Routes Manipulation & NAT

ACE Team

RFC1918 Routes Injection = Standard behavior of the Controller

- Once the Controller completes deploying the **attachments** between the Spoke Gateways and Transit Gateways, it will configure the three **RFC 1918** routes in the route tables to point to the ENIs 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

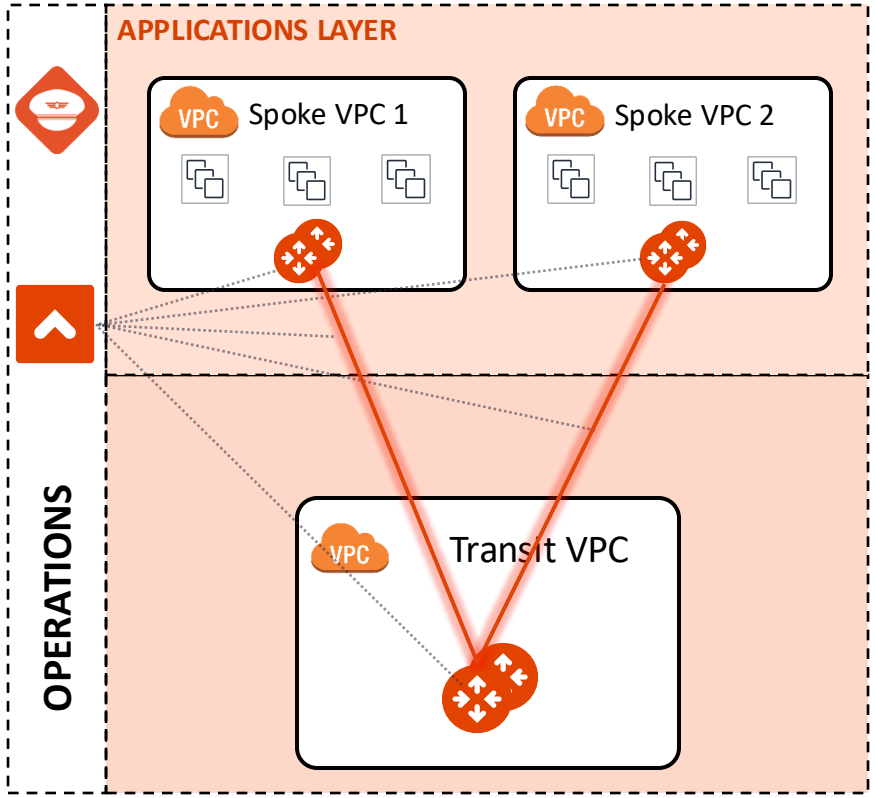
Public Route table

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (5)

