



Routes Manipulation & NAT

ACE Team

RFC1918 Routes Injection = Standard behavior of the Controller

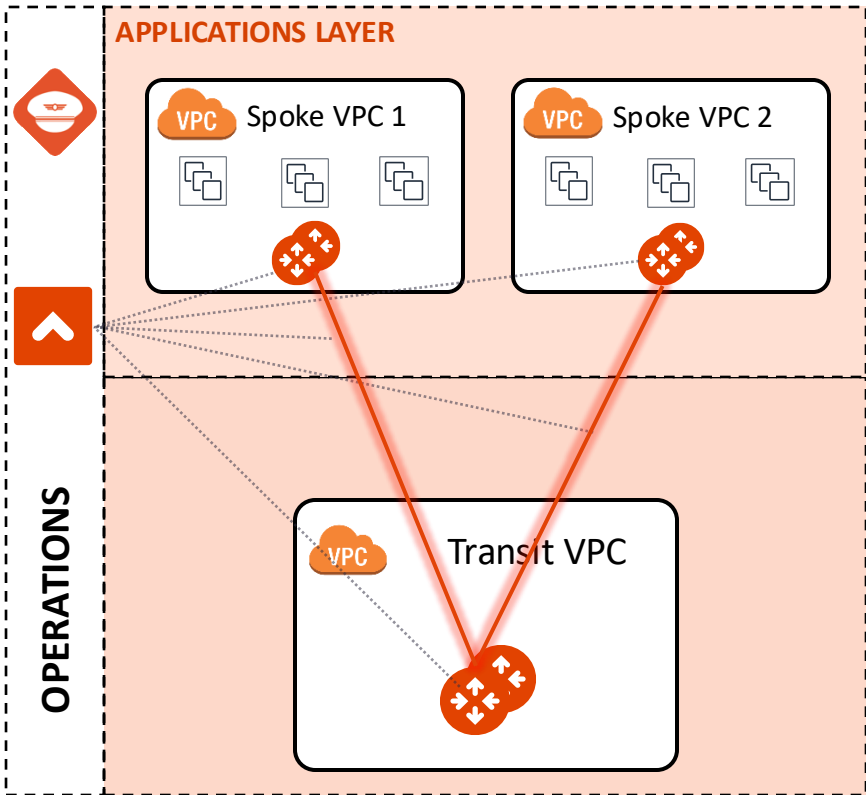
- As soon as the Controller completes the deployment of the **attachments** between Spoke Gateways and Transit Gateways, it will also program the *three RFC1918 routes* in the route tables to point to the ENI of the Spoke Gateways.

