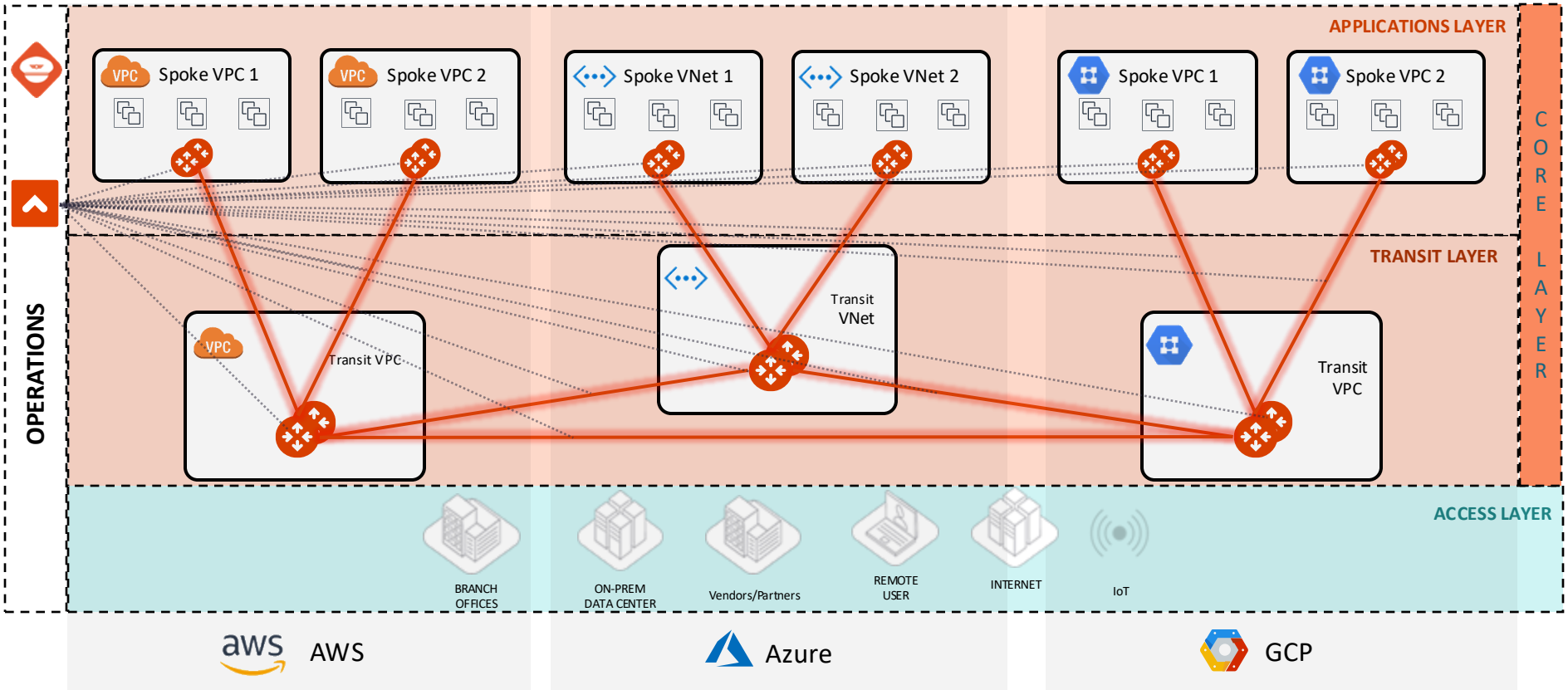
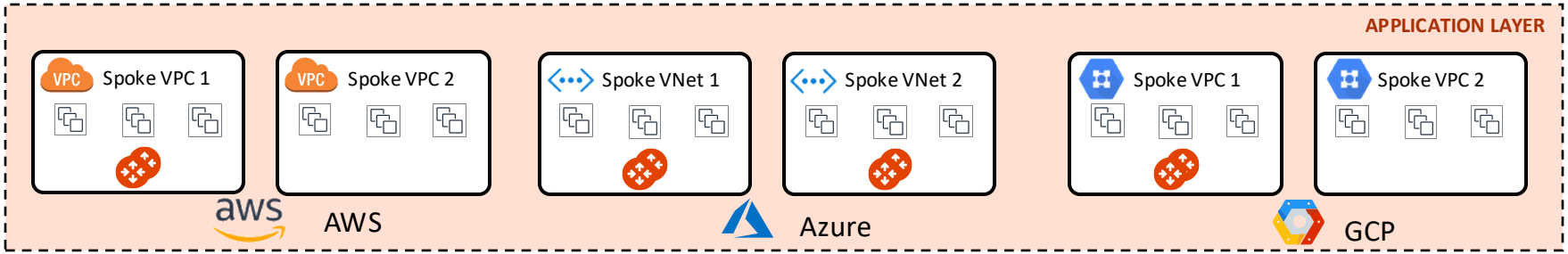
Transit Networking

ACE Technical Team

MCNA Deployment: the Foundations

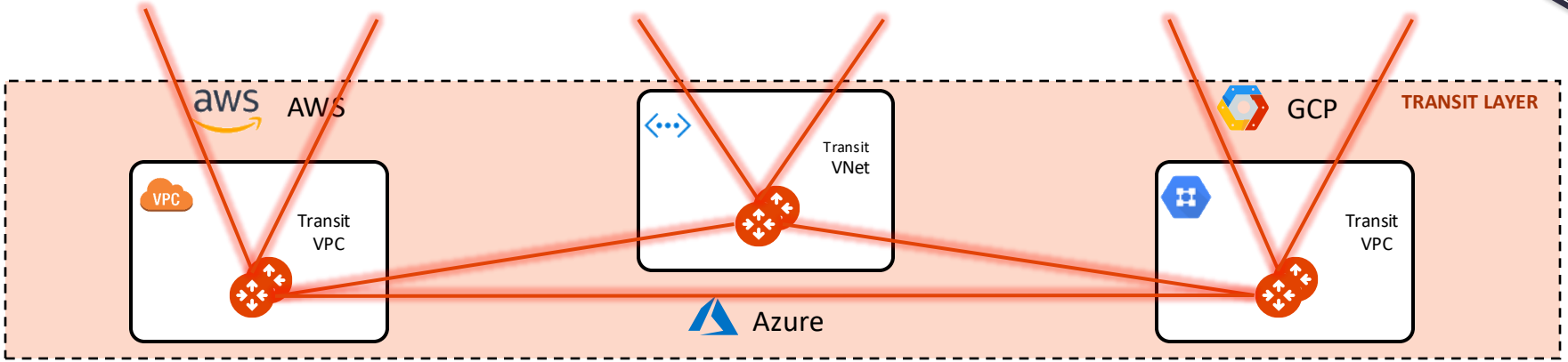


About Spoke Gateways



- 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 p rivate 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

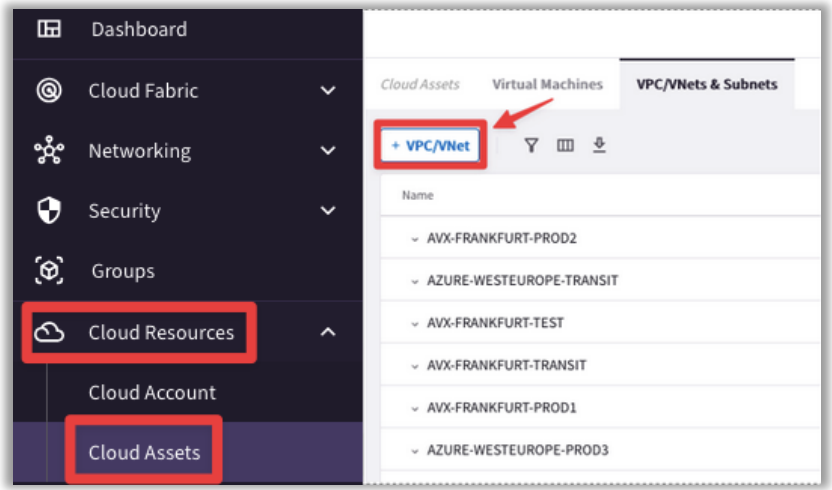


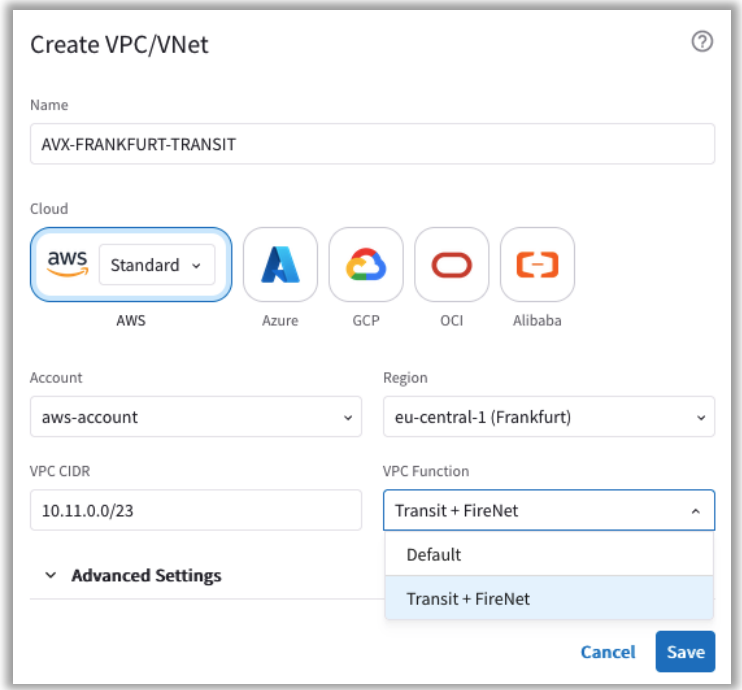
- In Aviatrix's Hub-and-Spoke Topology, a Transit Gateway connects a company's VPCs across the main Cloud Service Providers: AWS, Azure, GCP and OCI.
- The Transit Gateway connection provides **high-speed** and **secure data transfers** between networks while allowing for traffic engineering and multi-account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

