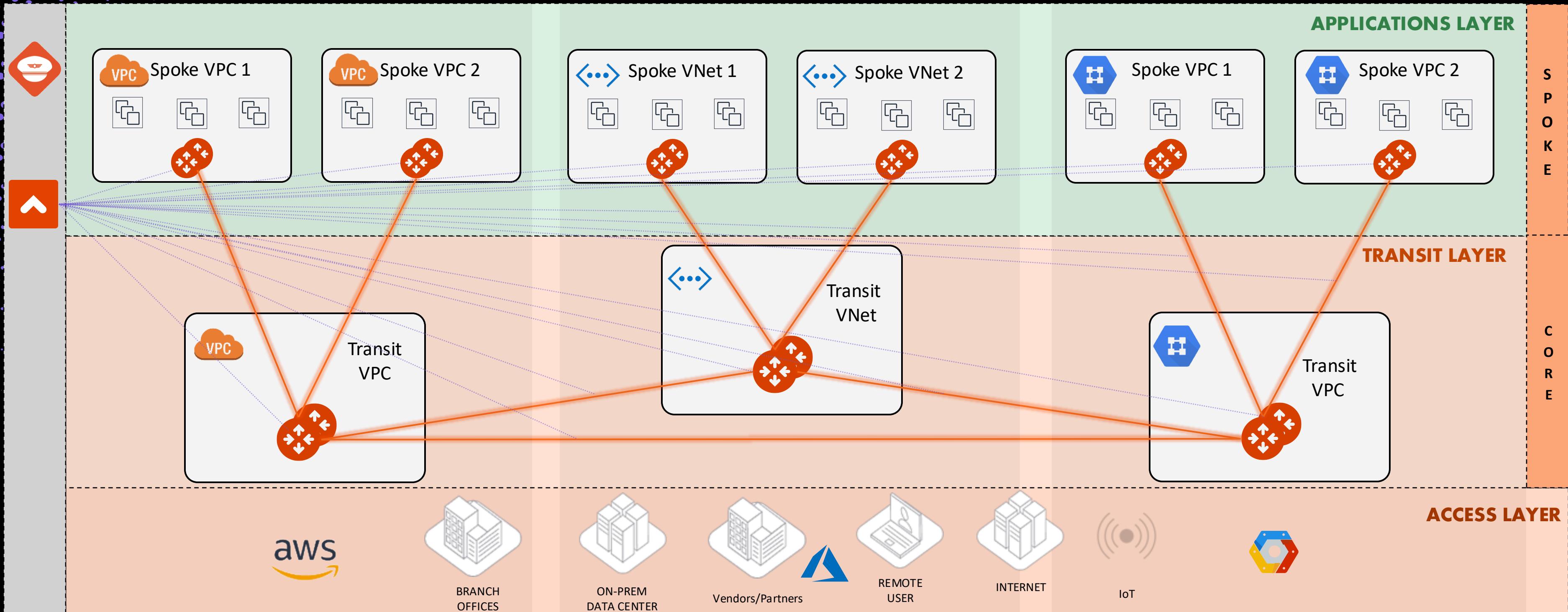




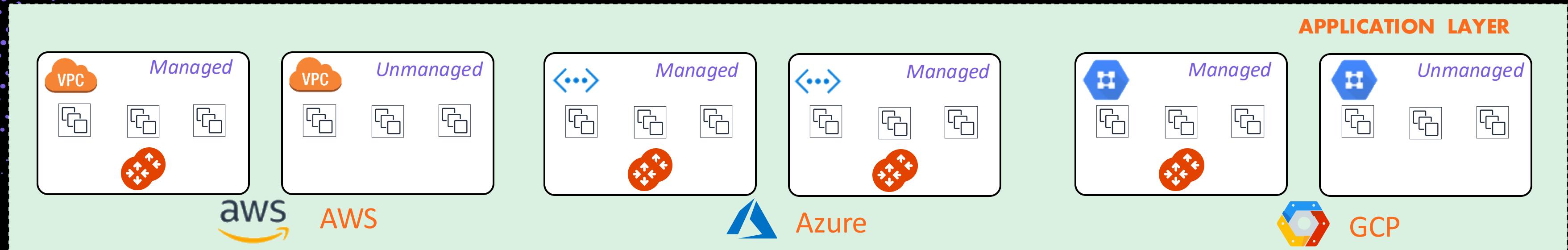
# Cloud Native Security Fabric

## Deployment

# Aviatrix Cloud Native Security Fabric: Deployment

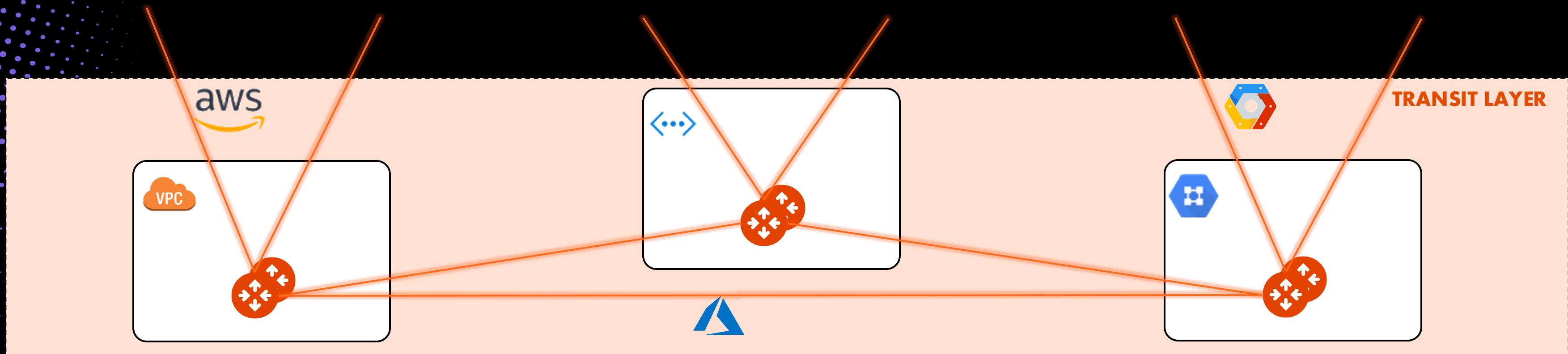


# Spoke Gateway



- A Spoke Gateway is a component of the Aviatrix CNSF that you deploy on Spoke VPCs, VNets or VCNs in a hub-and-spoke network topology (*default behaviour*).
- The presence of a Spoke GW allows to gain **deep visibility** into all the cloud resources inside any Application VPCs.
- Each Spoke Gateway deployed inside any Availability Zones will receive the traffic coming from the CSP router (i.e. all the private summary routes, RFC1918's routes, will point to the ENI of the Spoke Gateway).
- The Spoke Gateway will become an **Enforcement Security Point** as soon as the Distributed Cloud Firewall service is enabled, allowing to carry out the Network Segmentation, the Micro-Segmentation, the Security Group Orchestration, etc.
- You are not forced to insert a Spoke Gateway inside all the available VPCs, however **Unmanaged VPCs** (i.e. VPCs with no Aviatrix Gateway) will not benefit of the Aviatrix functionalities.

# Transit Gateway



- In Aviatrix's Hub-and-Spoke Topology, a Transit Gateway connects a company's VPCs across the main Cloud Service Providers: AWS, Azure, GCP and OCI.
- The Transit Gateway connection provides high-speed and secure data transfers between networks while allowing for traffic engineering and multi-account subscription monitoring.
- The Transit Gateway will have a **larger size** because it serves as the hub of a hub-and-spoke architecture, terminating multiple spokes. This means it will need **more IPSec throughput and performance** compared to Spoke gateways, which service only one VPC/VNET/VCN of workloads.
- The Transit Gateways are capable to maintain **multiple Routing Tables** (i.e. VRFs) when the Network Segmentation is enabled.

# Create VPC/VNet

## CLOUD ASSETS

- On the CoPilot you can create a new VPC/VNet/VCN.
- This feature is not only useful in a Greenfield deployment, but also if you need to add a new VPC/VNet/VCN on an existing environment, based on the architecture design.
- You can create two types of VPC/VNet/VCN:
  - Default (i.e. Spoke)
  - Transit + FireNet

The screenshot shows the CoPilot interface with a dark theme. On the left, there is a sidebar with the following menu items: Dashboard, Cloud Fabric, Networking, Security, Groups, Cloud Resources (which is highlighted with a red box), and Cloud Assets (which is also highlighted with a red box). The main area has tabs for Cloud Assets, Virtual Machines, and VPC/VNets & Subnets. A red arrow points from the 'Cloud Assets' tab to the '+ VPC/VNet' button, which is also highlighted with a red box. Below this, a list of existing VPC/VNet entries is shown, each preceded by a small downward arrow: AVX-FRANKFURT-PROD2, AZURE-WESTEUROPE-TRANSIT, AVX-FRANKFURT-TEST, AVX-FRANKFURT-TRANSIT, AVX-FRANKFURT-PROD1, and AZURE-WESTEUROPE-PROD3.

The screenshot shows the 'Create VPC/VNet' dialog box. It includes fields for Name (set to AVX-FRANKFURT-TRANSIT), Cloud provider selection (AWS Standard), Account (aws-account), Region (eu-central-1 (Frankfurt)), VPC CIDR (10.11.0.0/23), and VPC Function (Transit + FireNet, which is selected and highlighted with a blue box). There is also an 'Advanced Settings' section. At the bottom right are 'Cancel' and 'Save' buttons.

# Cloud Assets: Managed VPC vs. Unmanaged VPC

- CoPilot shows VPC/VNets that were created in the CSP environment as well as those that were created as part of deploying Aviatrix resources such as those created during the deployment of your Controller, CoPilot, and gateways.
- A VPC/VNet can be marked as Aviatrix managed where:
  - **Aviatrix Managed = Yes** — Indicates an Aviatrix gateway is running in the VPC/VNet.
  - **Aviatrix Managed = No** — Indicates no Aviatrix gateways exist in the VPC/VNet.

Name	Cloud	Region	IP Address CIDR	CSP Tags	SmartGroups	Aviatrix Managed
azure-west-us-spoke2	Azure ARM	westus	192.168.2.0/24	Aviatrix-Created-Resource: ..., + 1 more		Yes
gcp-us-central1-transit	GCP					Yes
gcp-us-central1-spoke1	GCP					Yes
aws-us-east-1-spoke1	AWS	us-east-1	10.0.12.0/24	Name: aws-us-east-1-spoke1, + 1 more		Yes
aws-us-east-2-spoke1	AWS	us-east-2	10.0.1.0/24	Name: aws-us-east-2-spoke1, + 1 more		Yes
azure-west-us-transit	Azure ARM	westus	192.168.10.0/23	Aviatrix-Created-Resource: ..., + 1 more		Yes
azure-west-us-spoke1	Azure ARM	westus	192.168.1.0/24	Aviatrix-Created-Resource: ..., + 1 more		Yes
aws-us-east-2-transit	AWS	us-east-2	10.0.10.0/23	Aviatrix-Created-Resource: ..., + 1 more		Yes
aws-us-east-1-transit	AWS	us-east-1	10.0.20.0/23	Name: aws-us-east-1-transit, + 1 more		Yes
vpc-574bab31	AWS	ap-southeast-1	172.31.0.0/16			No
vpc-3bf48952	AWS	ap-northeast-3	172.31.0.0/16			No
on-prem-partner1	AWS	us-east-1	172.16.1.0/24	Terraform: true, + 2 more		No
vpc-390a155e	AWS	sa-east-1	172.31.0.0/16			No
default	GCP					No
AviatrixVPC	AWS	us-east-1	172.16.0.0/16	aws:cloudformation:stack-..., + 4 more		No

**Note:** If you create a VPC/Vnet by using cloud provider tools instead of Aviatrix tools (i.e. CoPilot UI), the VPC/Vnet will be marked as unmanaged even if an Aviatrix gateway is running in it.

