



# COMMUNITY DAY

## Serverless Networking - How We Provide Cloud-Native Connectivity for IoT Devices

**Steffen Gebert, EMnify**  
[emnify.com/devs](http://emnify.com/devs)



**EMnify**

# Serverless Networking – How We Provide Cloud-Native Connectivity for IoT Devices

Steffen Gebert

AWS Community Day – Bay Area, 13.11.2020

# Abstract

In serverless, the network is taken for granted. But what if the network is the product? Is there a routerless? Does it still have a CLI? Interconnecting networks on AWS - most of us think of VPCs here - felt limited to something like pulling a cable from A to B. Deeper control - for those who miss their big fat routers - required own deployments in EC2 instances.

With AWS Transit Gateway, more complex networking architectures can finally be implemented in a serverless - sorry, routerless - fashion.

At EMnify, we run a connectivity platform for the Internet of Things based on cellular connectivity. Our customers' IoT devices often do not require access to the Internet, but are restricted to customer-owned networks reachable through VPN for security purposes.

Using AWS Transit Gateway (TGW), we are now able to wire customer VPCs securely with their IoT devices. By sharing the TGW with their AWS accounts, customer VPCs can be attached, while being isolated from other customers through routing domains.

The provisioning process is triggered by the customer through an API call and starts the execution of an AWS Step Functions workflow. The state machine ensures correct order of calls towards AWS APIs for creating resource shares, waiting up to 7 days for acceptance, and finally setting up routing in the TGW.

With such state machines, not only the happy path is handled serverless - and also humanless, but also error cases are caught to ensure failed provisionings do not leave stale resources behind.

Overall, serverless networking and serverless orchestration allowed us at EMnify to build our new Cloud-Native Connectivity features not only within short time, but with nearly no long-term maintenance efforts.

# | Thanks to Our Sponsors!



Platinum Sponsor



Silver Sponsors



Gold Sponsors



Fugue



# Agenda

- 1. Serverless for Network Enthusiasts**
- 2. Cellular IoT Connectivity**
- 3. Cloud Native IoT Connectivity**
  - Data Plane Implementation
  - Demo 🤝
  - Control Plane implementation

“

We ❤️ serverless

EVERYBODY

EMnify

# Serverless for Network Enthusiasts



# I About Myself



EMnify

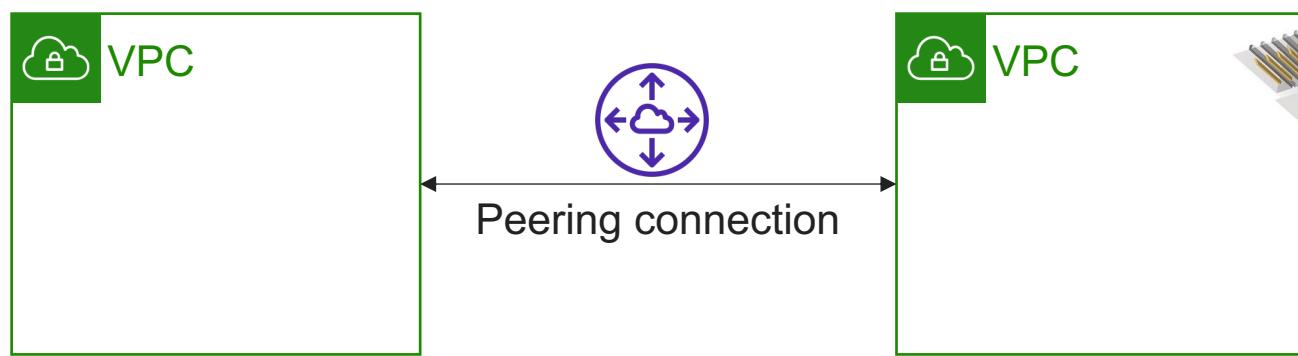


@StGebert

- Joined EMnify in 2017
- Started with AWS in 2017
- PhD on software based networking from University of Würzburg, Germany