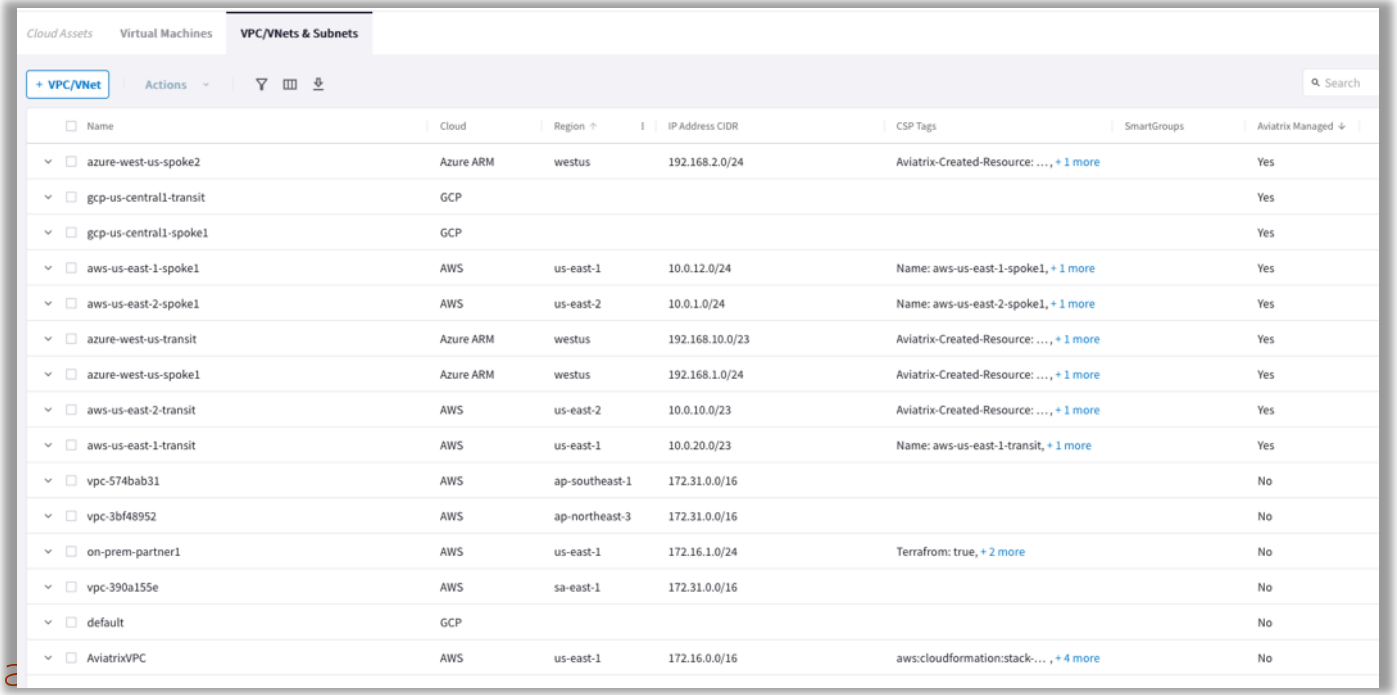
- On the CoPilot you can create a new VPC/VNet/VCN.
- This feature is not only useful in a Greenfield deployment, but also if you need to add a new VPC/VNet/VCN on an existing environment, based on the architecture design.
- You can create two types of VPC/VNet/VCN:
  - **Default** (i.e. Spoke)
  - **Transit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





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.

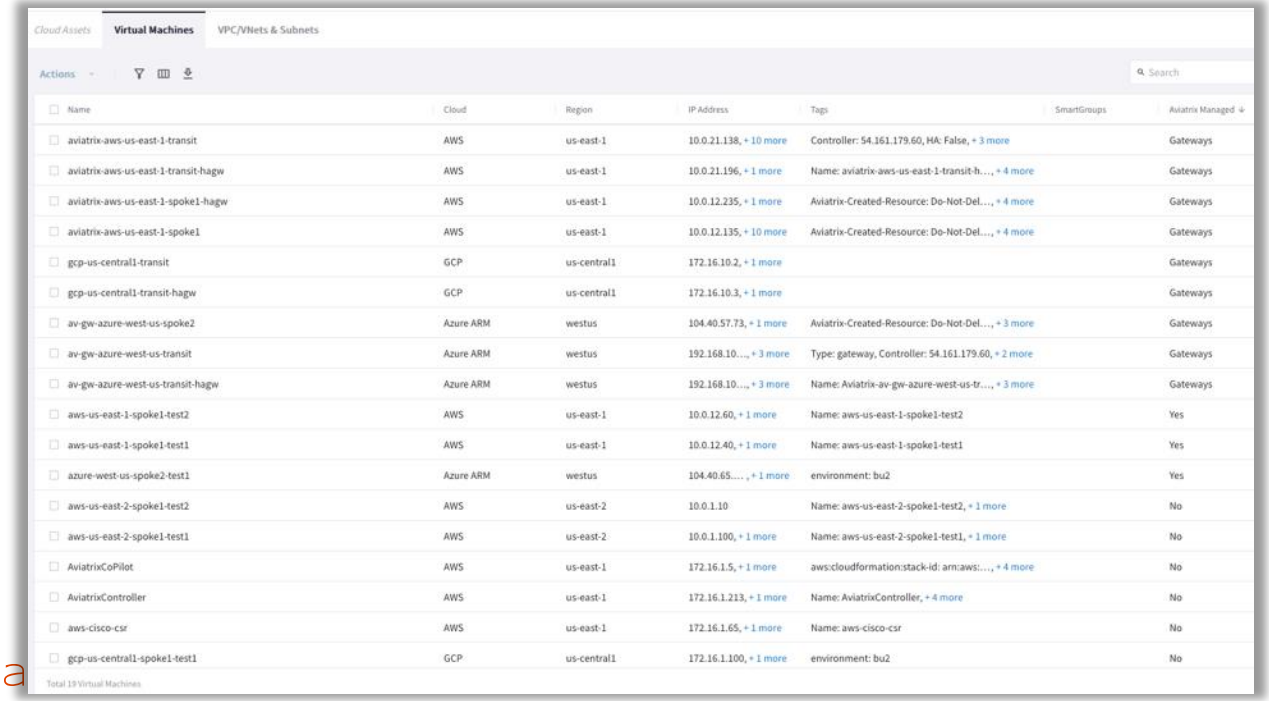


Name	Cloud	Region	IP Address CIDR	CSP Tags	SmartGroups	Aviatrix Managed
azure-west-us-spoke2	Azure ARM	westus	192.168.2.0/24	Aviatrix-Created-Resource: ..., + 1 more		Yes
gcp-us-central1-transit	GCP					Yes
gcp-us-central1-spoke1	GCP					Yes
aws-us-east-1-spoke1	AWS	us-east-1	10.0.12.0/24	Name: aws-us-east-1-spoke1, + 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	Terrafrom: 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 ineast 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)



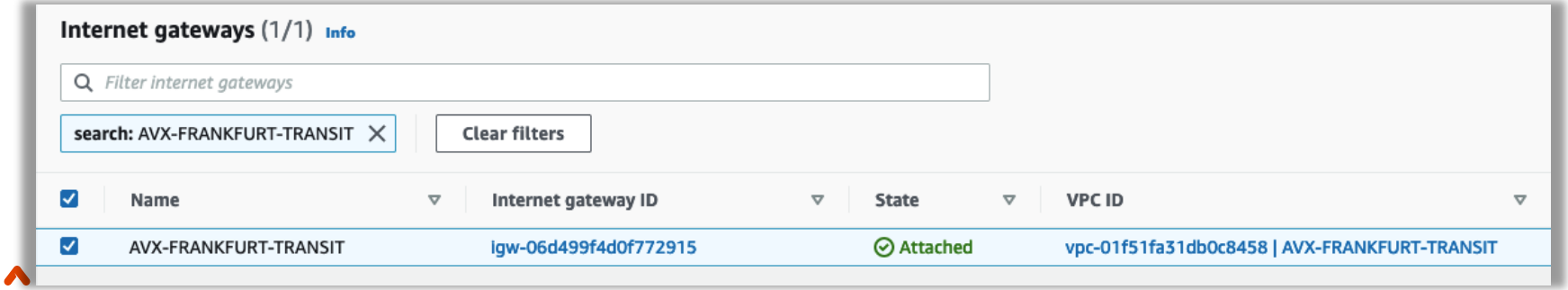
Greenfield Deployment (VPC/VNet/VCN creation)

