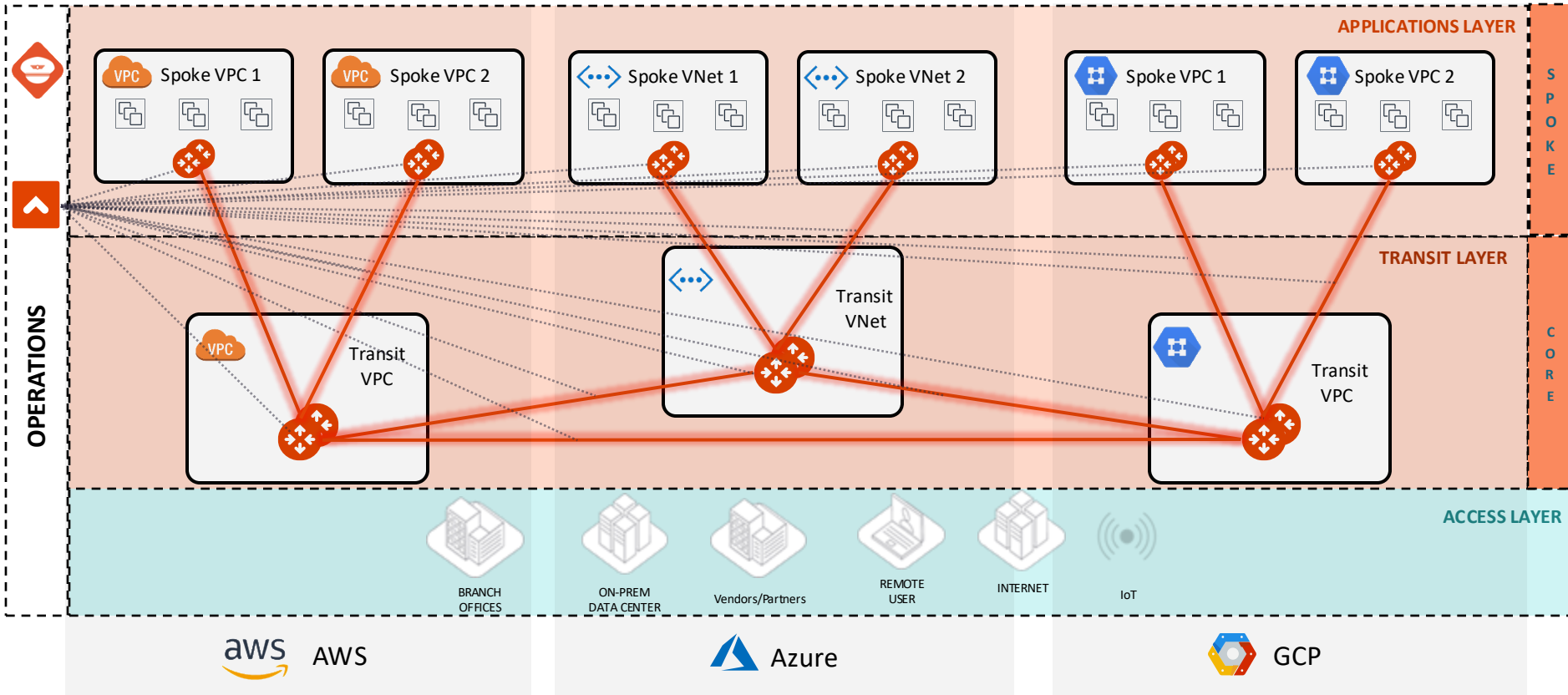




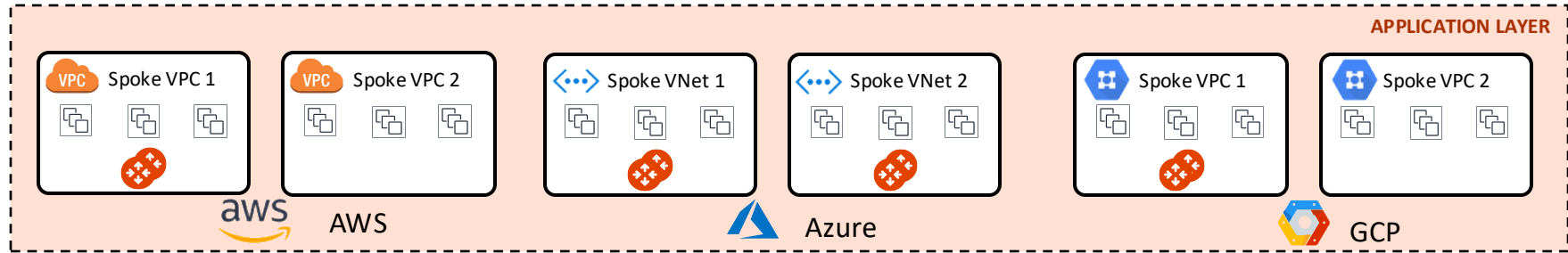
Transit Networking

ACE Team

Cloud Native Security Fabric (CNSF): the Deployment

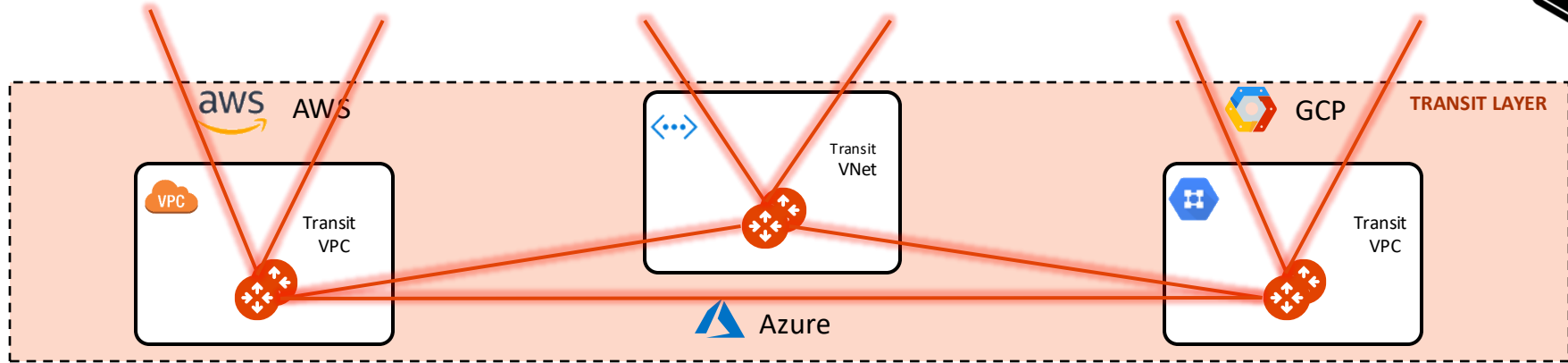


About Spoke Gateways



- A Spoke Gateway is a component of the Aviatrix Platform that you deploy on Spoke VPCs , VNets or VCNs in a hub-and-spoke network topology.
- 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.

