



---

# Network Segmentation

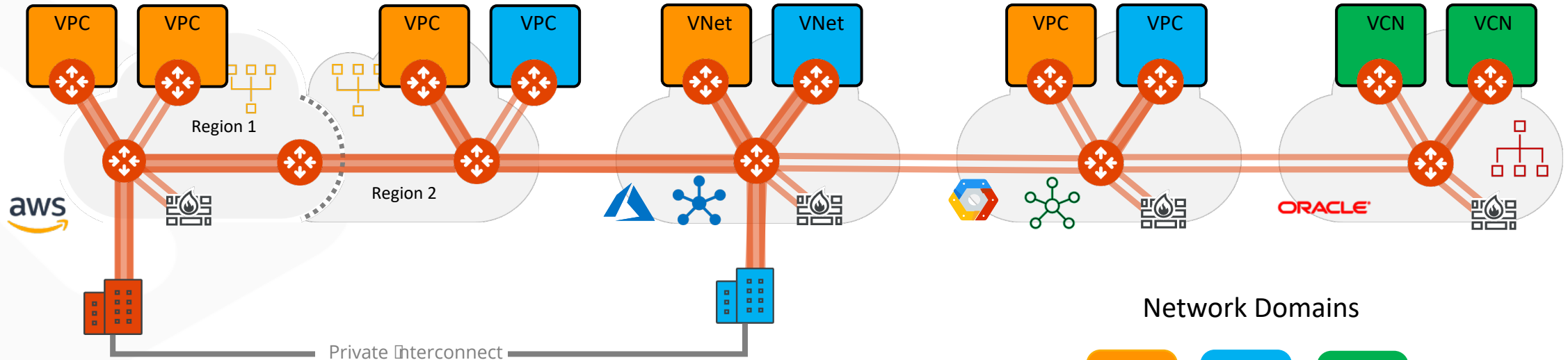
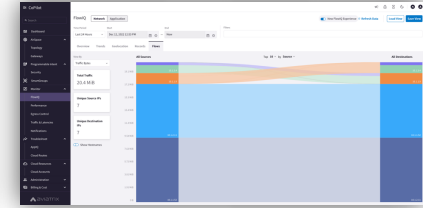
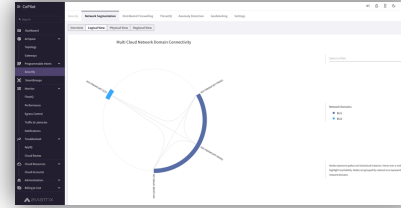
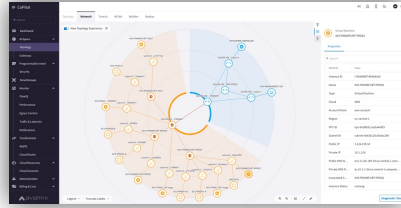
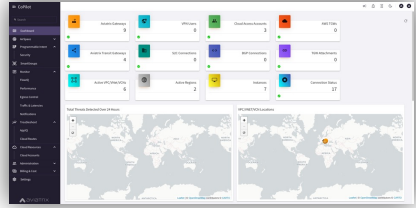
# Segmentation

---

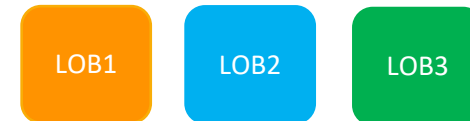
- Enables ZTNA across multi-region and multicloud, including on-premises environment
- Group VNets/VPCs/VCNs/Apps with similar security policies
- Define your own domains
- Use Cases
  - Compliance
  - Governance
  - Audits

