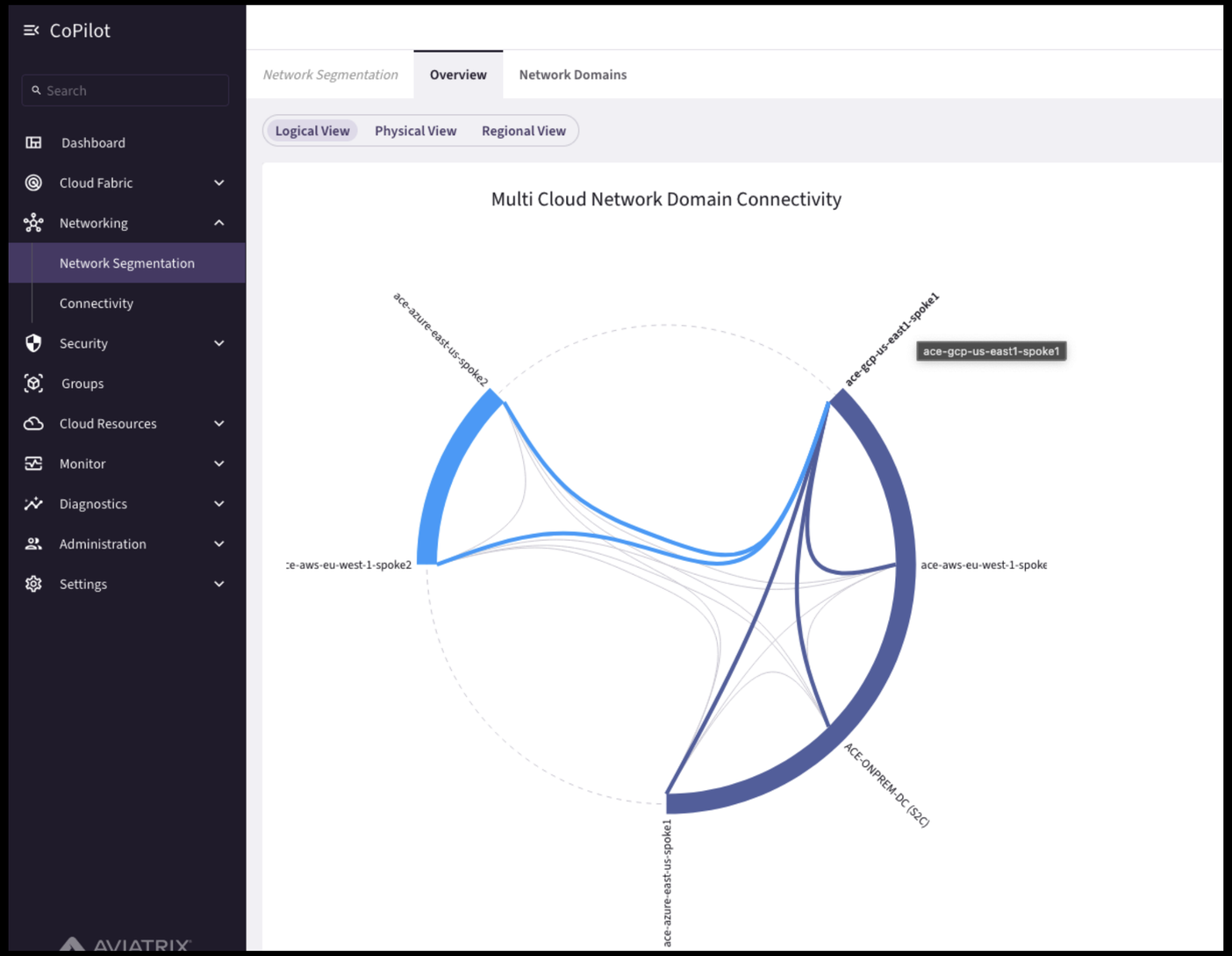
**PATH:** COPILOT > Networking> Network Segmentation > Network Domains > + Network Domain / pencil icon (*for editing an existing Segment*)



# 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