About Transit Gateways

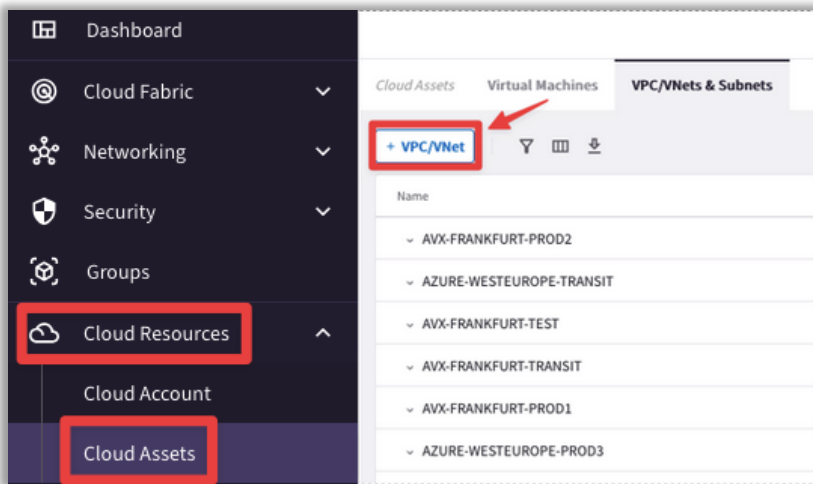
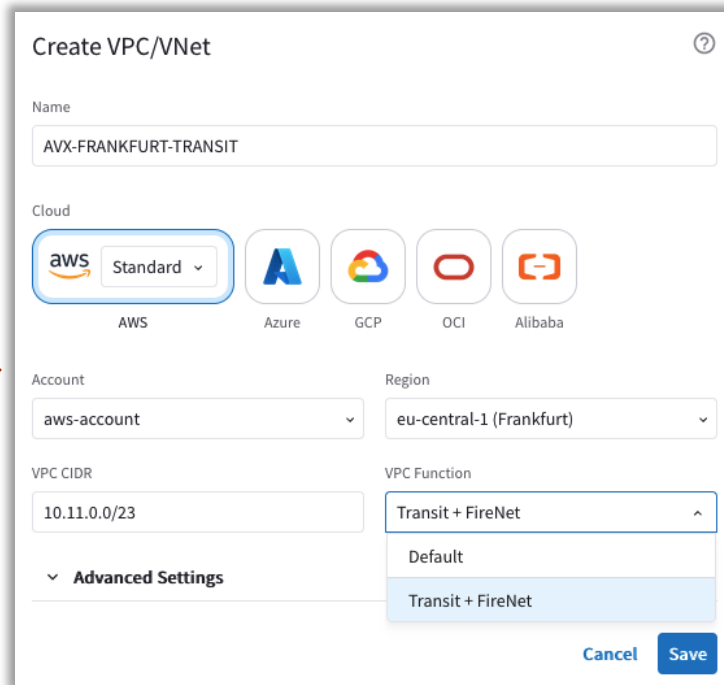


- In Aviatrix's Hub-and-Spoke Topology, a Transit Gateway connects a company's VPCs across the main Cloud Service Providers: AWS, Azure, GCP and OCI.
- The Transit Gateway connection provides **high-speed** and **secure data transfers** between networks while allowing for traffic engineering and multi-account 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 'Create VPC/VNet' form. The form includes the following fields and options:

- Name:** AVX-FRANKFURT-TRANSIT
- Cloud:** AWS (selected), Azure, GCP, OCI, Alibaba
- Account:** aws-account
- Region:** eu-central-1 (Frankfurt)
- VPC CIDR:** 10.11.0.0/23
- VPC Function:** Transit + FireNet (selected), Default
- Advanced Settings:** (collapsed)
- Buttons:** Cancel, Save

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.

Cloud Assets							
Virtual Machines							
VPC/VNets & Subnets							
+ VPC/VNet Actions Filter List Download Search							
<input type="checkbox"/> Name	Cloud	Region	IP Address CIDR	CSP Tags	SmartGroups	Aviatrix Managed	
<input type="checkbox"/> azure-west-us-spoke2	Azure ARM	westus	192.168.2.0/24	Aviatrix-Created-Resource: ..., + 1 more		Yes	
<input type="checkbox"/> gcp-us-central1-transit	GCP					Yes	
<input type="checkbox"/> gcp-us-central1-spoke1	GCP					Yes	
<input type="checkbox"/> aws-us-east-1-spoke1	AWS	us-east-1	10.0.12.0/24	Name: aws-us-east-1-spoke1, + 1 more		Yes	
<input type="checkbox"/> aws-us-east-2-spoke1	AWS	us-east-2	10.0.1.0/24	Name: aws-us-east-2-spoke1, + 1 more		Yes	
<input type="checkbox"/> azure-west-us-transit	Azure ARM	westus	192.168.10.0/23	Aviatrix-Created-Resource: ..., + 1 more		Yes	
<input type="checkbox"/> azure-west-us-spoke1	Azure ARM	westus	192.168.1.0/24	Aviatrix-Created-Resource: ..., + 1 more		Yes	
<input type="checkbox"/> aws-us-east-2-transit	AWS	us-east-2	10.0.10.0/23	Aviatrix-Created-Resource: ..., + 1 more		Yes	
<input type="checkbox"/> aws-us-east-1-transit	AWS	us-east-1	10.0.20.0/23	Name: aws-us-east-1-transit, + 1 more		Yes	
<input type="checkbox"/> vpc-574bab31	AWS	ap-southeast-1	172.31.0.0/16			No	
<input type="checkbox"/> vpc-3bf48952	AWS	ap-northeast-3	172.31.0.0/16			No	
<input type="checkbox"/> on-prem-partner1	AWS	us-east-1	172.16.1.0/24	Terraform: true, + 2 more		No	
<input type="checkbox"/> vpc-390a155e	AWS	sa-east-1	172.31.0.0/16			No	
<input type="checkbox"/> default	GCP					No	
<input type="checkbox"/> 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: Viewing virtual machines running in your Clouds

- 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)

Cloud Assets						
Virtual Machines						
VPC/VNets & Subnets						
Actions						
Search						
Name	Cloud	Region	IP Address	Tags	SmartGroups	Aviatrix Managed
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

Greenfield Deployment (VPC/VNet/VCN creation)

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

Creation of the Transit VPC

CIDR 10.11.0.0/23



- 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).