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

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

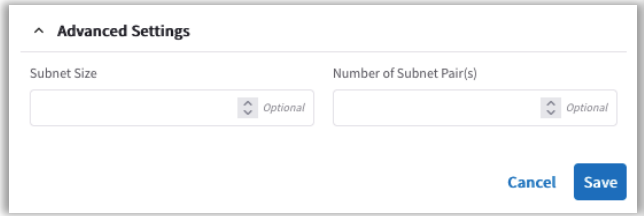


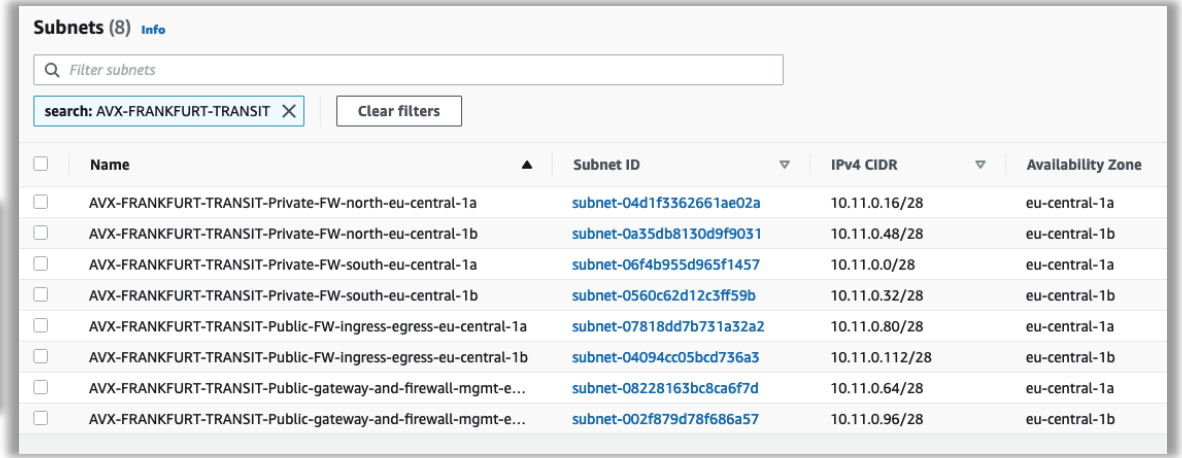
Greenfield Deployment (VPC/VNet/VCN creation)

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

- The subnets' size can be customized





Name	Subnet ID	IPv4 CIDR	Availability Zone
AVX-FRANKFURT-TRANSIT-Private-FW-north-eu-central-1a	subnet-04d1f3362661ae02a	10.11.0.16/28	eu-central-1a
AVX-FRANKFURT-TRANSIT-Private-FW-north-eu-central-1b	subnet-0a35db8130d9f9031	10.11.0.48/28	eu-central-1b
AVX-FRANKFURT-TRANSIT-Private-FW-south-eu-central-1a	subnet-06f4b955d965f1457	10.11.0.0/28	eu-central-1a
AVX-FRANKFURT-TRANSIT-Private-FW-south-eu-central-1b	subnet-0560c62d12c3ff59b	10.11.0.32/28	eu-central-1b
AVX-FRANKFURT-TRANSIT-Public-FW-ingress-egress-eu-central-1a	subnet-07818dd7b731a32a2	10.11.0.80/28	eu-central-1a
AVX-FRANKFURT-TRANSIT-Public-FW-ingress-egress-eu-central-1b	subnet-04094cc05bcd736a3	10.11.0.112/28	eu-central-1b
AVX-FRANKFURT-TRANSIT-Public-gateway-and-firewall-mgmt-e...	subnet-08228163bc8ca6f7d	10.11.0.64/28	eu-central-1a
AVX-FRANKFURT-TRANSIT-Public-gateway-and-firewall-mgmt-e...	subnet-002f879d78f686a57	10.11.0.96/28	eu-central-1b

Aviatrix Transit VPC – Aviatrix Official Documentation

Greenfield Deployment (VPC/VNet/VCN creation)

Creation of the Transit VPC

- 2x Routing Tables will be created:
  - Public RTB will encompass the 4 public subnets

Destination	Target
0.0.0.0/0	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

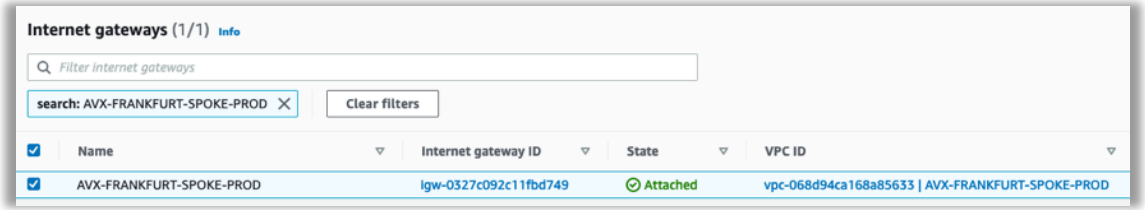
Filter route tables

search: AVX-FRANKFURT-TRANSIT | Clear filters

Name	Route table ID	Explicit subnet associations
AVX-FRANKFURT-TRANSIT-Public-rtb	rtb-0e5a22d0060c17eac	4 subnets
AVX-FRANKFURT-TRANSIT-Private-rtb	rtb-085cf49590ee4592d	4 subnets

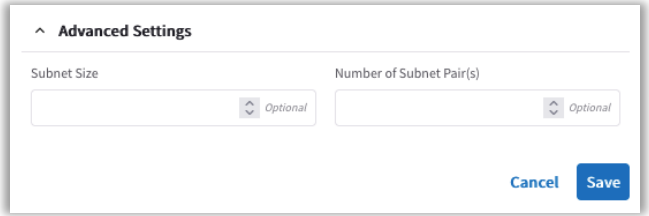
Greenfield Deployment (VPC/VNet/VCN creation)

- **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



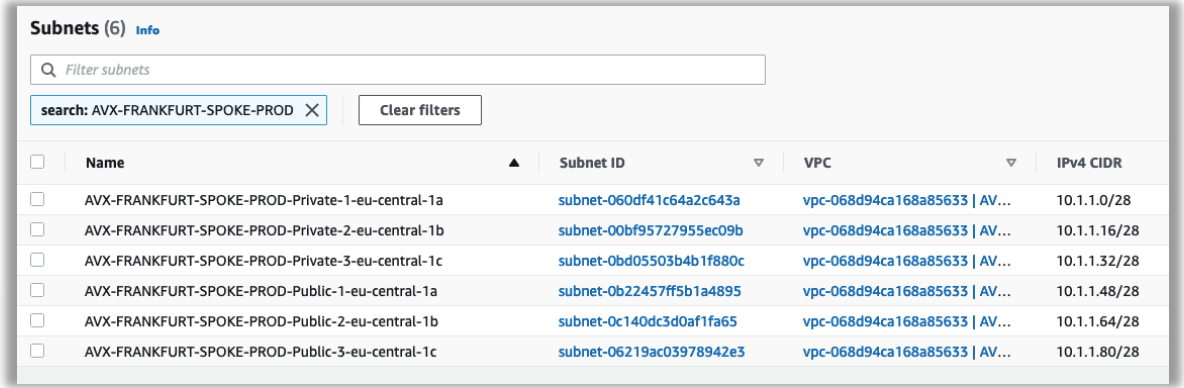
Greenfield Deployment (VPC/VNet/VCN creation)

- The subnets' size can be customized



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



Aviatrix Spoke VPC – Aviatrix Official Documentation

Greenfield Deployment (VPC/VNet/VCN creation)