Private Route table

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		

Public Route table

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		

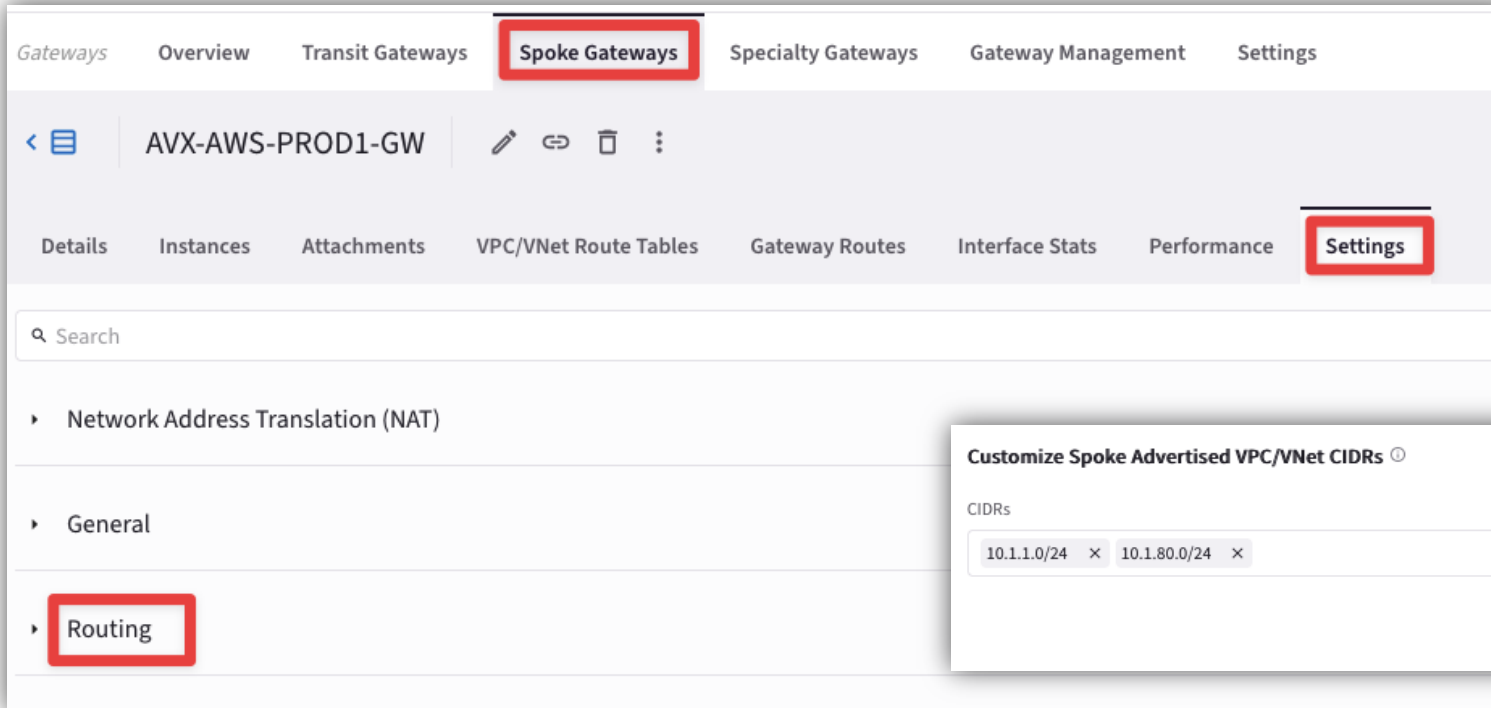


Routes Manipulation – Customize Spoke Advertised VPC CIDRs

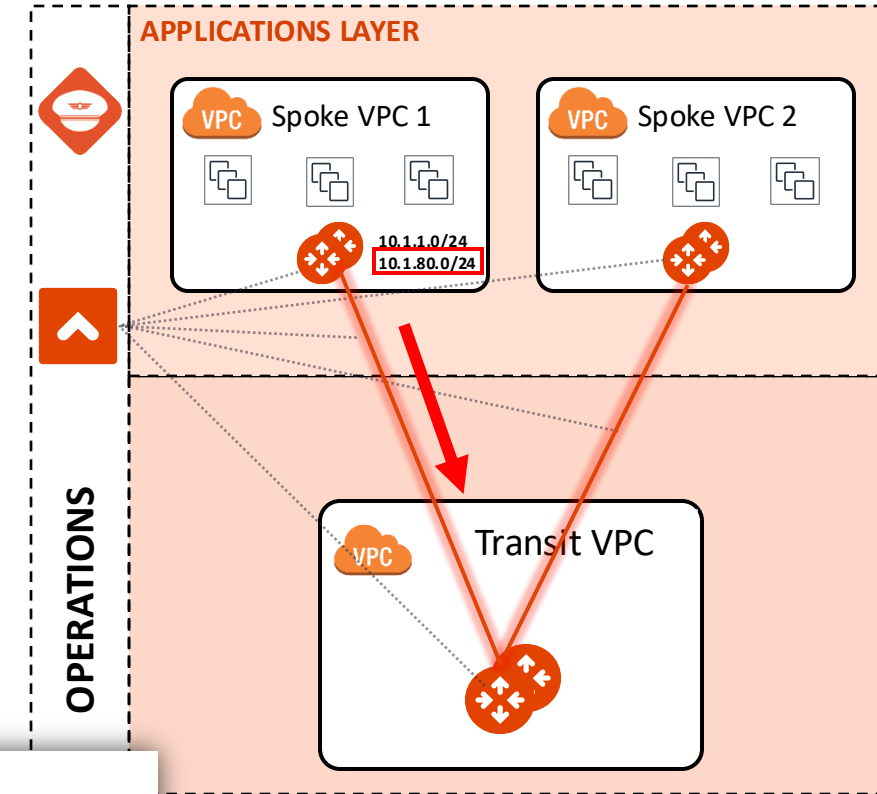
- For example, if you decide to add another CIDR block to an existing VPC, in that case you can also advertise the new CIDR within your MCNA.

CIDRs	
Address type	CIDR
IPv4	10.1.1.0/24
IPv4	10.1.80.0/24

- PATH:** COPILOT > Cloud Fabric > Gateways > Spoke Gateways > select the relevant GW > Settings > Routing > **Customize Spoke Advertised VPC/VNet CIDRs**