[AVXERR-TOOLS-0030] VPC/VNet CIDR size must be between 16 to 23. e.g. 10.0.0.0/20

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

Internet gateways (1/1) [Info](#)

Filter internet gateways

search: AVX-FRANKFURT-TRANSIT

Clear filters

<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input checked="" type="checkbox"/>	AVX-FRANKFURT-TRANSIT	lgw-06d499f4d0f772915	Attached	vpc-01f51fa31db0c8458 AVX-FRANKFURT-TRANSIT

Greenfield Deployment (VPC/VNet/VCN creation)

CIDR 10.11.0.0/23



❖ The subnets' size can be customized

Advanced Settings

Subnet Size: Optional

Number of Subnet Pair(s): Optional

[Cancel](#) [Save](#)

❑ 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) [Info](#)

Filter subnets

search: AVX-FRANKFURT-TRANSIT X Clear filters

<input type="checkbox"/>	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

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
 - Private RTB will encompass the 4 private subnets

Destination	Target
0.0.0.0/0	lgw-06d499f4d0f772915
10.11.0.0/23	local

Destination	Target
10.11.0.0/23	local

Route tables (2) Info			
<input type="text" value="Filter route tables"/>			
<div> <div>search: AVX-FRANKFURT-TRANSIT X</div> <div>Clear filters</div> </div>			
<input type="checkbox"/>	Name	Route table ID	Explicit subnet associations
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Public-rtb	rtb-0e5a22d0060c17eac	4 subnets
<input type="checkbox"/>	AVX-FRANKFURT-TRANSIT-Private-rtb	rtb-085cf49590ee4592d	4 subnets

Greenfield Deployment (VPC/VNet/VCN creation)

CIDR 10.1.1.0/24



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

A screenshot of the AWS Management Console showing the 'Internet gateways' page. The page title is 'Internet gateways (1/1) Info'. There is a search bar with the text 'Filter internet gateways'. Below it, a search filter is applied: 'search: AVX-FRANKFURT-SPOKE-PROD'. A table lists the internet gateway. The table has columns: Name, Internet gateway ID, State, and VPC ID. The row shows 'AVX-FRANKFURT-SPOKE-PROD' with ID 'igw-0327c092c11fbd749', state 'Attached', and VPC ID 'vpc-068d94ca168a85633 | AVX-FRANKFURT-SPOKE-PROD'.

<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID
<input checked="" type="checkbox"/>	AVX-FRANKFURT-SPOKE-PROD	igw-0327c092c11fbd749	Attached	vpc-068d94ca168a85633 AVX-FRANKFURT-SPOKE-PROD

Greenfield Deployment (VPC/VNet/VCN creation)

CIDR 10.1.1.0/24



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

Subnets (6) [Info](#)

Filter subnets

search: AVX-FRANKFURT-SPOKE-PROD X Clear filters

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

❖ The subnets' size can be customized

Advanced Settings

Subnet Size: Optional

Number of Subnet Pair(s): Optional

Cancel Save

[Aviatrix Spoke VPC – Aviatrix Official Documentation](#)

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	lgw-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

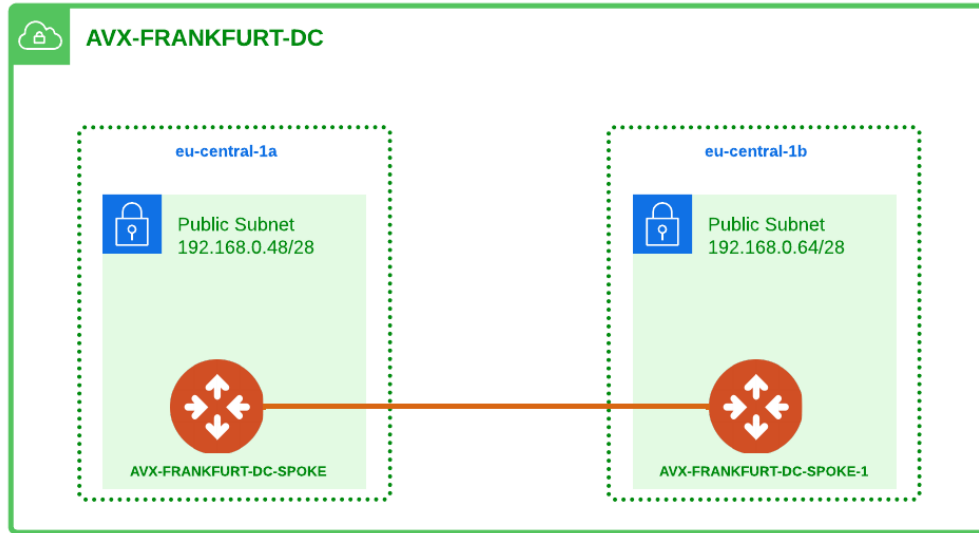
Route tables (6) [Info](#)

search: AVX-FRANKFURT-SPOKE-PROD

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associations
<input type="checkbox"/>	AVX-FRANKFURT-SPOKE-PROD-Private-1-eu-central-1a-rtb	rtb-0ca98234a5088dceb	subnet-060df41c64a2c643a / AVX-FRANKFURT-SPOKE-PROD-Private-1-eu-central-1a
<input type="checkbox"/>	AVX-FRANKFURT-SPOKE-PROD-Private-2-eu-central-1b-rtb	rtb-0cad721a70d6256d9	subnet-00bf95727955ec09b / AVX-FRANKFURT-SPOKE-PROD-Private-2-eu-central-1b
<input type="checkbox"/>	AVX-FRANKFURT-SPOKE-PROD-Private-3-eu-central-1c-rtb	rtb-04afaa976264662ac	subnet-0bd05503b4b1f880c / AVX-FRANKFURT-SPOKE-PROD-Private-3-eu-central-1c
<input type="checkbox"/>	AVX-FRANKFURT-SPOKE-PROD-Public-1-eu-central-1a-rtb	rtb-0c52cd5084b440f2d	subnet-0b22457ff5b1a4895 / AVX-FRANKFURT-SPOKE-PROD-Public-1-eu-central-1a
<input type="checkbox"/>	AVX-FRANKFURT-SPOKE-PROD-Public-2-eu-central-1b-rtb	rtb-0c973dec3847ae8ce	subnet-0c140dc3d0af1fa65 / AVX-FRANKFURT-SPOKE-PROD-Public-2-eu-central-1b
<input type="checkbox"/>	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.

CLUSTER

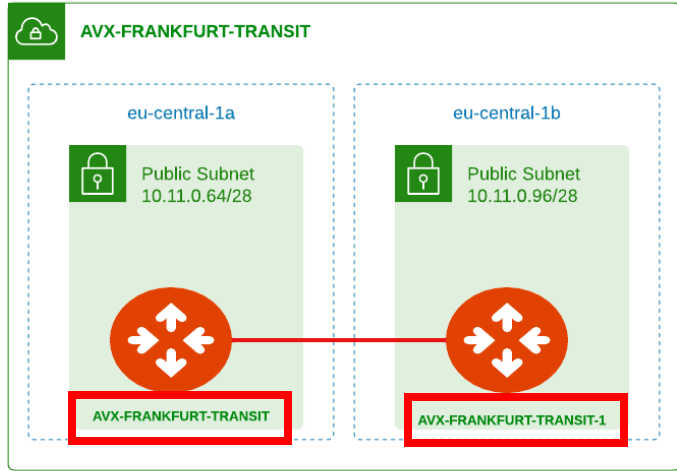
GW #1

GW #2

•	AVX-FRANKFURT-DC-SPOKE	eu-central-1	vpc-04d947b7b73180e3c~~AVX-FRANKFURT-DC	
•	AVX-FRANKFURT-DC-SPOKE	eu-central-1	vpc-04d947b7b73180e3c~~AVX-FRANKFURT-DC	192.168.0.48/28
•	AVX-FRANKFURT-DC-SPOKE-1	eu-central-1	vpc-04d947b7b73180e3c~~AVX-FRANKFURT-DC	192.168.0.64/28