CIDR 10.1.1.0/24

AVX-FRANKFURT-SPOKE-PROD

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) Info

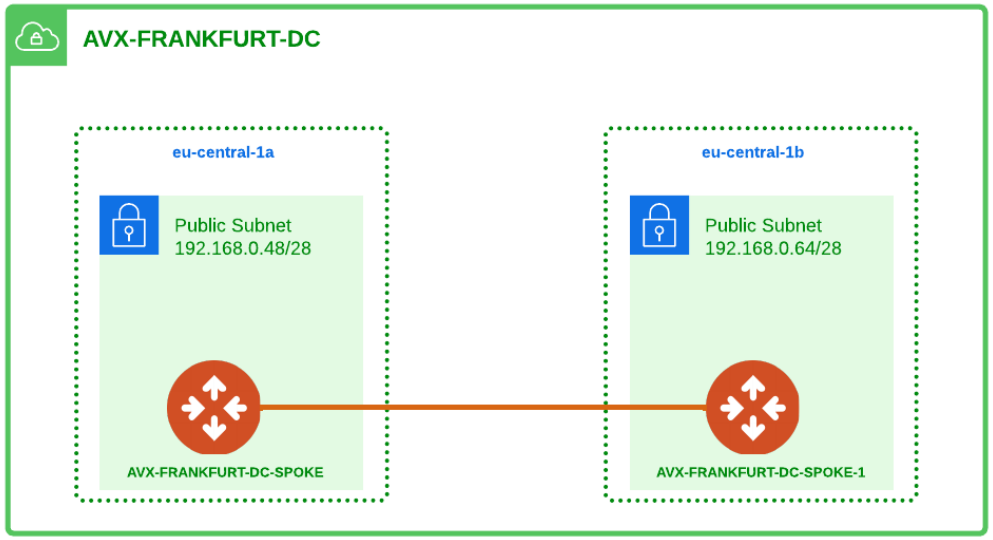
Filter route tables

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

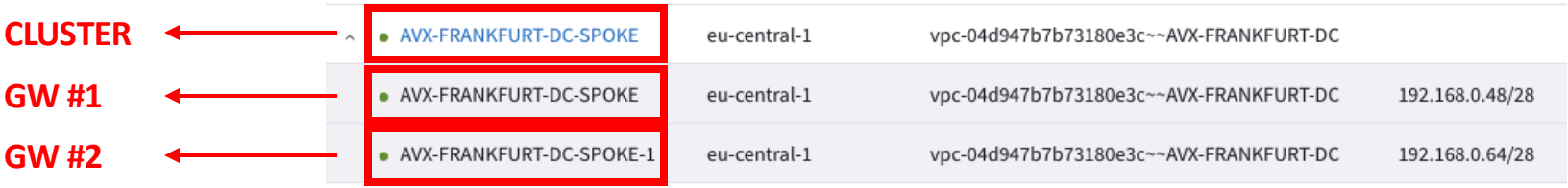
Name	Route table ID	Explicit subnet associations
AVX-FRANKFURT-SPOKE-PROD-Private-1-eu-central-1a-rtb	rtb-0ca98234a5088dceb	subnet-060df41c64a2c643a / AVX-FRANKFURT-SPOKE-PROD-Private-1-eu-central-1a
AVX-FRANKFURT-SPOKE-PROD-Private-2-eu-central-1b-rtb	rtb-0cad721a70d6256d9	subnet-00bf95727955ec09b / 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

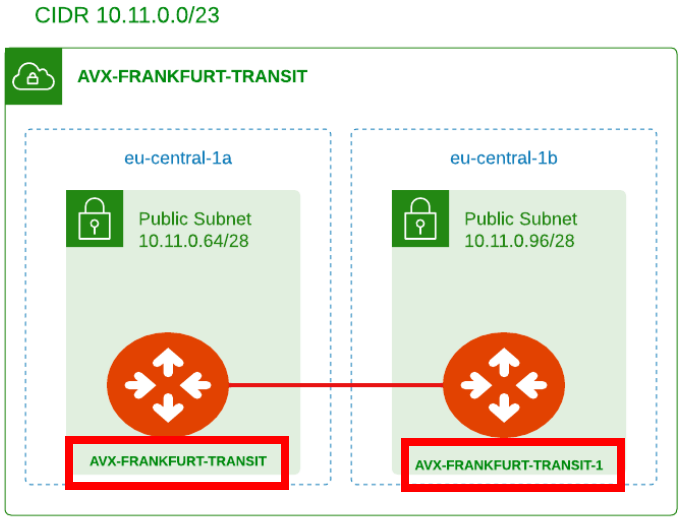
Cluster of Gateways



- 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.

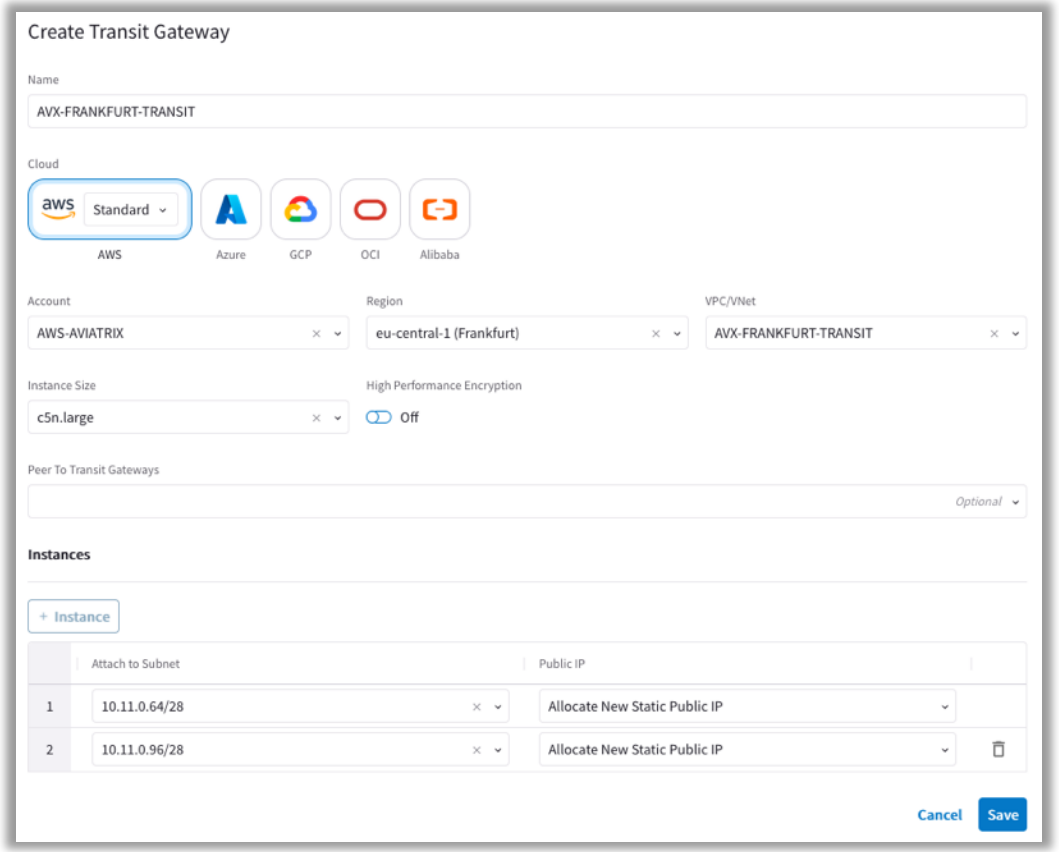


Greenfield Deployment (Transit Gateways deployment)

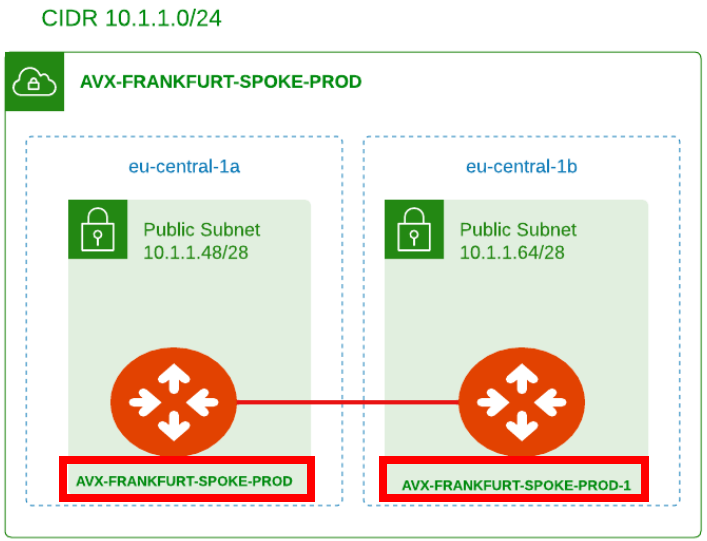


- The connection between the Transit Gateways is automatically created by the Controller.
- **Best Practice:** always deploy the Transit Gateway-1 (i.e the second gateway), and choose a different AZ.
- Only two Transit Gateways can be deployed per Transit VPC
- Aviatrix gateways are deployed in Public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

Transit Gateways Deployment through the CoPilot

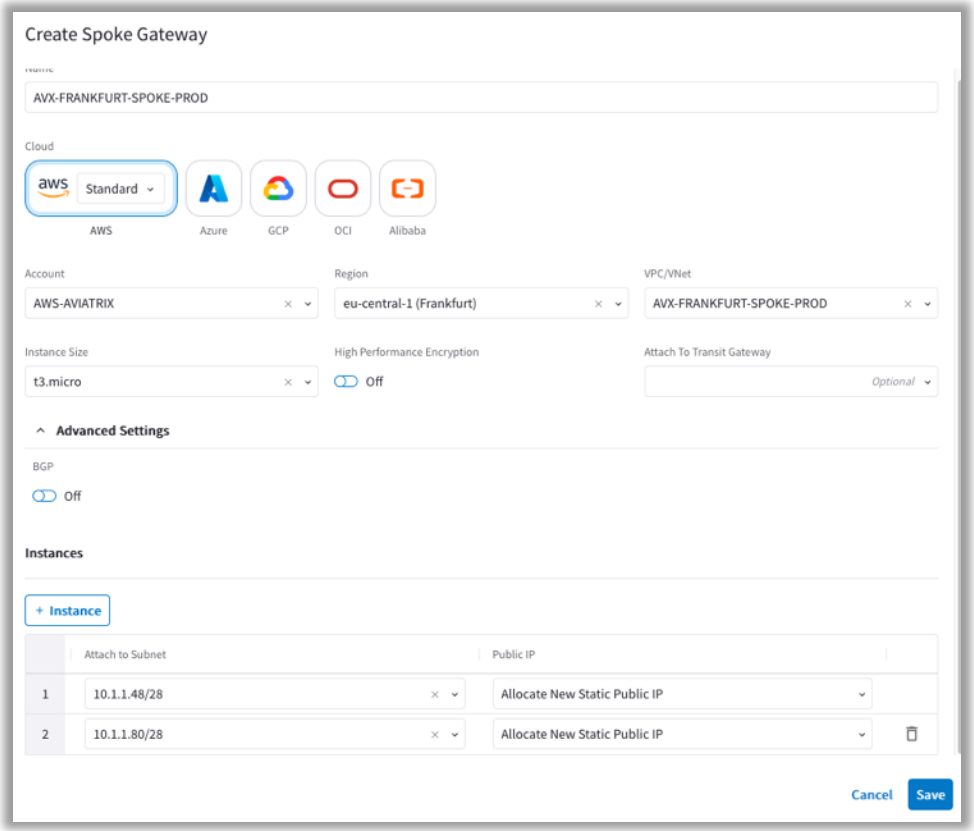


Greenfield Deployment (Spoke Gateways deployment)

