

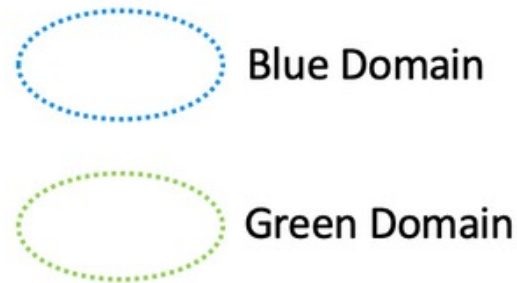


Network Segmentation

ACE Solutions Architecture Team

Network Segmentation - Overview

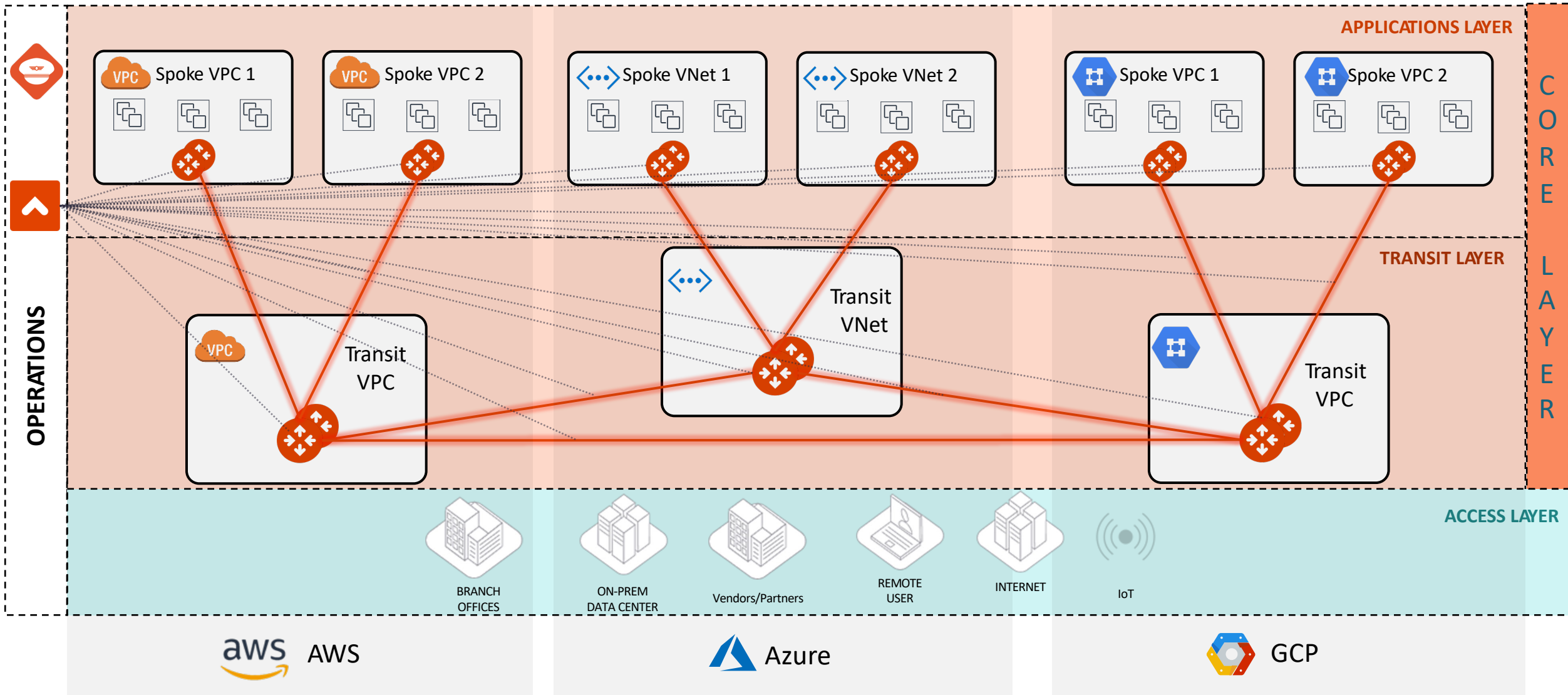
- When you identify groups of spoke and edge VPC/VNets in your infrastructure with the same requirements from a networking point of view (network reachability), you may want to group them in what Aviatrix calls “network domains”.
- A *network domain* is an Aviatrix enforced network of one or more spoke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