The screenshot shows the AWS Management Console interface. The 'Spoke Gateways' tab is selected under the 'Gateways' section. The 'Settings' tab is also selected. Under the 'Settings' tab, the 'Routing' section is highlighted. A modal window titled 'Customize Spoke Advertised VPC/VNet CIDRs' is open, showing a list of CIDRs: 10.1.1.0/24 and 10.1.80.0/24.



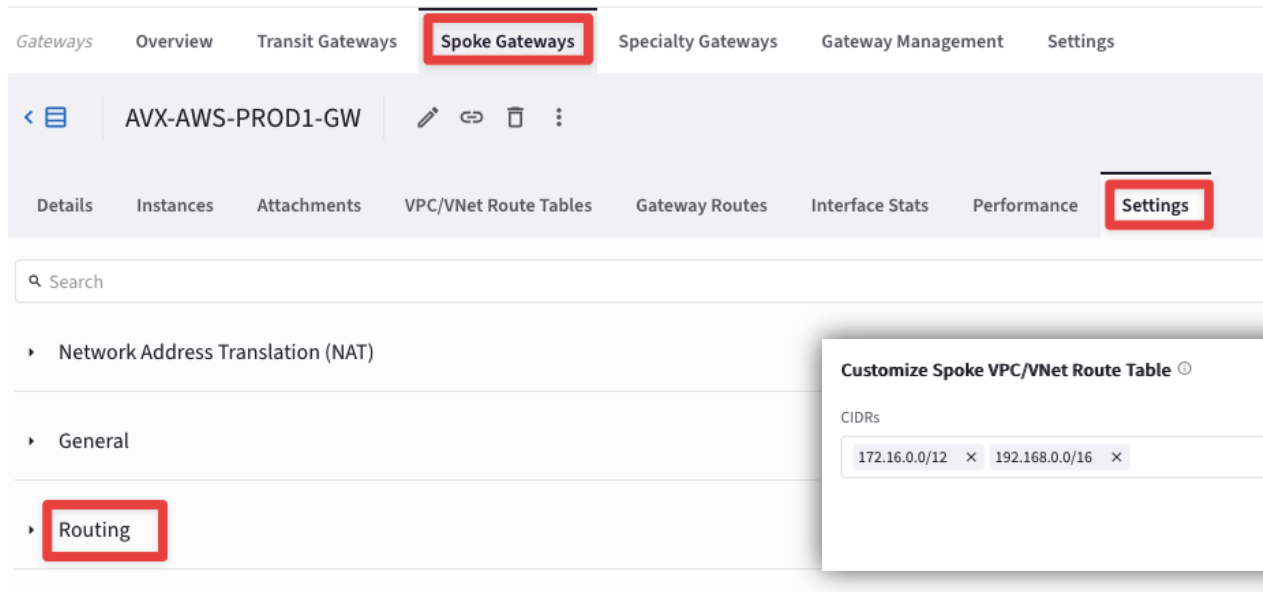
Routes Manipulation – Customize Spoke VPC Routing Table

- You can also decide to withdraw an RFC1918 route that was previously injected by the Controller, customizing the VPC/Vnet/VCN routing table.