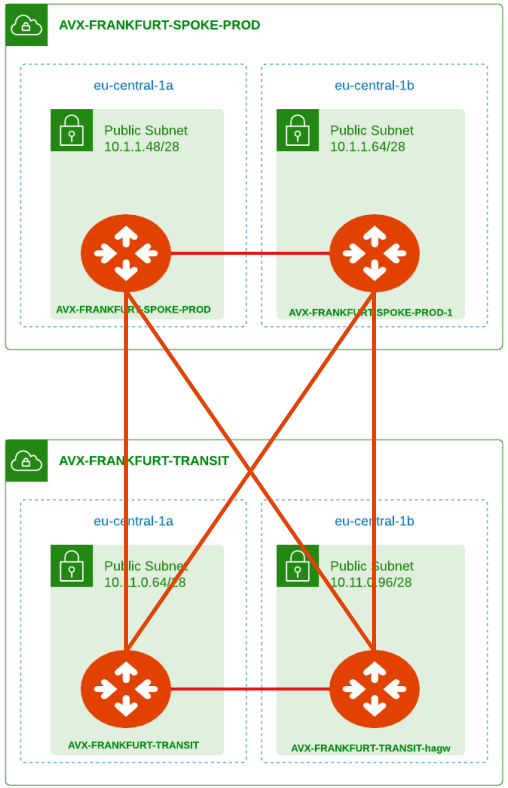


- The connection between the Spoke Gateways is automatically created by the Controller.
- **Best Practice:** deploy the Spoke Gateway-1 (i.e the second gateway) on a different AZ.
- You can deploy up to **15** Spoke Gateways per each Spoke VPC
- Aviatrix gateways are deployed in Public subnets

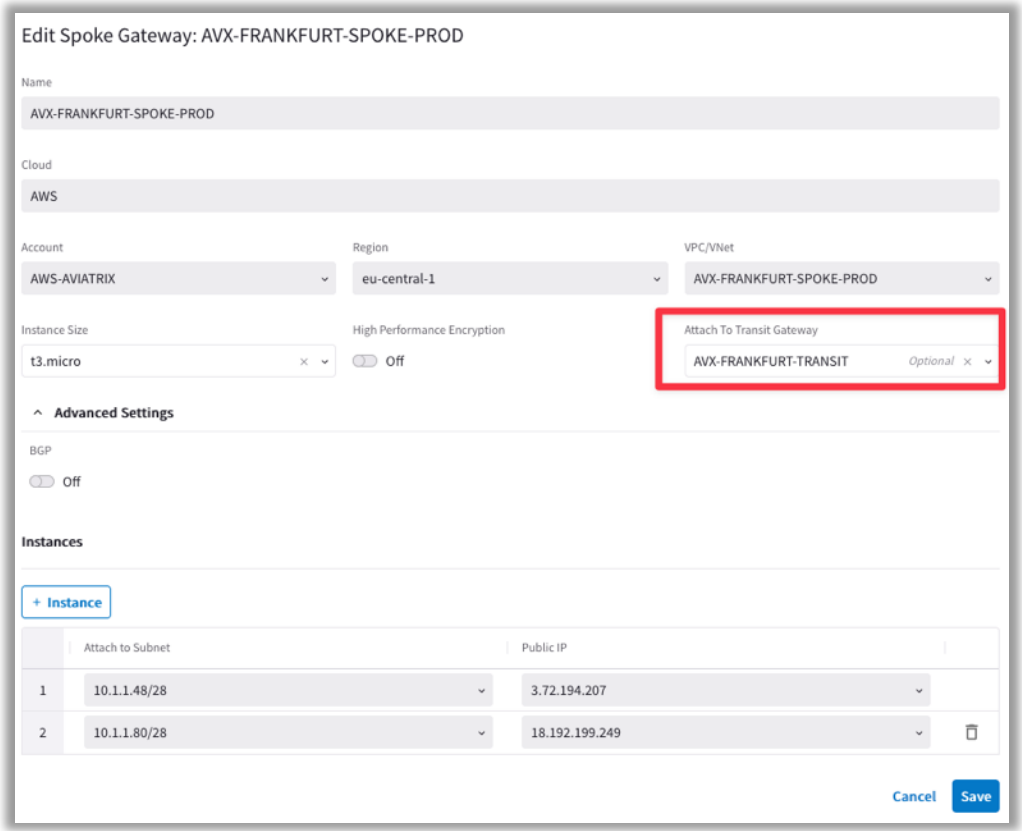
Spoke Gateways Deployment through the CoPilot



Greenfield Deployment (Attachment deployment)



- **Deployment of the attachments through the CoPilot**



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

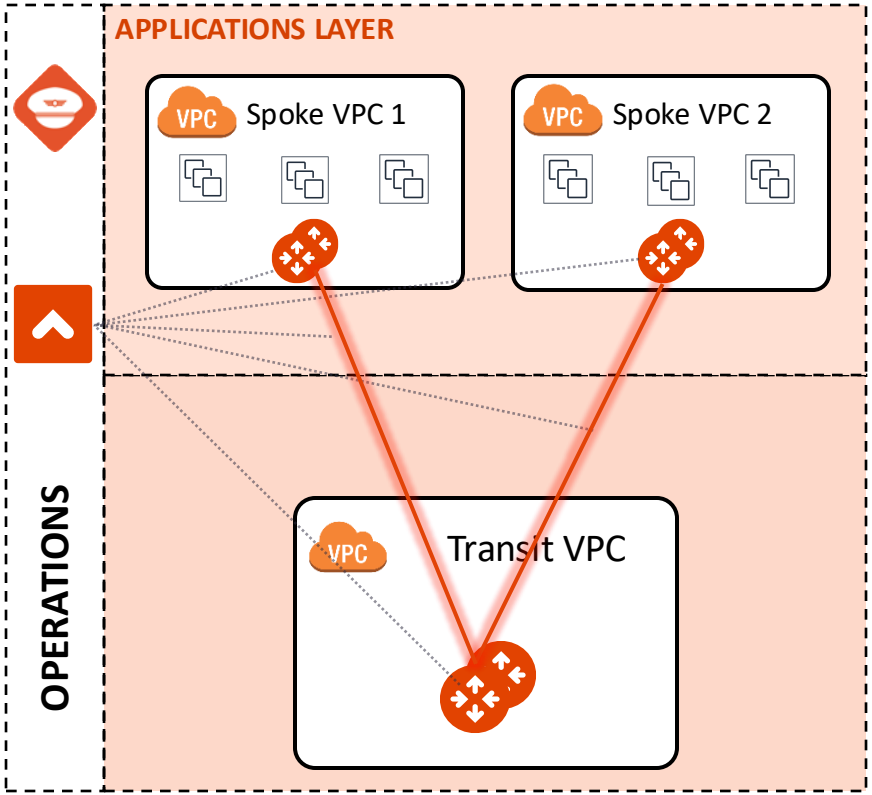
Routes (5)