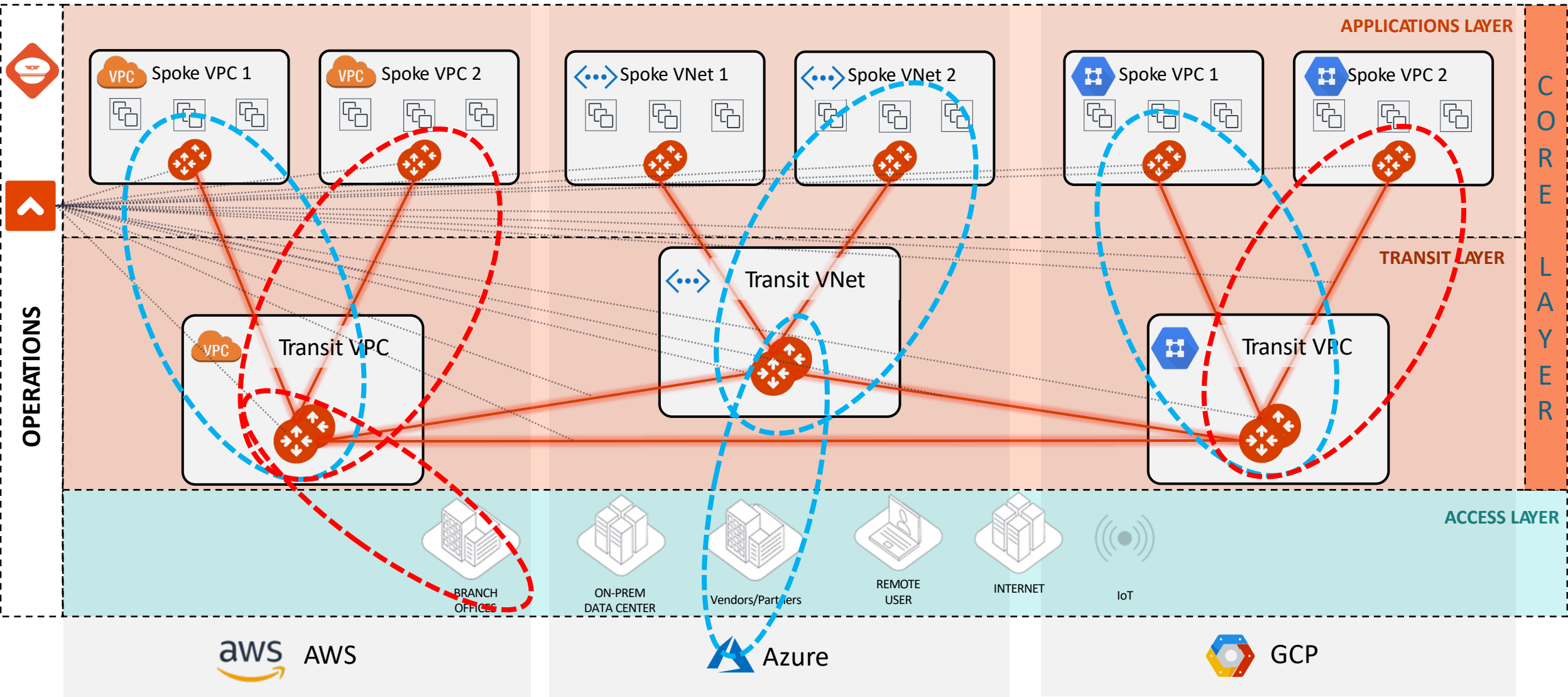
Implementing Network Segmentation in an Aviatrix-Managed Network (official documentation link):