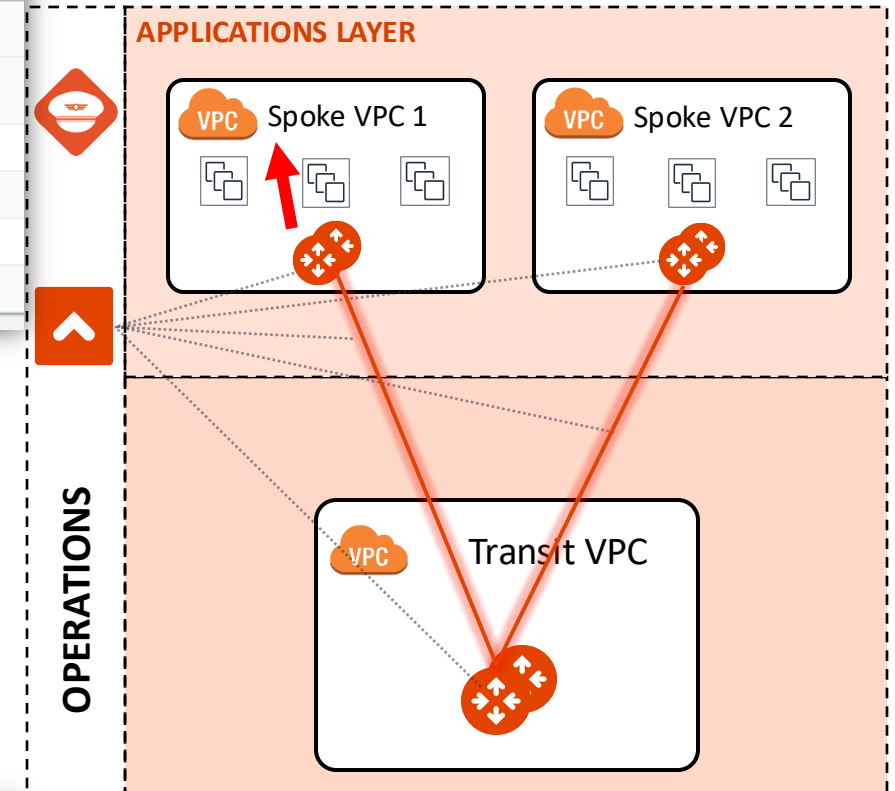
Destination	Target
10.0.0.0/8	eni-019dbf18ad5b8857f
10.1.3.0/24	local
172.16.0.0/12	eni-019dbf18ad5b8857f
192.168.0.0/16	eni-019dbf18ad5b8857f

DELETE

- PATH:** COPILOT > Cloud Fabric > Gateways > Spoke Gateways > select the relevant GW > Settings > Routing > **Customize Spoke VPC/VNet Route Table**



The screenshot shows the AviaTriX console interface. The 'Spoke Gateways' tab is selected under 'Gateways'. The 'Settings' tab is selected for the 'AVX-AWS-PROD1-GW' gateway. The 'Routing' section is expanded, and the 'Customize Spoke VPC/VNet Route Table' dialog is open, showing a list of CIDRs: 172.16.0.0/12 and 192.168.0.0/16.



Routes Manipulation – Exclude Learned CIDRs to Spoke VPC/VNet Route Table

- You can also decide to filter out a route from the routing table of a Spoke GW.

Gateway Instance

AVX-AWS-SPOKE-GW-PROD1

Network Domain

All

	Destination	Via	Interface	Next Hop IP	Next Hop Gateway	Metric
	10.1.1.0/24	10.1.1.49	eth0	10.1.1.49		0
	10.1.1.49/32		eth0			100
	<div>10.1.2.0/24</div> <div>+ 2 more</div>		tun-0A010147-0	10.1.1.71	AVX-AWS-SPOKE-GW-PROD...	200

- PATH:** COPILOT > Cloud Fabric > Gateways > Spoke Gateways > select the relevant GW > Settings > Routing > **Exclude Learned CIDRs to Spoke VPC/Vnet Route Table**

Gateways

Overview

Transit Gateways

Spoke Gateways

Specialty Gateways

Gateway Management

Settings

< ☰

AVX-AWS-PROD1-GW

✎ 🔗 🗑 ⋮

Details

Instances

Attachments

VPC/VNet Route Tables

Gateway Routes

Interface Stats

Performance

Settings

🔍 Search

▸ Network Address Translation (NAT)