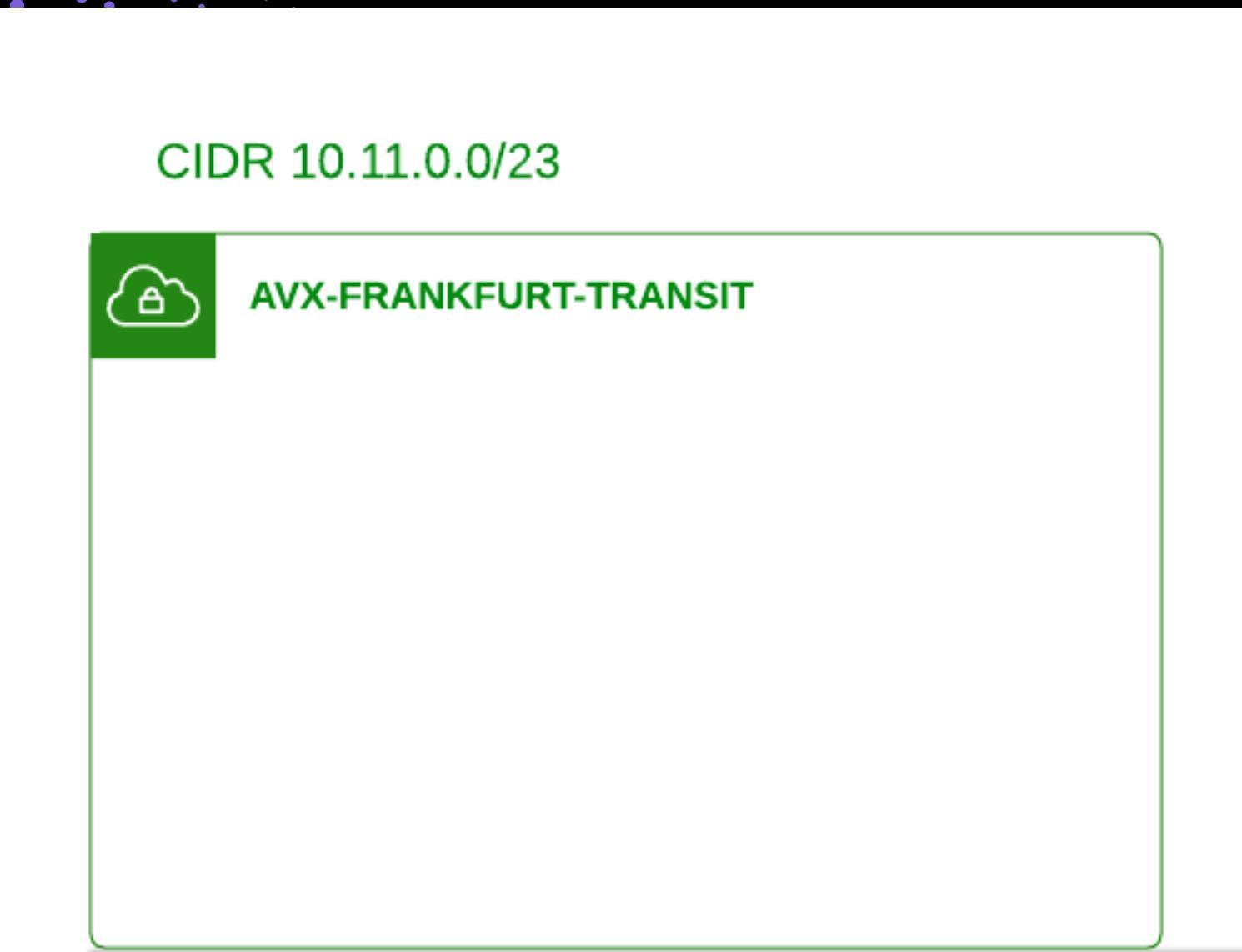
# Cloud Assets: Virtual Machines

- CoPilot shows in a central location all the virtual machines running in your clouds for cloud accounts onboarded onto Aviatrix Controller.
- A VM can be marked as *Aviatrix managed* where:
  - Aviatrix Managed = Yes** — Indicates the VM is behind an Aviatrix Gateway; that is running in a VPC/VNet where an Aviatrix gateway is deployed.
  - Aviatrix Managed = No** — Indicates the VM is running in a VPC/VNet where no Aviatrix gateways exist.
  - Aviatrix Managed = Gateways** — Indicates the VM is running an Aviatrix Gateway (Transit, Spoke, or Specialty/Other)

Virtual Machines							
Name	Cloud	Region	IP Address	Tags	SmartGroups	Aviatrix Managed	Actions
aviatrix-aws-us-east-1-transit	AWS	us-east-1	10.0.21.138, + 10 more	Controller: 54.161.179.60, HA: False, + 3 more		Gateways	
aviatrix-aws-us-east-1-transit-hagw	AWS	us-east-1	10.0.21.196, + 1 more	Name: aviatrix-aws-us-east-1-transit-h..., + 4 more		Gateways	
aviatrix-aws-us-east-1-spoke1-hagw	AWS	us-east-1	10.0.12.235, + 1 more	Aviatrix-Created-Resource: Do-Not-Del..., + 4 more		Gateways	
aviatrix-aws-us-east-1-spoke1	AWS	us-east-1	10.0.12.135, + 10 more	Aviatrix-Created-Resource: Do-Not-Del..., + 4 more		Gateways	
gcp-us-central1-transit	GCP	us-central1	172.16.10.2, + 1 more			Gateways	
gcp-us-central1-transit-hagw	GCP	us-central1	172.16.10.3, + 1 more			Gateways	
av-gw-azure-west-us-spoke2	Azure ARM	westus	104.40.57.73, + 1 more	Aviatrix-Created-Resource: Do-Not-Del..., + 3 more		Gateways	
av-gw-azure-west-us-transit	Azure ARM	westus	192.168.10..., + 3 more	Type: gateway, Controller: 54.161.179.60, + 2 more		Gateways	
av-gw-azure-west-us-transit-hagw	Azure ARM	westus	192.168.10..., + 3 more	Name: Aviatrix-av-gw-azure-west-us-tr..., + 3 more		Gateways	
aws-us-east-1-spoke1-test2	AWS	us-east-1	10.0.12.60, + 1 more	Name: aws-us-east-1-spoke1-test2		Yes	
aws-us-east-1-spoke1-test1	AWS	us-east-1	10.0.12.40, + 1 more	Name: aws-us-east-1-spoke1-test1		Yes	
azure-west-us-spoke2-test1	Azure ARM	westus	104.40.65..., + 1 more	environment: bu2		Yes	
aws-us-east-2-spoke1-test2	AWS	us-east-2	10.0.1.10	Name: aws-us-east-2-spoke1-test2, + 1 more		No	
aws-us-east-2-spoke1-test1	AWS	us-east-2	10.0.1.100, + 1 more	Name: aws-us-east-2-spoke1-test1, + 1 more		No	
AviatrixCoPilot	AWS	us-east-1	172.16.1.5, + 1 more	aws:cloudformation:stack-id: arn:aws:..., + 4 more		No	
AviatrixController	AWS	us-east-1	172.16.1.213, + 1 more	Name: AviatrixController, + 4 more		No	
aws-cisco-csr	AWS	us-east-1	172.16.1.65, + 1 more	Name: aws-cisco-csr		No	
gcp-us-central1-spoke1-test1	GCP	us-central1	172.16.1.100, + 1 more	environment: bu2		No	
Total 19 Virtual Machines							

# Greenfield Deployment (VPC/VNet/VCN creation)

**Caveat:** for the sake of simplicity, only the deployment in AWS is explained



Internet gateways (1/1) <a href="#">Info</a>				
<input type="text"/> Filter internet gateways				
<input type="text" value="search: AVX-FRANKFURT-TRANSIT"/> <a href="#">X</a> <a href="#">Clear filters</a>				
<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input checked="" type="checkbox"/>	AVX-FRANKFURT-TRANSIT	igw-06d499f4d0f772915	Attached	vpc-01f51fa31db0c8458   AVX-FRANKFURT-TRANSIT

## □ Creation of the Transit VPC

- The VPC CIDR range for a Transit VPC is from /16 to /23
- There is a specific reason why the Aviatrix Controller does not allow less than /23 prefix length for the Transit VPC (this will be discussed on the **HPE** lecture).



- An IGW with the same name of the Transit VPC will be created and attached to the VPC, automatically

# Greenfield Deployment (VPC/Vnet/VCN creation)

CIDR 10.11.0.0/23



## □ Creation of the Transit VPC

- The Aviatrix Controller will create 8 subnets, in two availability zones:
  - 4x Private subnets for the FW
  - 2x Public subnets for Ingress-Egress
  - 2x Public subnets for GW-FW-mgmt.
- All the subnets will have a /28 prefix length

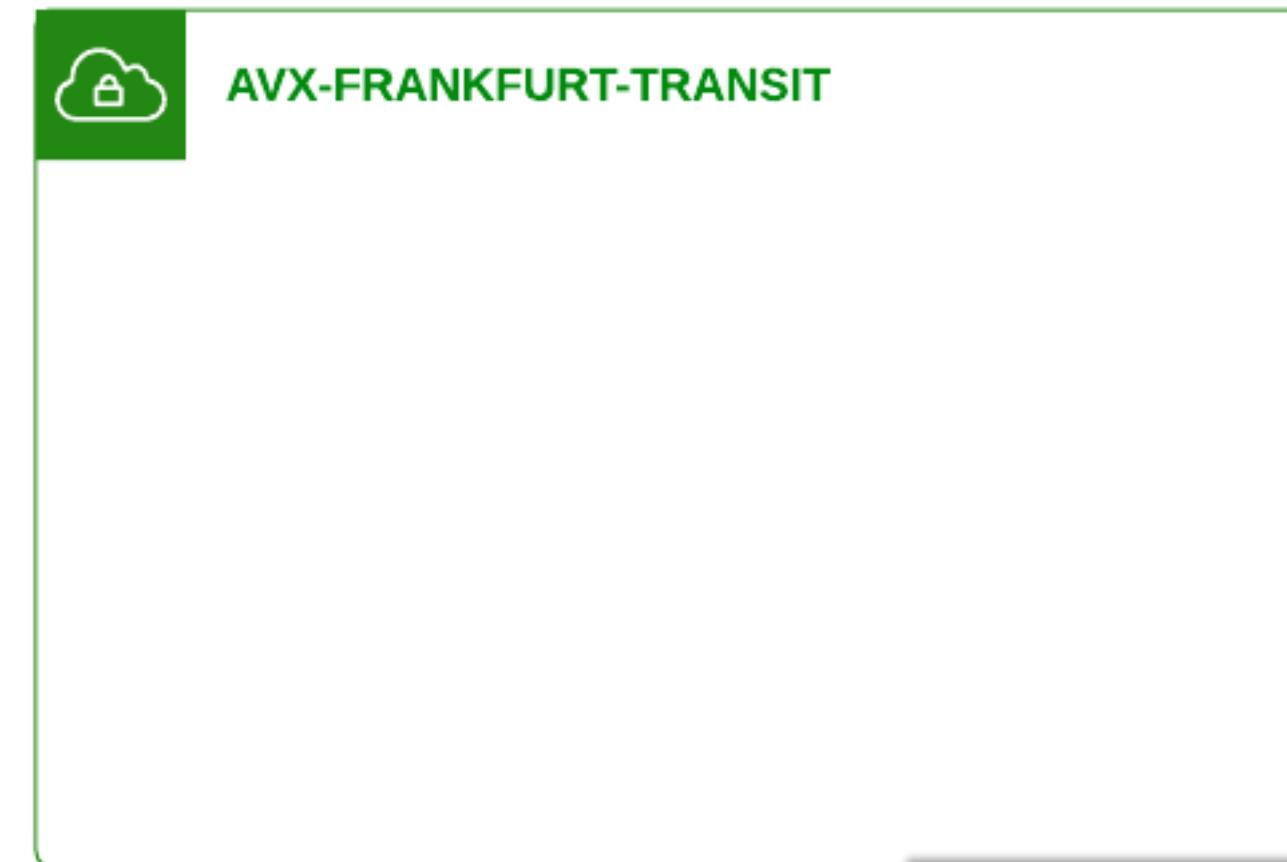
Subnets (8) <a href="#">Info</a>					
<input type="text"/> Filter subnets					
<input type="text"/> search: AVX-FRANKFURT-TRANSIT <a href="#">X</a> <a href="#">Clear filters</a>					
	Name	Subnet ID	IPv4 CIDR		Availability Zone
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Private-FW-north-eu-central-1a	subnet-04d1f3362661ae02a	10.11.0.16/28		eu-central-1a
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Private-FW-north-eu-central-1b	subnet-0a35db8130d9f9031	10.11.0.48/28		eu-central-1b
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Private-FW-south-eu-central-1a	subnet-06f4b955d965f1457	10.11.0.0/28		eu-central-1a
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Private-FW-south-eu-central-1b	subnet-0560c62d12c3ff59b	10.11.0.32/28		eu-central-1b
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Public-FW-ingress-egress-eu-central-1a	subnet-07818dd7b731a32a2	10.11.0.80/28		eu-central-1a
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Public-FW-ingress-egress-eu-central-1b	subnet-04094cc05bcd736a3	10.11.0.112/28		eu-central-1b
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Public-gateway-and-firewall-mgmt-e...	subnet-08228163bc8ca6f7d	10.11.0.64/28		eu-central-1a
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Public-gateway-and-firewall-mgmt-e...	subnet-002f879d78f686a57	10.11.0.96/28		eu-central-1b

- ❖ The subnets' size can be customized

The screenshot shows the "Advanced Settings" section of the Aviatrix Controller. It includes fields for "Subnet Size" and "Number of Subnet Pair(s)", both with "Optional" dropdowns. At the bottom are "Cancel" and "Save" buttons.

# Greenfield Deployment (VPC/Vnet/VCN creation)

CIDR 10.11.0.0/23



## □ Creation of the Transit VPC

- 2x Routing Tables will be created:

➤ Public RTB will encompass the 4 public subnets

Destination	Target
0.0.0.0	igw-06d499f4d0f772915
10.11.0.0/23	local

➤ Private RTB will encompass the 4 private subnets

Destination	Target
10.11.0.0/23	local

## Route tables (2) Info

Filter route tables

search: AVX-FRANKFURT-TRANSIT X

Clear filters

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associations
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Public-rtb	<a href="#">rtb-0e5a22d0060c17eac</a>	4 subnets
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Private-rtb	<a href="#">rtb-085cf49590ee4592d</a>	4 subnets

# Greenfield Deployment (VPC/Vnet/VCN creation)

CIDR 10.1.1.0/24



Internet gateways (1/1) <small>Info</small>				
<input type="text"/> Filter internet gateways				
<input type="text" value="search: AVX-FRANKFURT-SPOKE-PROD"/> <span>X</span> <span>Clear filters</span>				
<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input checked="" type="checkbox"/>	AVX-FRANKFURT-SPOKE-PROD	igw-0327c092c11fdbd749	Attached	vpc-068d94ca168a85633   AVX-FRANKFURT-SPOKE-PROD

## □ Creation of the Application/Spoke VPC

- The VPC CIDR range for a Spoke VPC is from /16 to /24
- An IGW with the same name of the Spoke VPC will be created and attached to the VPC, automatically

# Greenfield Deployment (VPC/Vnet/VCN creation)

The screenshot shows the Aviatrix Controller interface for creating a VPC. At the top, it displays the CIDR range **CIDR 10.1.1.0/24**. Below this, a green cloud icon labeled **AVX-FRANKFURT-SPOKE-PROD** is shown. A modal window titled "Subnets (6)" is open, displaying a list of six subnets with their details:

Name	Subnet ID	VPC	IPv4 CIDR
AVX-FRANKFURT-SPOKE-PROD-Private-1-eu-central-1a	subnet-060df41c64a2c643a	vpc-068d94ca168a85633   AV...	10.1.1.0/28
AVX-FRANKFURT-SPOKE-PROD-Private-2-eu-central-1b	subnet-00bf95727955ec09b	vpc-068d94ca168a85633   AV...	10.1.1.16/28
AVX-FRANKFURT-SPOKE-PROD-Private-3-eu-central-1c	subnet-0bd05503b4b1f880c	vpc-068d94ca168a85633   AV...	10.1.1.32/28
AVX-FRANKFURT-SPOKE-PROD-Public-1-eu-central-1a	subnet-0b22457ff5b1a4895	vpc-068d94ca168a85633   AV...	10.1.1.48/28
AVX-FRANKFURT-SPOKE-PROD-Public-2-eu-central-1b	subnet-0c140dc3d0af1fa65	vpc-068d94ca168a85633   AV...	10.1.1.64/28
AVX-FRANKFURT-SPOKE-PROD-Public-3-eu-central-1c	subnet-06219ac03978942e3	vpc-068d94ca168a85633   AV...	10.1.1.80/28

At the bottom of the modal, there are "Advanced Settings" and "Optional" dropdowns for Subnet Size and Number of Subnet Pair(s), along with "Cancel" and "Save" buttons.