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

MCNA Deployment: the Foundations



Global Segmentation with Network Domains

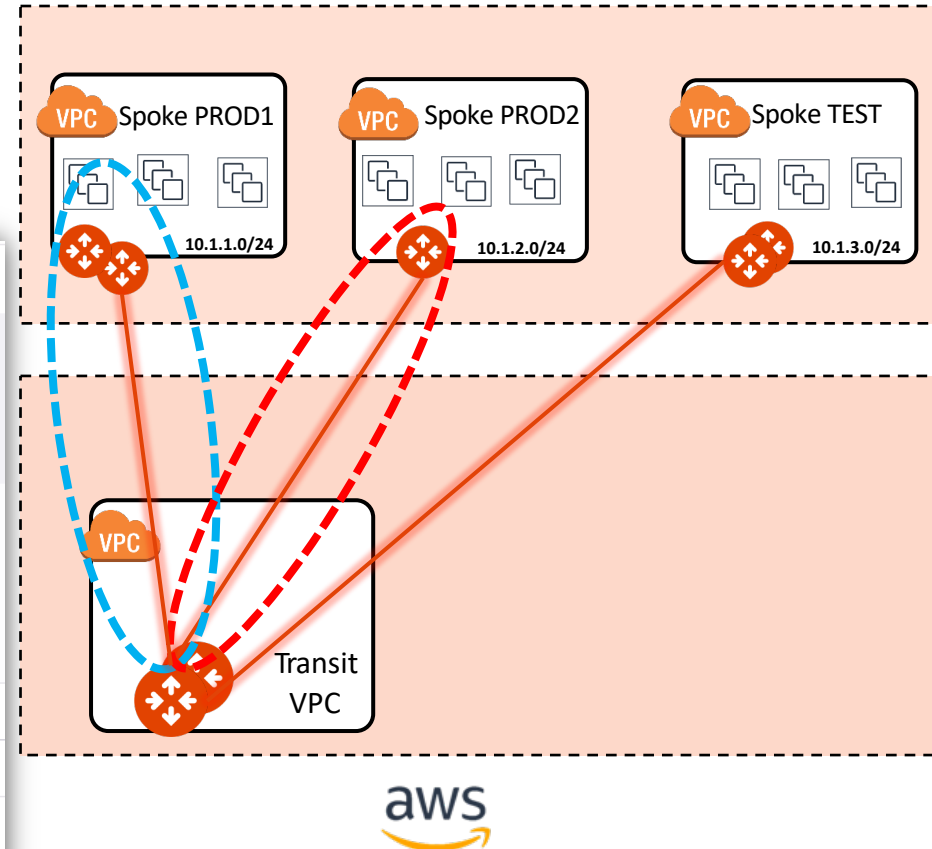


Order of Operations for activating the Network Segmentation

- 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*)

The screenshot shows the AWS Transit Gateway console for 'AVX-AWS-TRANSIT-GW'. The 'Route DB' tab is active, displaying a table of routes. A purple circle highlights the 'Segmentation enabled' toggle, with a purple arrow pointing to it from the right. The table below lists three routes:

CIDR	Type	Table ID	AS Path	AS Path Len	Metric	Next Hop Gateway/Connection
10.1.1.0/24	vpc	BLUE_rtb		0	50	AVX-AWS-SPOKE-GW-PROD1
10.1.2.0/24	vpc	RED_rtb		0	50	AVX-AWS-SPOKE-GW-PROD2
10.1.3.0/24	vpc	main		0	50	AVX-AWS-SPOKE-GW-TEST