# Multicloud Network Segmentation

Aviatrix  
CoPilot



Network Domains



# Multicloud Network Segmentation

## Policy Based Network Segmentation

- Global
- Consistent / Repeatable
- Across accounts, subscriptions & projects

## Cloud and Connection Agnostic

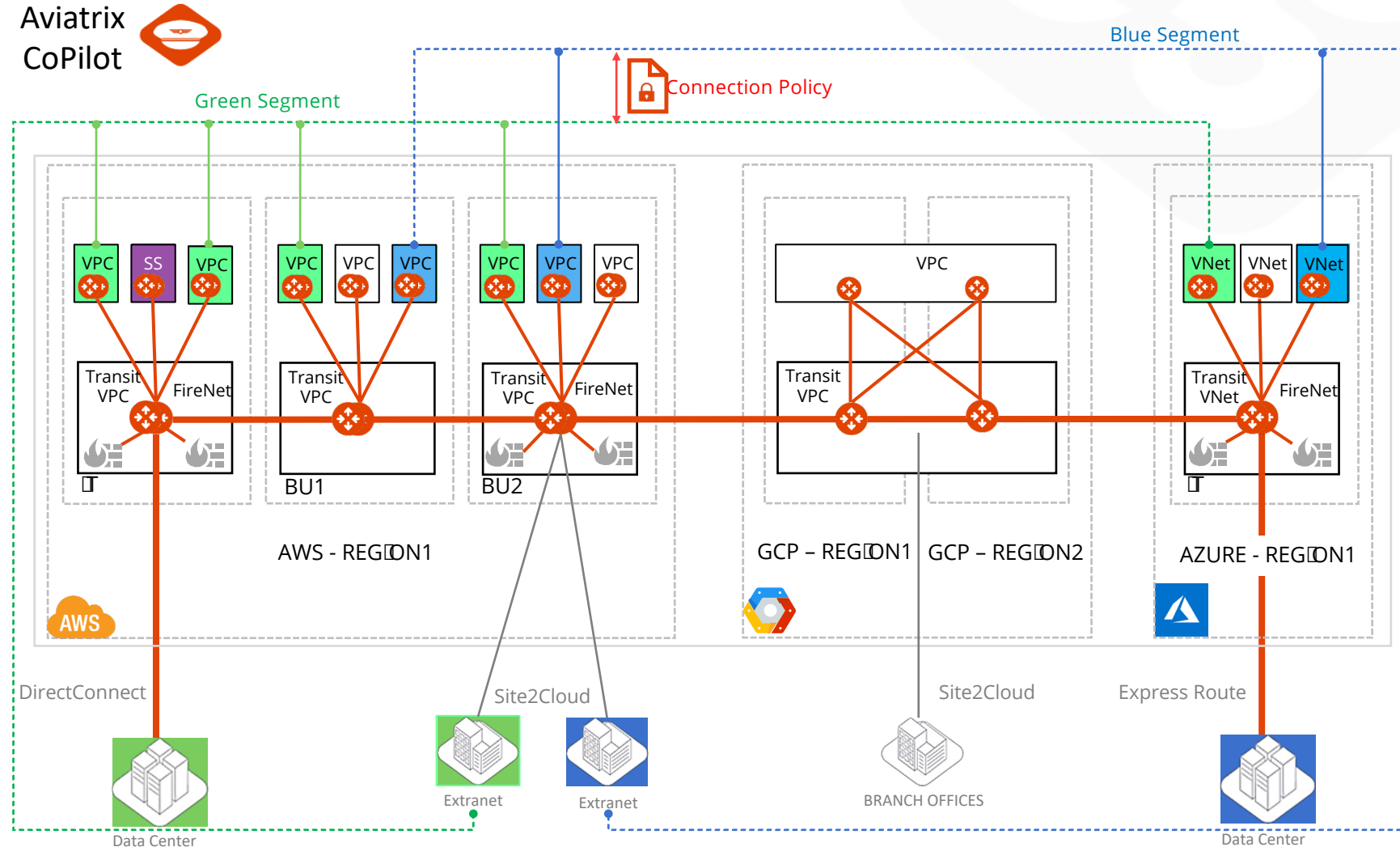
- Single cloud
- Intra-region or inter-region
- Multiple clouds