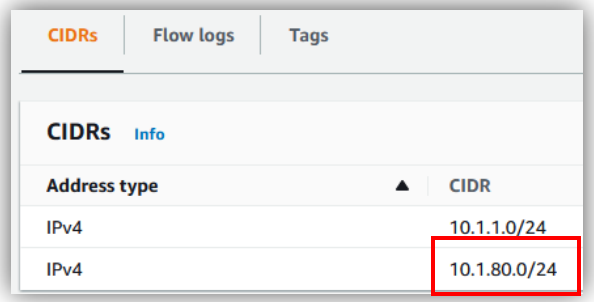
Filter routes

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

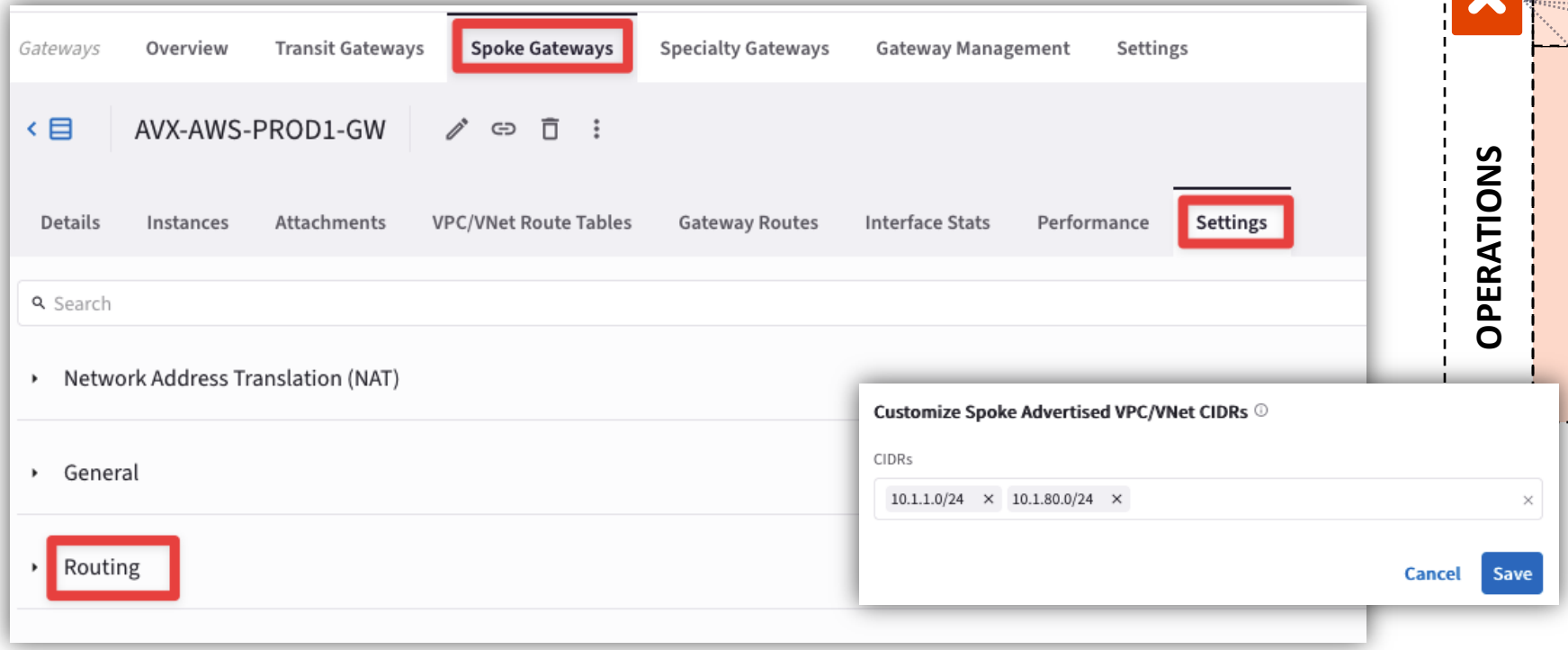


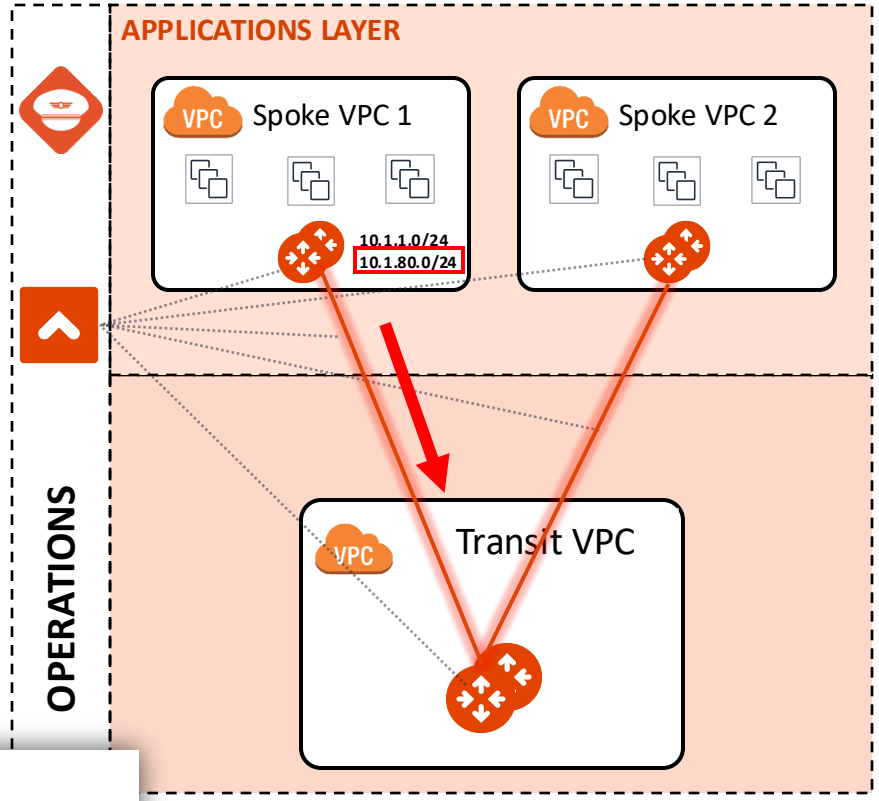
Routes Manipulation – Customize Spoke Advertised VPC CIDRs

- 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.



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

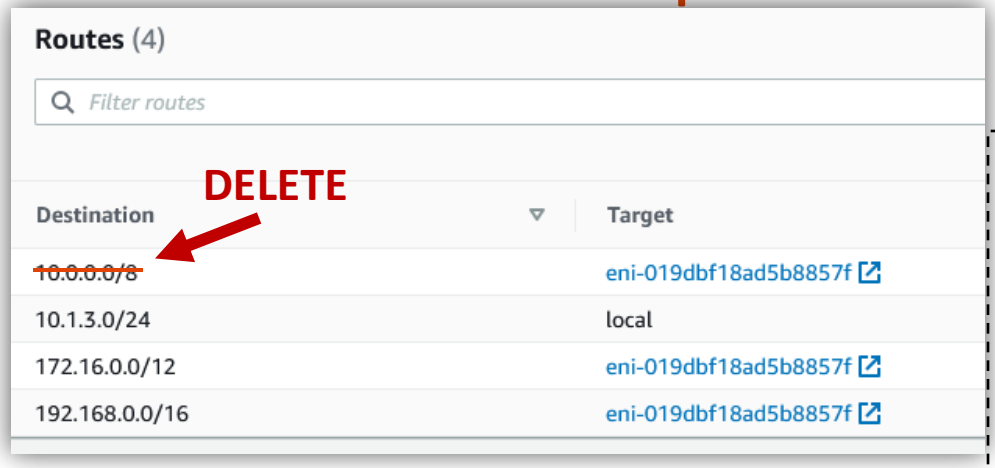




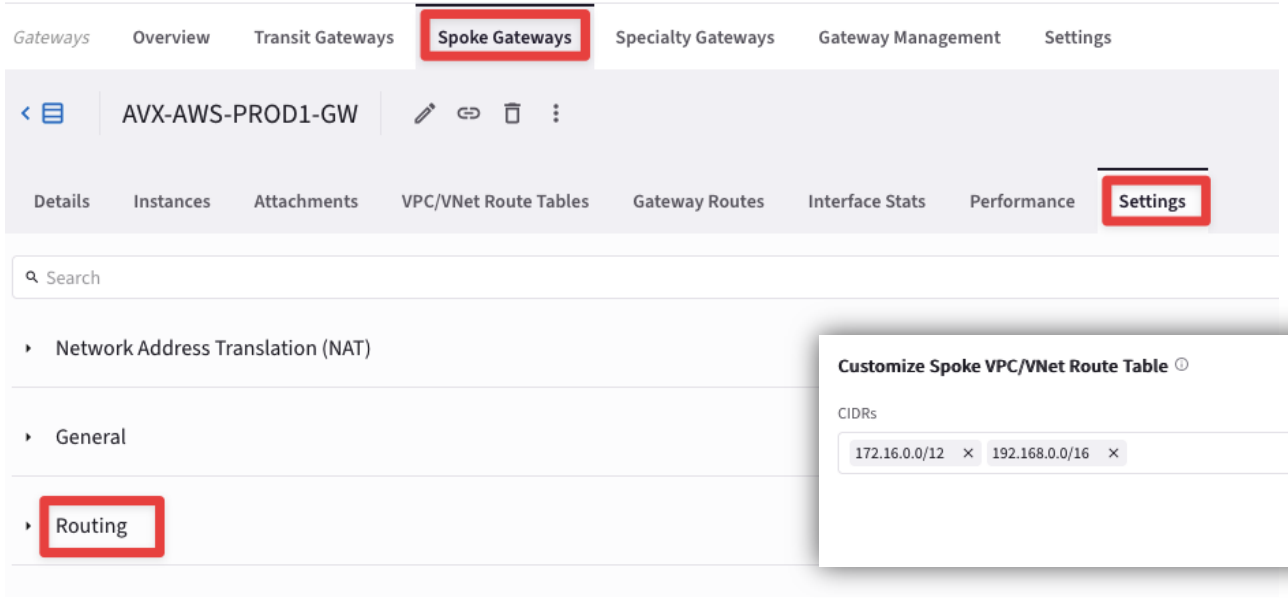
- This feature affects the Spoke-Transit routes advertisement