## □ Creation of the Application/Spoke VPC

- The Aviatrix Controller will create a pair of subnets, a public subnet and a private subnet, on each availability zone
- All the subnets will have a /28 prefix length

❖ The subnets' size can be customized

This screenshot shows the "Advanced Settings" section of the VPC creation interface. It includes fields for "Subnet Size" and "Number of Subnet Pair(s)", both of which are marked as "Optional". At the bottom, there are "Cancel" and "Save" buttons.

# Greenfield Deployment (VPC/Vnet/VCN creation)

CIDR 10.1.1.0/24



## □ Creation of the Application/Spoke VPC

- a Public RTB per each availability zone will encompass the corresponding subnet

Destination	Target
0.0.0.0/0	igw-0327c092c11fbd749
10.1.1.0/24	local

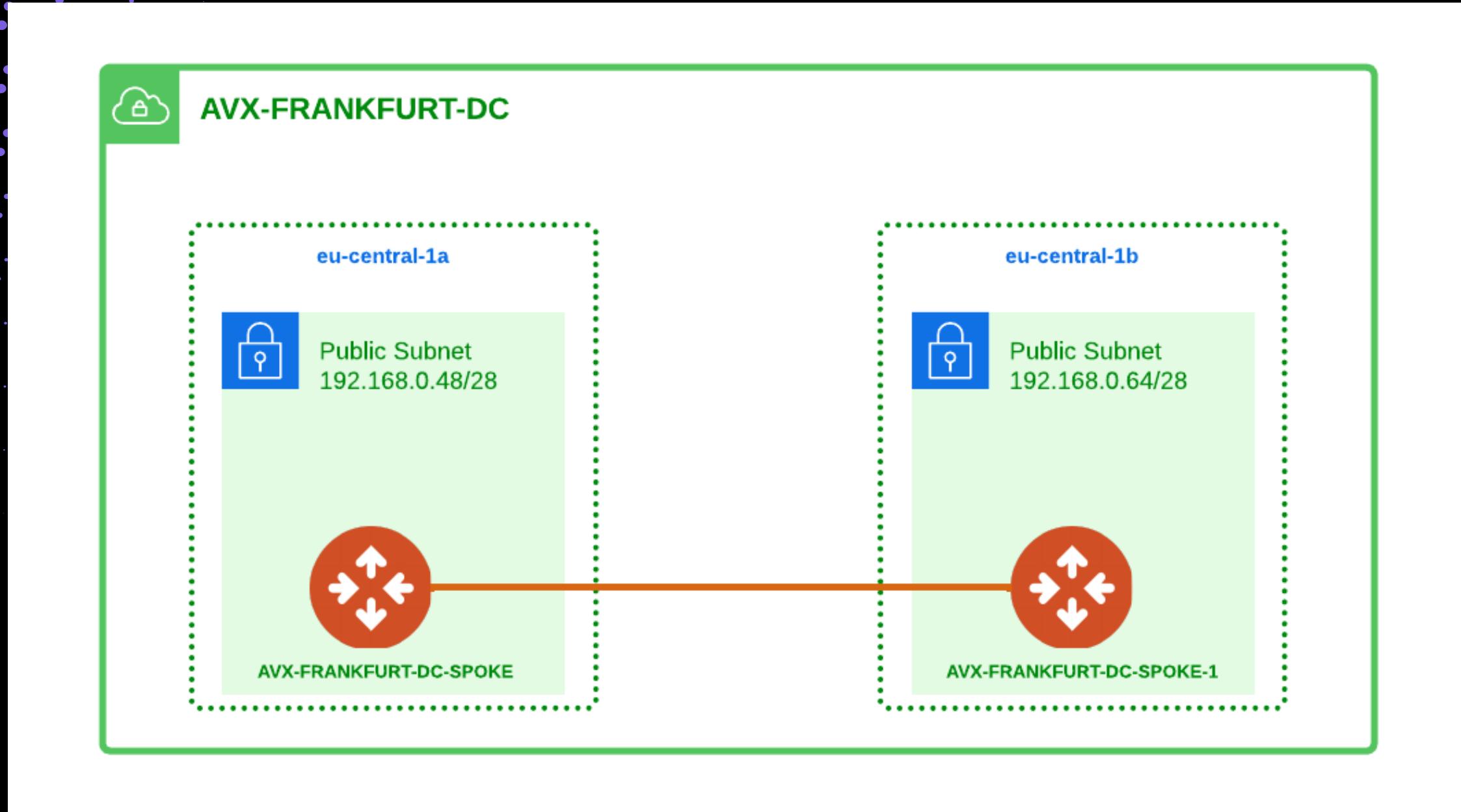
- a Private RTB per each availability zone will encompass the corresponding subnet

Destination	Target
10.1.1.0/24	local

Route tables (6) <a href="#">Info</a>			
<input type="text"/> Filter route tables			
search: AVX-FRANKFURT-SPOKE-PROD <a href="#">X</a>	<a href="#">Clear filters</a>		
Name	Route table ID	Explicit subnet associations	
AVX-FRANKFURT-SPOKE-PROD-Private-1-eu-central-1a-rtb	rtb-0ca98234a5088dceb	subnet-060df41c64a2c643a / AVX-FRANKFURT-SPOKE-PROD-Private-1-eu-central-1a	
AVX-FRANKFURT-SPOKE-PROD-Private-2-eu-central-1b-rtb	rtb-0cad721a70d6256d9	subnet-00bf95727955ec09b / AVX-FRANKFURT-SPOKE-PROD-Private-2-eu-central-1b	
AVX-FRANKFURT-SPOKE-PROD-Private-3-eu-central-1c-rtb	rtb-04afaa976264662ac	subnet-0bd05503b4b1f880c / AVX-FRANKFURT-SPOKE-PROD-Private-3-eu-central-1c	
AVX-FRANKFURT-SPOKE-PROD-Public-1-eu-central-1a-rtb	rtb-0c52cd5084b440f2d	subnet-0b22457ff5b1a4895 / AVX-FRANKFURT-SPOKE-PROD-Public-1-eu-central-1a	
AVX-FRANKFURT-SPOKE-PROD-Public-2-eu-central-1b-rtb	rtb-0c973dec3847ae8ce	subnet-0c140dc3d0af1fa65 / AVX-FRANKFURT-SPOKE-PROD-Public-2-eu-central-1b	
AVX-FRANKFURT-SPOKE-PROD-Public-3-eu-central-1c-rtb	rtb-099810bbea6608f17	subnet-06219ac03978942e3 / AVX-FRANKFURT-SPOKE-PROD-Public-3-eu-central-1c	

# Name Convention with Multiple Gateways

## Cluster of Gateways

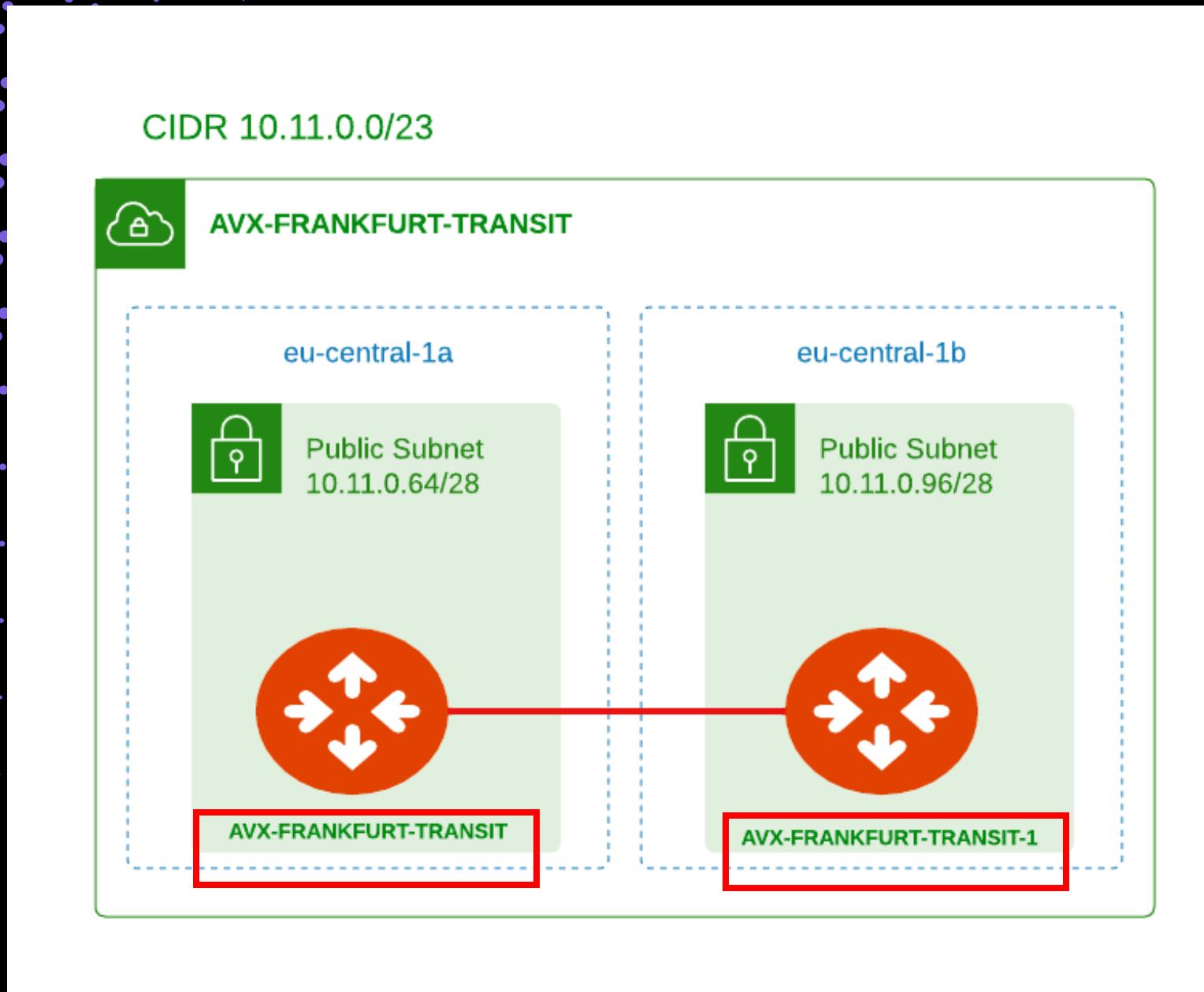


- ❖ If you create two or more Gateways, they will be encompassed inside a cluster.
- ❖ The name of the cluster will match the name of the first gateway.
- ❖ The second gateway will have the string “-1” appended to its name.
- ❖ The third gateway will have the string “-2” appended to its name.
- 
- 
- 
- ❖ The fifteenth gateway will have the string “-14” appended to its name.

<b>CLUSTER</b>	AVX-FRANKFURT-DC-SPOKE	eu-central-1	vpc-04d947b7b73180e3c~~AVX-FRANKFURT-DC
<b>GW #1</b>	AVX-FRANKFURT-DC-SPOKE	eu-central-1	vpc-04d947b7b73180e3c~~AVX-FRANKFURT-DC 192.168.0.48/28
<b>GW #2</b>	AVX-FRANKFURT-DC-SPOKE-1	eu-central-1	vpc-04d947b7b73180e3c~~AVX-FRANKFURT-DC 192.168.0.64/28

# Greenfield Deployment (Transit Gateways deployment)

## □ Transit Gateways Deployment through the CoPilot



Create Transit Gateway

Name: AVX-FRANKFURT-TRANSIT

Cloud: AWS Standard

Account: AWS-AVIATRIX

Region: eu-central-1 (Frankfurt)

VPC/VNet: AVX-FRANKFURT-TRANSIT

Instance Size: c5n.large

High Performance Encryption: Off

Peer To Transit Gateways:

Instances:

+ Instance

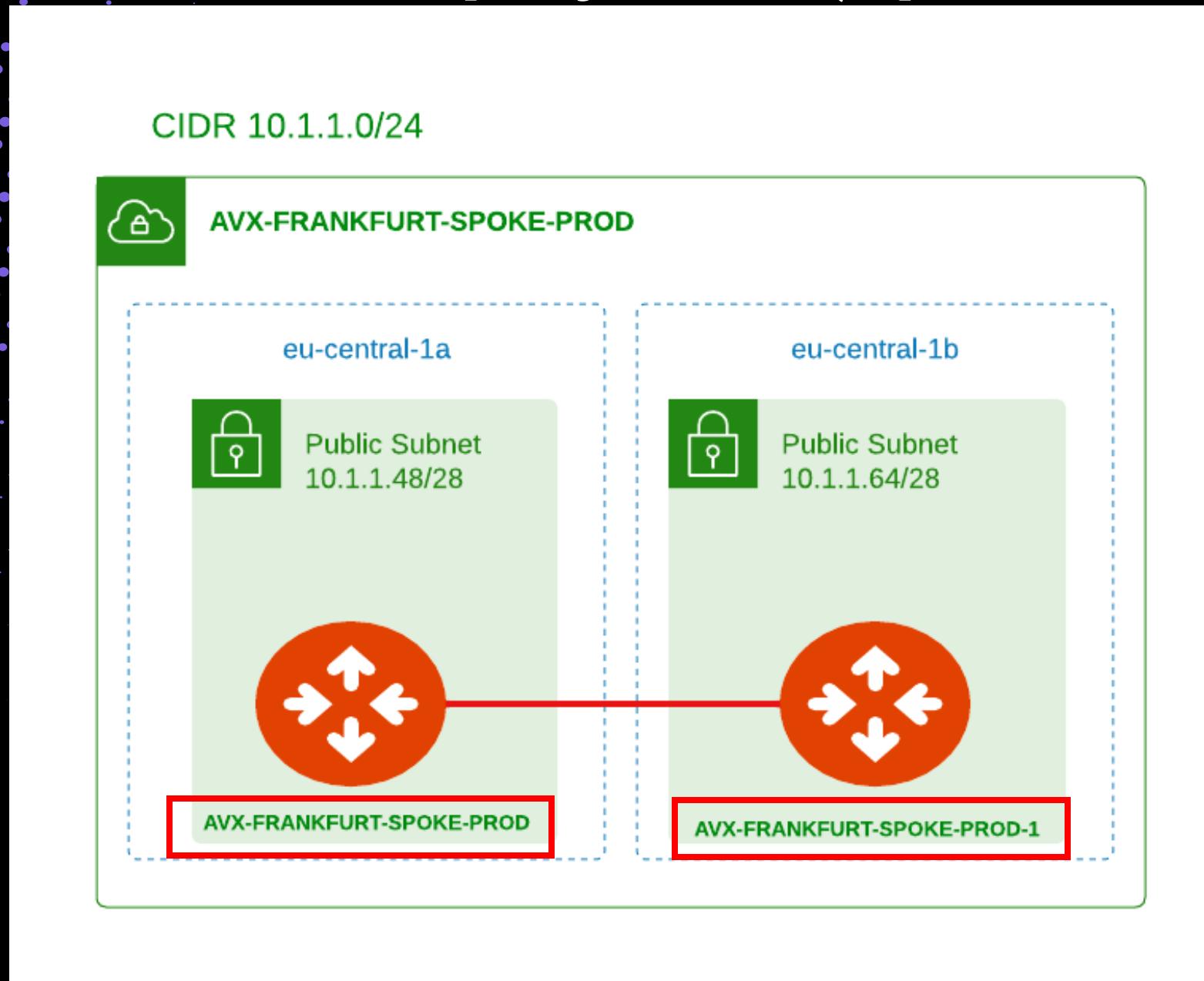
	Attach to Subnet	Public IP
1	10.11.0.64/28	Allocate New Static Public IP
2	10.11.0.96/28	Allocate New Static Public IP

Cancel Save

This screenshot shows the 'Create Transit Gateway' interface in the Aviatrix CoPilot. It includes fields for Name, Cloud (AWS Standard), Account (AWS-AVIATRIX), Region (eu-central-1 (Frankfurt)), VPC/VNet (AVX-FRANKFURT-TRANSIT), Instance Size (c5n.large), and High Performance Encryption (Off). The 'Instances' section shows two subnets attached to the gateway. The 'Public IP' column indicates that new static public IPs will be allocated for both subnets. At the bottom right are 'Cancel' and 'Save' buttons.

- ❖ The connection between the Transit Gateways is automatically created by the Controller.
- ❖ **Best Practice:** always deploy the Transit Gateway-1 (i.e. the second gateway), and choose a different AZ.
- ❖ Only two Transit Gateways can be deployed per Transit VPC
- ❖ Aviatrix gateways are deployed in Public subnets

# Greenfield Deployment (Spoke Gateways deployment)



## □ Spoke Gateways Deployment through the CoPilot

Create Spoke Gateway

NAME: AVX-FRANKFURT-SPOKE-PROD

Cloud: AWS Standard

Account: AWS-AVIATRIX

Region: eu-central-1 (Frankfurt)

VPC/VNet: AVX-FRANKFURT-SPOKE-PROD

Instance Size: t3.micro

High Performance Encryption: Off

Advanced Settings: BGP Off

Instances:

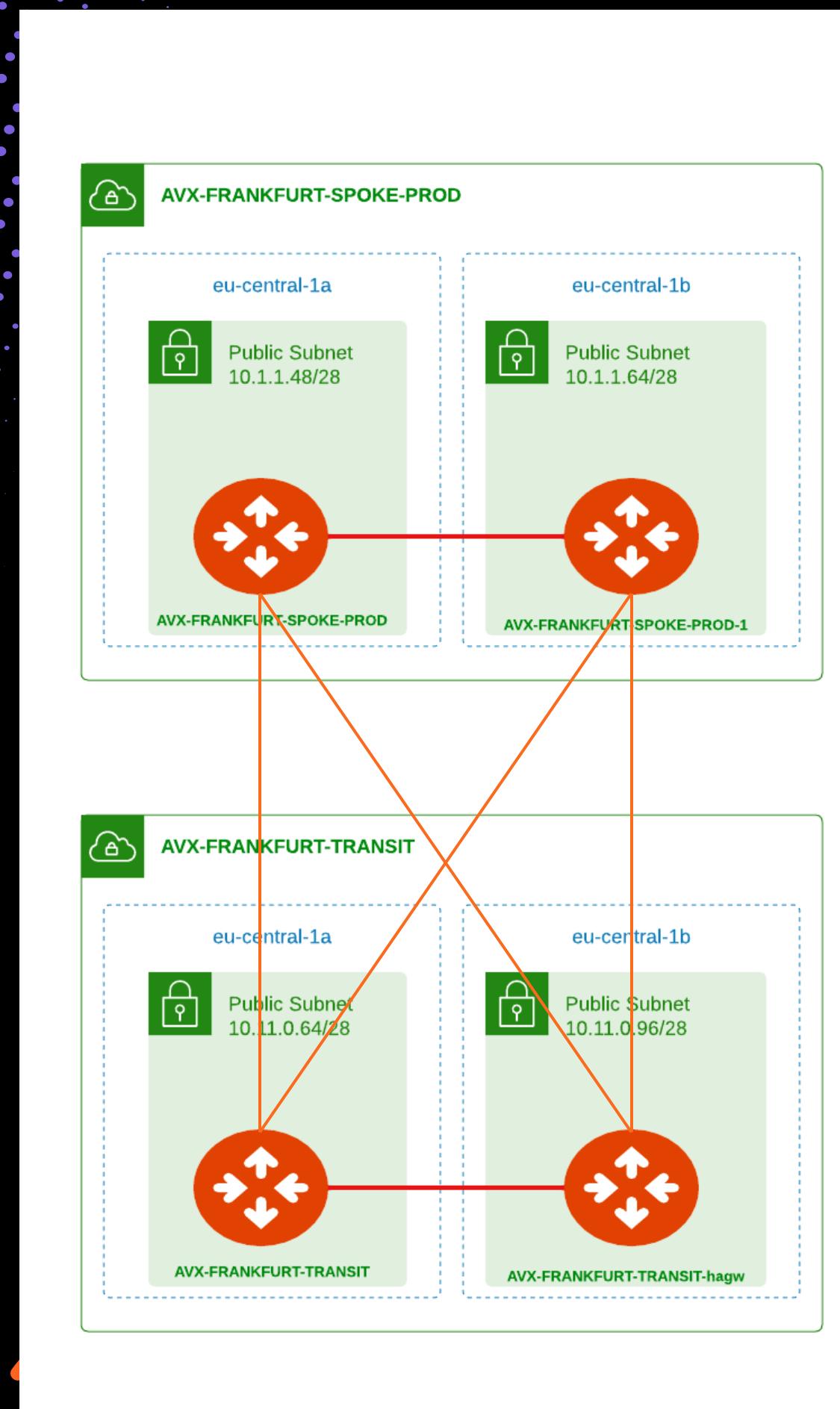
Attach to Subnet		Public IP
1	10.1.1.48/28	Allocate New Static Public IP
2	10.1.1.80/28	Allocate New Static Public IP

Optional: Attach To Transit Gateway

Cancel Save

- ❖ The connection between the Spoke Gateways is automatically created by the Controller.
- ❖ **Best Practice:** deploy the Spoke Gateway-1 (i.e the second gateway) on a different AZ.
- ❖ You can deploy up to **15** Spoke Gateways per each Spoke VPC
- ❖ Aviatrix gateways are deployed in Public subnets

# Greenfield Deployment (Attachments deployment)



□ Deployment of the attachments through the CoPilot

Edit Spoke Gateway: AVX-FRANKFURT-SPOKE-PROD

Name: AVX-FRANKFURT-SPOKE-PROD

Cloud: AWS

Account: AWS-AVIATRIX

Region: eu-central-1

VPC/VNet: AVX-FRANKFURT-SPOKE-PROD

Instance Size: t3.micro

High Performance Encryption: Off

Attach To Transit Gateway: AVX-FRANKFURT-TRANSIT (Optional)

Advanced Settings: BGP Off

Instances:

+ Instance

	Attach to Subnet	Public IP
1	10.1.1.48/28	3.72.194.207
2	10.1.1.80/28	18.192.199.249

Cancel Save

# Greenfield Deployment (Attachments deployment)

- As soon as the Controller completes the deployment of the **attachments** between Spoke Gateways and Transit Gateways, it will also program the *three RFC1918 routes* in the route tables to point to the ENI of the Spoke Gateways.

Routes	Subnet associations	Edge associations	Route propagation	Tags
<b>Routes (4)</b>				
Filter routes				
Destination	▼	Target		
10.0.0.0/8		eni-08ac50fc16cd8c4a5		
10.1.1.0/24		local		
172.16.0.0/12		eni-08ac50fc16cd8c4a5		
192.168.0.0/16		eni-08ac50fc16cd8c4a5		

Routes	Subnet associations	Edge associations	Route propagation	Tags
<b>Routes (5)</b>				
Filter routes				
Destination	▼	Target		
0.0.0.0/0		igw-07c6ddedd190d12d3		
10.0.0.0/8		eni-08ac50fc16cd8c4a5		
10.1.1.0/24		local		
172.16.0.0/12		eni-08ac50fc16cd8c4a5		
192.168.0.0/16		eni-08ac50fc16cd8c4a5		