## Edge/Access Segmentation

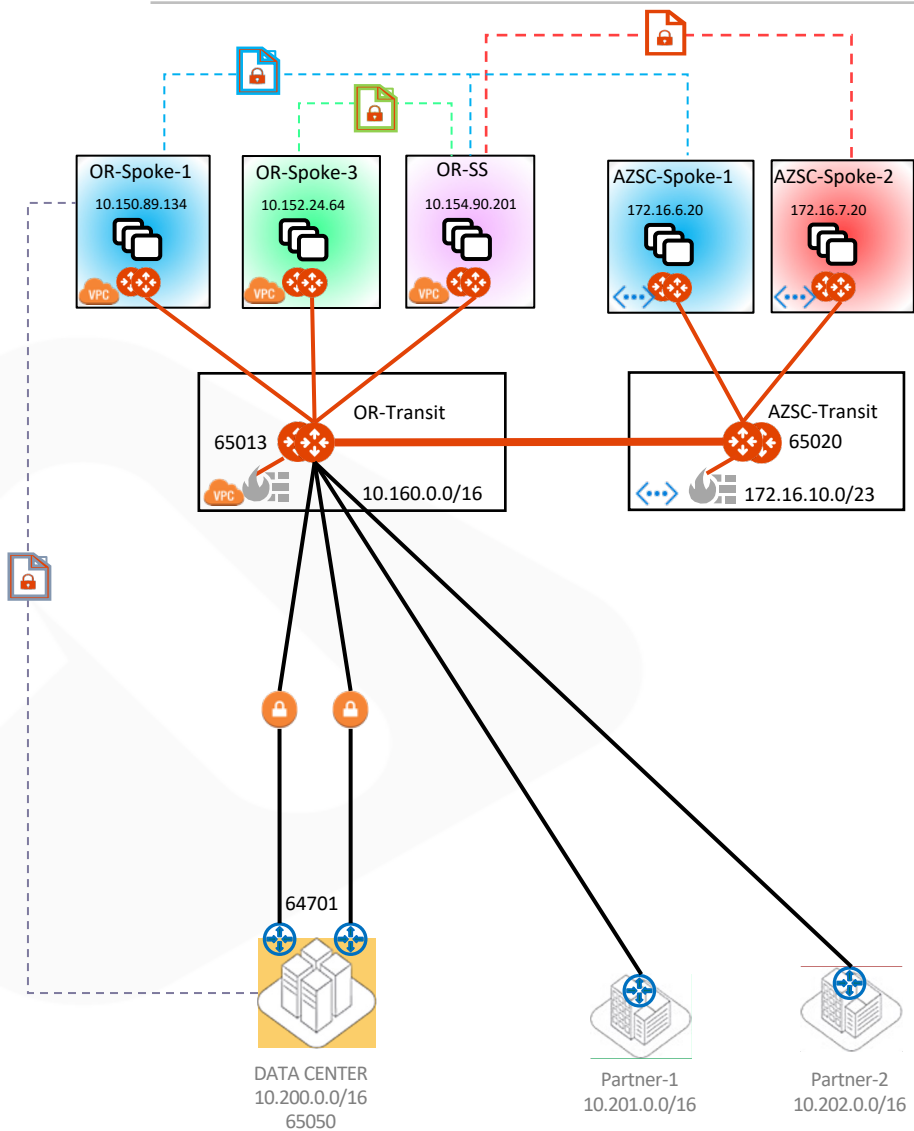
- On-Prem DCs
- Branches
- Extranets
- Cloud Peering