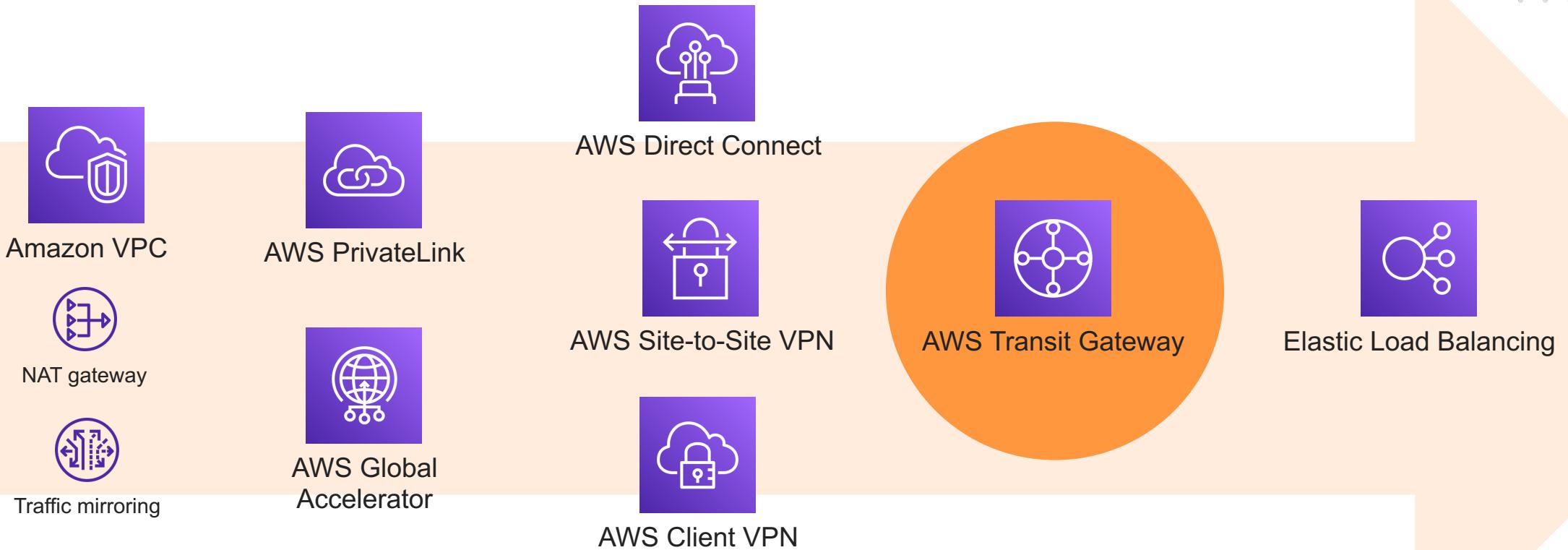
# The Network

# | VPC Peering?



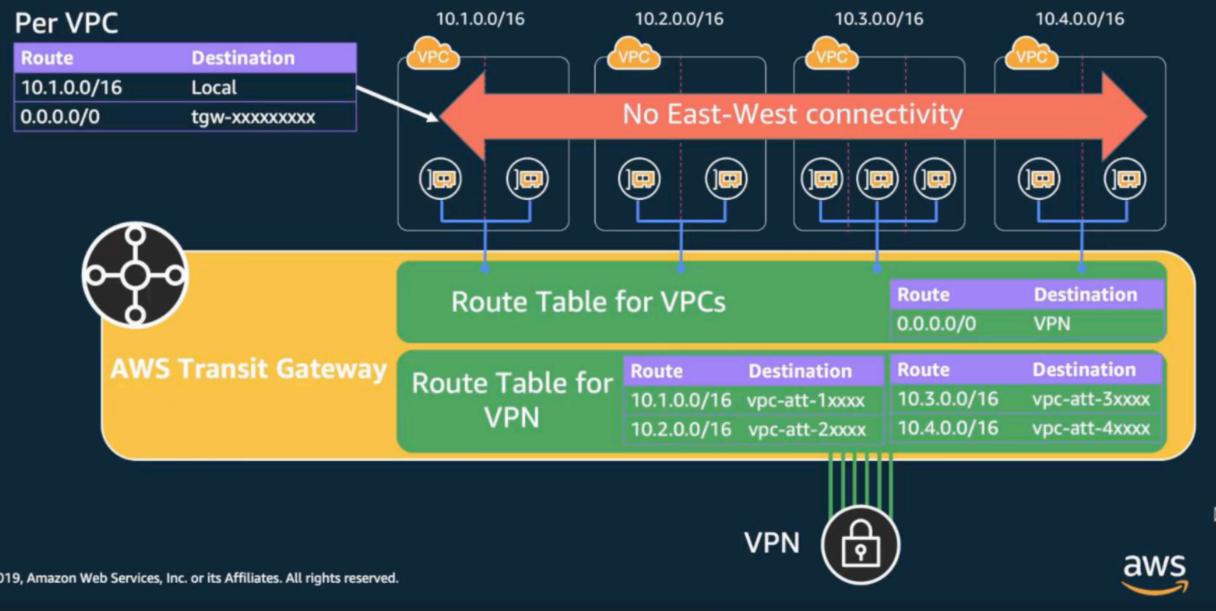
# Network Functions

# Serverless'y Network Functions



# I AWS Transit Gateway

## Segmented Network



- Essentially a router
  - Attachments ("the cables")
  - Routing table – per attachment
- Separate routing domains possible
  - Flat, Isolated, ..
  - More than just routing
- Implemented by AWS HyperPlane

Source: AWS Transit Gateway Reference  
Architectures for Many Amazon VPCs

# Attachment Types

VPCs  
(via ENI)

VPN  
(Site-to-Site IPsec)

Direct Connect

Other TGWs  
(in other regions)