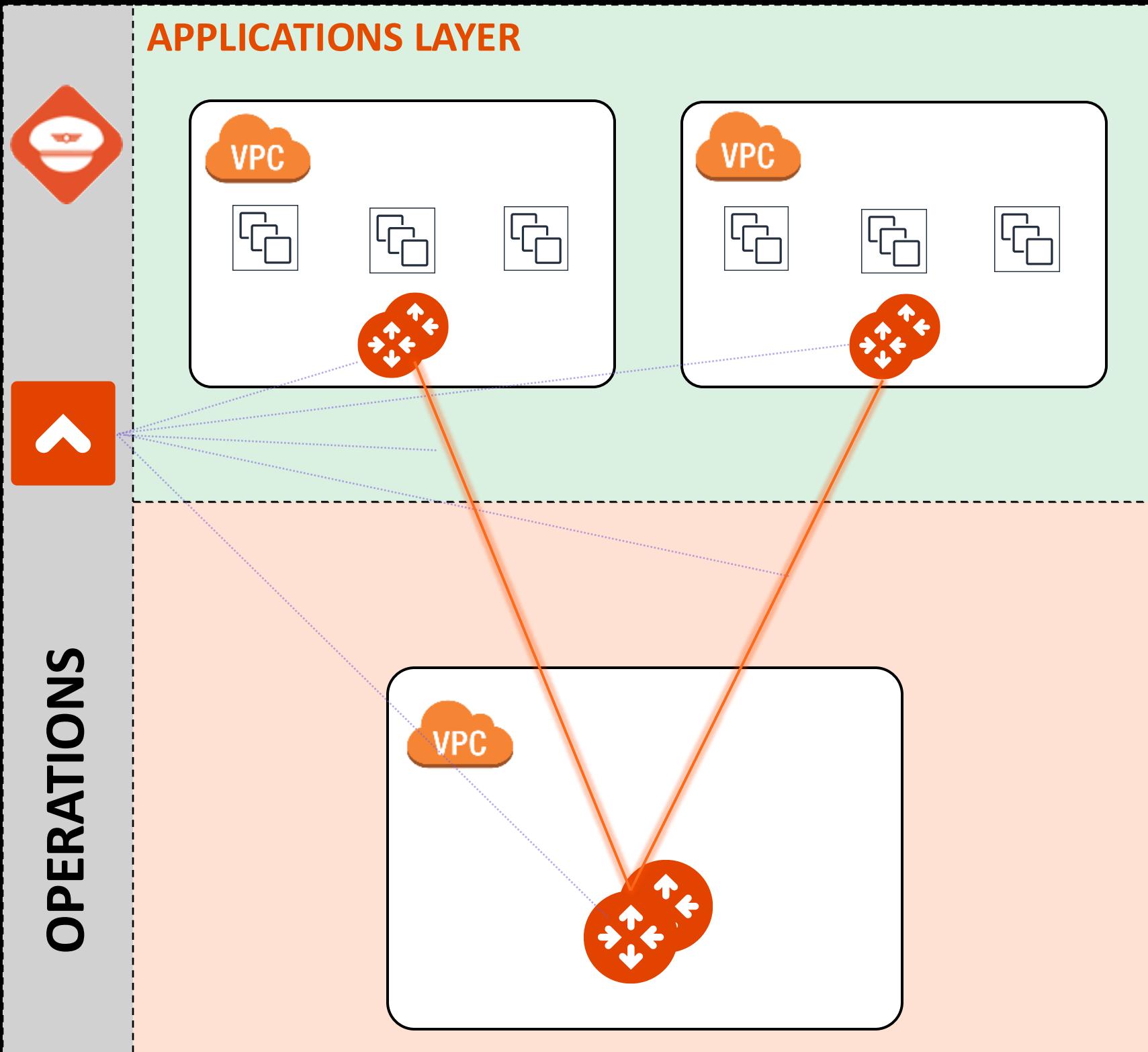
Route table for  
Private Subnet



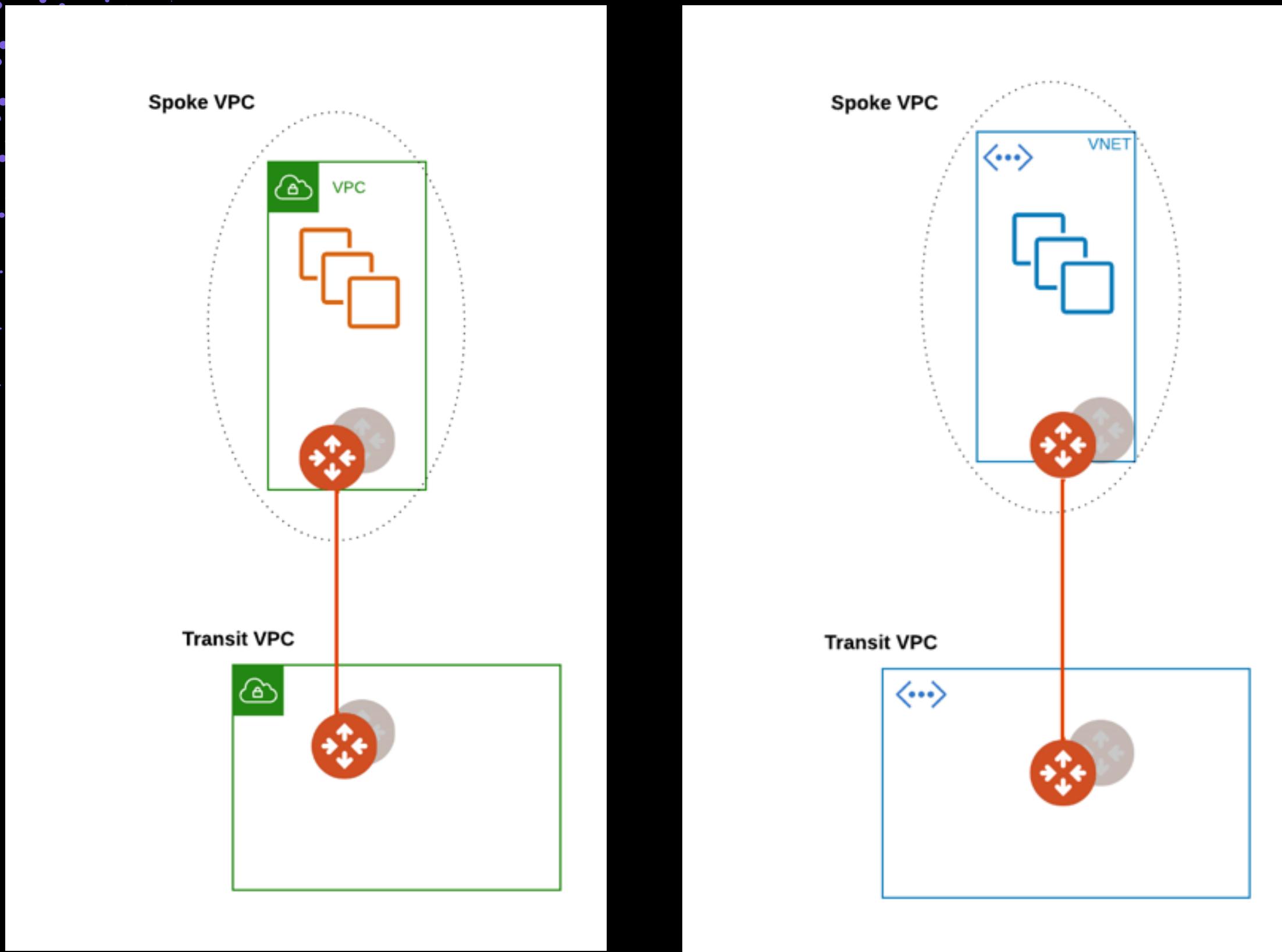
Route table for  
Public Subnet



□ **Attachment = RFC1918 Routes Injection**

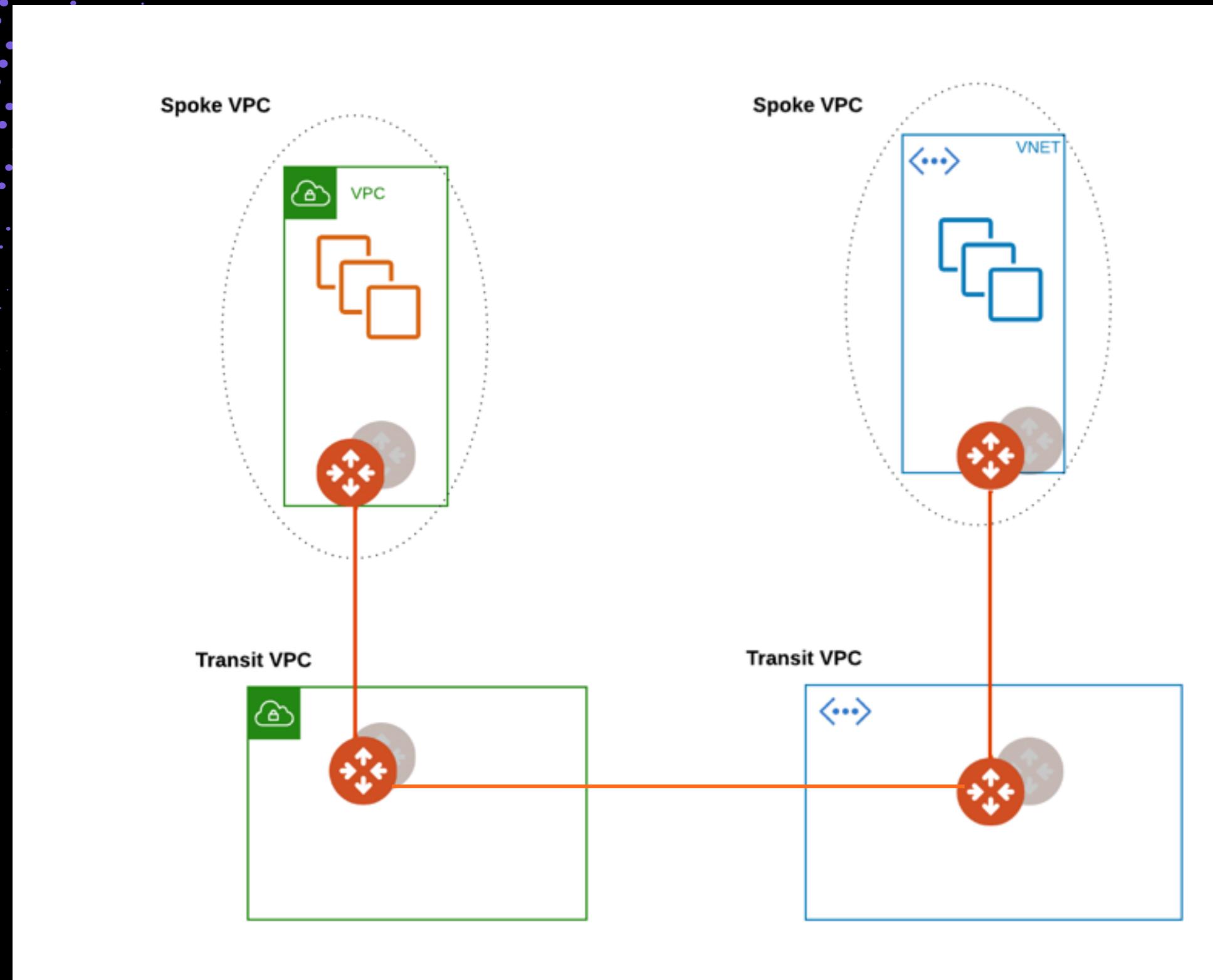


# Greenfield Deployment (Repeatable Design)



- ❑ The hub and spoke topology can be extended to another CSP or to another region within the same CSP
- ❑ In Azure all subnets are public by nature
- ❑ Aviatrix Controller creates “Private” subnets:
  - Aviatrix Controller programs a **default route 0.0.0.0 pointing to the next hop type “None”**: in User Defined Route Table (UDR) for all private subnets it creates
  - This will blackhole 0/0 traffic

# Greenfield Deployment (Peering Deployment)



- The creation of the Transit Peering represents the last step for the completion of the **CNSF**.

Edit Transit Gateway: AVX-FRANKFURT-TRANSIT

Name	AVX-FRANKFURT-TRANSIT									
Cloud	AWS									
Account	AWS-AVIATRIX									
Region	eu-central-1									
VPC/VNet	AVX-FRANKFURT-TRANSIT									
Instance Size	c5n.large									
High Performance Encryption	Off									
Peer To Transit Gateways	AZURE-WESTEUROPE-TRANSIT									
Instances	<table border="1"><thead><tr><th>+ Instance</th><th>Attach to Subnet</th><th>Public IP</th></tr></thead><tbody><tr><td>1</td><td>10.11.0.64/28</td><td>3.75.164.186</td></tr><tr><td>2</td><td>10.11.0.96/28</td><td>3.127.251.156</td></tr></tbody></table>	+ Instance	Attach to Subnet	Public IP	1	10.11.0.64/28	3.75.164.186	2	10.11.0.96/28	3.127.251.156
+ Instance	Attach to Subnet	Public IP								
1	10.11.0.64/28	3.75.164.186								
2	10.11.0.96/28	3.127.251.156								