## On-Demand Compliance/Governance

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



# Multicloud Network Segmentation



Name: AZSC-Spoke1-AGW

DESTINATION	VIA	DEV	NEXTHOP IP	NEXTHOP GATEWAY
default	172.16.6.65	eth0		
10.154.0.0/16		tun-AC100A44-0	172.16.10.68	AZSC-Transit-AGW
10.150.0.0/16		tun-AC100A44-0	172.16.10.68	AZSC-Transit-AGW
10.200.0.0/16		tun-AC100A44-0	172.16.10.68	AZSC-Transit-AGW
172.16.6.0/24	172.16.6.65	eth0		
172.16.6.64/26		eth0		
172.16.6.132		tun-3499E255-0	52.153.226.85	AZSC-Spoke1-AGW-hagw

Purple

Remote-Blue

Yellow

Local-Blue

# Configuration – CoPilot

## 1. Enable Transit Gateway for Segmentation

The screenshot displays the Aviatrix CoPilot interface. On the left is a dark sidebar with a menu. The 'Networking' and 'Network Segmentation' items are highlighted with red boxes. The main panel shows the 'Network Domains' tab, with the 'Transit Gateways' sub-tab also highlighted with a red box. A modal window titled 'Configure Transit Gateways for Network Segmentation' is open in the foreground. It contains a table with four transit gateways. The first gateway, 'aws-us-east1-transit', has its toggle switch set to 'Disabled'. The other three gateways ('aws-us-east2-transit', 'azure-us-west-transit', and 'gcp-us-central1-transit') have their toggle switches set to 'Enabled'. These three 'Enabled' toggle switches are grouped together and highlighted with a red box. At the bottom of the modal are 'Cancel' and 'Save' buttons.

**CoPilot**

Search

Dashboard

Cloud Fabric

**Networking**

**Network Segmentation**

Connectivity

Security

SmartGroups

Cloud Resources

Monitor

Diagnostics

Billing & Cost

Administration

Settings

Network Segmentation Overview **Network Domains**

+ Network Domain **Transit Gateways**

Name

Blue

Green

### Configure Transit Gateways for Network Segmentation

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

Search

Name	Cloud	Region	IP Address Space	
aws-us-east1-transit	aws	us-east-1	10.0.20.0/23	<input type="checkbox"/> Disabled
aws-us-east2-transit	aws	us-east-2	10.0.10.0/23	<input checked="" type="checkbox"/> Enabled
azure-us-west-transit	arm	West US	192.168.10.0/23	<input checked="" type="checkbox"/> Enabled
gcp-us-central1-transit	gcp	us-central1	172.16.10.0/24,172.16.11.0/2...	<input checked="" type="checkbox"/> Enabled