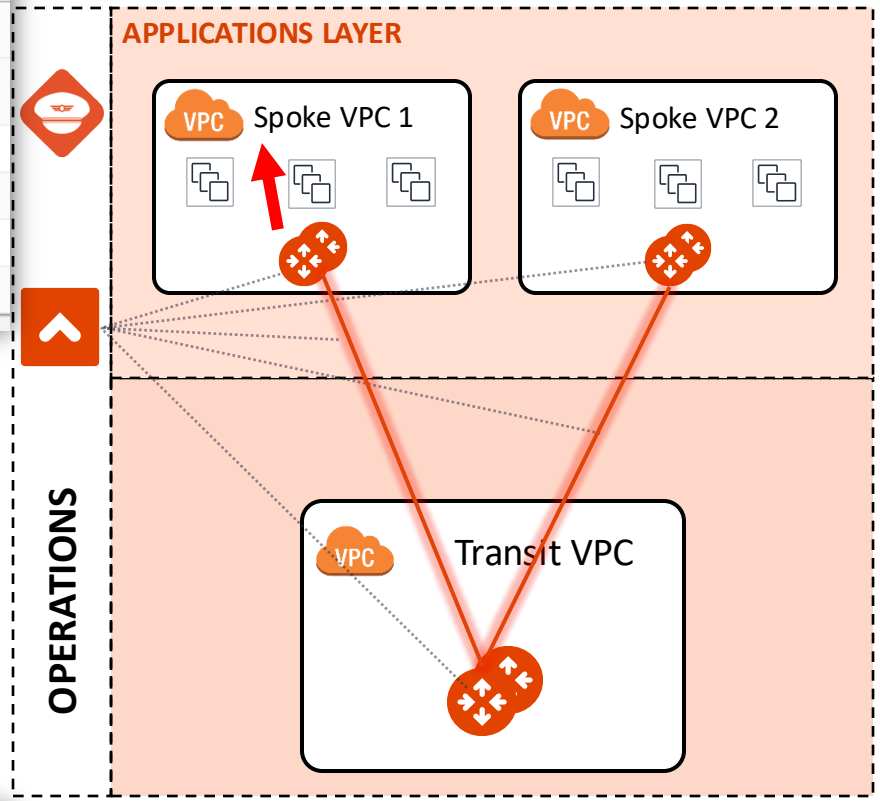
Routes Manipulation – Customize Spoke VPC Routing Table

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



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

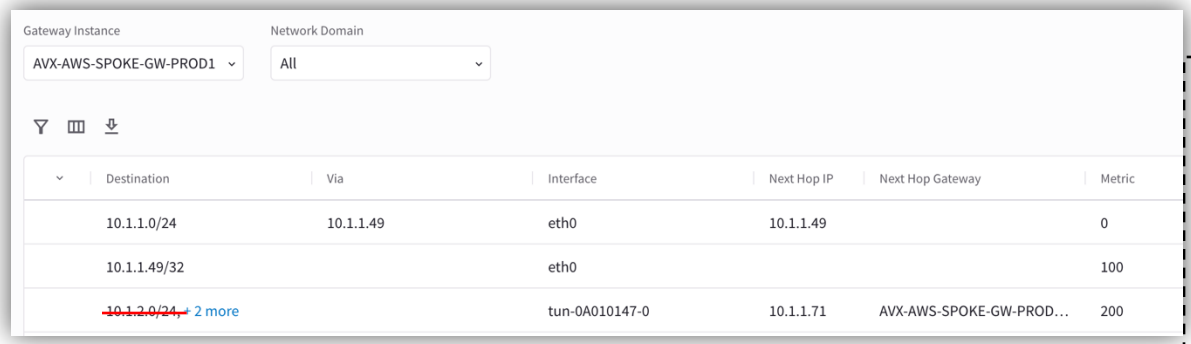




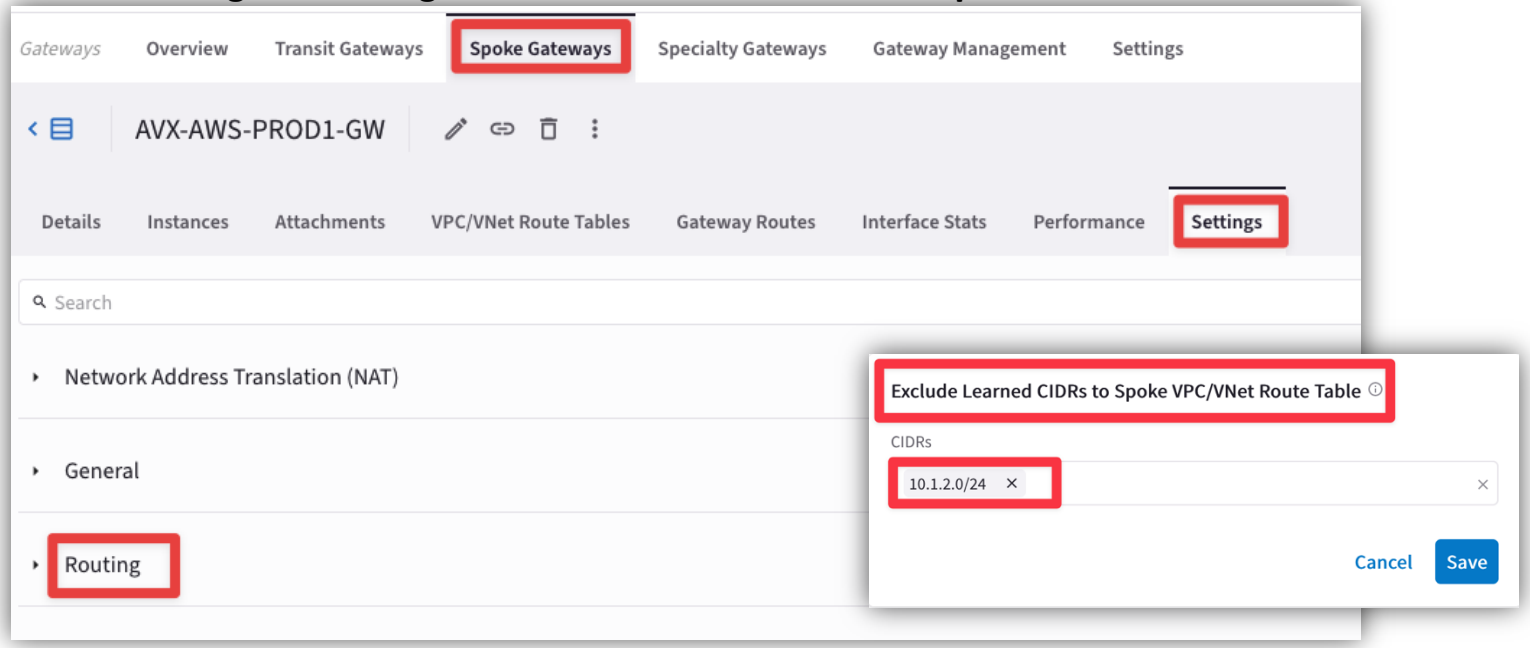
This feature affects the routes installed inside the VPC/Vnet/VCN routing tables.