# | Serverless Feelings

API

Horizontally  
Scalable

Somebody else  
fixes it

“

**Is this called “routerless”?**

NOBODY

“

**Another fleet of EC2 instances  
to terminate**

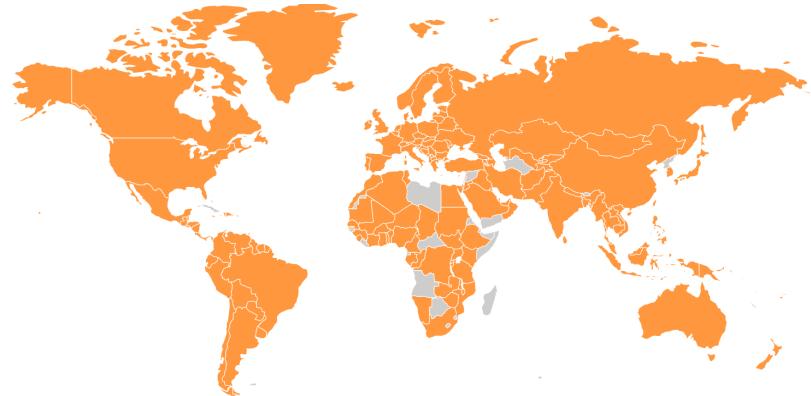
STEFFEN

EMnify

# Connecting the Internet of Things



# Cellular Connectivity Anywhere in the World



180 countries  
540 networks

2G, 3G, 4G,  
LTE-M, NB-IoT

Pay-as-you go pricing  
with data pooling



# Supporting Global IoT Deployments

Traditional Operators



Home-routing of roaming SIM data  
prevents distributed architecture

EMnify Connectivity



EMnify's mobile core network is  
deployed in multiple AWS regions  
– keeping data local

# Connectivity Management

## Complete Cost & Network Control

- SIM contract lifecycle to activate & suspend SIM at any time

## Real-time Insights

- Visibility and management of networks, devices and connectivity
- Remote Device Access
- Business Reports

The screenshot shows the EMnify platform's "Connected Devices" section. The interface includes a sidebar with navigation links like Dashboard, Connected Devices (which is selected), Orders, Integrations, Device Policies, Reports, and SIM Inventory. The main area is titled "Connected Devices" and displays a table of connected devices. The columns in the table are NAME, STATUS, SIM, and MONTHLY USAGE. The data rows are:

NAME	STATUS	SIM	MONTHLY USAGE
GPS tracker 1	Enabled	60 MB	
GPS tracker 2	Enabled	no usage	
GPS tracker 3	Enabled	no usage	
GPS tracker 4	Enabled	63 MB	
Scooter 1	Enabled	44 MB	

At the bottom of the table, there are pagination controls (1-5 from 9) and a "Rows per page" dropdown set to 5. A "Need Help? Chat with us" button is located at the bottom left of the main content area.

# I Built for Integration

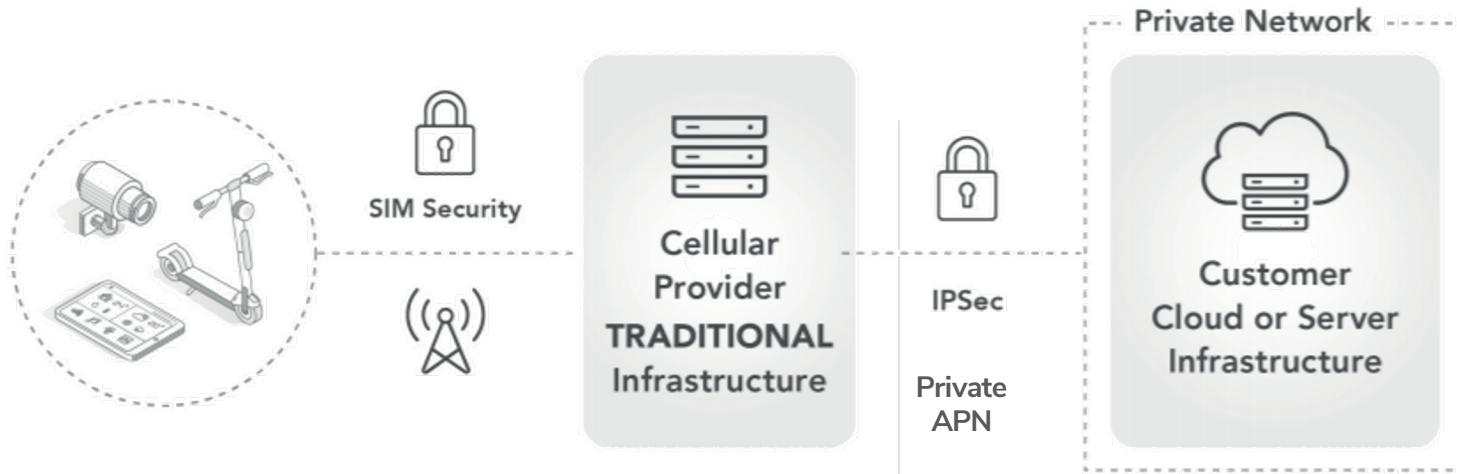
## API-First Approach

- RESTful APIs for device management, SMS & USSD webhooks
- DataStreamer to cloud and 3<sup>rd</sup> party services: AWS QuicksSght, PowerBI, BigQuery, Salesforce, Keen.io, Datadog, Devicepilot, Automate.io