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

Multiple Routing Domains on the Transit GW

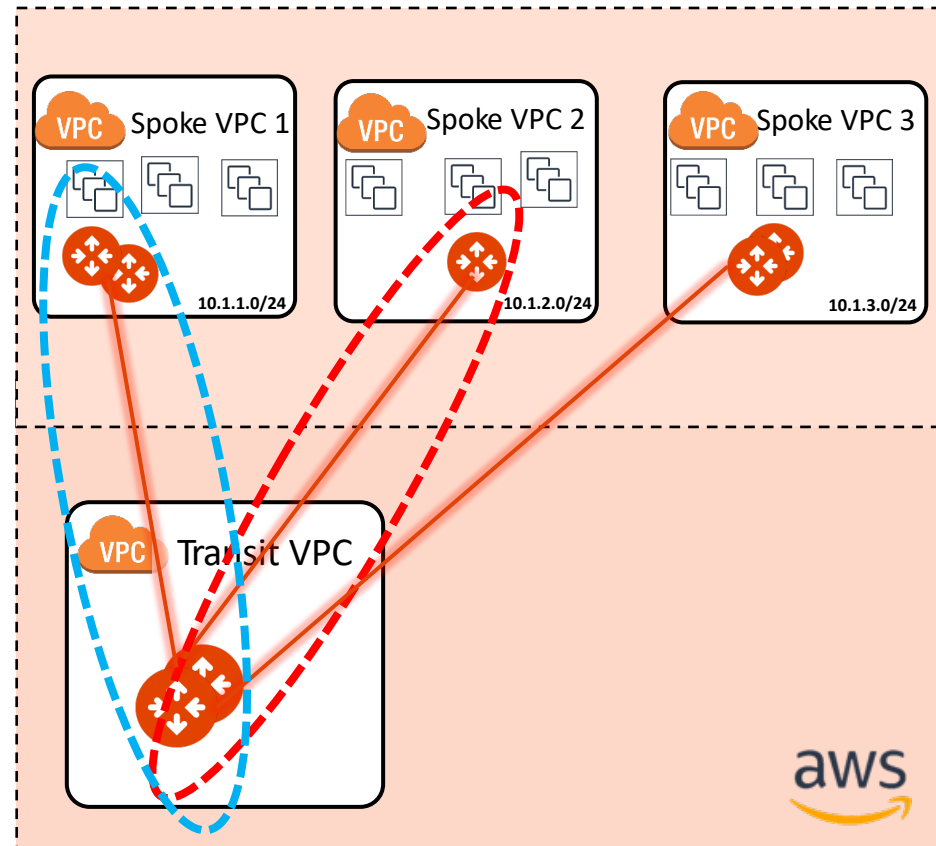


Gateway Instance: AVX-AWS-TRANSIT-GW, Network Domain: BLUE

Destination	Via	Interface	Next Hop IP	Next Hop Gateway	Metric
default	blackhole				400
10.1.1.0/24		tun-034790D0-0	3.71.144.208	AVX-AWS-SPOKE-GW-PROD1	100
		tun-129D3D38-0	18.157.61.56	AVX-AWS-SPOKE-GW-PROD1-1	100
10.1.1.0/24		tun-0A0B0068-0	10.11.0.104	AVX-AWS-TRANSIT-GW-1	200

Gateway Instance: AVX-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-0349032B-0	3.73.3.43	AVX-AWS-SPOKE-GW-PROD2	100
10.1.2.0/24		tun-0A0B0068-0	10.11.0.104	AVX-AWS-TRANSIT-GW-1	200