Greenfield Deployment (Transit Gateways deployment)

CIDR 10.11.0.0/23



Transit Gateways Deployment through the CoPilot

Create Transit Gateway

Name: AVX-FRANKFURT-TRANSIT

Cloud: ☒ AWS Standard ☐ Azure ☐ GCP ☐ OCI ☐ Alibaba

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: Optional

Instances

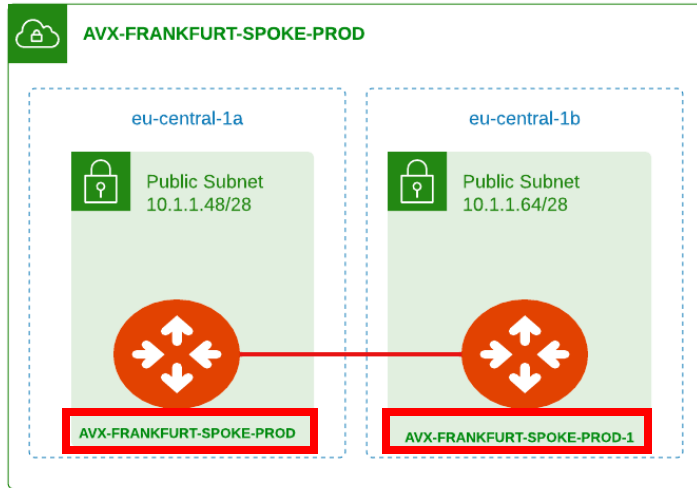
	Attach to Subnet	Public IP
1	10.11.0.64/28	Allocate New Static Public IP
2	10.11.0.96/28	Allocate New Static Public IP

Cancel Save

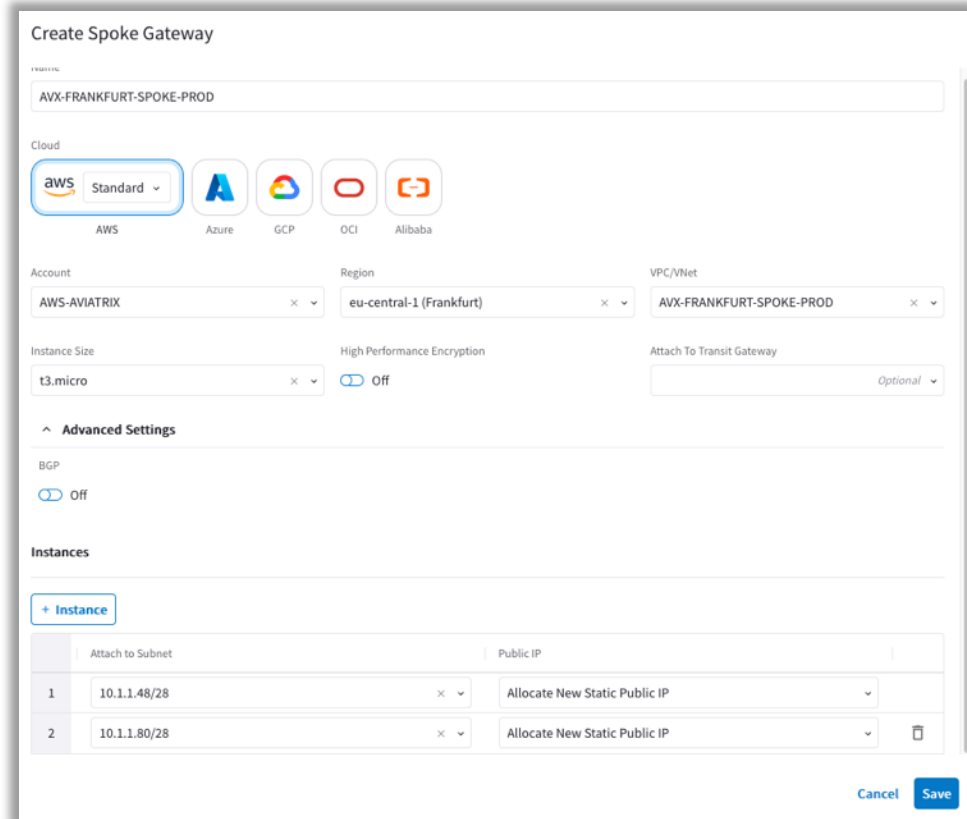
- ❖ The connection between the Transit Gateways is automatically created by the Controller.
- ❖ **Best Practice:** always deploy the Transit Gateway-1 (i.e the second gateway), and choose a different AZ.
- ❖ Only two Transit Gateways can be deployed per Transit VPC
- ❖ Aviatrix gateways are deployed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

Greenfield Deployment (Spoke Gateways deployment)

CIDR 10.1.1.0/24



Spoke Gateways Deployment through the CoPilot



Create Spoke Gateway

NAME: AVX-FRANKFURT-SPOKE-PROD

Cloud: ☐ AWS ☐ Azure ☐ GCP ☐ OCI ☐ Alibaba

Account: AWS-AVIATRIX Region: eu-central-1 (Frankfurt) VPC/VNet: AVX-FRANKFURT-SPOKE-PROD

Instance Size: t3.micro High Performance Encryption: ☐ Off Attach To Transit Gateway: ☐ Optional

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

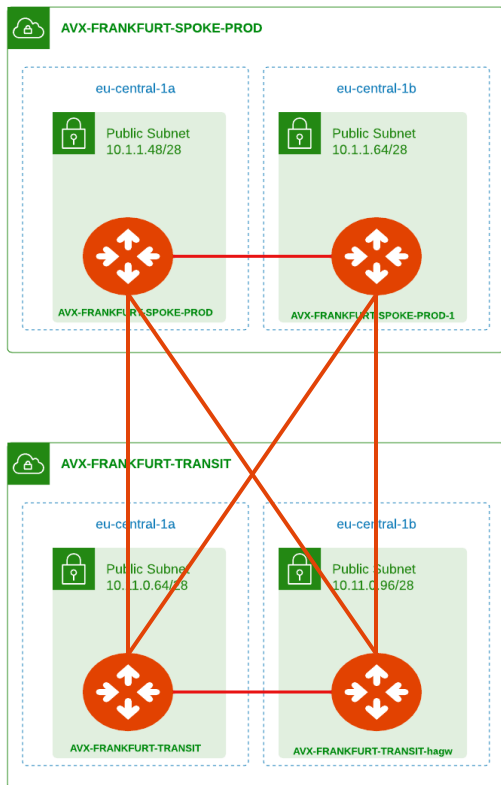
Cancel Save

- ❖ 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 (Attachment 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

	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 (Attachment 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.