EMnify

The image displays two screenshots of the EMnify system interface. The top screenshot shows the 'EMnify Rest API' documentation page on a browser, featuring a Swagger UI. It includes a search bar, a 'Servers' dropdown set to 'https://cdn.emnify.net/', and a 'Root Entry' section with a 'GET /api/v1' endpoint. Below this are sections for 'Authentication' with various methods like POST /api/v1/authenticate and PATCH /api/v1/user/mfa/{id}, and a 'Filter by tag' input field. The bottom screenshot shows a comprehensive dashboard titled 'Org Usage & Device Data'. The dashboard features several data visualizations: a line chart for 'Lux, Humidity, Temp Sensor Data' over time; a bar chart for 'VR / 5GNN Location Updates last 2 hours'; a donut chart for 'Sim activations vs suspensions' showing 6 segments; a total cost of '€79.88'; and a total volume of '649.91 MB'. Other charts include 'Volume RX/TX last 7 days', 'Top 5 MNCs by Data Volume', and 'Top 5 Endpoints by Data Volume'.

# Secure Private Network for Cellular IoT



## Why required in IoT B2B?

- Remote access for support teams
- Additional security layer
- Circumvent carrier grade NAT

## Drawbacks

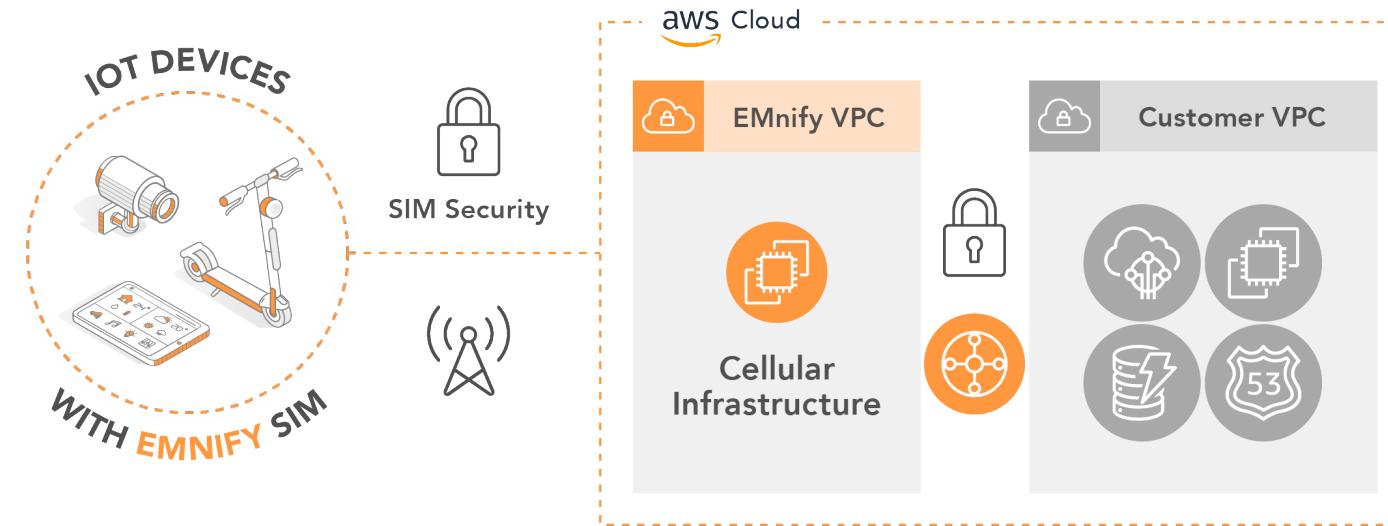
- Setup and recurring costs (private APN, static IP, IPsec, RADIUS)
- Complex IP config to setup redundant tunnels over public internet
- Time to deliver: 2-6 weeks