Filter routes

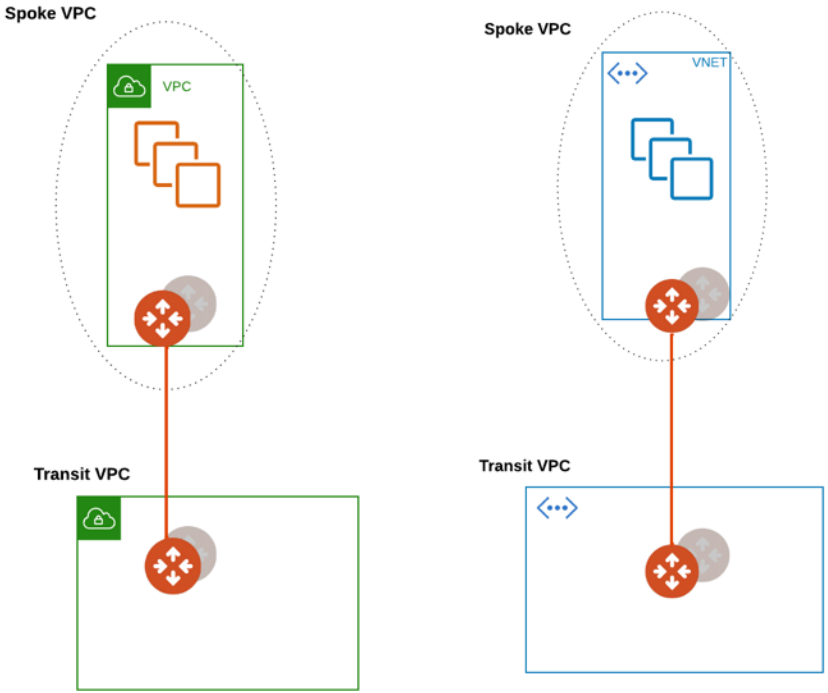
Destination	Target
0.0.0.0/0	igw-07c6ddedd190d12d3
10.0.0.0/8	eni-08ac50fc16cd8c4a5
10.1.1.0/24	local
172.16.0.0/12	eni-08ac50fc16cd8c4a5
192.168.0.0/16	eni-08ac50fc16cd8c4a5

Route table for Public Subnet

Attachment = RFC1918 Routes Injection

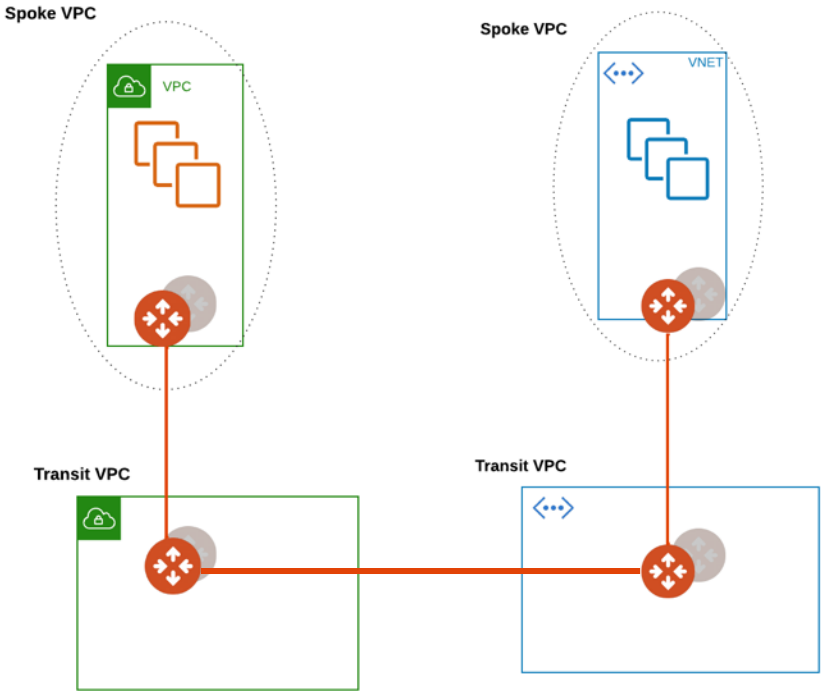


Greenfield Deployment (Repeatable Design)

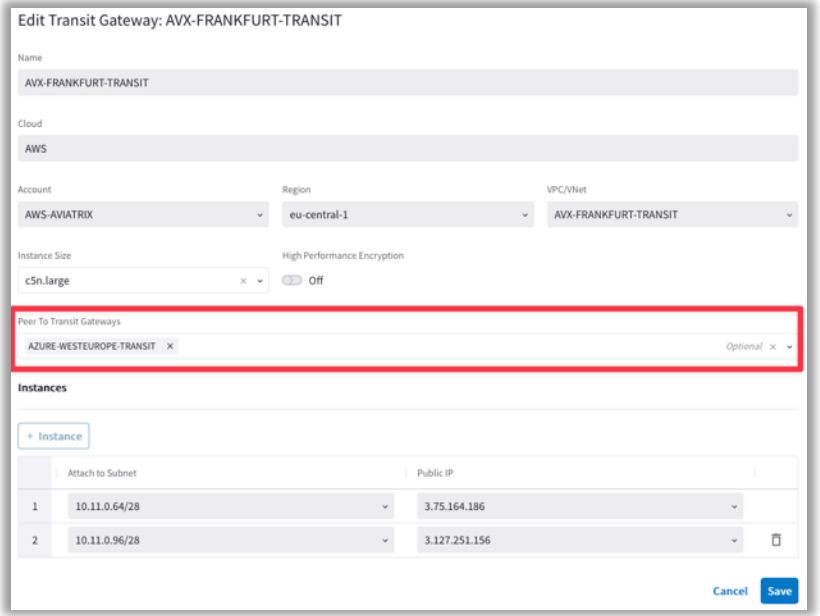


- The hub and spoke topology can be extended to another CSP or to another region within the same CSP
- In Azure all subnets are public by nature
- Aviatrix Controller creates “Private” subnets:
  - Aviatrix Controller programs a **default route 0.0.0.0 pointing to the next hop type “None”:** in User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

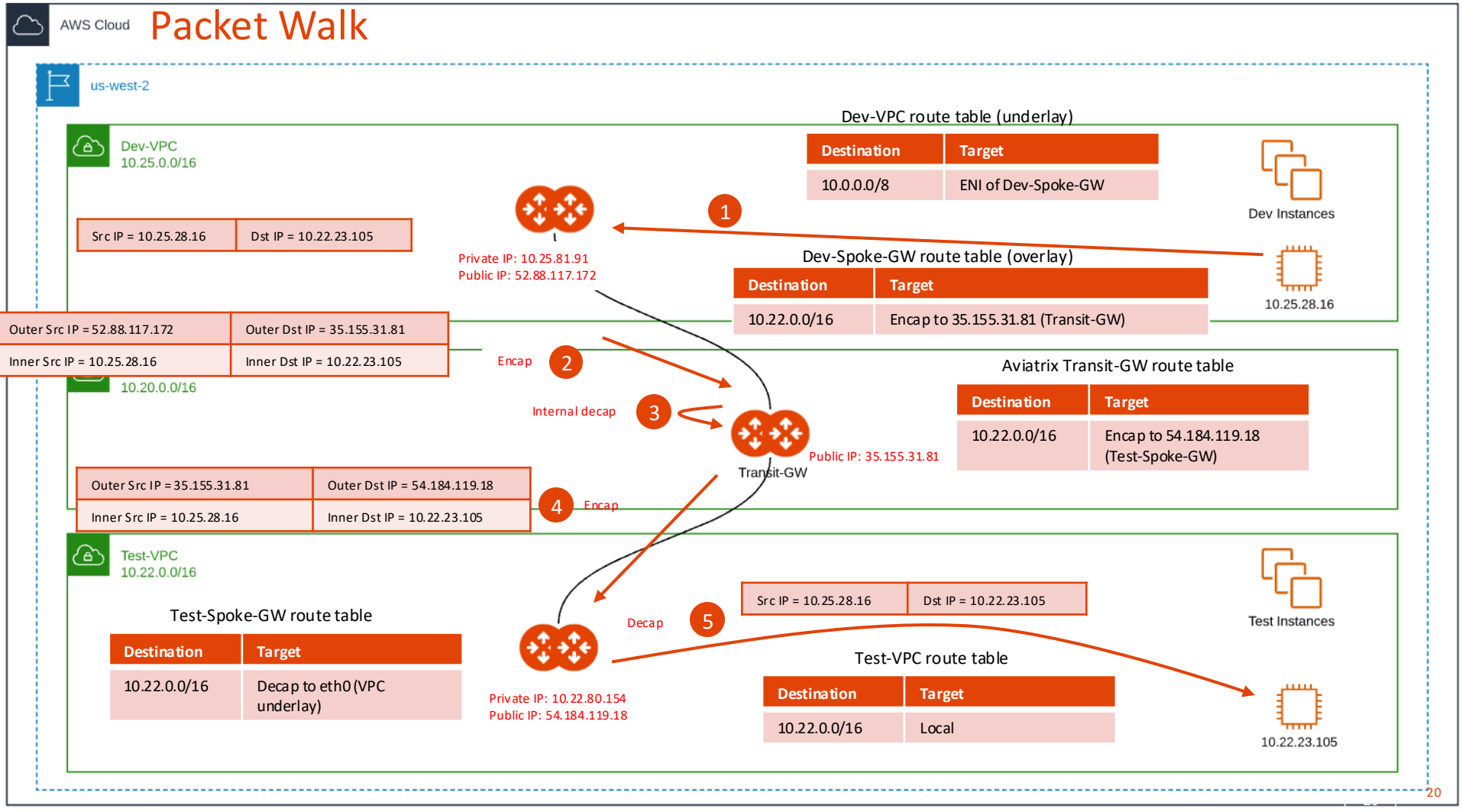
Greenfield Deployment (Peering deployment)



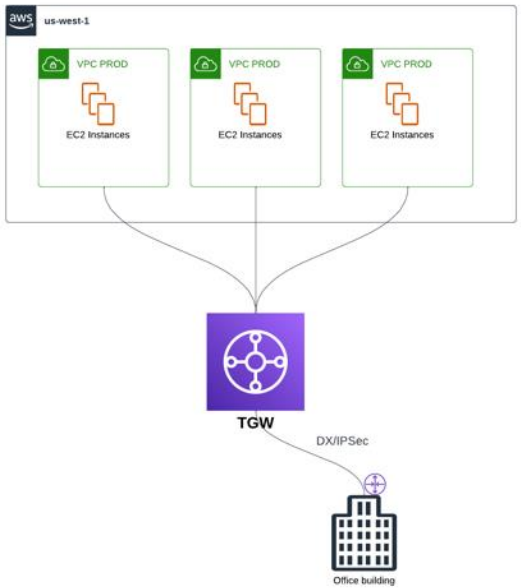
- The creation of the Transit Peering represents the last step for the completion of the **MCNA**.