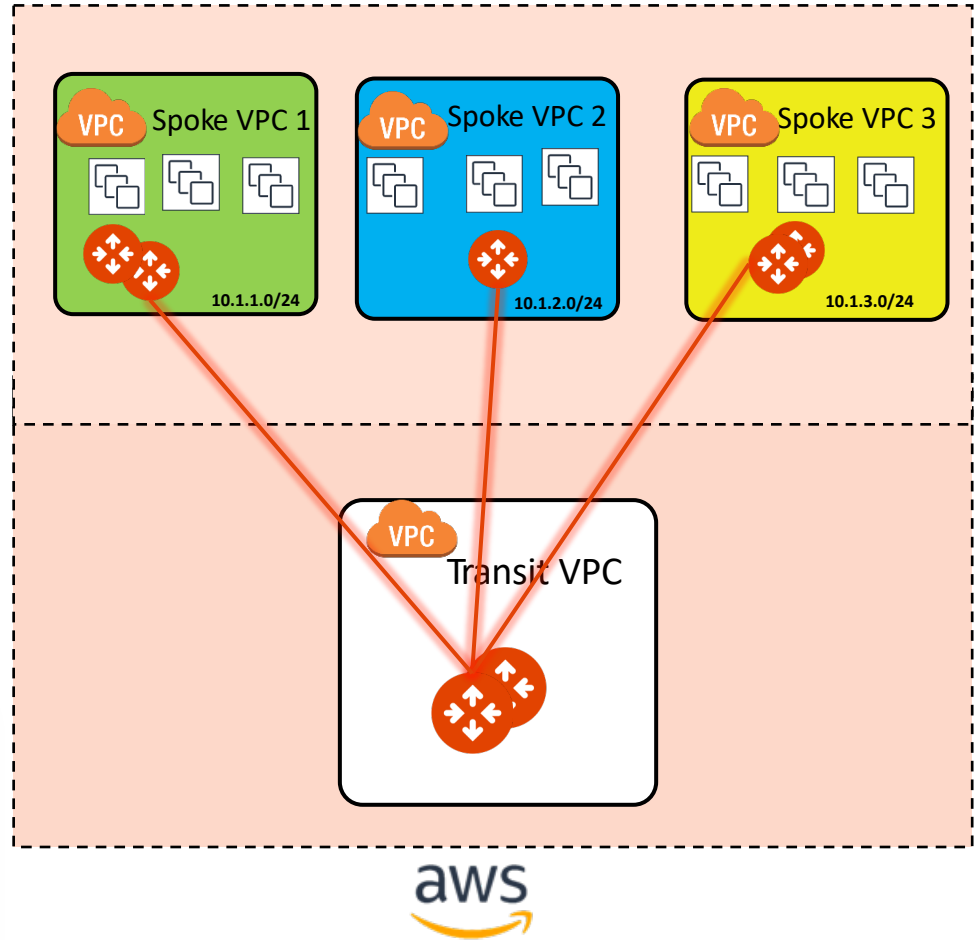


- A single Spoke gateway or a Cluster of Spoke Gateways can be associated to a unique domain!
- **PATH:** COPILOT > Cloud Fabric > Gateways > Transit Gateways > select the relevant GW > **Gateway Routes** and then filter based on the network domain (i.e. VRF)

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 (is akin to the *vrf leaking* from the MPLS technology).
- 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).