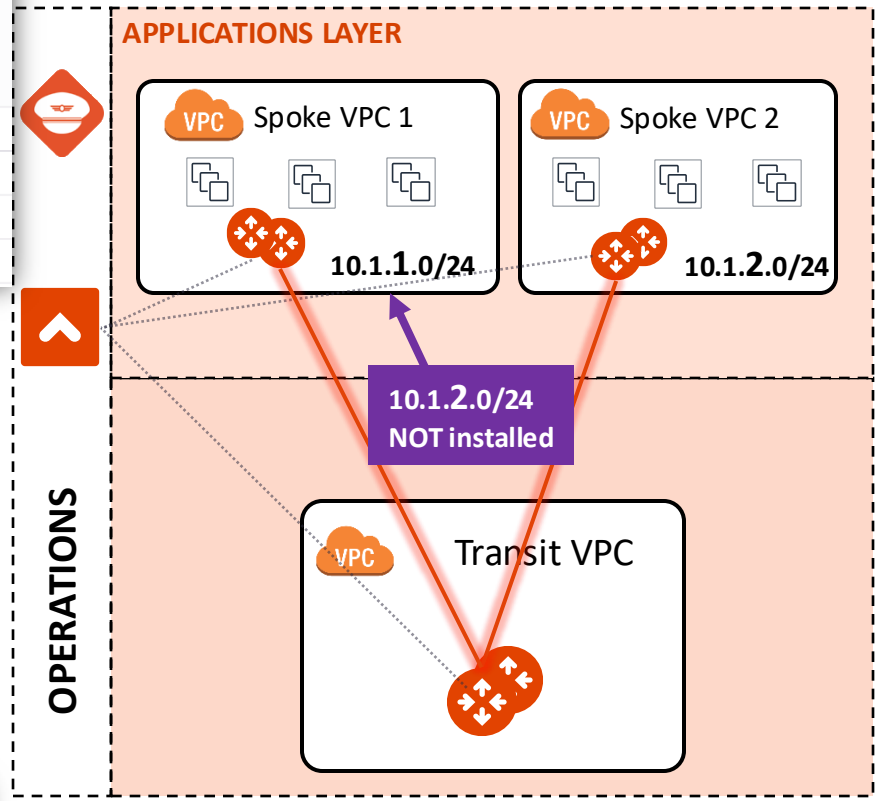
Routes Manipulation – Exclude Learned CIDRs to Spoke VPC/VNet Route Table

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



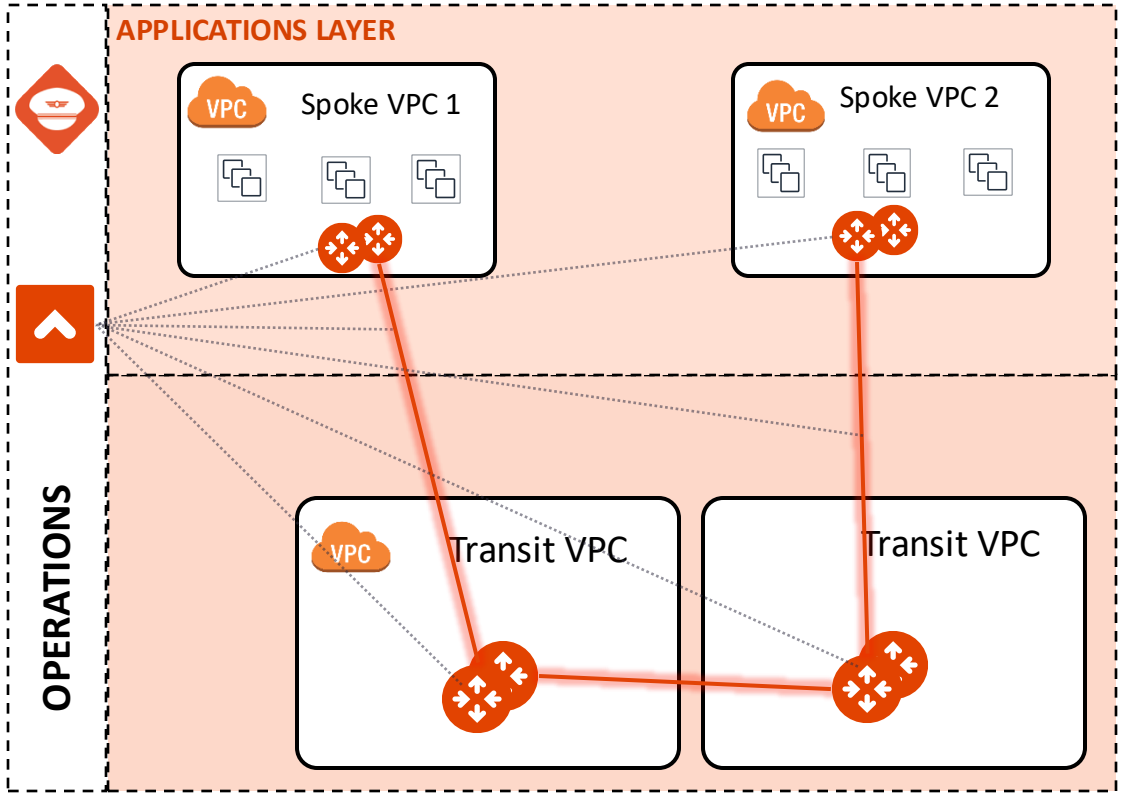
- **PATH:** COPILOT > Cloud Fabric > Gateways > Spoke Gateways > select the relevant GW > Settings > Routing > **Exclude Learned CIDRs to Spoke VPC/Vnet Route Table**



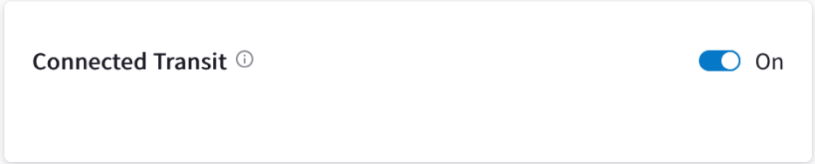


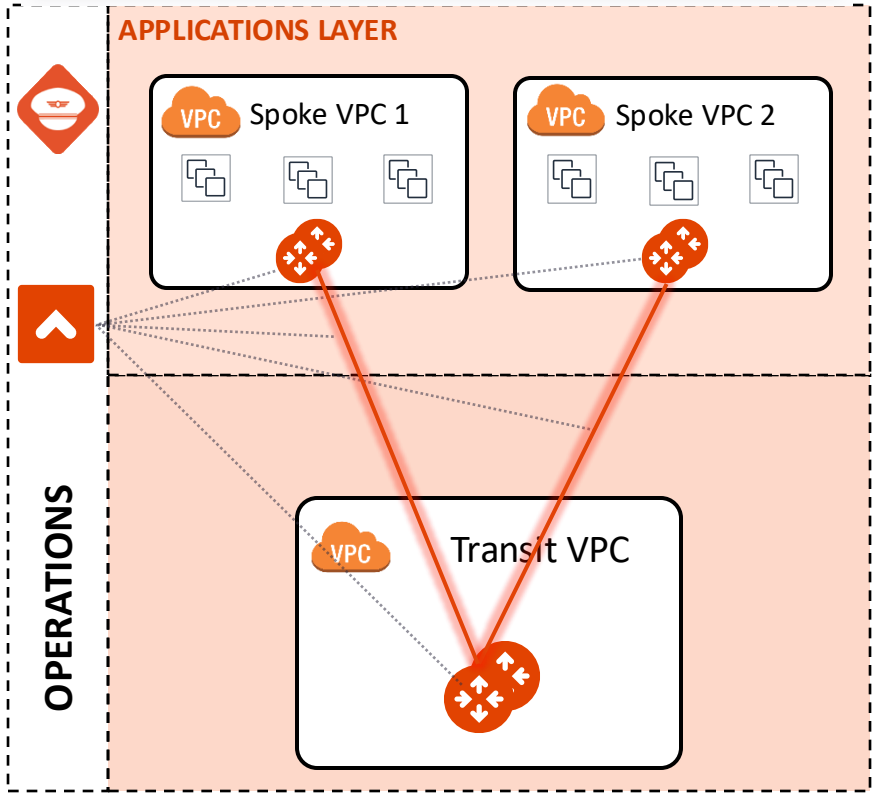
Routes Manipulation – Connected Transit

- **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.