Packet Walk

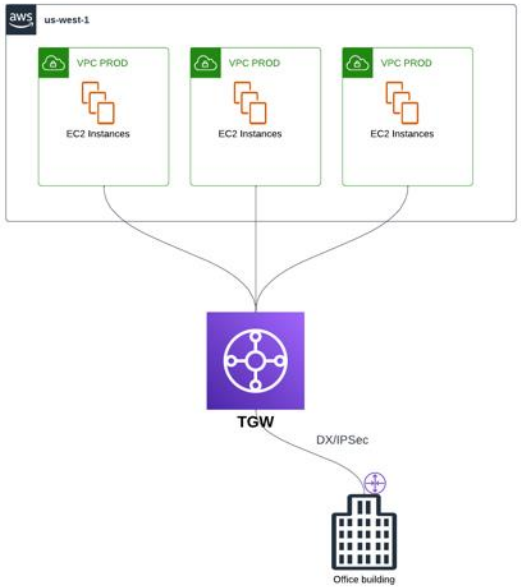

AWS Cloud
us-west-2
Dev-VPC
10.25.0.0/16
Dev-VPC route table (underlay)
Destination
Target
10.0.0.0/8
ENI of Dev-Spoke-GW
Dev Instances
10.25.28.16
Src IP = 10.25.28.16
Dst IP = 10.22.23.105
1
Private IP: 10.25.81.91
Public IP: 52.88.117.172
Dev-Spoke-GW route table (overlay)
Destination
Target
10.22.0.0/16
Encap to 35.155.31.81 (Transit-GW)
Outer Src IP = 52.88.117.172
Outer Dst IP = 35.155.31.81
Inner Src IP = 10.25.28.16
Inner Dst IP = 10.22.23.105
Encap
2
10.20.0.0/16
Internal decap
3
Aviatrix Transit-GW route table
Destination
Target
10.22.0.0/16
Encap to 54.184.119.18
(Test-Spoke-GW)
Transit-GW
Public IP: 35.155.31.81
Outer Src IP = 35.155.31.81
Outer Dst IP = 54.184.119.18
Inner Src IP = 10.25.28.16
Inner Dst IP = 10.22.23.105
4
Encap
Test-VPC
10.22.0.0/16
Test-Spoke-GW route table
Destination
Target
10.22.0.0/16
Decap to eth0 (VPC underlay)
Decap
5
Src IP = 10.25.28.16
Dst IP = 10.22.23.105
Test Instances
Test-VPC route table
Destination
Target
10.22.0.0/16
Local
Private IP: 10.22.80.154
Public IP: 54.184.119.18
10.22.23.105

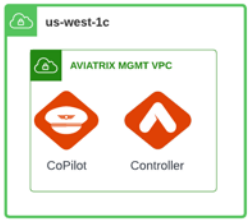
Typical Migration Deployment



- **Initial environment in a brownfield scenario:**
  - Several Application VPCs that are connected to the TGW as attachments
  - OnPrem connectivity (hybrid – can be DX/IPSec)

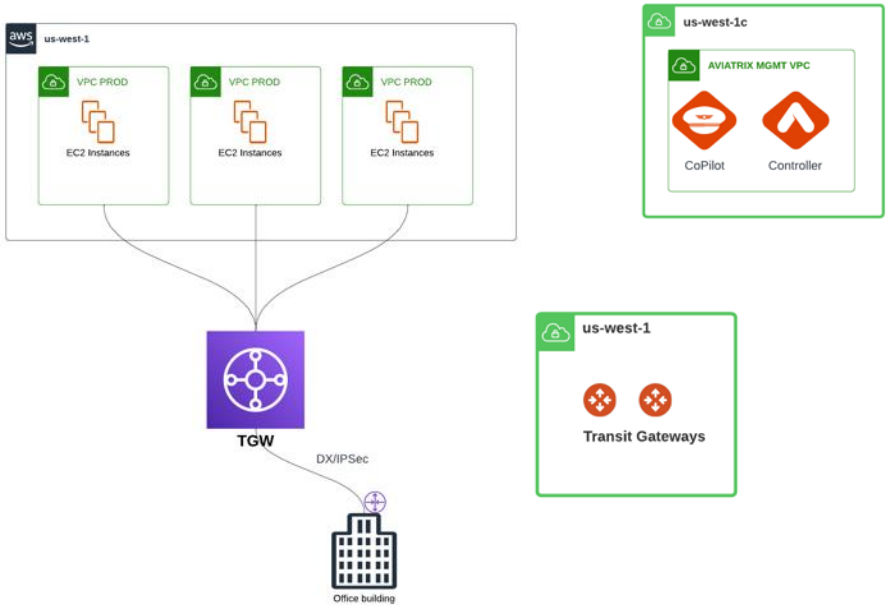
Typical Migration Deployment





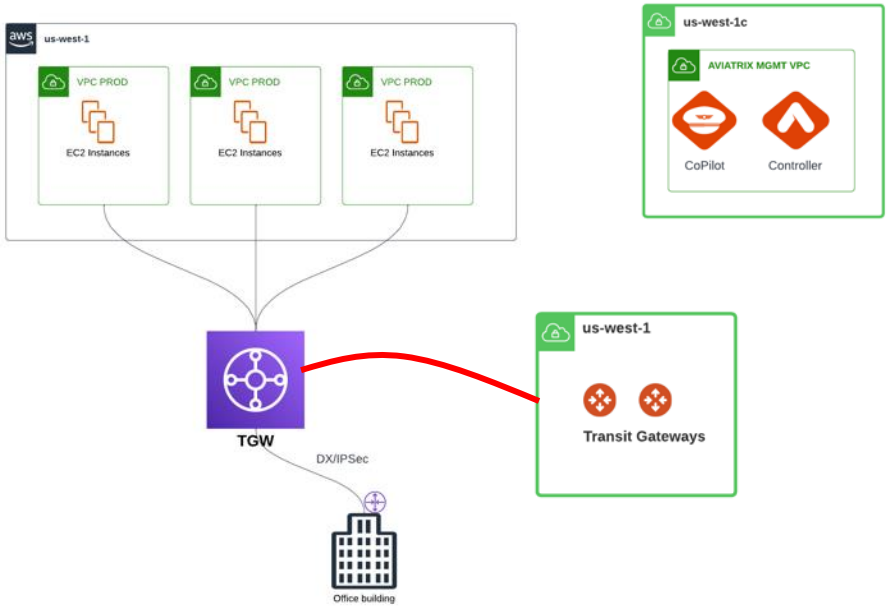
- **Initial environment in a brownfield scenario:**
  - Several Application VPCs that are connected to the TGW as attachments
  - OnPrem connectivity (hybrid – can be DX/IPSec)
- **Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed (best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

Typical Migration Deployment



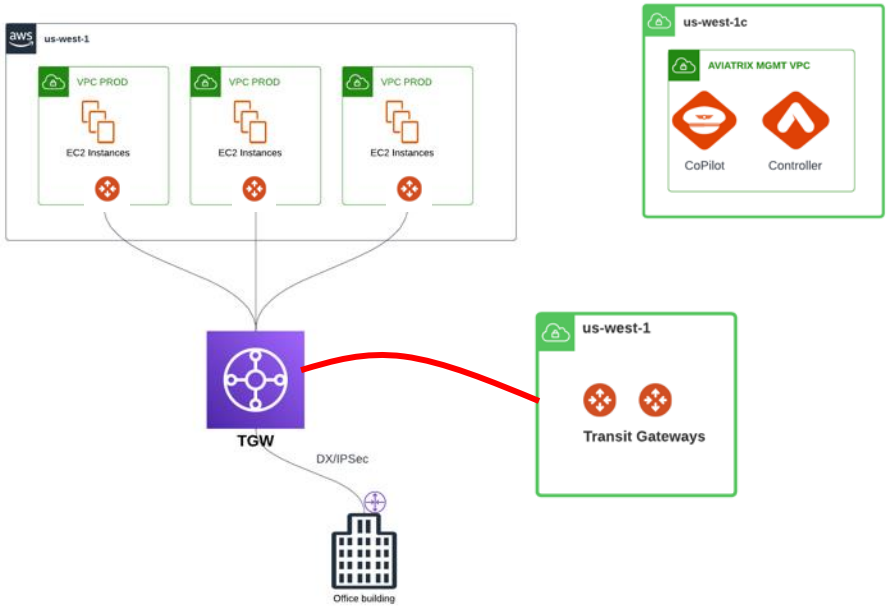
- **Initial environment in a brownfield scenario:**
  - Several Application VPCs that are connected to the TGW as attachments
  - OnPrem connectivity (hybrid – can be DX/IPSec)
- **Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed (best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