EMnify

# Implementing EMnify's Cloud Native Connectivity (CNC)



# | Simplifying Private Networks with EMnify & AWS



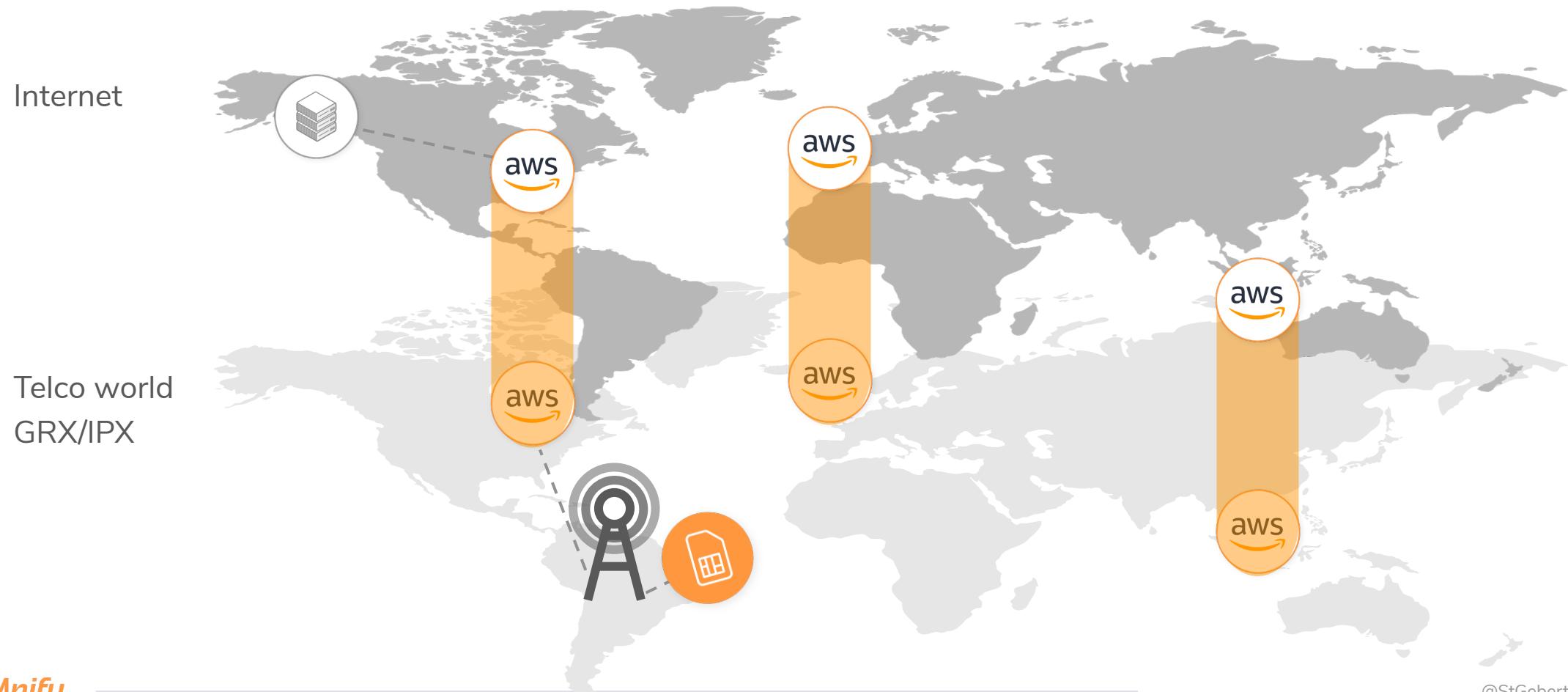
## AWS Native Implementation

- EMnify secures data up to AWS
- Private network connection using AWS-native features

## Benefits

- No need for private APN, IPsec
- Highly available by design
- Available immediately

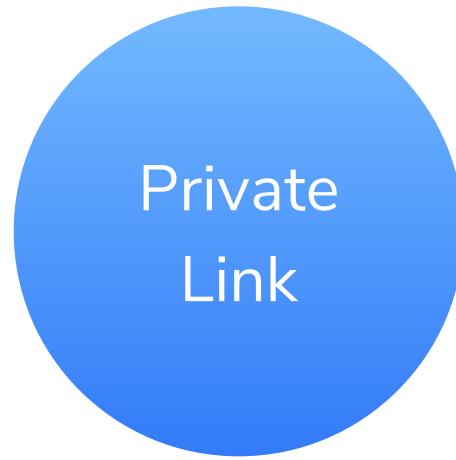
# Roaming-based Internet Access



# | Solution Space for Private Connectivity



No fun area



Private  
Link

Limits use cases  
(one-way connectivity,  
TCP only)