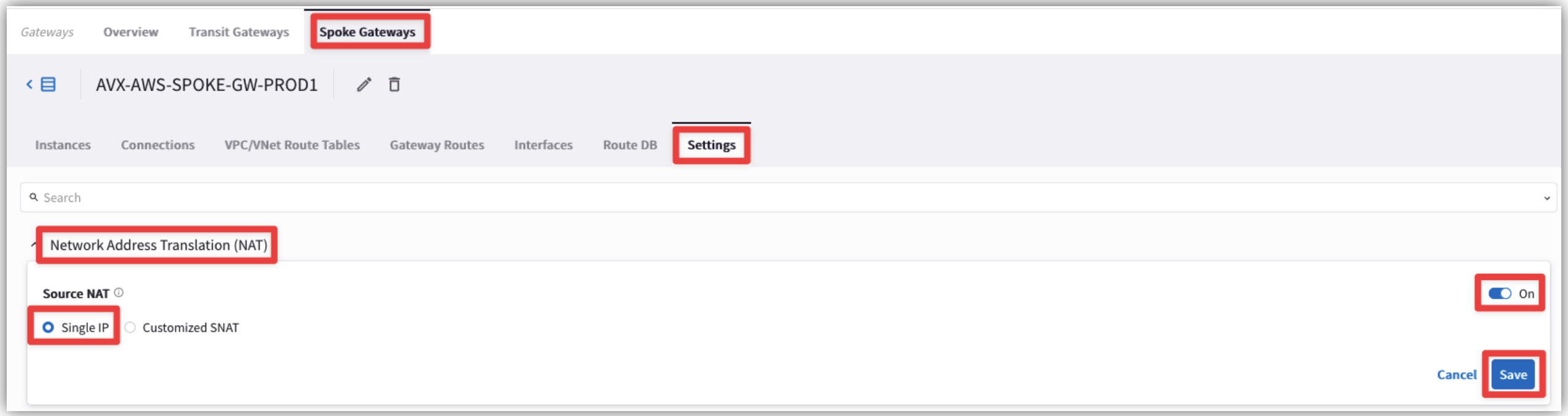


NAT - Overview

- 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**

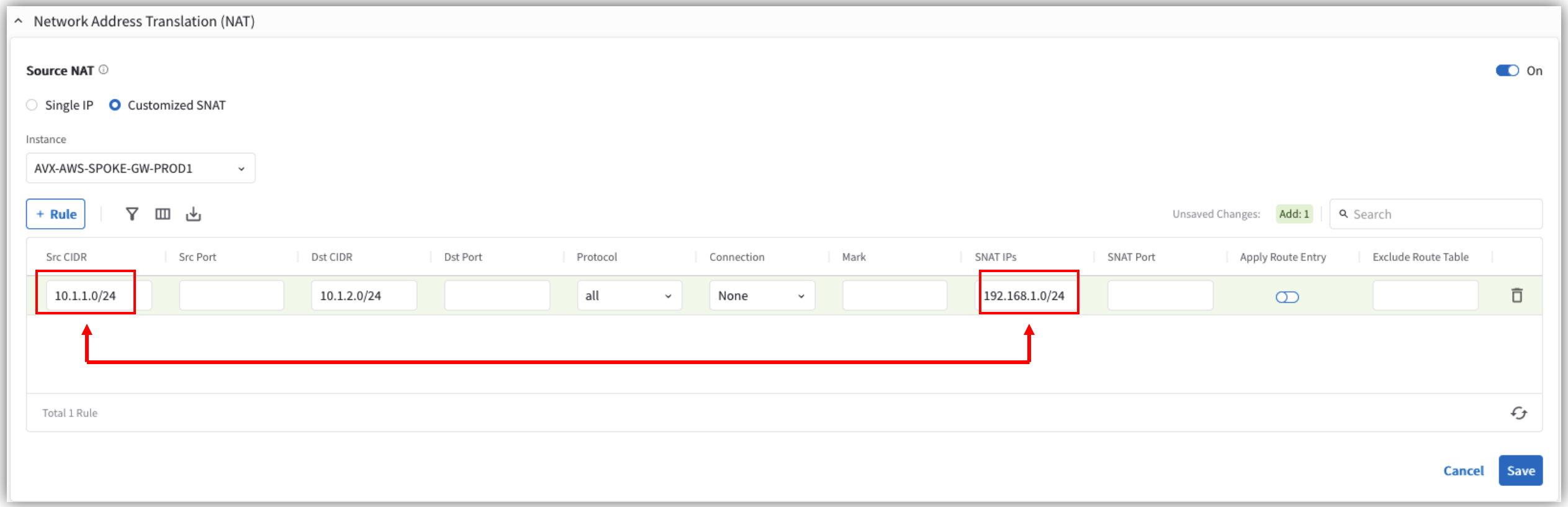
Source NAT: Single IP



- **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.