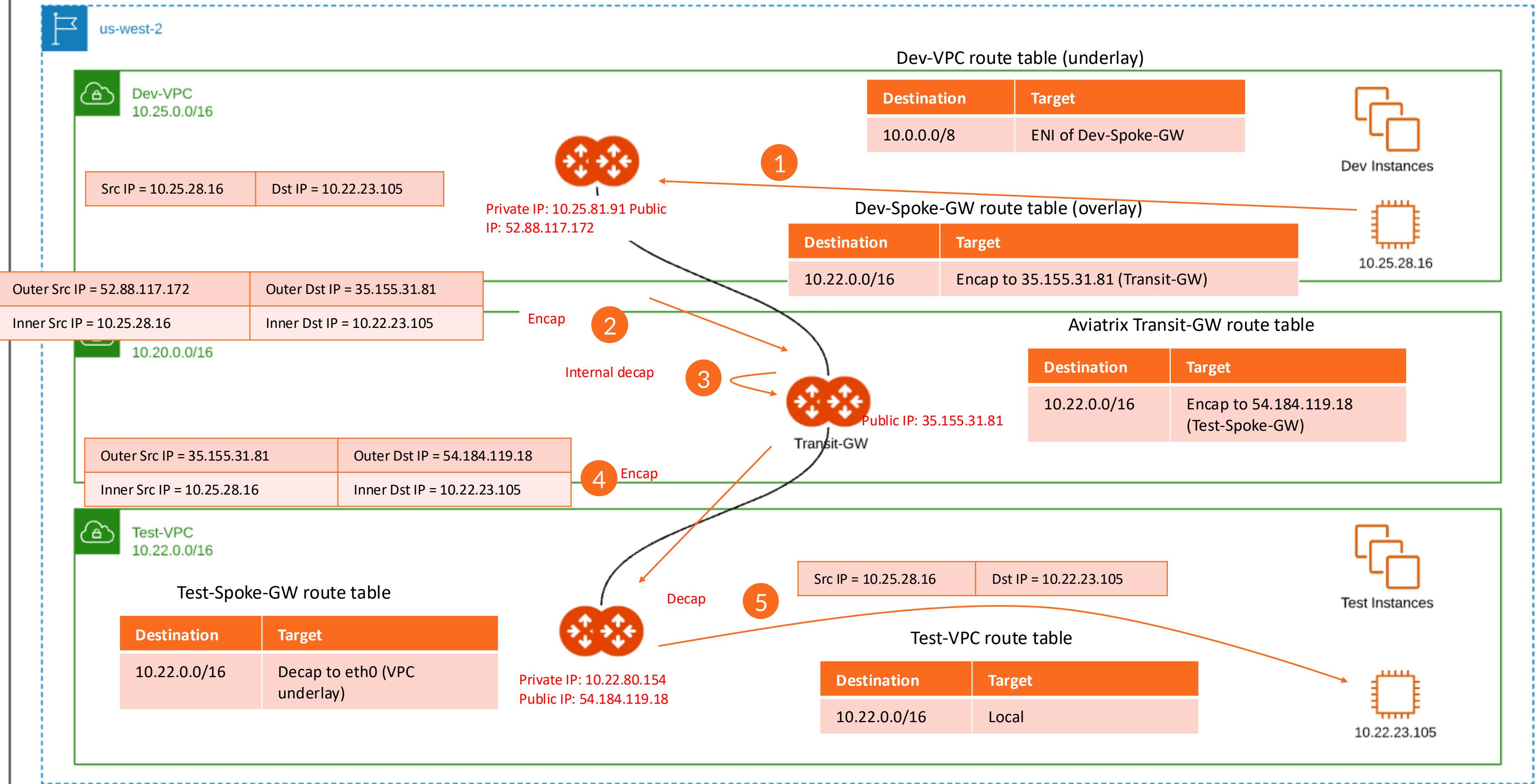


AWS Cloud

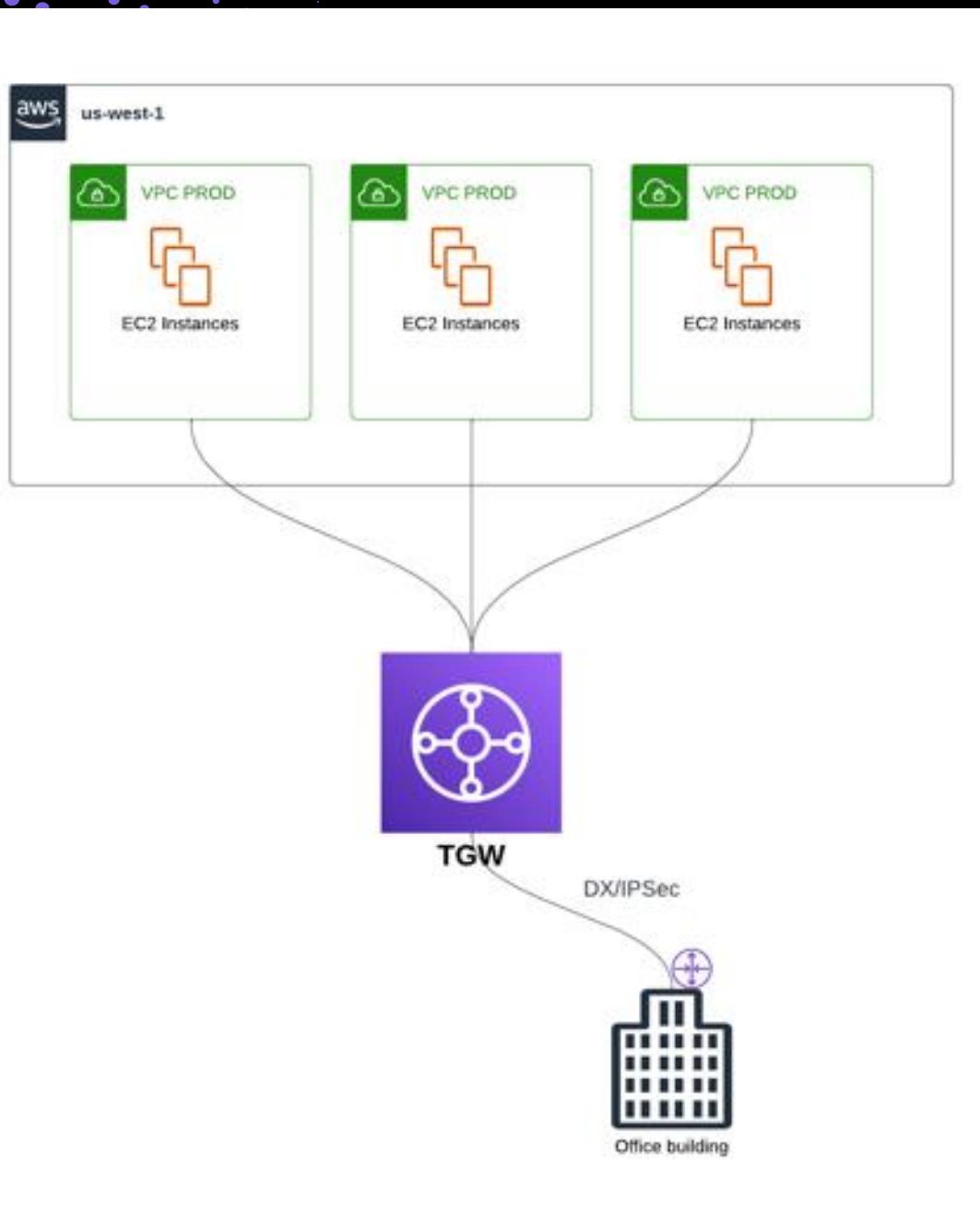
# Packet Walk



us-west-2



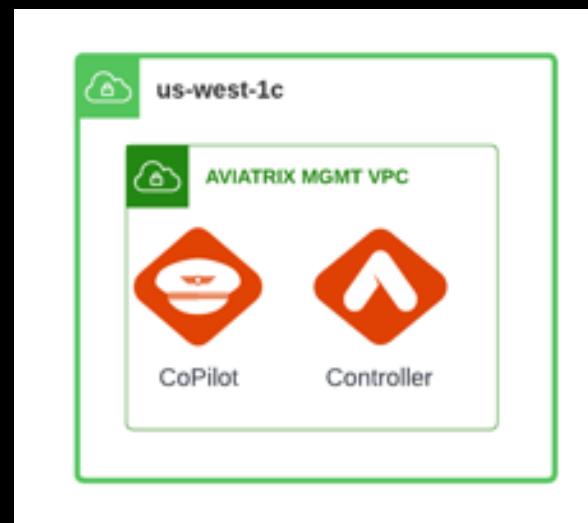
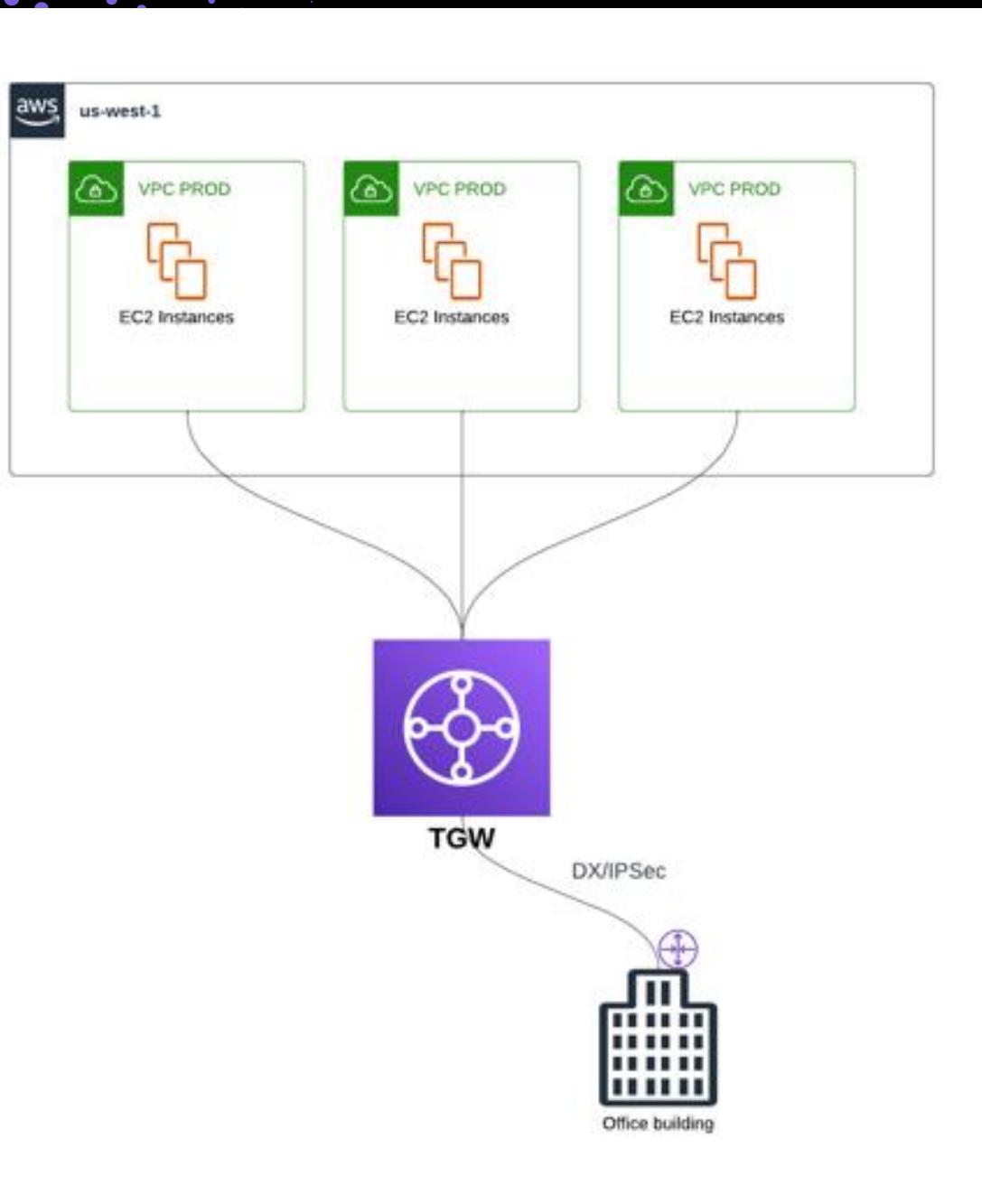
# Migration Deployment: Example



## Initial environment in a brownfield scenario:

- Several Application VPCs that are connected to the TGW as attachments
- OnPrem connectivity (hybrid – can be DX/IPSec)

# Migration Deployment: Example

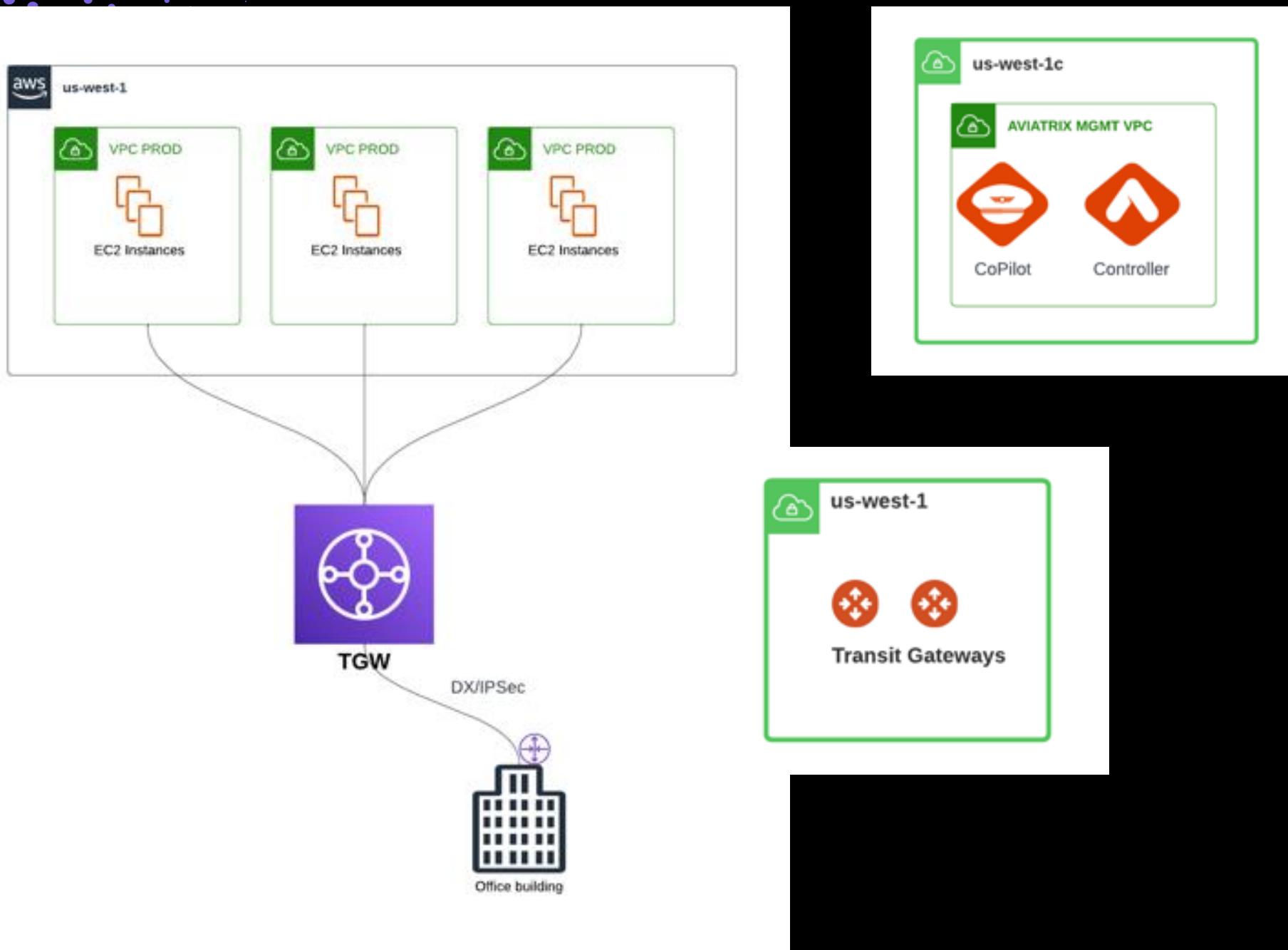


## □ Initial environment in a brownfield scenario:

- Several Application VPCs that are connected to the TGW as attachments
- OnPrem connectivity (hybrid – can be DX/IPSec)