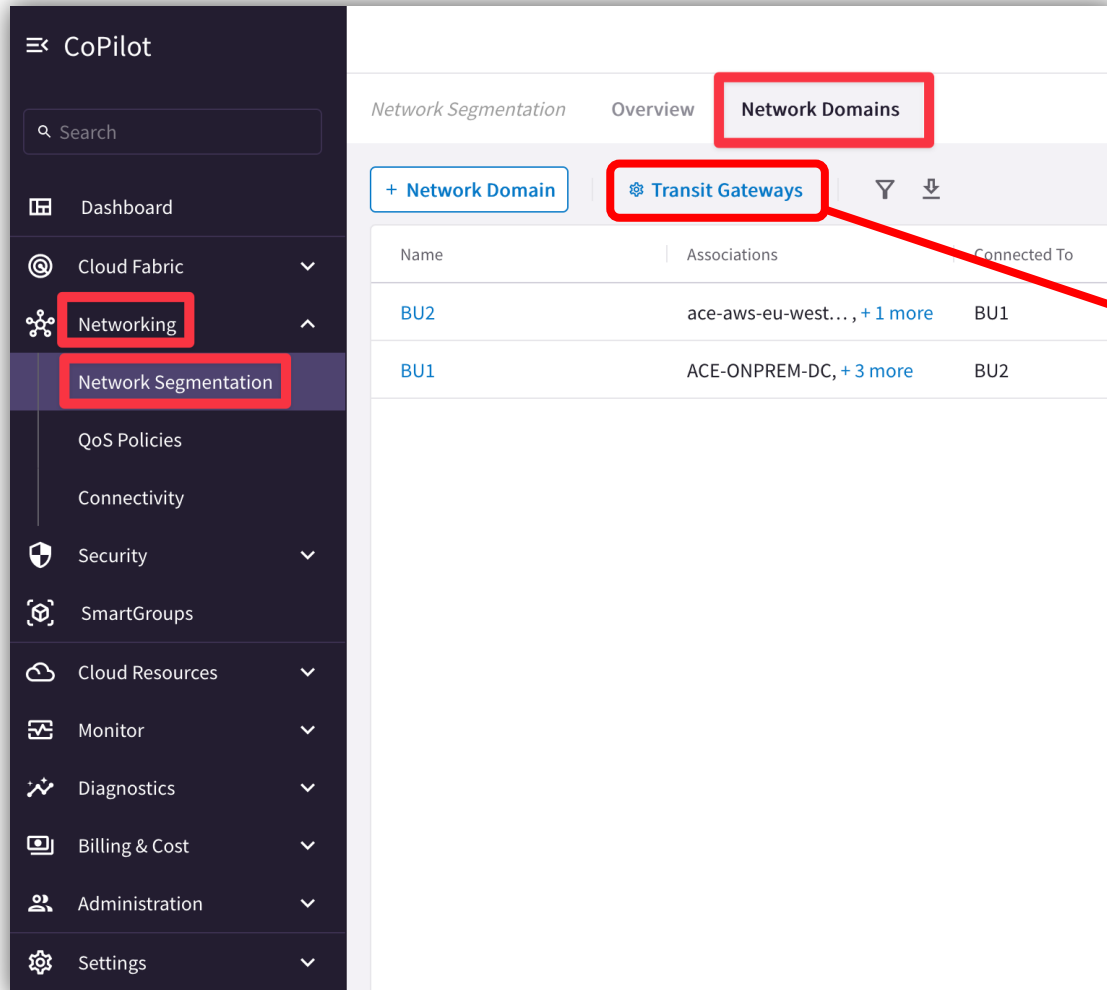


Tools for Operating Network Segmentation

Network Segmentation Visibility

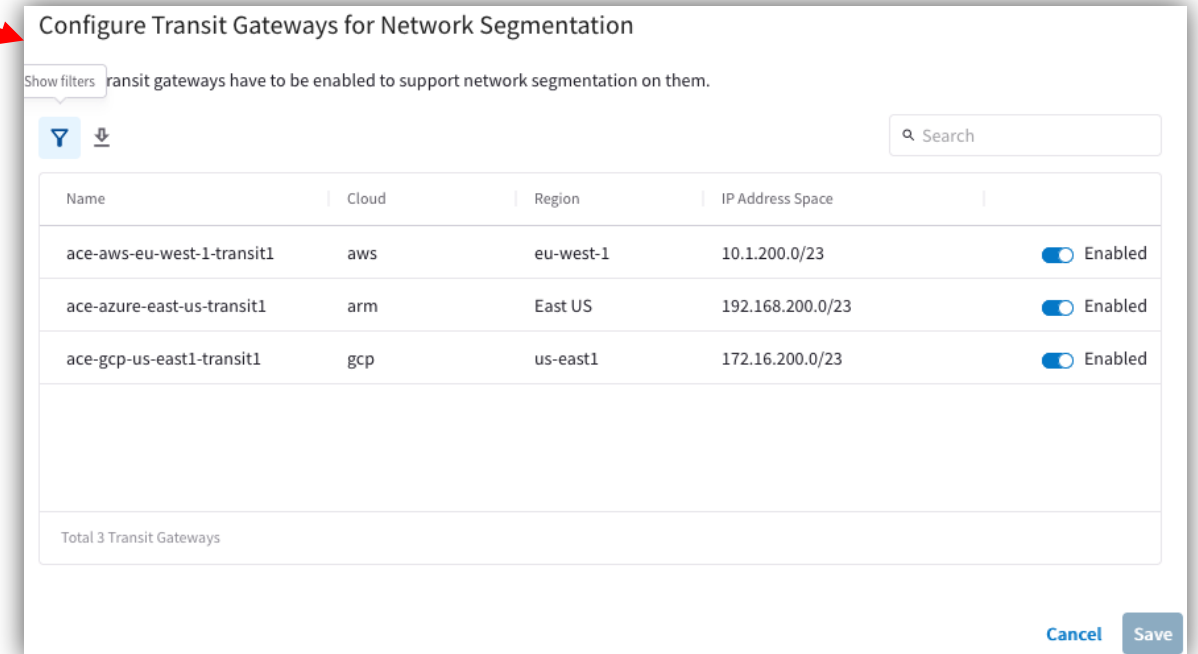
- CoPilot: verify the Network Domains

PATH: COPILOT > Networking > Network Segmentation > Network Domains



The screenshot shows the Aviatrix CoPilot interface. The left sidebar contains a navigation menu with the following items: Dashboard, Cloud Fabric, Networking, Network Segmentation, QoS Policies, Connectivity, Security, SmartGroups, Cloud Resources, Monitor, Diagnostics, Billing & Cost, Administration, and Settings. The 'Networking' and 'Network Segmentation' items are highlighted with red boxes. The main content area shows the 'Network Segmentation' overview with tabs for 'Overview' and 'Network Domains'. The 'Network Domains' tab is selected and highlighted with a red box. Below the tabs, there is a '+ Network Domain' button and a 'Transit Gateways' button, both highlighted with red boxes. A red arrow points from the 'Transit Gateways' button to the right-hand screenshot.

Name	Associations	Connected To
BU2	ace-aws-eu-west-1-transit1, + 1 more	BU1
BU1	ACE-ONPREM-DC, + 3 more	BU2



The screenshot shows the 'Configure Transit Gateways for Network Segmentation' dialog box. It features a search bar and a table of transit gateways. The table has columns for Name, Cloud, Region, IP Address Space, and a status toggle. All three gateways shown are 'Enabled'. A red arrow from the previous screenshot points to the top of this dialog box.

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

Name	Cloud	Region	IP Address Space	Status
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





Cancel Save

Network Segmentation Visibility

- CoPilot: create/modify the Network Domains