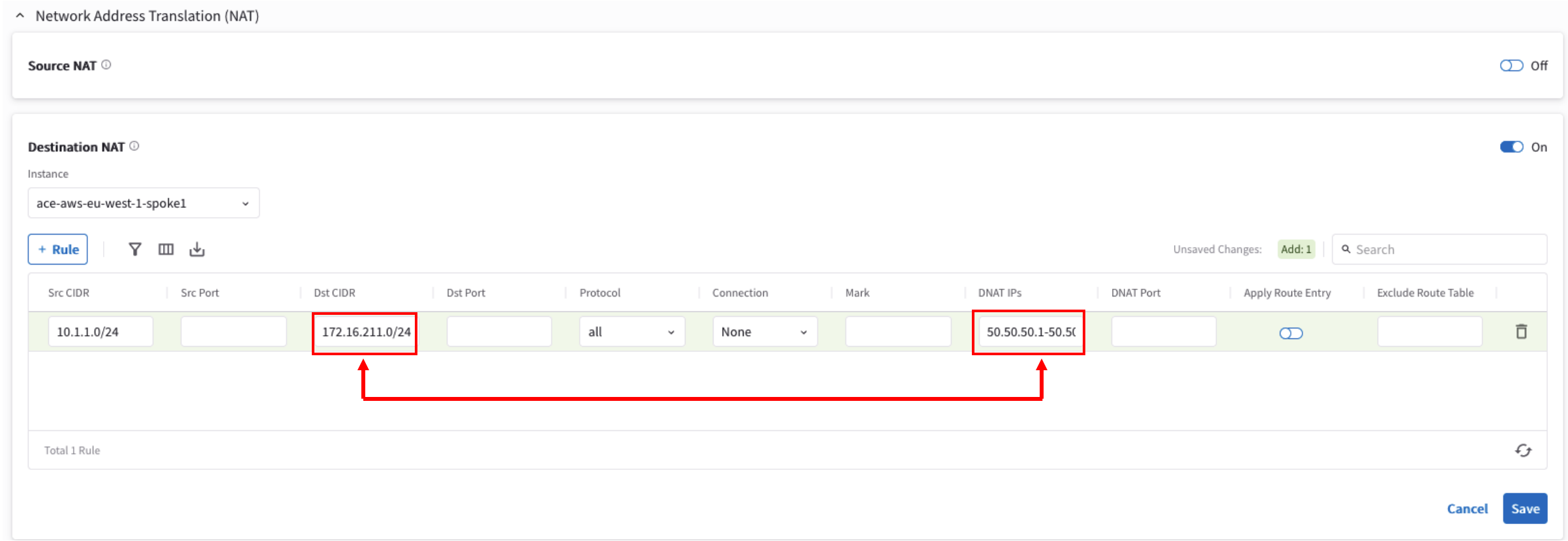
Source NAT: Customized SNAT

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



Destination NAT

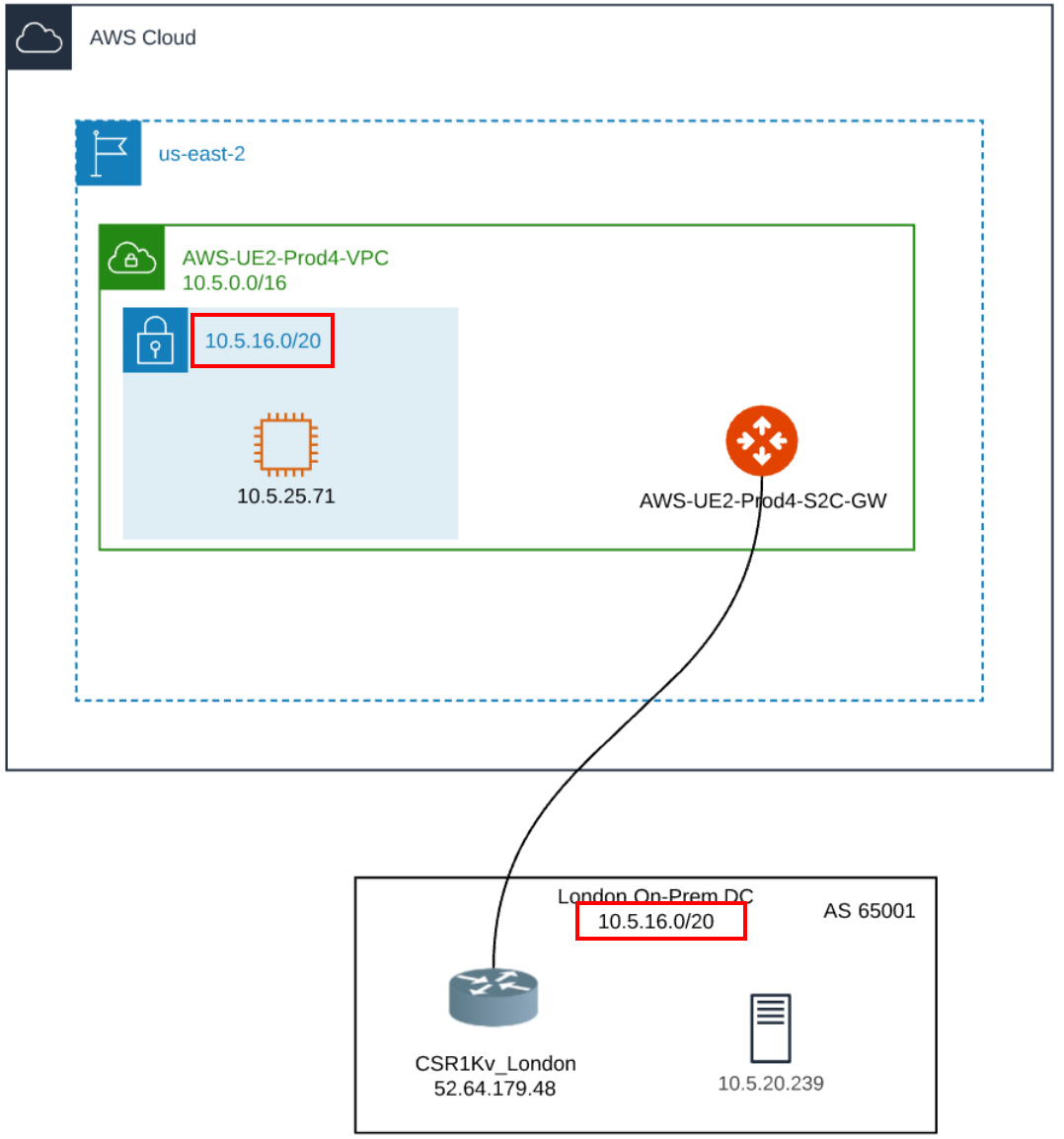
- Destination NAT (**DNAT**) allow you to change the destination to a virtual address range.