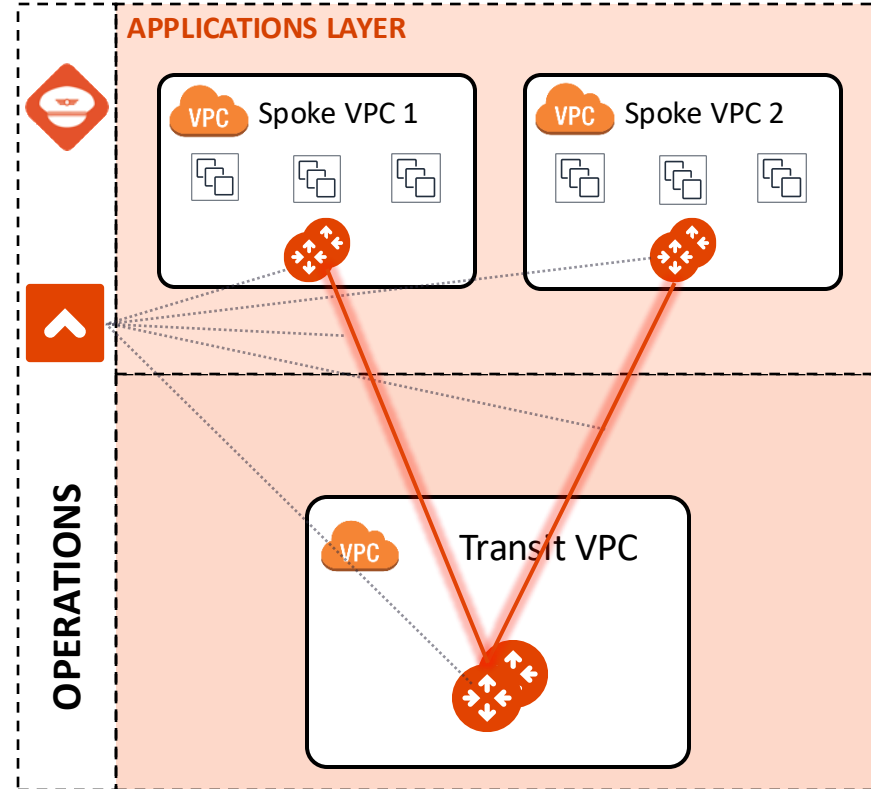
Routes	Subnet associations	Edge associations	Route propagation	Tags
Routes (4)				
Filter routes				
Destination		Target		
10.0.0.0/8		eni-08ac50fc16cd8c4a5		
10.1.1.0/24		local		
172.16.0.0/12		eni-08ac50fc16cd8c4a5		
192.168.0.0/16		eni-08ac50fc16cd8c4a5		

Route table for
Private Subnet

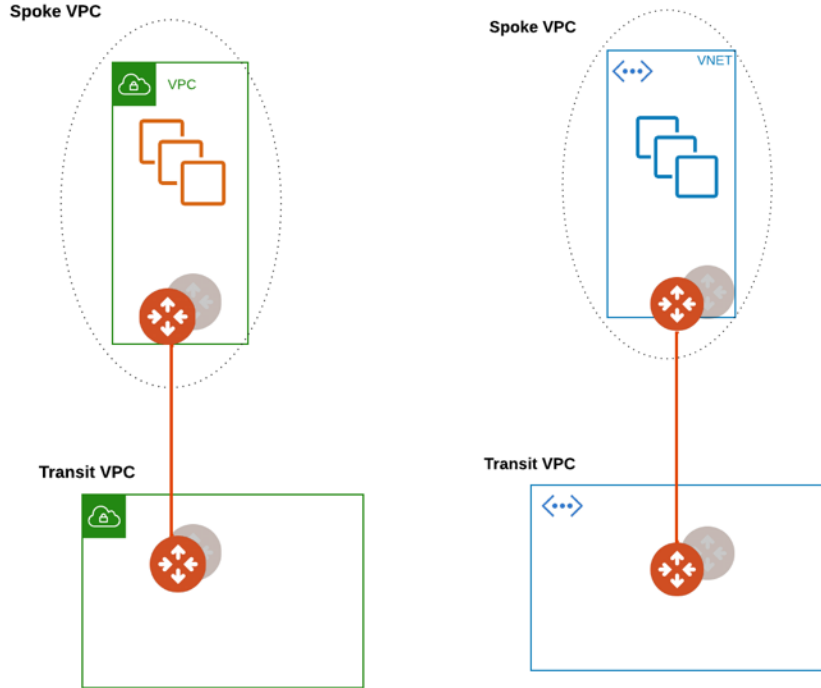
Routes	Subnet associations	Edge associations	Route propagation	Tags
Routes (5)				
Filter routes				
Destination		Target		
0.0.0.0/0		igw-07c6ddedd190d12d3		
10.0.0.0/8		eni-08ac50fc16cd8c4a5		
10.1.1.0/24		local		
172.16.0.0/12		eni-08ac50fc16cd8c4a5		
192.168.0.0/16		eni-08ac50fc16cd8c4a5		

Route table for
Public Subnet

Attachment = RFC1918 Routes Injection

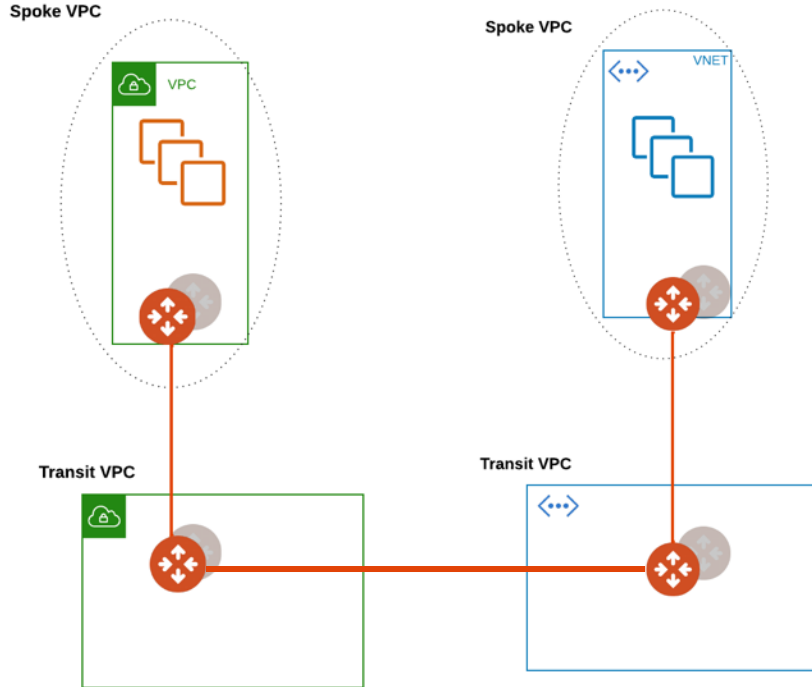


Greenfield Deployment (Repeatable Design)



- ❑ 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 **MCNA**.