▸ General

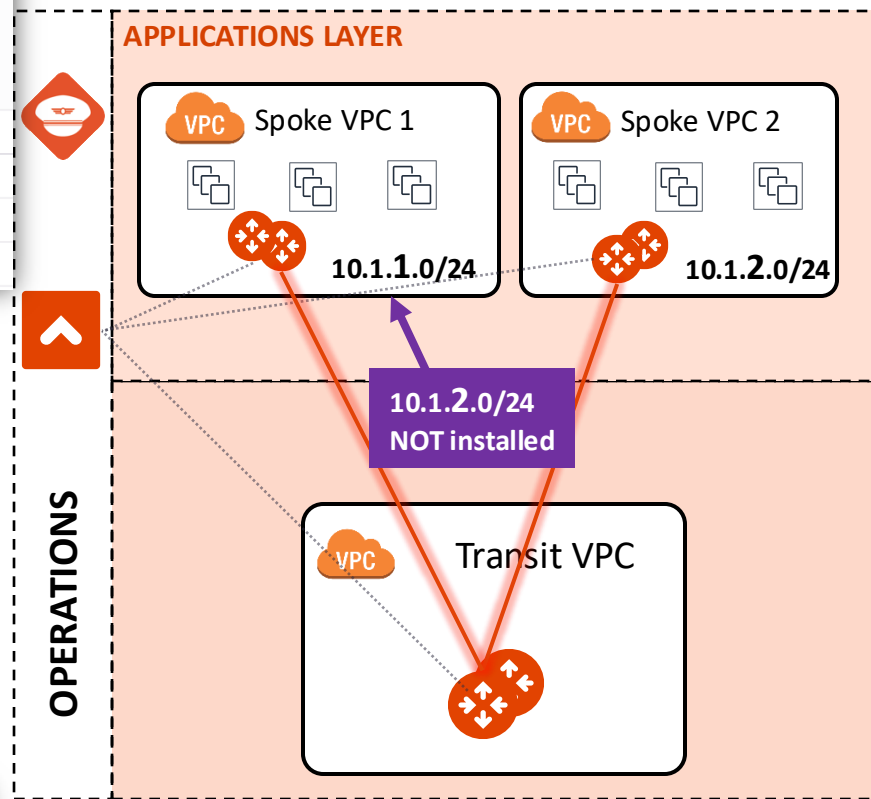
▸ Routing

Exclude Learned CIDRs to Spoke VPC/VNet Route Table ⓘ

CIDRs

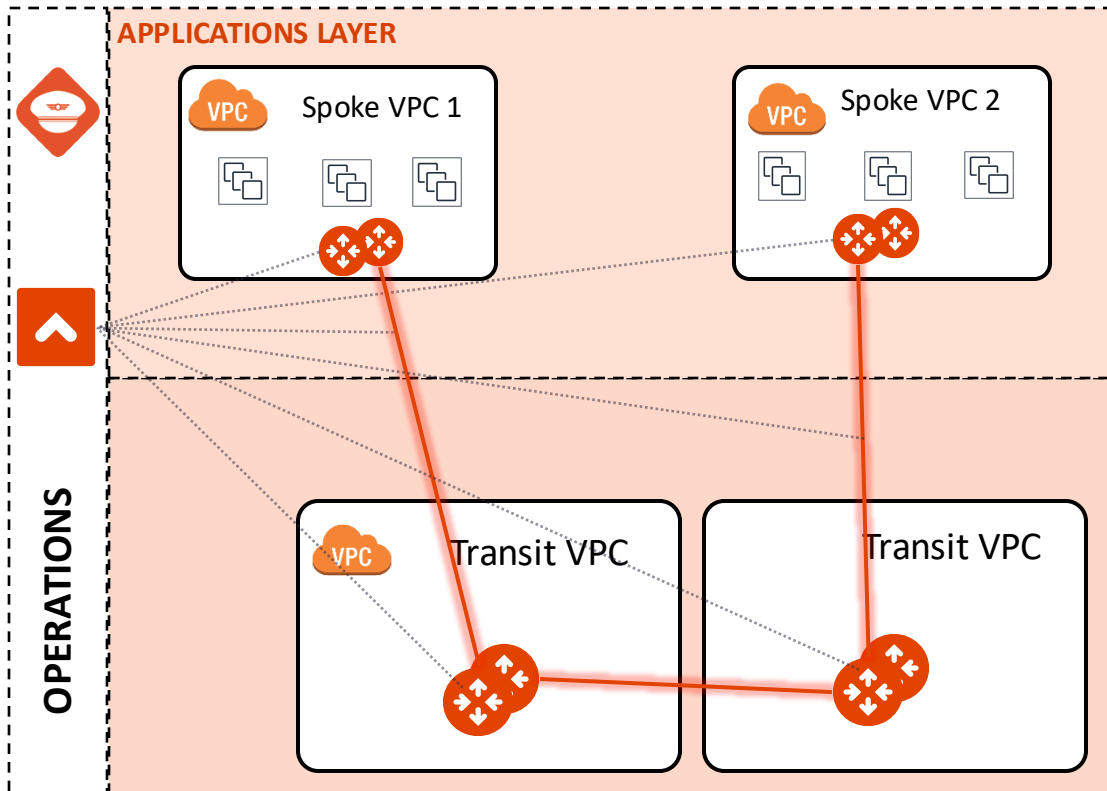
10.1.2.0/24 ×

Cancel Save

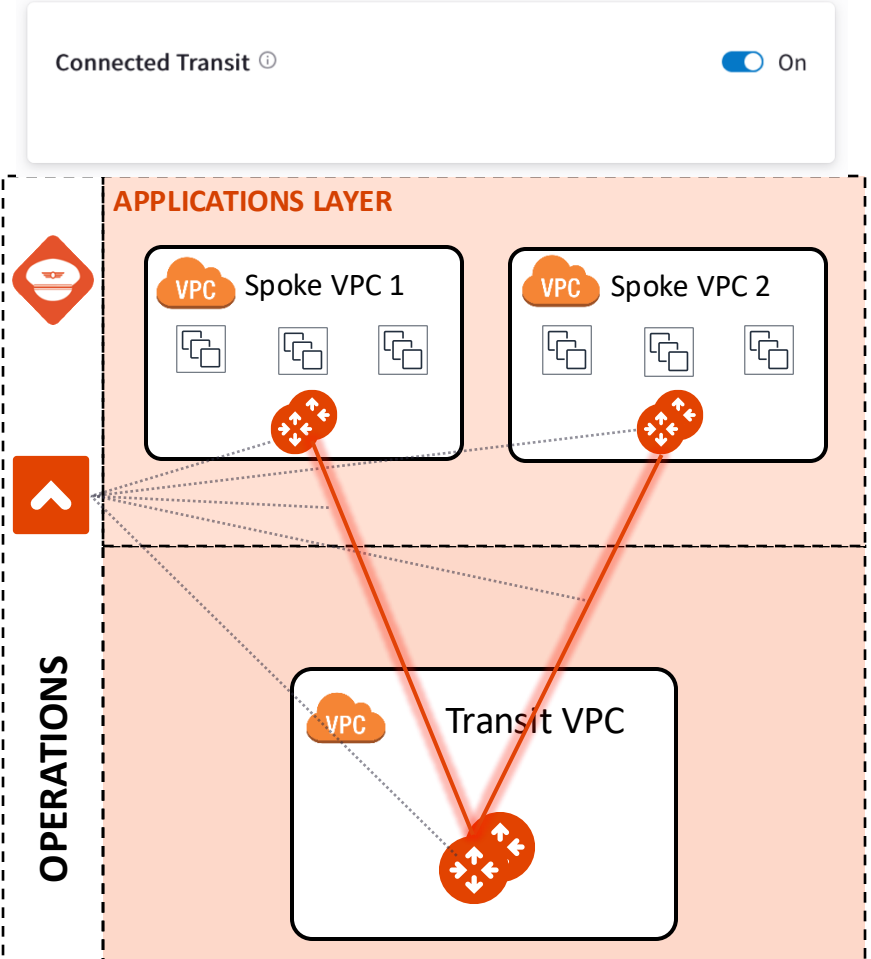


Routes Manipulation – Connected Transit

- **By default**, AviaTriX Spoke VPCs/VNets do not have routing established to communicate with each other via Transit. They are completely segmented.
- Each Spoke VPC should be connected to its own dedicated Transit VPC.



- If you would like to build a full mesh network where Spoke VPCs/VNets communicate with each other via Transit GW, you can achieve that by enabling **Connected Transit** mode.



NAT - Overview

- The Aviatrix Spoke Gateways provide advanced NAT capabilities.
- Three NAT functions are supported:
 - ❑ **Source NAT:**
 - Two modes of Source NAT are supported:
 - Single IP
 - Customized SNAT
 - ❑ **Destination NAT**
 - ❑ **Mapped NAT**

Source NAT: Single IP



The screenshot shows the AWS Management Console interface for configuring a Spoke Gateway. The navigation path is: Gateways > Overview > Transit Gateways > **Spoke Gateways**. The selected gateway is **AVX-AWS-SPOKE-GW-PROD1**. The sub-tab **Settings** is active. Under the **Network Address Translation (NAT)** section, the **Source NAT** toggle is turned **On**. The configuration method is set to **Single IP** (selected) instead of Customized SNAT. A **Save** button is visible at the bottom right of the settings panel.