Overlapping IP Issue

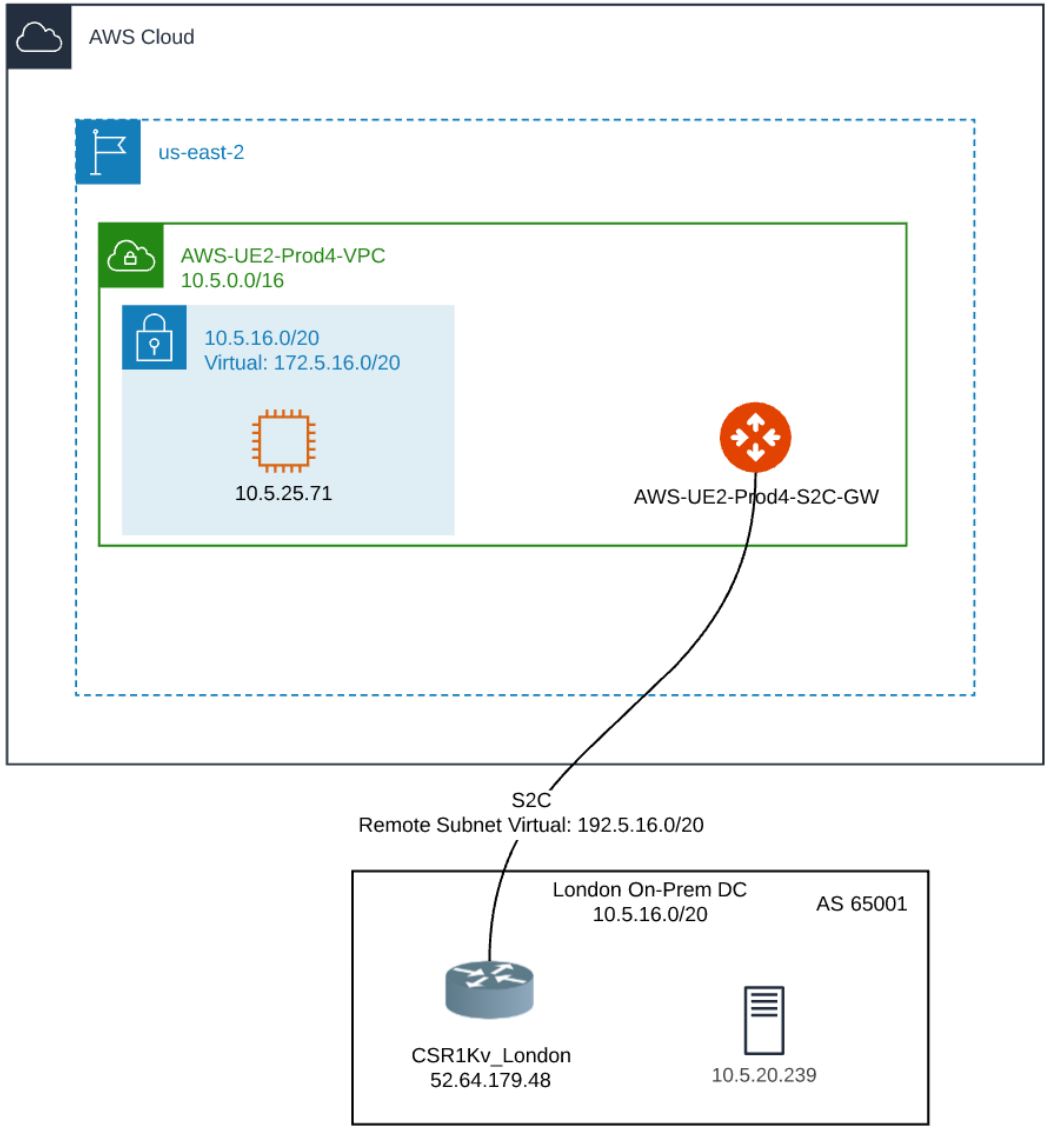
Mapped NAT - Overview

- 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



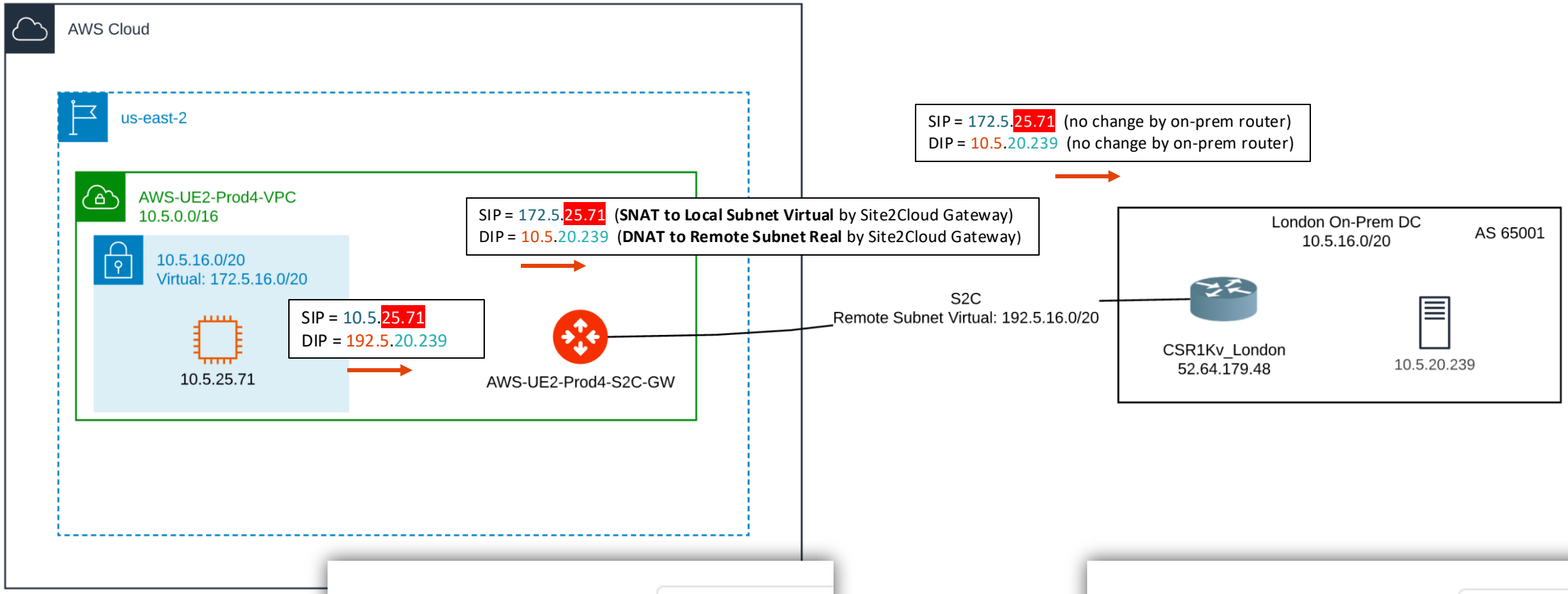
Mapped NAT – Virtual Subnets

- 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



AVIATRIX

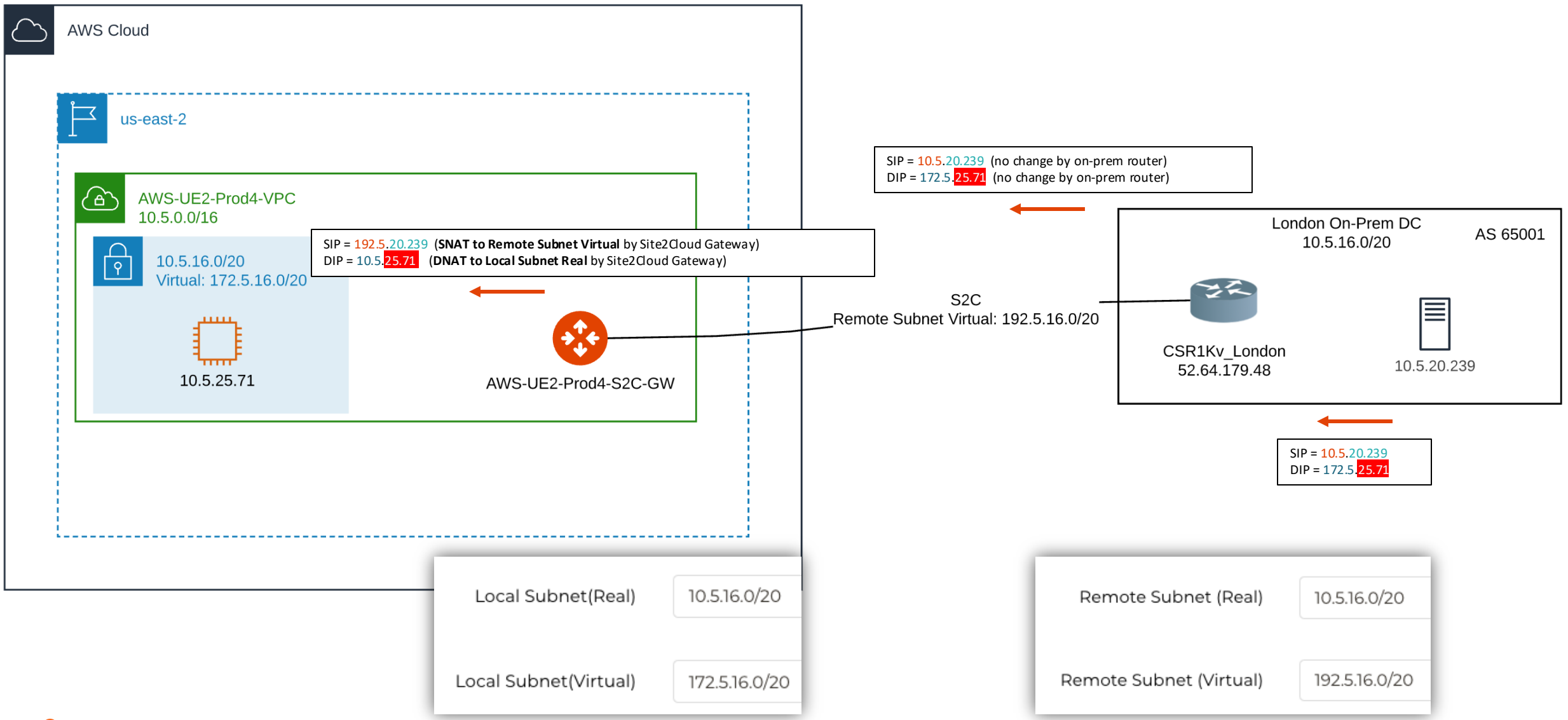
Mapped NAT – Packet Walk (from Local to Remote)