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 x Optional x

Instances

+ Instance

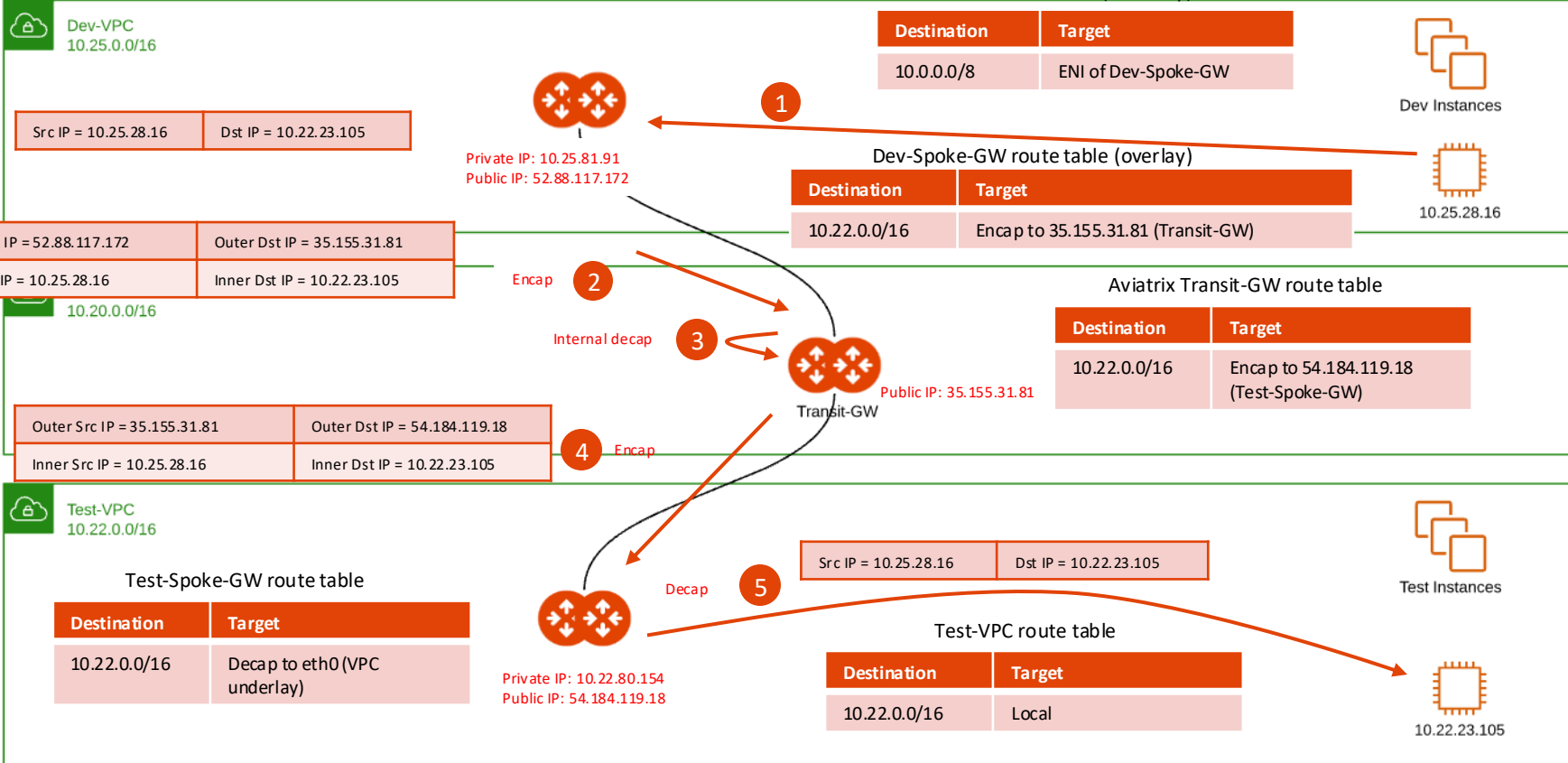
	Attach to Subnet	Public IP
1	10.11.0.64/28	3.75.164.186
2	10.11.0.96/28	3.127.251.156

Cancel Save

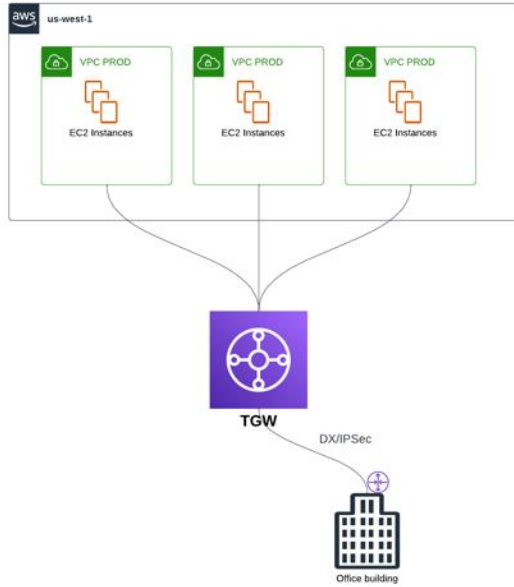
Packet Walk



us-west-2



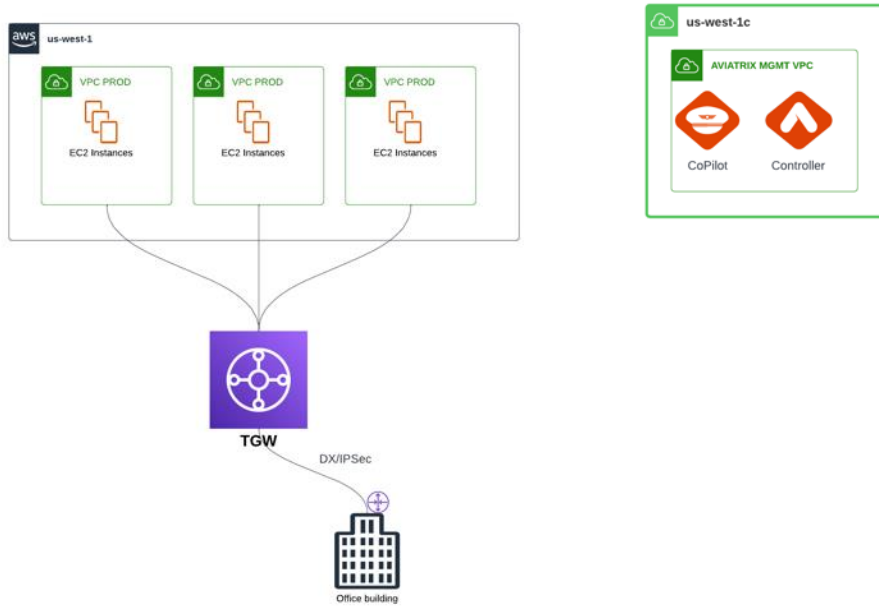
Typical Migration Deployment



Initial environment in a brownfield scenario:

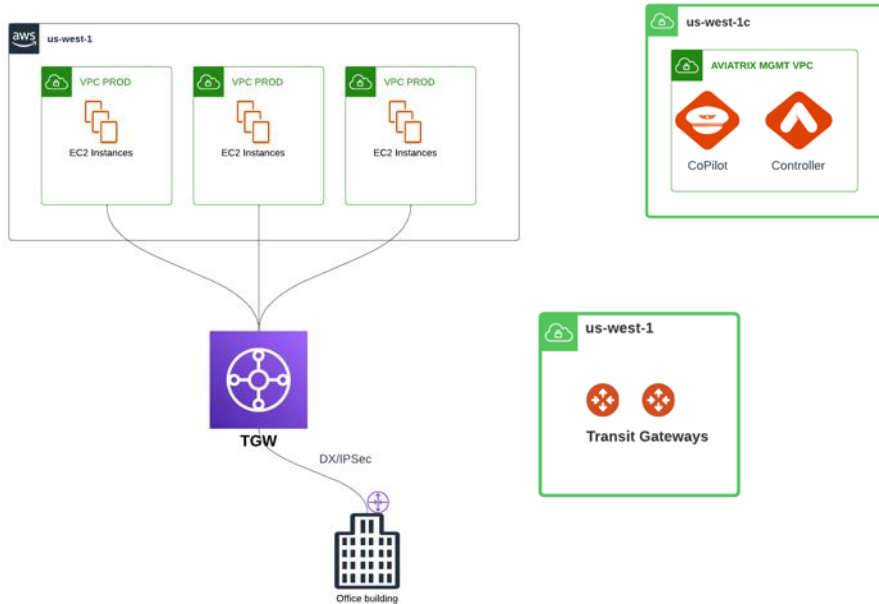
- Several Application VPCs that are connected to the TGW as attachments
- OnPrem connectivity (hybrid – can be DX/IPSec)

Typical Migration Deployment



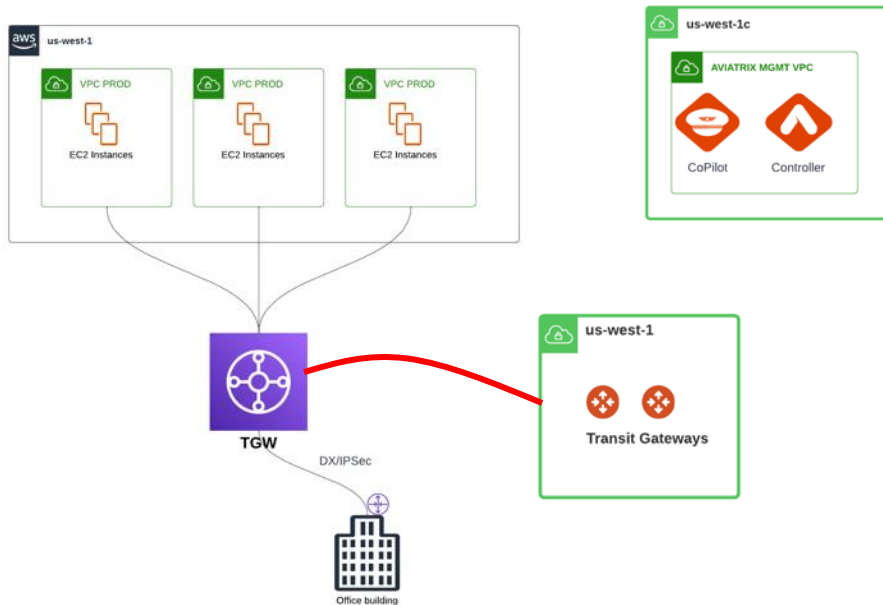
- ❑ **Initial environment in a brownfield scenario:**
 - Several Application VPCs that are connected to the TGW as attachments
 - OnPrem connectivity (hybrid – can be DX/IPSec)
- ❑ **Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed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

Typical Migration Deployment



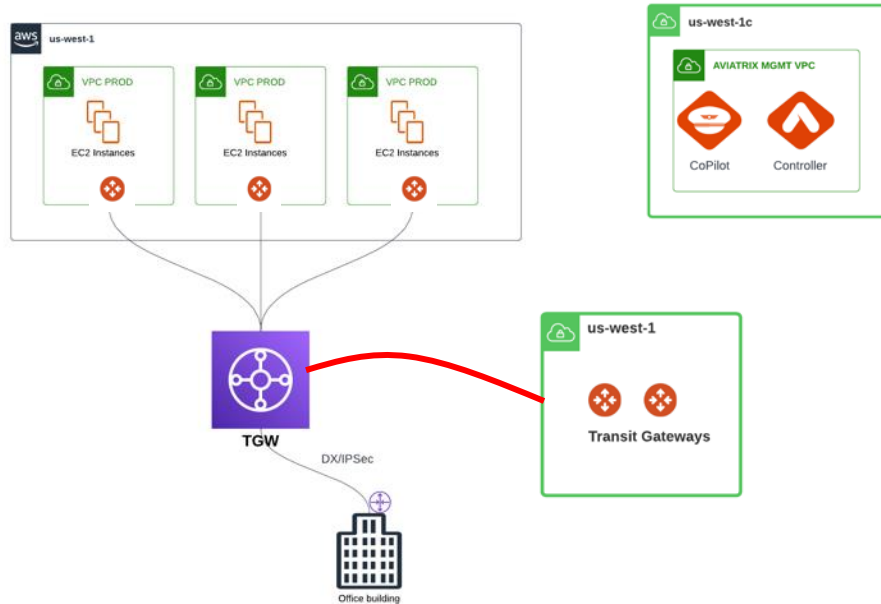
- ❑ **Initial environment in a brownfield scenario:**
 - Several Application VPCs that are connected to the TGW as attachments
 - OnPrem connectivity (hybrid – can be DX/IPSec)
- ❑ **Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed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

Typical Migration Deployment



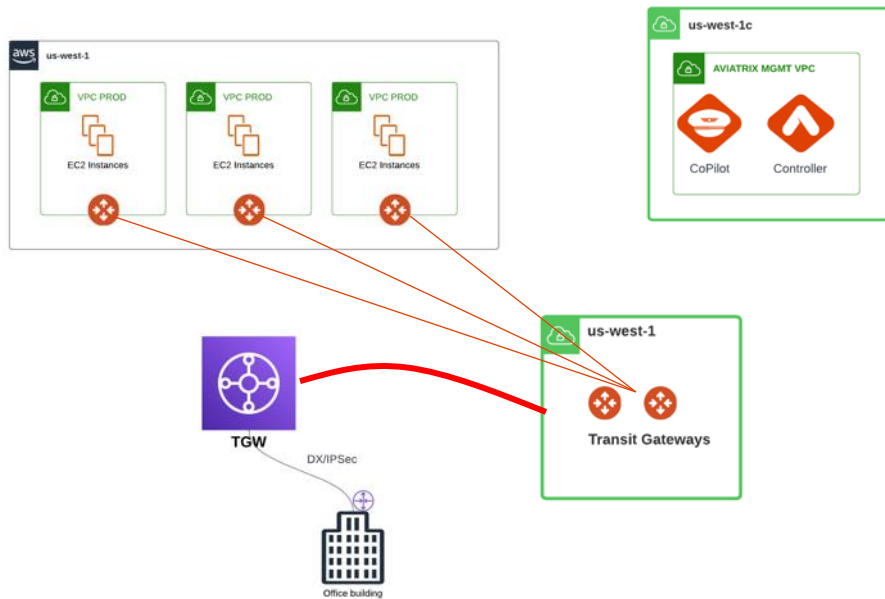
- ❑ **Initial environment in a brownfield scenario:**
 - Several Application VPCs that are connected to the TGW as attachments
 - OnPrem connectivity (hybrid – can be DX/IPSec)
- ❑ **Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed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