- **PATH:** COPILOT > Cloud Fabric > Gateways > Spoke Gateways > select the relevant gateway > Settings > **NAT**
- In addition to the RFC1918 routes, the Controller will also install a *quad zero* route that points to the ENI of the Spoke Gateway.

Source NAT: Customized SNAT

- When **Customized SNAT** is selected, the gateway can translate source IP address ranges to different SNAT address and ports.


Network Address Translation (NAT)


Source NAT ⓘ On

☐ Single IP ☒ Customized SNAT

Instance: AVX-AWS-SPOKE-GW-PROD1

[+ Rule](#) | [Filter](#) [Grid](#) [Download](#) | Unsaved Changes: [Add: 1](#) |

Src CIDR	Src Port	Dst CIDR	Dst Port	Protocol	Connection	Mark	SNAT IPs	SNAT Port	Apply Route Entry	Exclude Route Table	
10.1.1.0/24		10.1.2.0/24		all	None		192.168.1.0/24		<input type="checkbox"/>		

Total 1 Rule 

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

Destination NAT

- Destination NAT (**DNAT**) allow you to change the destination to a virtual address range.

^ Network Address Translation (NAT)

Source NAT Off

Destination NAT On

Instance
ace-aws-eu-west-1-spoke1

+ Rule | Filter | Download

Unsaved Changes: Add: 1 | Search

Src CIDR	Src Port	Dst CIDR	Dst Port	Protocol	Connection	Mark	DNAT IPs	DNAT Port	Apply Route Entry	Exclude Route Table
10.1.1.0/24		172.16.211.0/24		all	None		50.50.50.1-50.50.50.254		<input type="checkbox"/>	