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

The screenshot displays the Aviatrix CoPilot interface. On the left is a dark sidebar with navigation options: CoPilot, Search, 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 content area shows the 'Network Segmentation' section with tabs for 'Overview' and 'Network Domains' (the latter is highlighted with a red box). Below the tabs is a '+ Network Domain' button and a 'Transit Gateways' filter. 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		 

A red arrow points to the edit icon for the BU2 domain. An 'Edit Network Domain: BU2' dialog box is open, showing the following fields:

- Name*: BU2
- Associations: ace-azure-east-us-spoke2 x ace-aws-eu-west-1-spoke2 x
- Connect to Network Domain: BU1 x
- Selected domains: BU1

Buttons at the bottom of the dialog include 'Select All', 'Cancel', and 'Save'.

Network Segmentation Visibility

- CoPilot: verify the Network Relationships

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

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, Network Segmentation (highlighted), QoS Policies, Connectivity, Security, SmartGroups, Cloud Resources, Monitor, Diagnostics, Billing & Cost, Administration, and Settings. The main content area shows the 'Network Segmentation Overview' page with tabs for 'Logical View', 'Physical View', and 'Regional View'. The 'Logical View' is active, showing a diagram titled 'Multi Cloud Network Domain Connectivity'. The diagram features a central spine labeled 'E-ONPREM-DC (S2C)' and several cloud spokes: 'ace-gcp-us-east1-spoke1', 'ace-aws-eu-west-1-spoke2', 'ace-azure-east-us-spoke1', and 'ace-azure-east-us-spoke2'. Blue lines represent network connections between these domains.



Next:
Lab 1 Network Domains
&
Lab 2 Connection Policy