Typical Migration Deployment



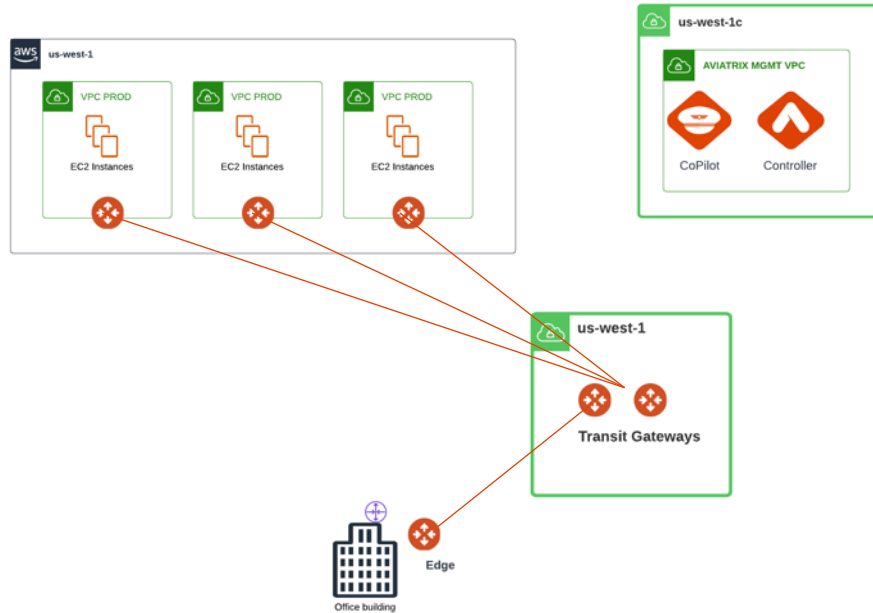
- ❑ **Initial environment in a brownfield scenario:**
 - Several Application VPCs that are connected to the TGW as attachments
 - OnPrem connectivity (hybrid – can be DX/IPSec)
- ❑ **Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed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

Typical Migration Deployment



- ❑ **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**

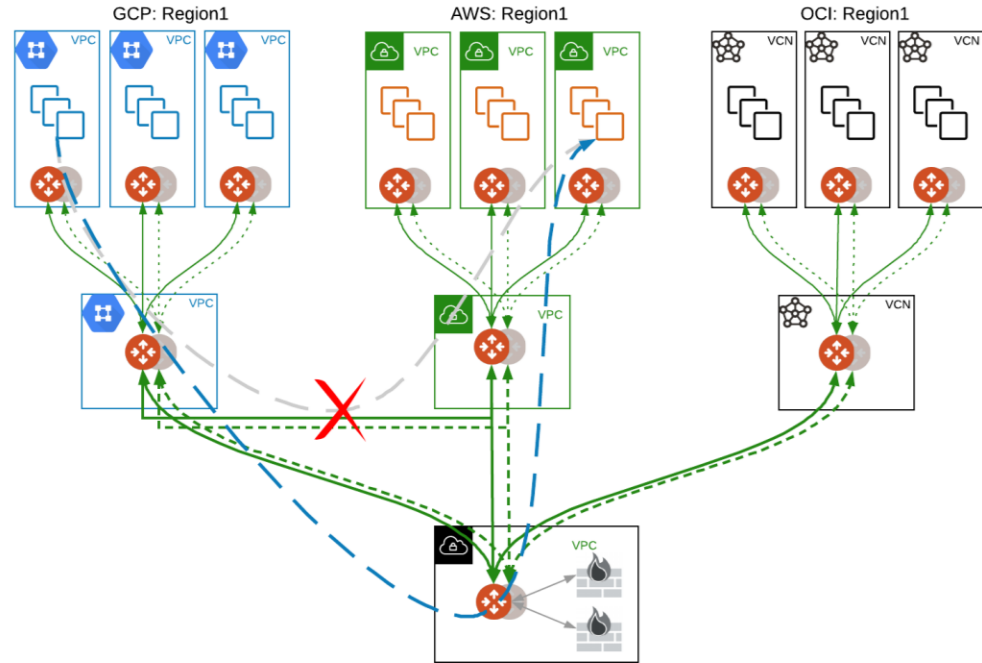
Typical Migration Deployment



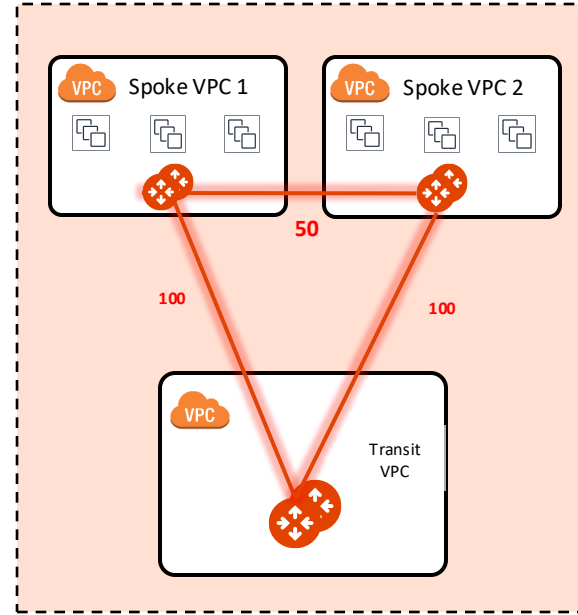
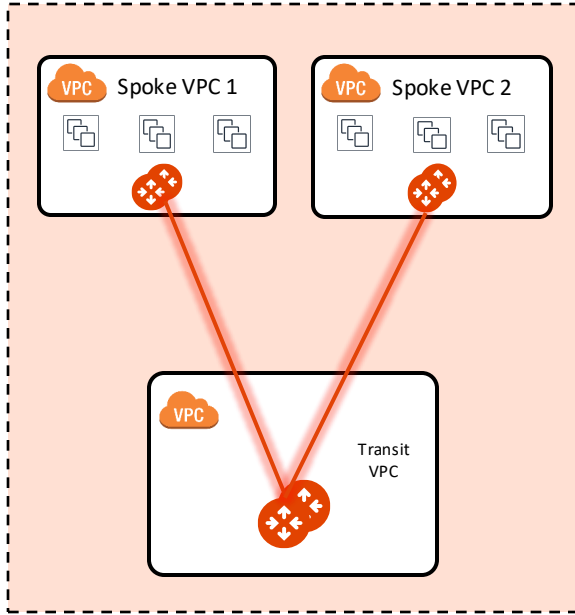
- ❑ **Initial environment in a brownfield scenario:**
 - Several Application VPCs that are connected to the TGW as attachments
 - OnPrem connectivity (hybrid – can be DX/IPSec)
- ❑ **Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed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



Next: Lab 2 – (MCNA) Transit
Networking