Total 1 Rule

Cancel Save

Overlapping IP Issue



Jason.22



Local

Mark.22

Jason.22



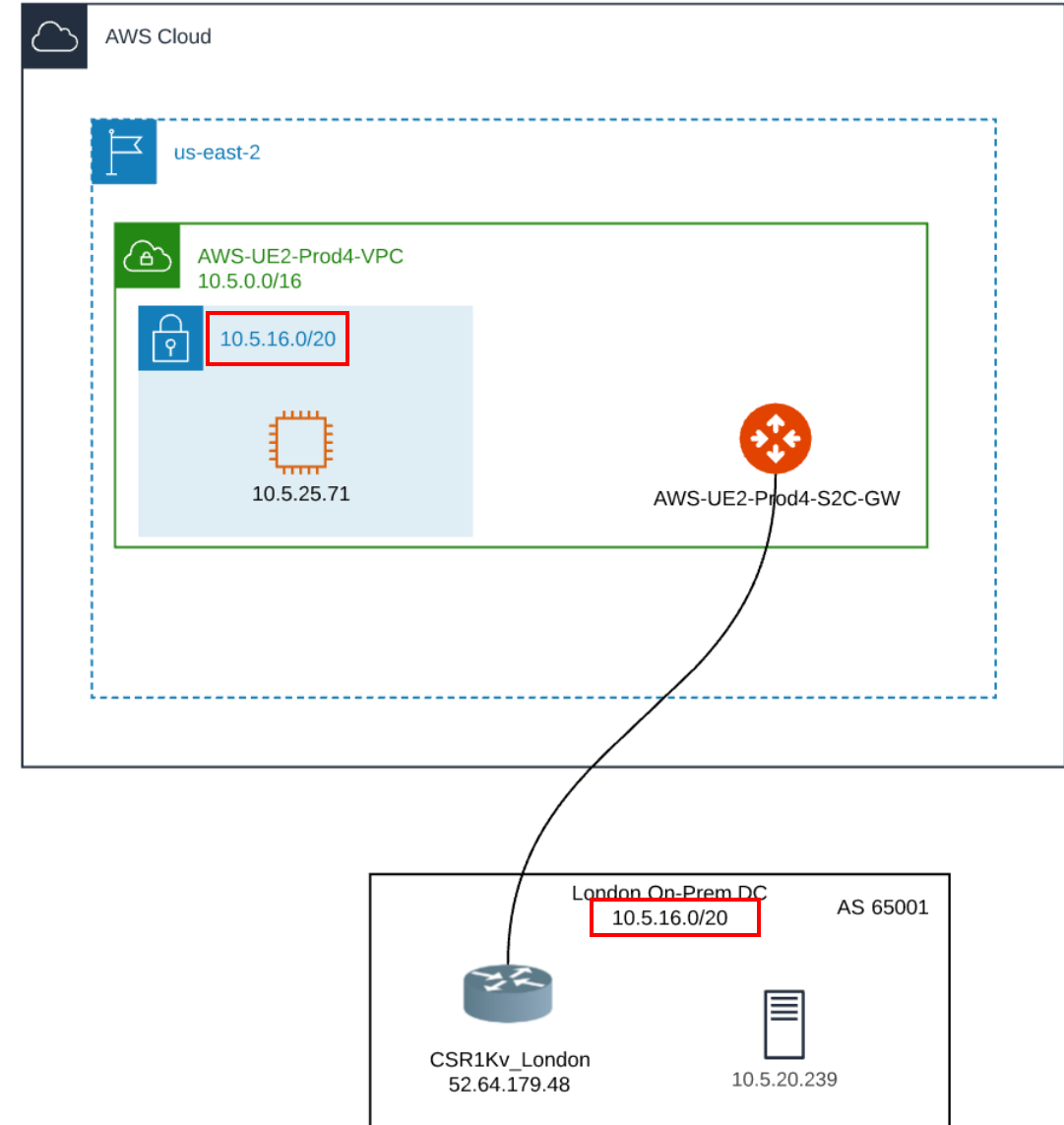
Remote

Frank.22



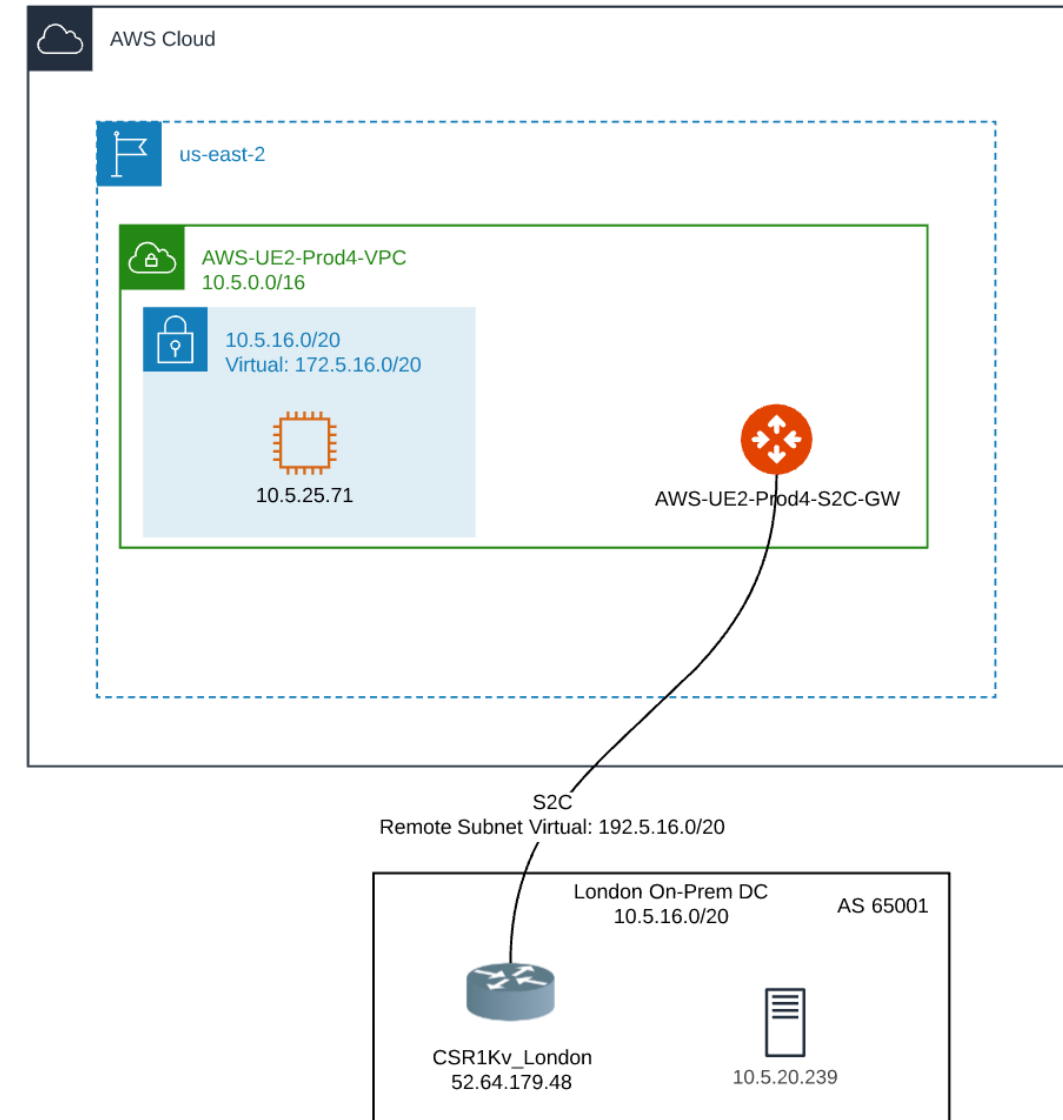
Mapped NAT - Overview

- Need to connect overlapping networks between the cloud and on-prem
- Don't want the on-prem router to implement any NAT
 - Keep it simple with no on-prem dependency
 - Many on-prem routers have no NAT, or very limited NAT
- The host information must be preserved
- No NAT overload requirement anywhere
- The configuration must be simple and scalable