Typical Migration Deployment



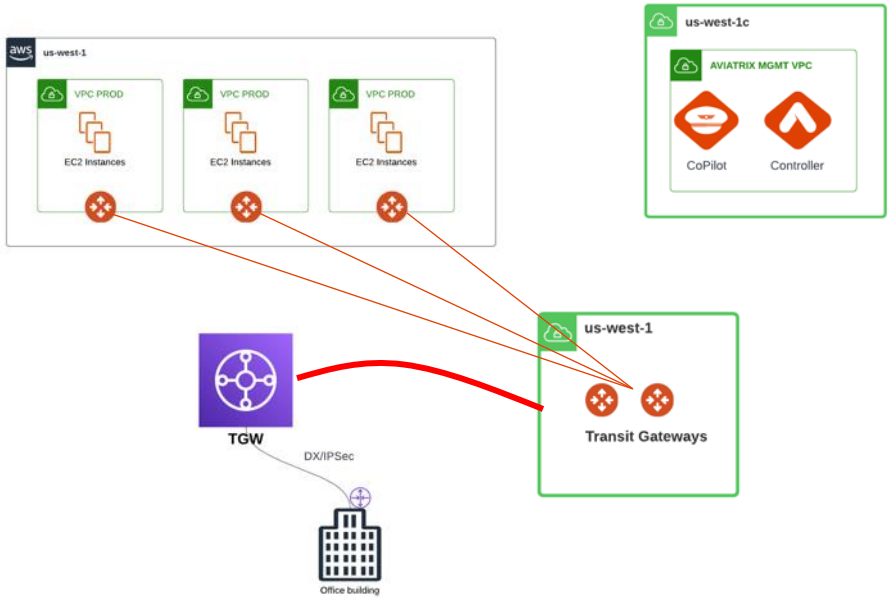
- **Initial environment in a brownfield scenario:**
  - Several Application VPCs that are connected to the TGW as attachments
  - OnPrem connectivity (hybrid – can be DX/IPSec)
- **Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed (best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



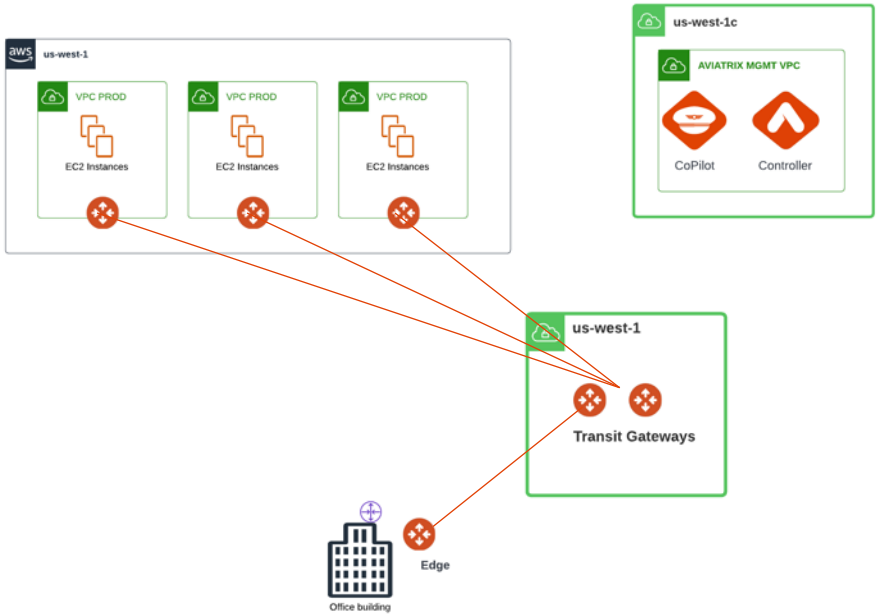
- Initial environment in a brownfield scenario:
  - Several Application VPCs that are connected to the TGW as attachments
  - OnPrem connectivity (hybrid – can be DX/IPSec)
- Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed (best practice)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

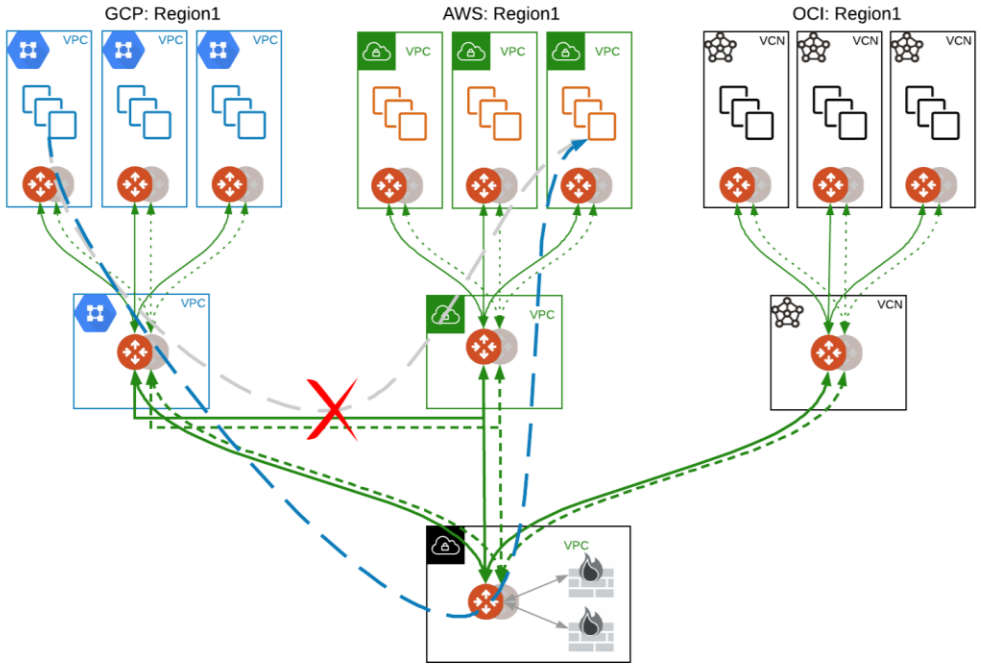
Typical Migration Deployment



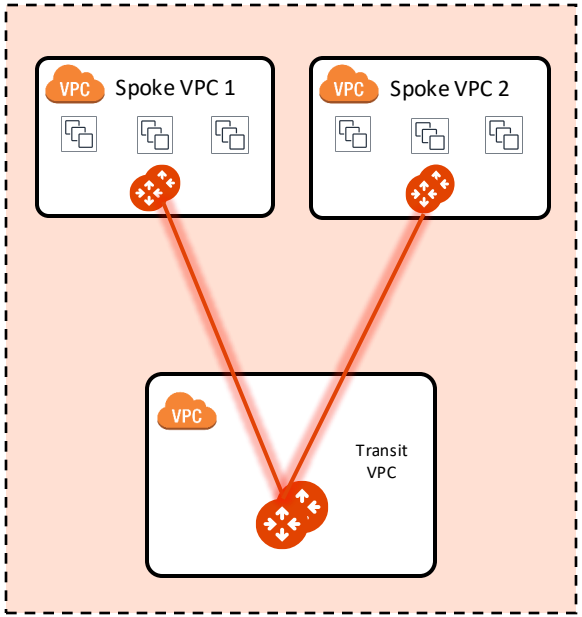
- Initial environment in a brownfield scenario:
  - Several Application VPCs that are connected to the TGW as attachments
  - OnPrem connectivity (hybrid – can be DX/IPSec)
- Deploy the Aviatrix Controller and CoPilot in a dedicated VPC, in a different AZ where there are no gateways deployed (best practice)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

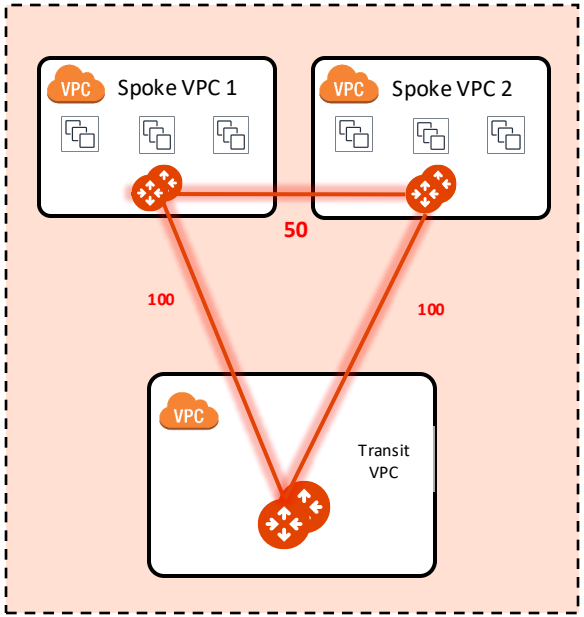
Multi-Tier Transit (MTT)

- *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