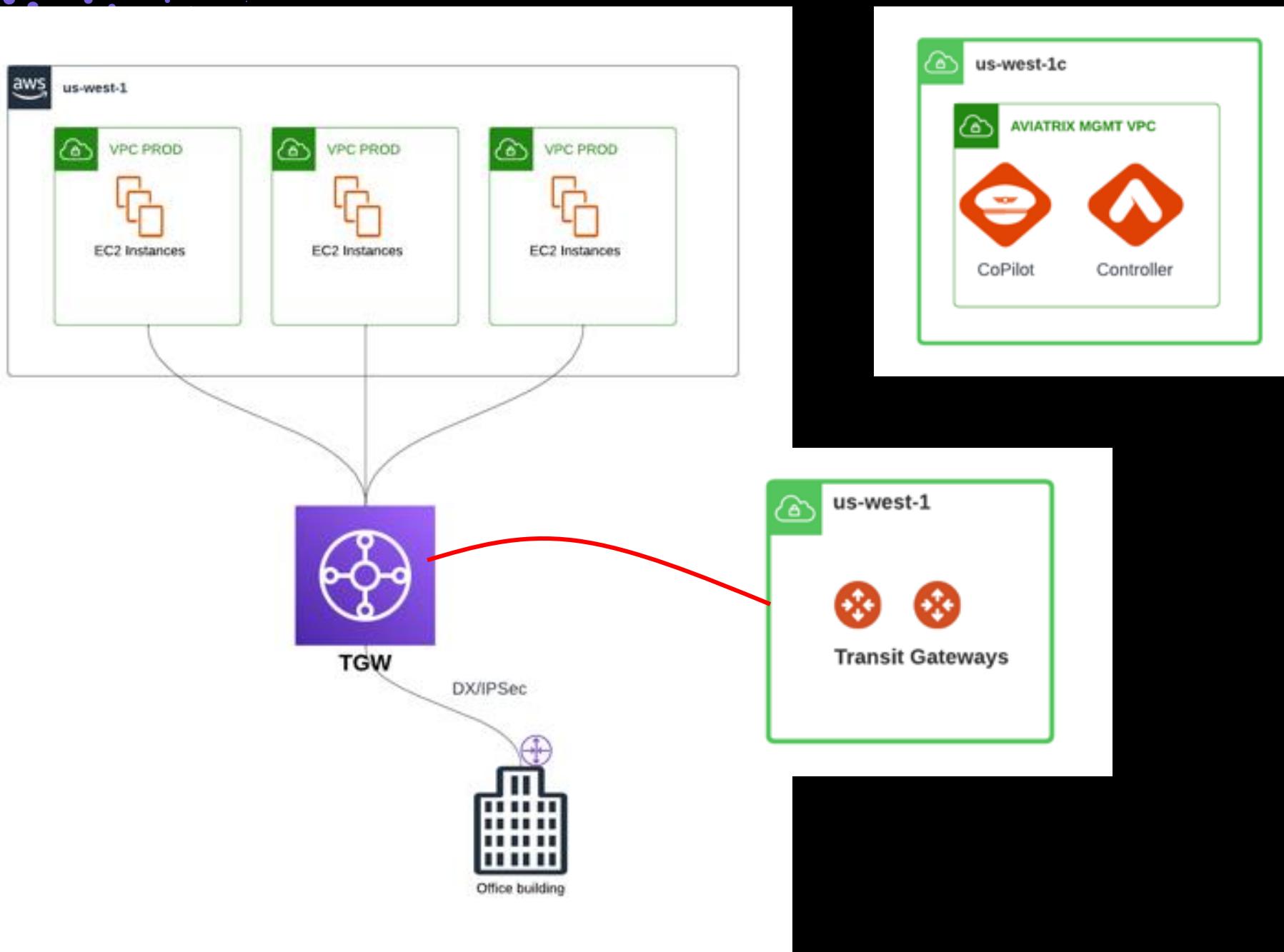
## □ Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed (best practice)

# Migration Deployment: Example



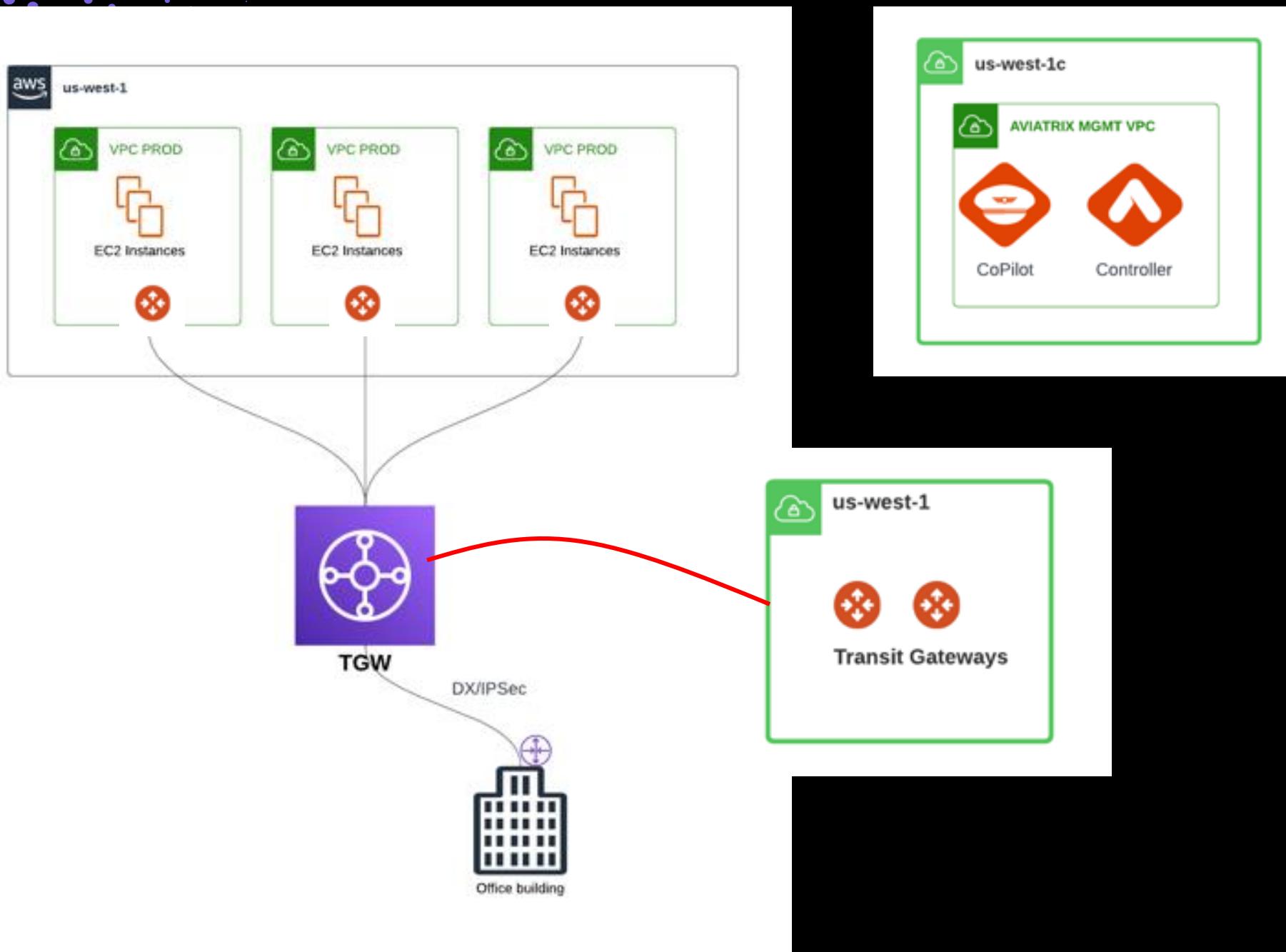
- Initial environment in a brownfield scenario:
  - Several Application VPCs that are connected to the TGW as attachments
  - OnPrem connectivity (hybrid – can be DX/IPSec)
- Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed (best practice)
- Deploy a Transit VPC and deploy a pair of Transit Gateways

# Migration Deployment: Example



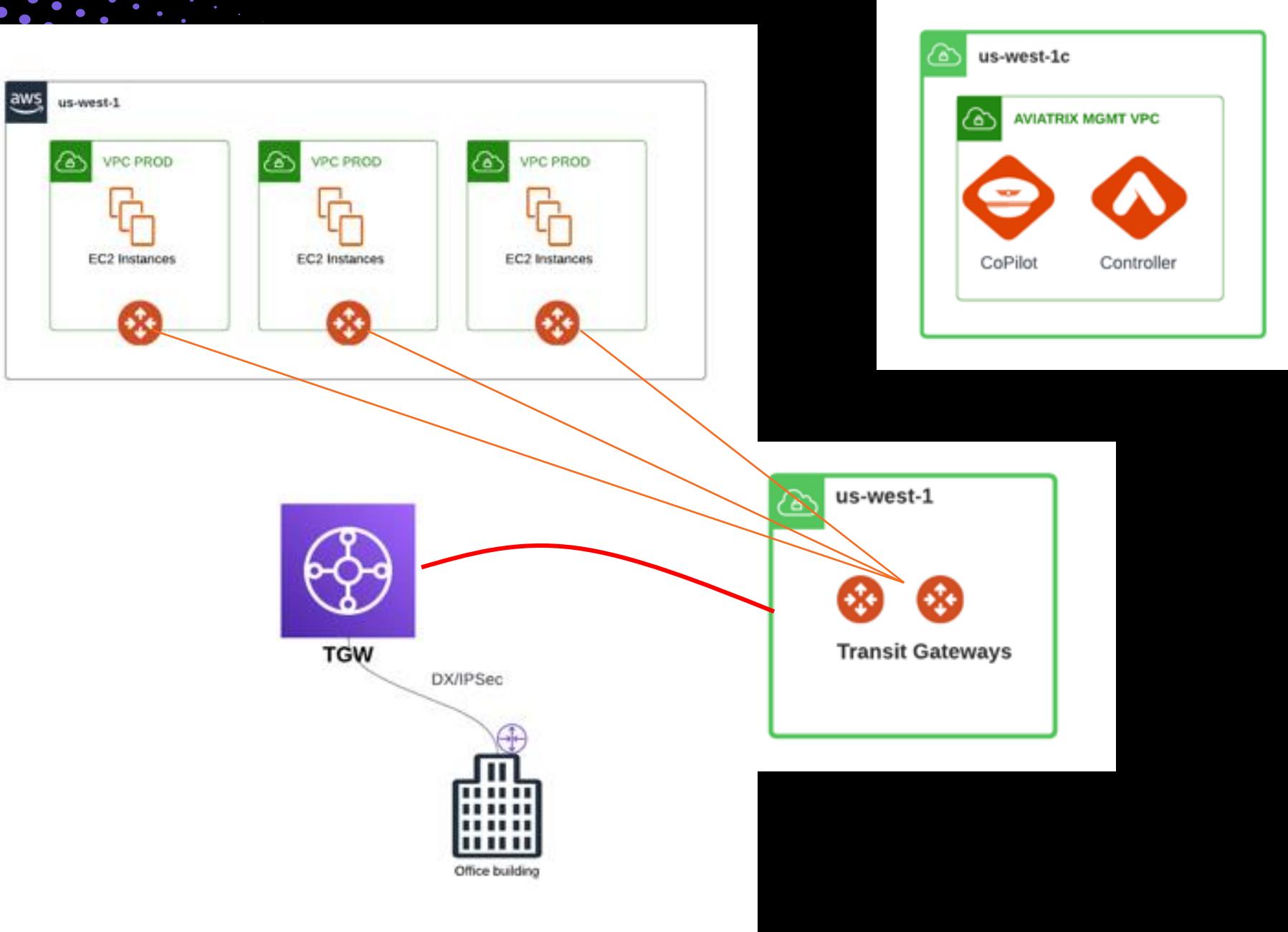
- ❑ Initial environment in a brownfield scenario:
  - Several Application VPCs that are connected to the TGW as attachments
  - OnPrem connectivity (hybrid – can be DX/IPSec)
- ❑ Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed (best practice)
- ❑ Deploy a Transit VPC and deploy a pair of Transit Gateways
- ❑ Establish a back-to-back connection between the Aviatrix Transit Gateways and the AWS TGW

# Migration Deployment: Example



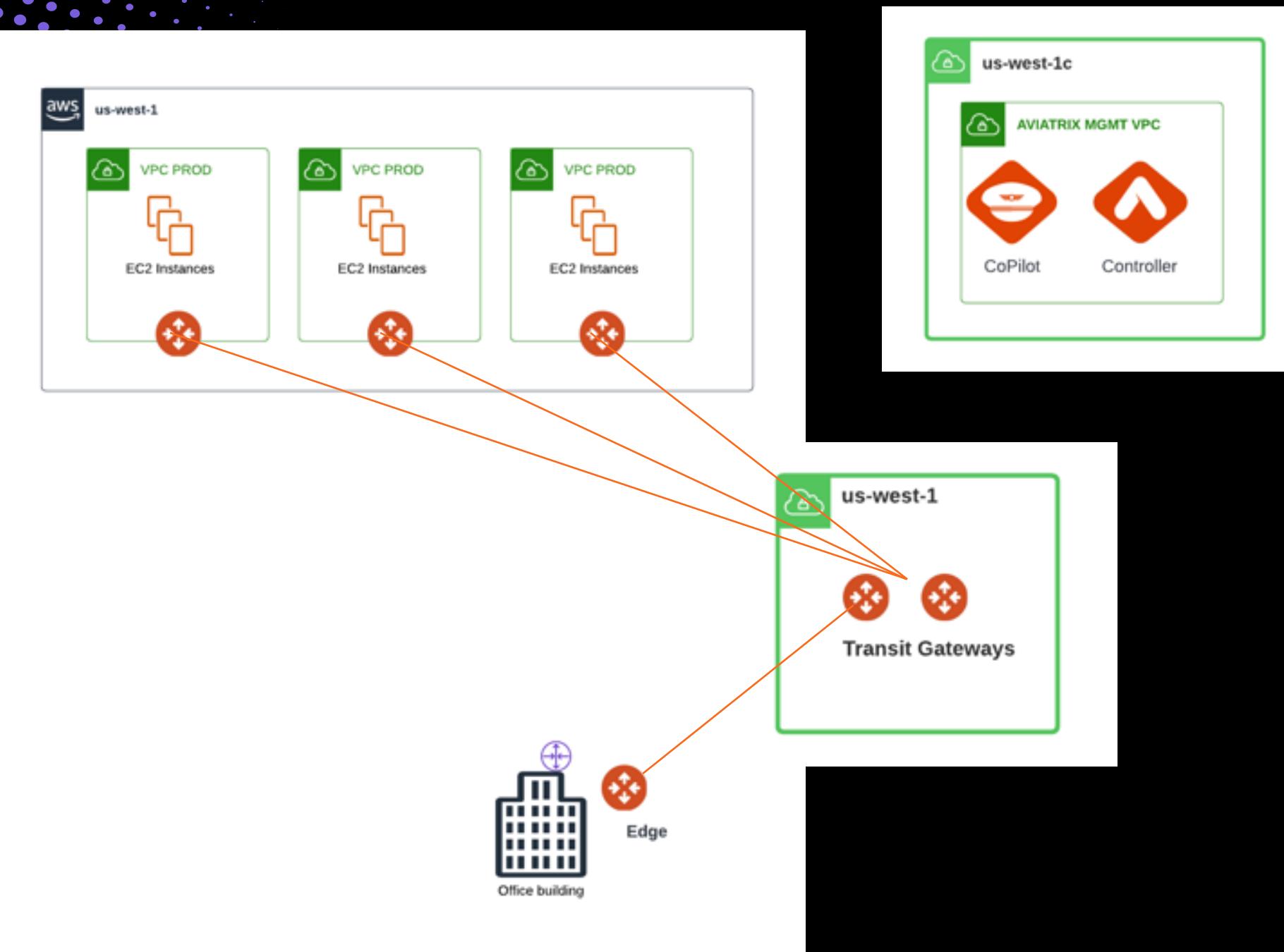
- Initial environment in a brownfield scenario:
  - Several Application VPCs that are connected to the TGW as attachments
  - OnPrem connectivity (hybrid – can be DX/IPSec)
- Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed (best practice)
- Deploy a Transit VPC and deploy a pair of Transit Gateways
- Establish a back-to-back connection between the Aviatrix Transit Gateways and the AWS TGW
- Deploy the Spoke Gateways inside the Application VPCs (this action will not change any routing)