Local Subnet(Real)	10.5.16.0/20
Local Subnet(Virtual)	172.5.16.0/20

Remote Subnet (Real)	10.5.16.0/20
Remote Subnet (Virtual)	192.5.16.0/20

Mapped NAT – Packet Walk (from Remote to Local)

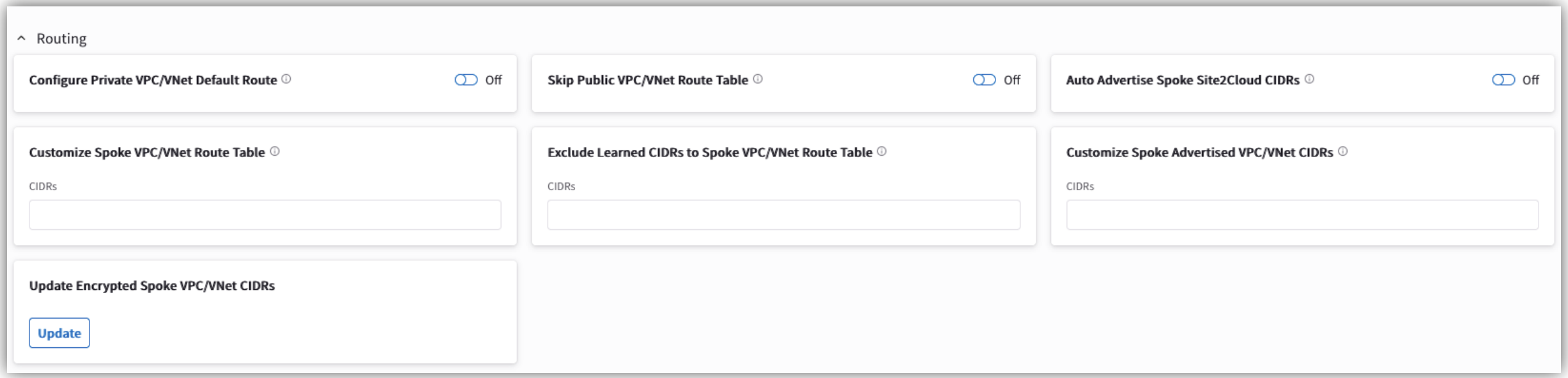


AVIATRIX

Tools for Operating your Routes Manipulation & NAT

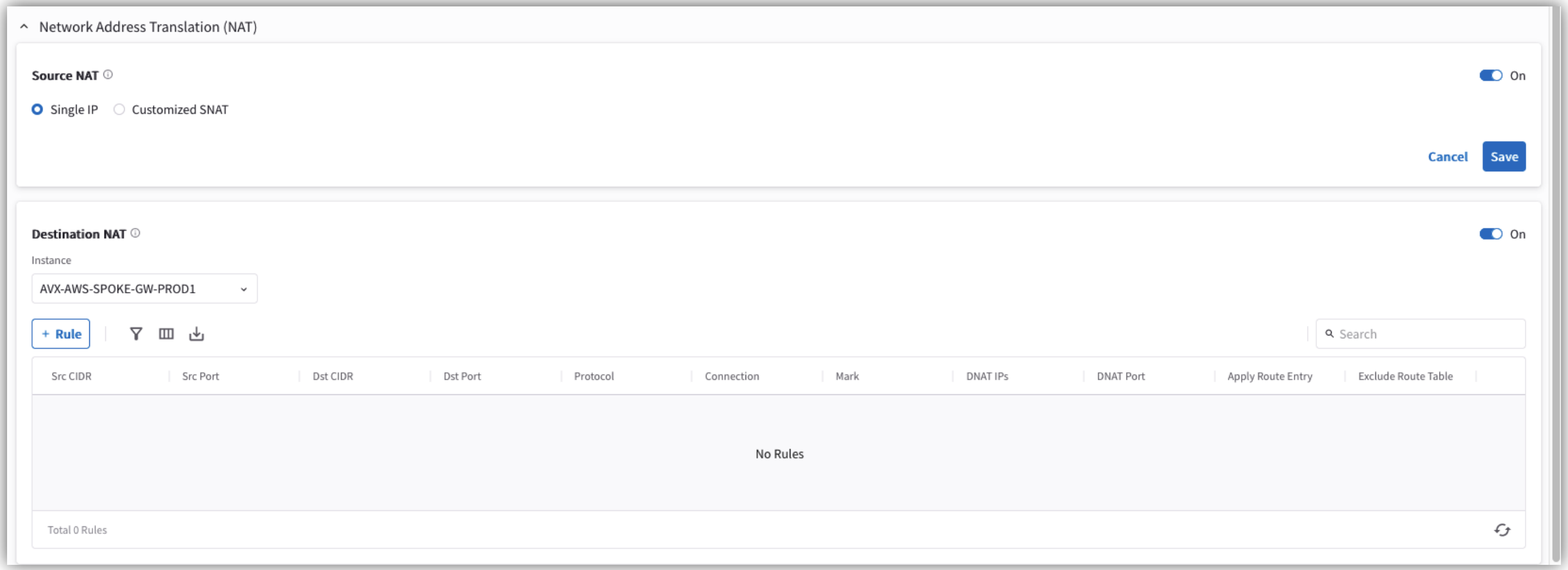
Routes Manipulation - ACTIONS

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



NAT

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



Next:

Lab 5 Routes Manipulation & NAT