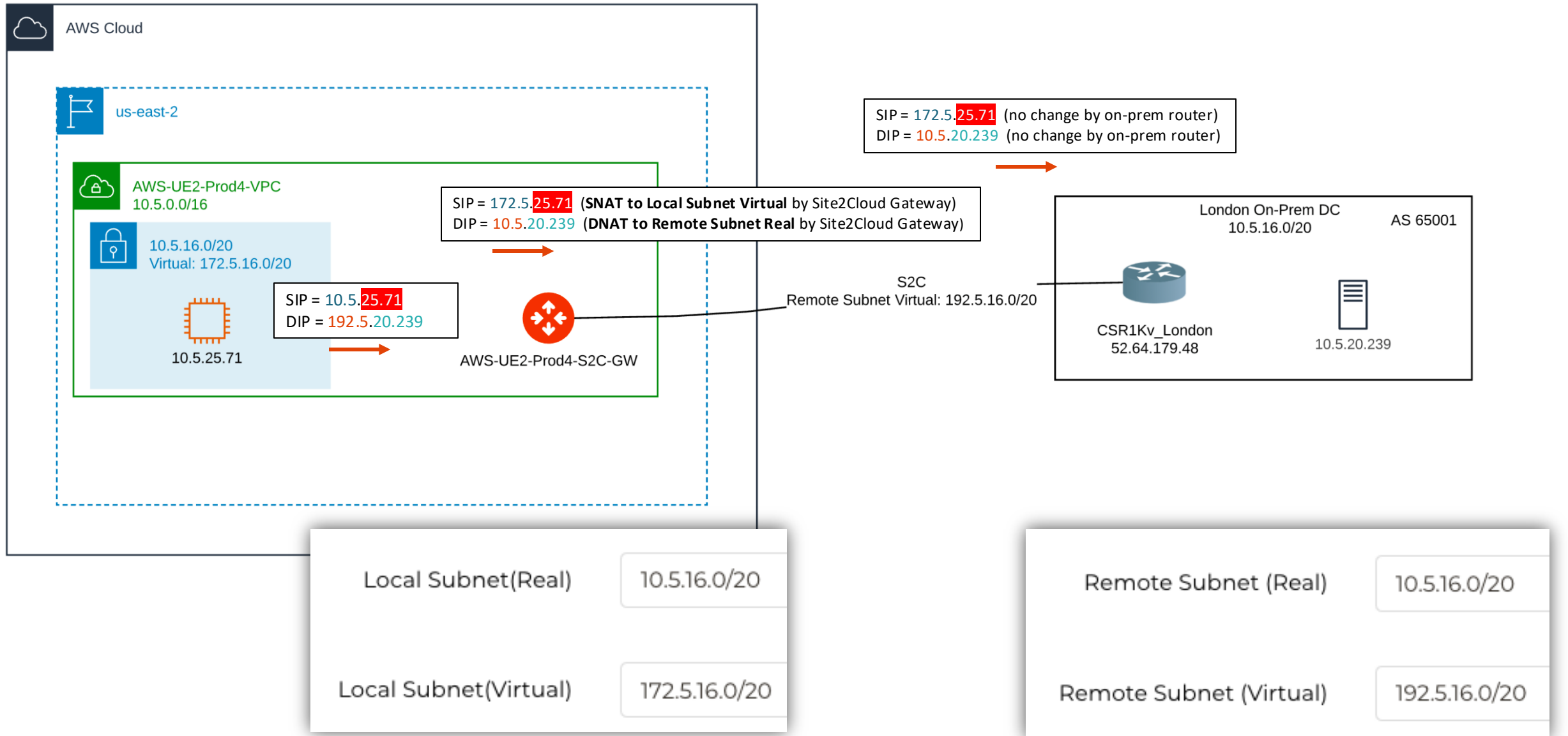


Mapped NAT – Virtual Subnets

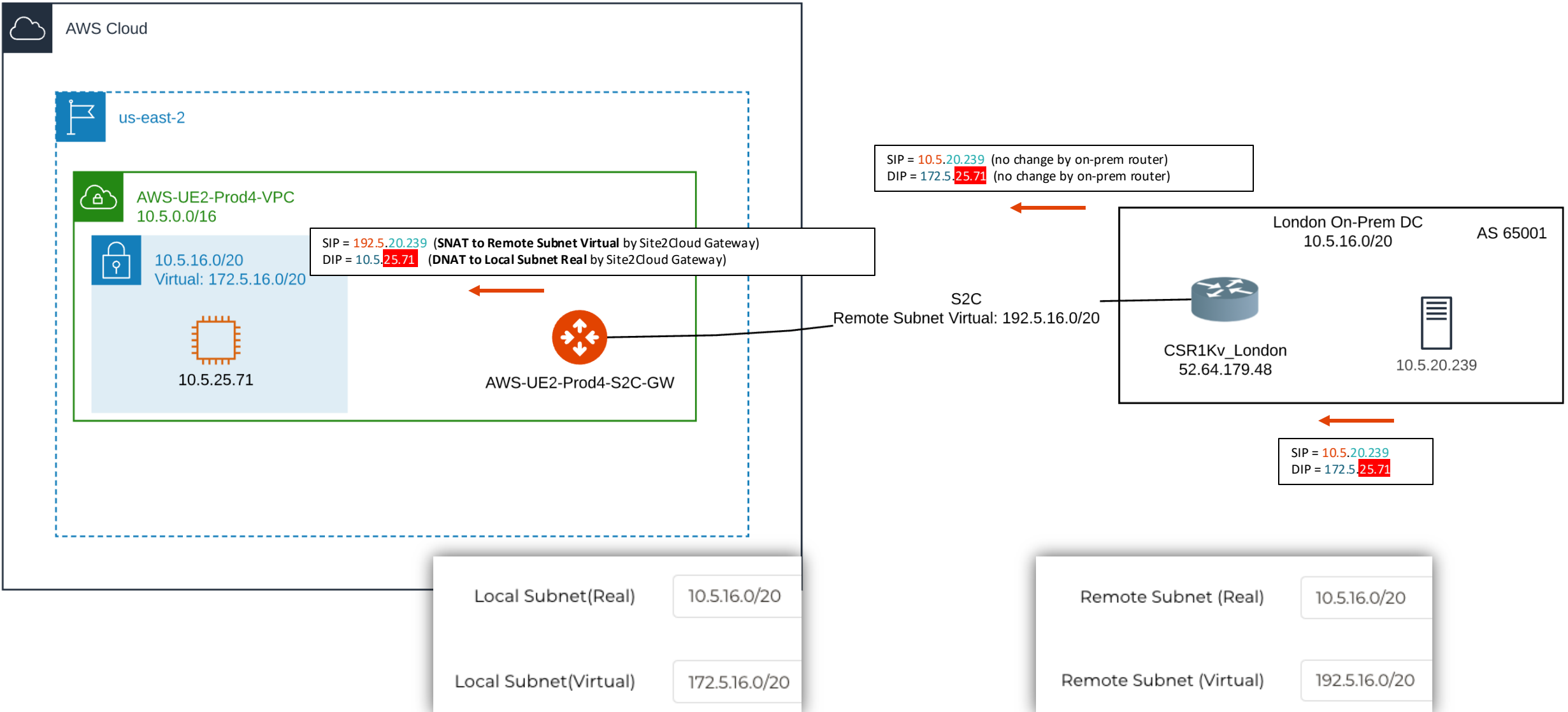
- **Virtual subnets**, which are defined to be unique (not necessarily RFC1918), are used for communication between overlapping VPC and on-prem
- The Site2Cloud Gateway **NATs between real subnets and virtual subnets**, while **preserving the host information** in the IP
- There is **no need for any on-prem NAT** operations
- The configuration is extremely **simple**, and it does not require individual /32 NAT rules
- It works with both **Route-based IPSec** and **Policy-based IPSec** required



Mapped NAT – Packet Walk (from Local to Remote)



Mapped NAT – Packet Walk (from Remote to Local)





Tools for Operating your Routes Manipulation & NAT

Routes Manipulation - ACTIONS

- **PATH:** COPILOT > Cloud Fabric > Gateways > Spoke Gateways > select the relevant GW > Settings > **Routing**

^ Routing

Configure Private VPC/VNet Default Route ⓘ

☐ Off

Customize Spoke VPC/VNet Route Table ⓘ

CIDRs

Update Encrypted Spoke VPC/VNet CIDRs

Update

Skip Public VPC/VNet Route Table ⓘ

☐ Off

Exclude Learned CIDRs to Spoke VPC/VNet Route Table ⓘ

CIDRs

Auto Advertise Spoke Site2Cloud CIDRs ⓘ

☐ Off

Customize Spoke Advertised VPC/VNet CIDRs ⓘ

CIDRs

NAT



- **PATH:** COPILOT > Fabric > Gateways > Spoke Gateways > select the relevant GW > Settings > NAT

^ Network Address Translation (NAT)

Source NAT ⓘ

Single IP

Customized SNAT

On

Cancel

Save

Destination NAT ⓘ

On

Instance

AVX-AWS-SPOKE-GW-PROD1

+ Rule

Search

Src CIDR	Src Port	Dst CIDR	Dst Port	Protocol	Connection	Mark	DNAT IPs	DNAT Port	Apply Route Entry	Exclude Route Table
No Rules										

Total 0 Rules



Next:

Lab 5 Routes Manipulation & NAT