Total 4 Transit Gateways

Cancel Save

# Configuration – CoPilot

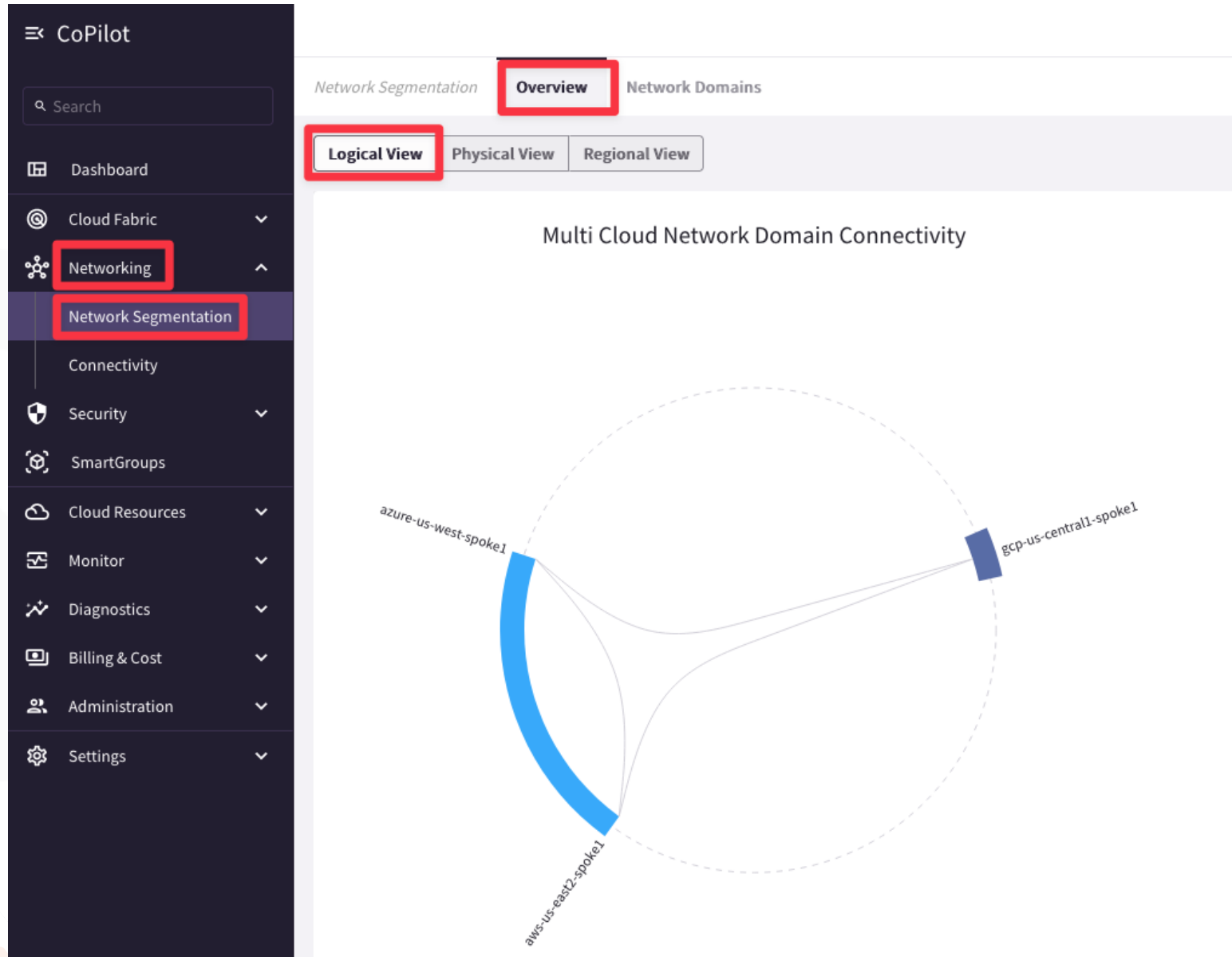
2. Create Network Domains
3. Associate Spoke Gateways or Site2Cloud connections to Segments
4. (Optional) Create Connection Policy

The screenshot shows the CoPilot interface with the following elements highlighted by red boxes:

- Left Sidebar:**
  - CoPilot** (header)
  - Search** (input field)
  - Dashboard** (icon)
  - Cloud Fabric** (icon)
  - Networking** (icon, highlighted)
  - Network Segmentation** (icon, highlighted)
  - Connectivity** (icon)
  - Security** (icon)
  - SmartGroups** (icon)
  - Cloud Resources** (icon)
  - Monitor** (icon)
  - Diagnostics** (icon)
  - Billing & Cost** (icon)
  - Administration** (icon)
  - Settings** (icon)
- Top Tabs:**
  - Network Segmentation**
  - Overview**
  - Network Domains** (highlighted)
- Buttons:**
  - + Network Domain** (highlighted)
  - Transit Gateways** (icon)
- Table:**

Name	Associations	Connected To
Blue	gcp-us-central1-spoke1	Green
Green	aws-us-east2-spoke1	Blue
- Modal: Edit Network Domain: Green**
  - Name\***: Green (highlighted)
  - Associations**: azure-us-west-spoke1 x aws-us-east2-spoke1 x (highlighted)
  - Connect to Network Domain**: Blue x (highlighted)
  - Connectivity**: Connectivity is bidirectional
  - Buttons**: Cancel, Save (highlighted)

# Visibility – CoPilot







Next: Lab 3 - Network Segmentation