# Migration Deployment: Example



- Initial environment in a brownfield scenario:
  - Several Application VPCs that are connected to the TGW as attachments
  - OnPrem connectivity (hybrid – can be DX/IPSec)
- Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed (best practice)
- Deploy a Transit VPC and deploy a pair of Transit Gateways
- Establish a back-to-back connection between the Transit Gateways and the TGW
- Deploy the Spoke Gateways inside the Application VPCs (this action will not change any routing)
- Remove the connections between the VPCs and the TGW and deploy the attachments between the Spoke Gateways and the Transit Gateways

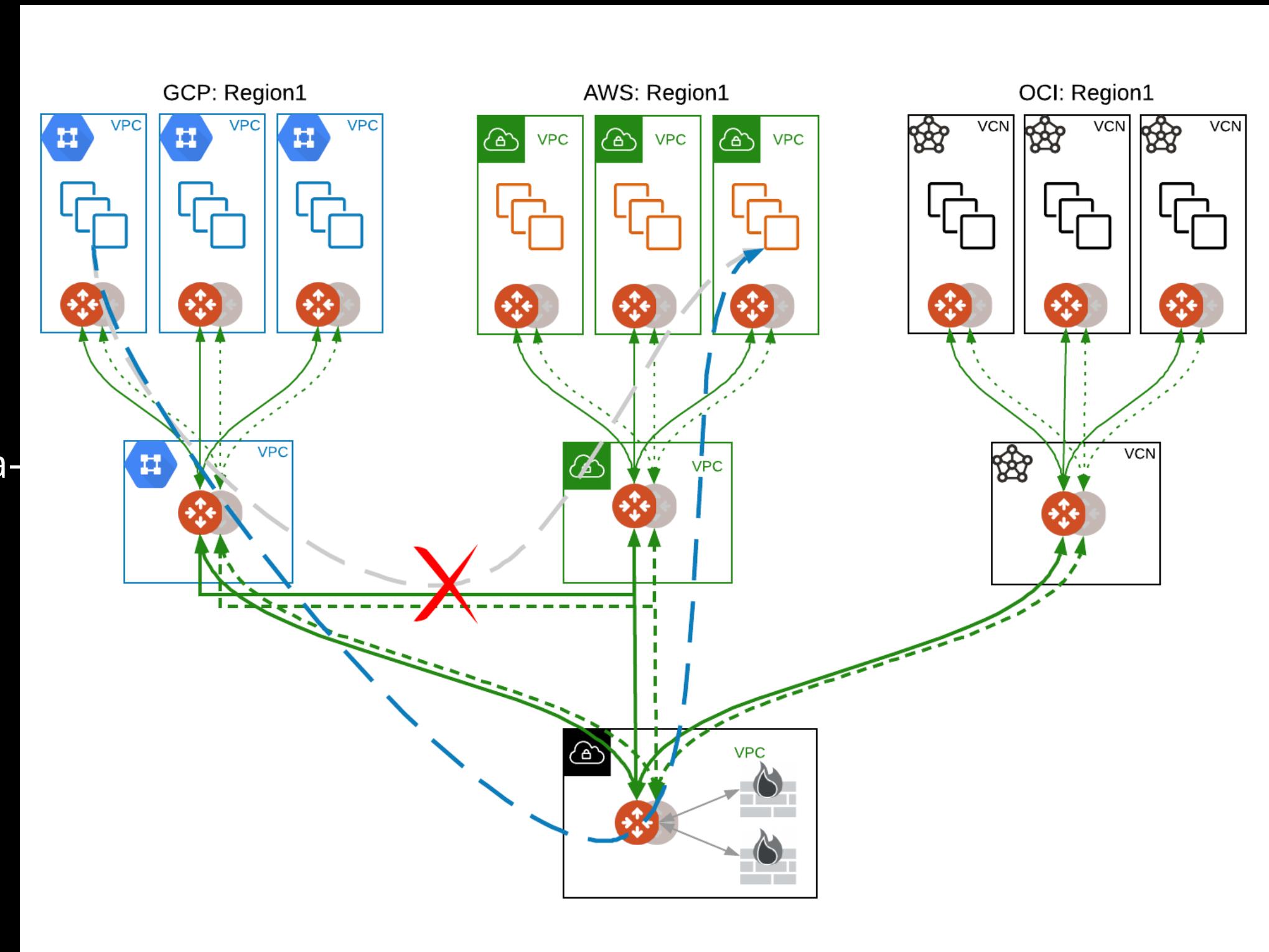
# Migration Deployment: Example



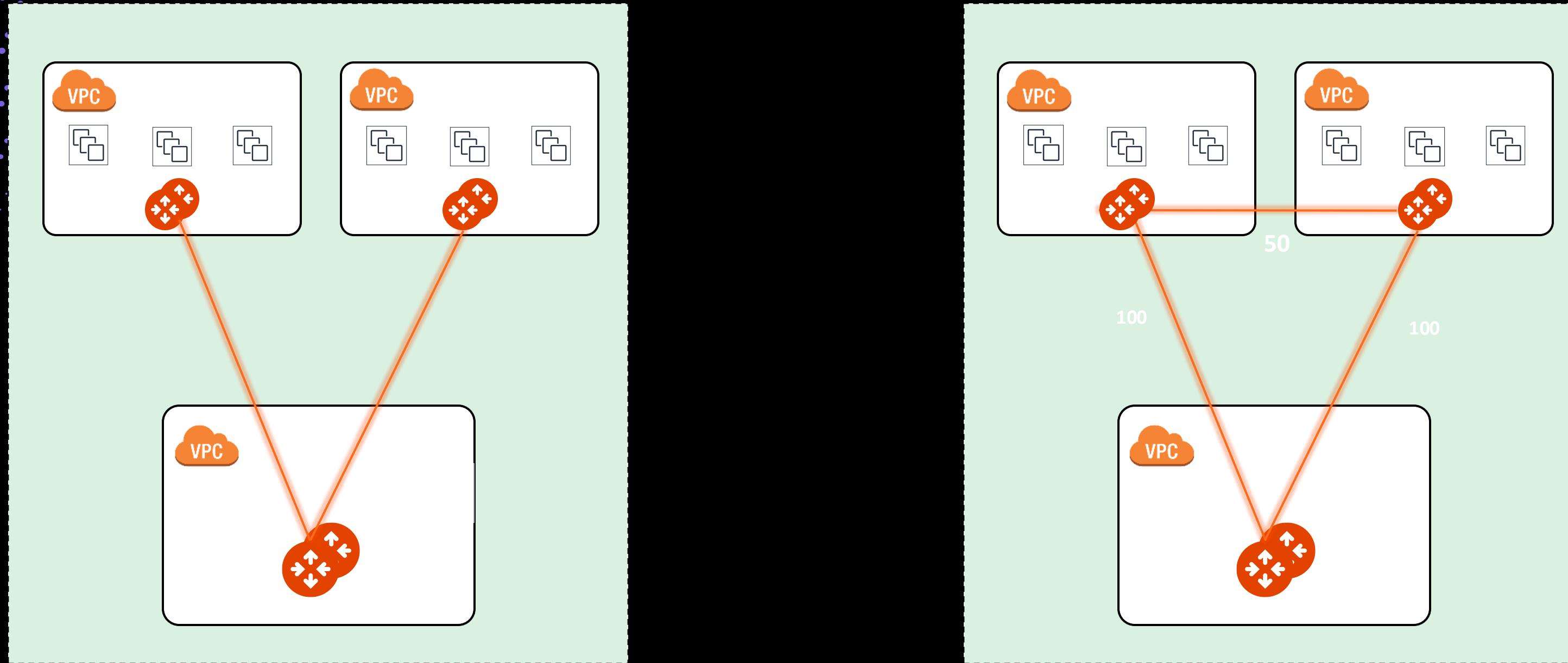
- ❑ Initial environment in a brownfield scenario:
  - Several Application VPCs that are connected to the TGW as attachments
  - OnPrem connectivity (hybrid – can be DX/IPSec)
- ❑ Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed (best practice)
- ❑ Deploy a Transit VPC and deploy a pair of Transit Gateways
- ❑ Establish a back-to-back connection between the Transit Gateways and the TGW
- ❑ Deploy the Spoke Gateways inside the Application VPCs (this action will not change any routing)
- ❑ Remove the connections between the VPCs and the TGW and deploy the attachments between the Spoke Gateways and the Transit Gateways
- ❑ Deploy an Aviatrix Edge and then connect the Edge to the Transit Gateways. If you are not looking for HPE, you can also connect the WAN router as an IPSec connectivity to the Transit Gateways. Last but not least, remove the TGW.

# Multi-Tier Transit (MTT)

- Is the full mesh compulsory on the transit layer? **NO**
- Improves operational simplicity by aggregating multiple Aviatrix Transits (no need for full mesh between transits)
- Additional failover option (pictured in the diagram)
- Allows for centralized firewall design for multiple Aviatrix-Transits in a single region, which allows intra-cloud traffic without any inspection
- To configure Multi-Tier Transit, go to Multi-cloud Transit -> Advanced Config. Select the Transit Gateway and enable the Multi-Tier Transit feature



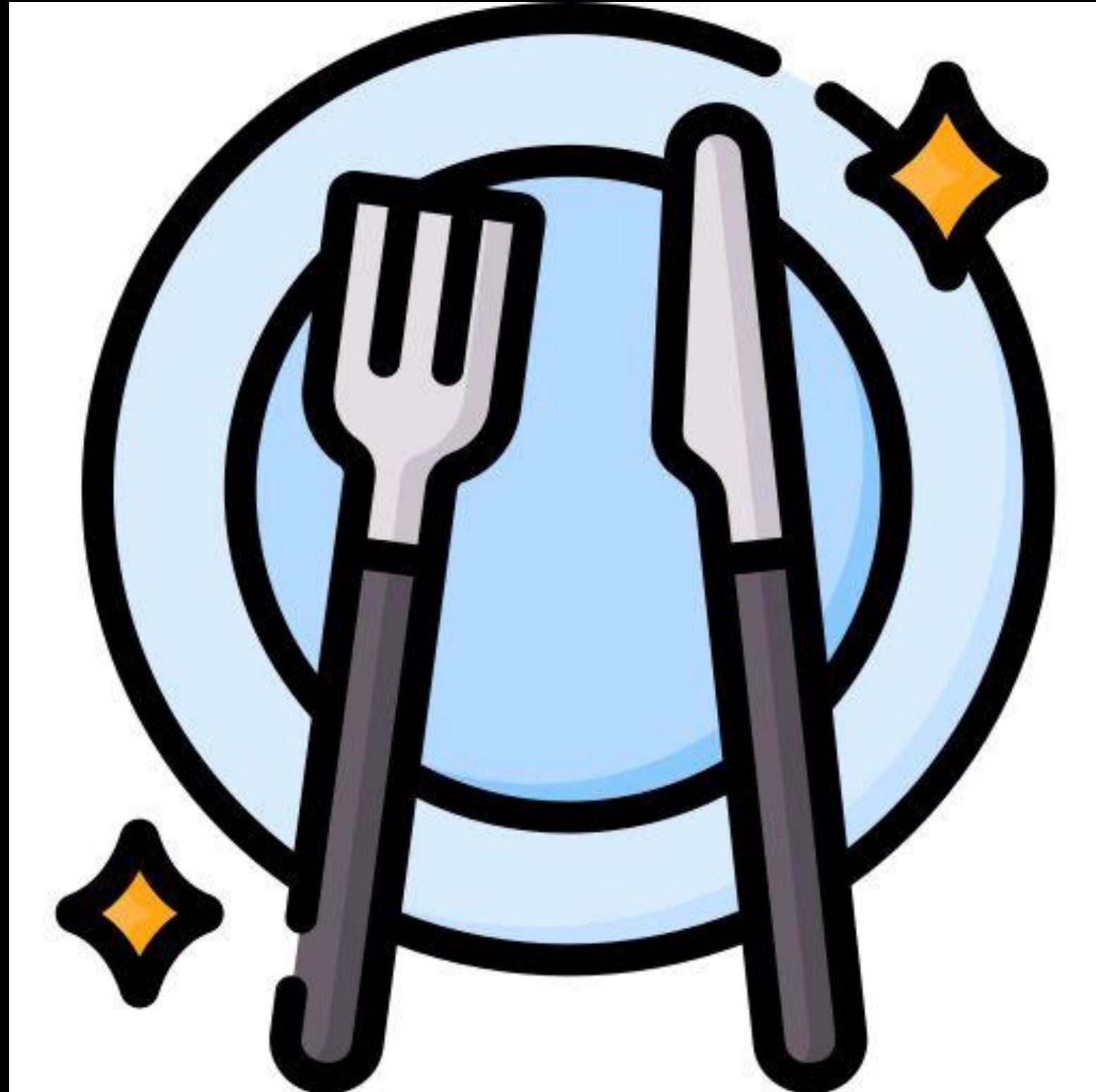
# Spoke-to-Spoke Attachment



- The *Hub and Spoke* model is the default design, however, is NOT compulsory.
- If you require **direct Spoke to Spoke communication**, you can establish an attachment between two Spoke GWs deployed in two different VPCs. The Aviatrix Controller will configure a metric equal to 50.

# Aviatrix Cloud Lunch break

- Core feature: **1 hour break**



# Next: Network Segmentation

---