VPC  
Peering

Limits scale



Transit  
Gateway

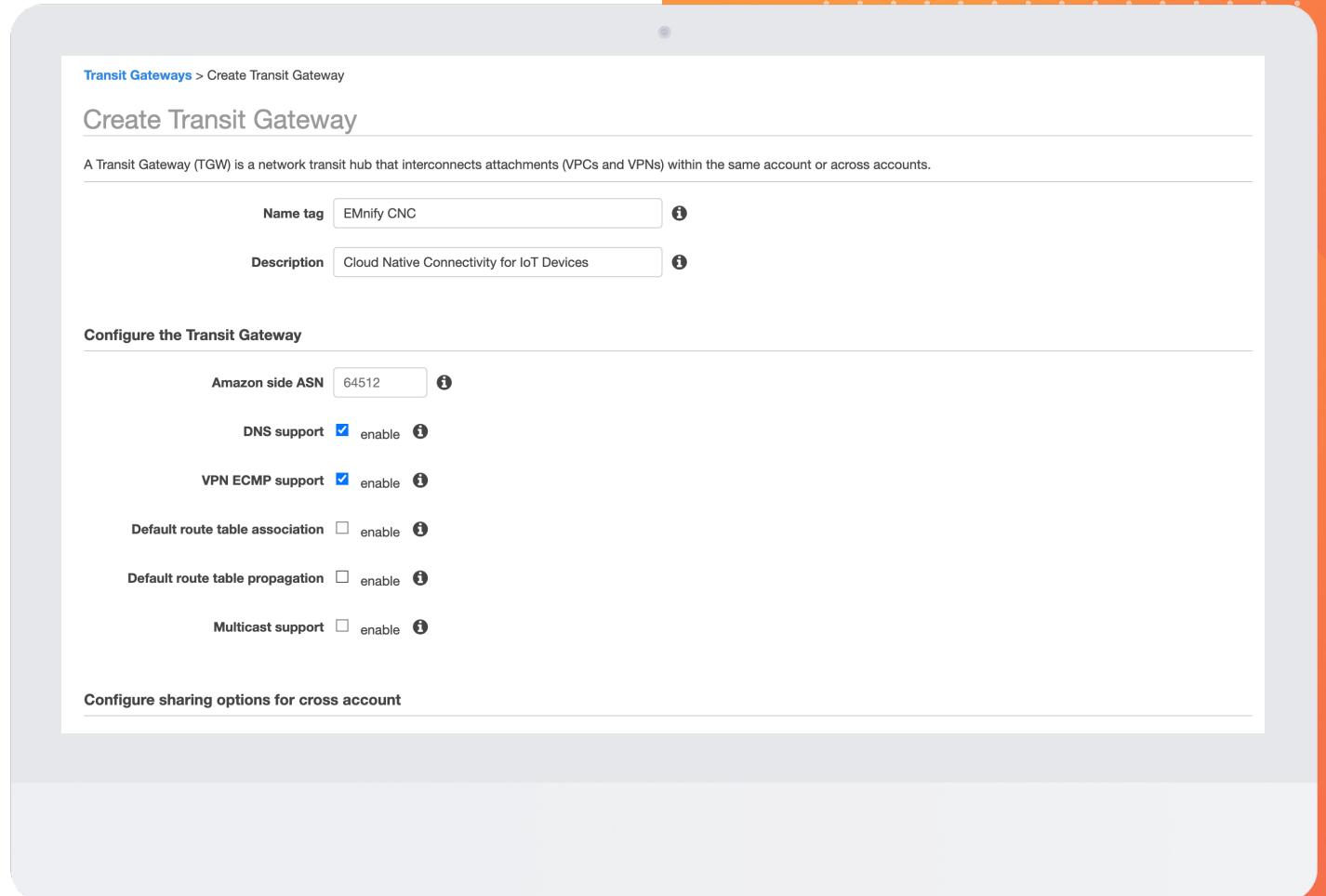


# | CNC Transit Gateway Setup

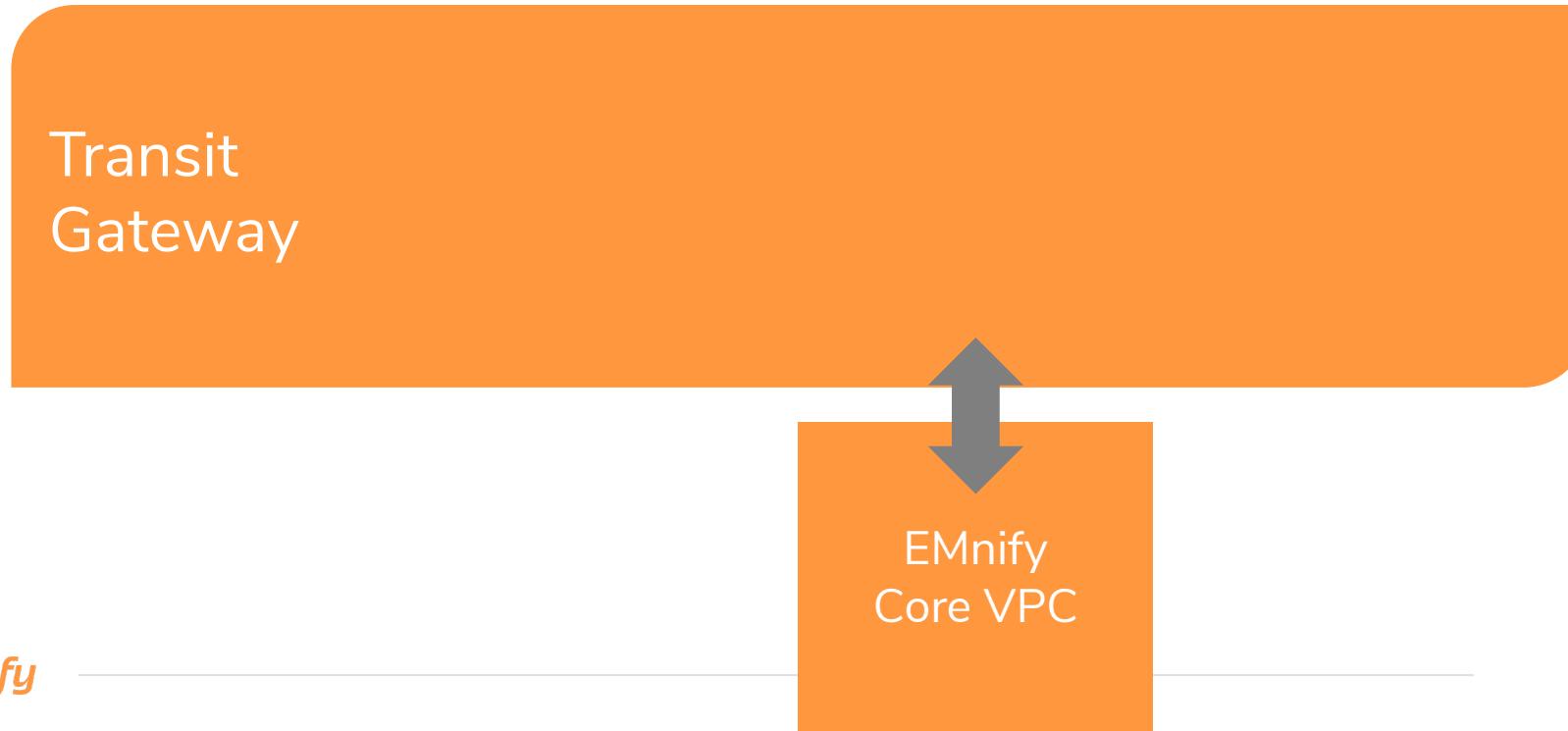
Transit  
Gateway

# TGW Creation

- Regional resource
- Automatically available in all AZs

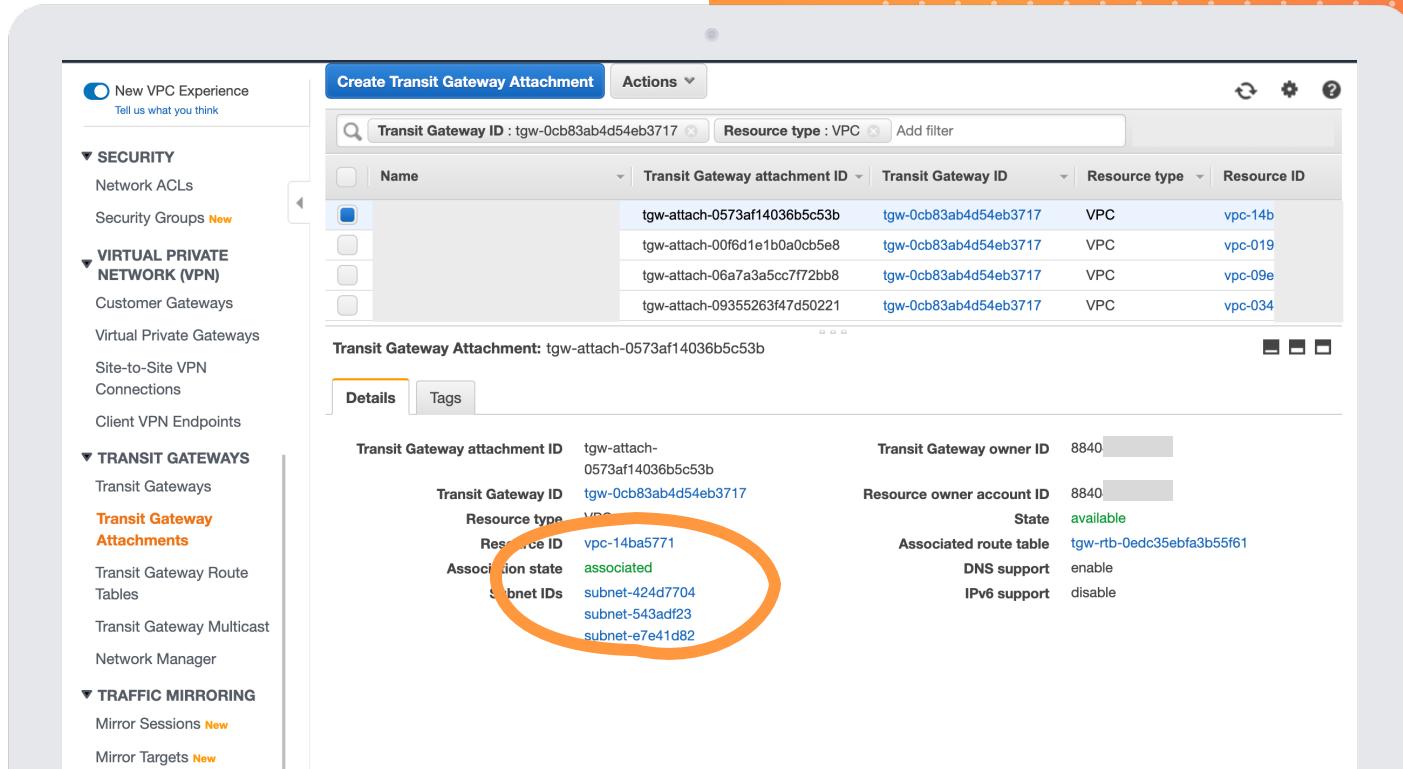


# CNC Transit Gateway Setup

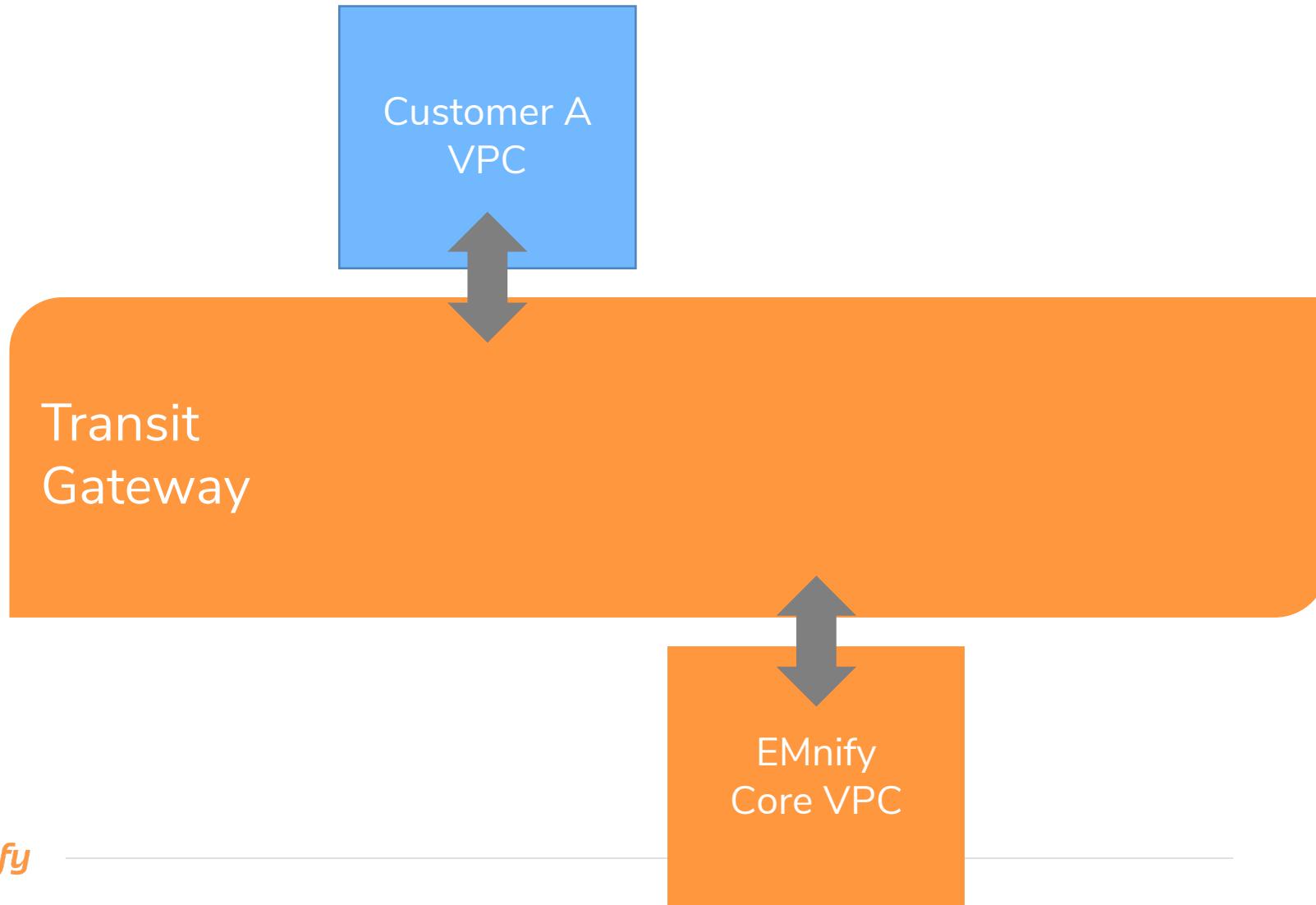


# Attachment EMnify Core VPC

- Associate with subnets in all used AZs!
- Add route to routing table



# CNC Transit Gateway Setup



# Resource Share



AWS Resource Access Manager

- Resource Share needed to be later shared with specific customer accounts.

The screenshot shows the AWS CloudFront console interface. On the left, a sidebar lists several categories: SECURITY (Network ACLs, Security Groups), VIRTUAL PRIVATE NETWORK (VPN) (Customer Gateways, Virtual Private Gateways, Site-to-Site VPN Connections, Client VPN Endpoints), TRANSIT GATEWAYS (Transit Gateways, Transit Gateway Attachments, Transit Gateway Route Tables, Transit Gateway Multicast, Network Manager), and TRAFFIC MIRRORING (Mirror Sessions, Mirror Targets). The TRANSIT GATEWAYS section is currently selected. In the main content area, a table displays a single row for a Transit Gateway:

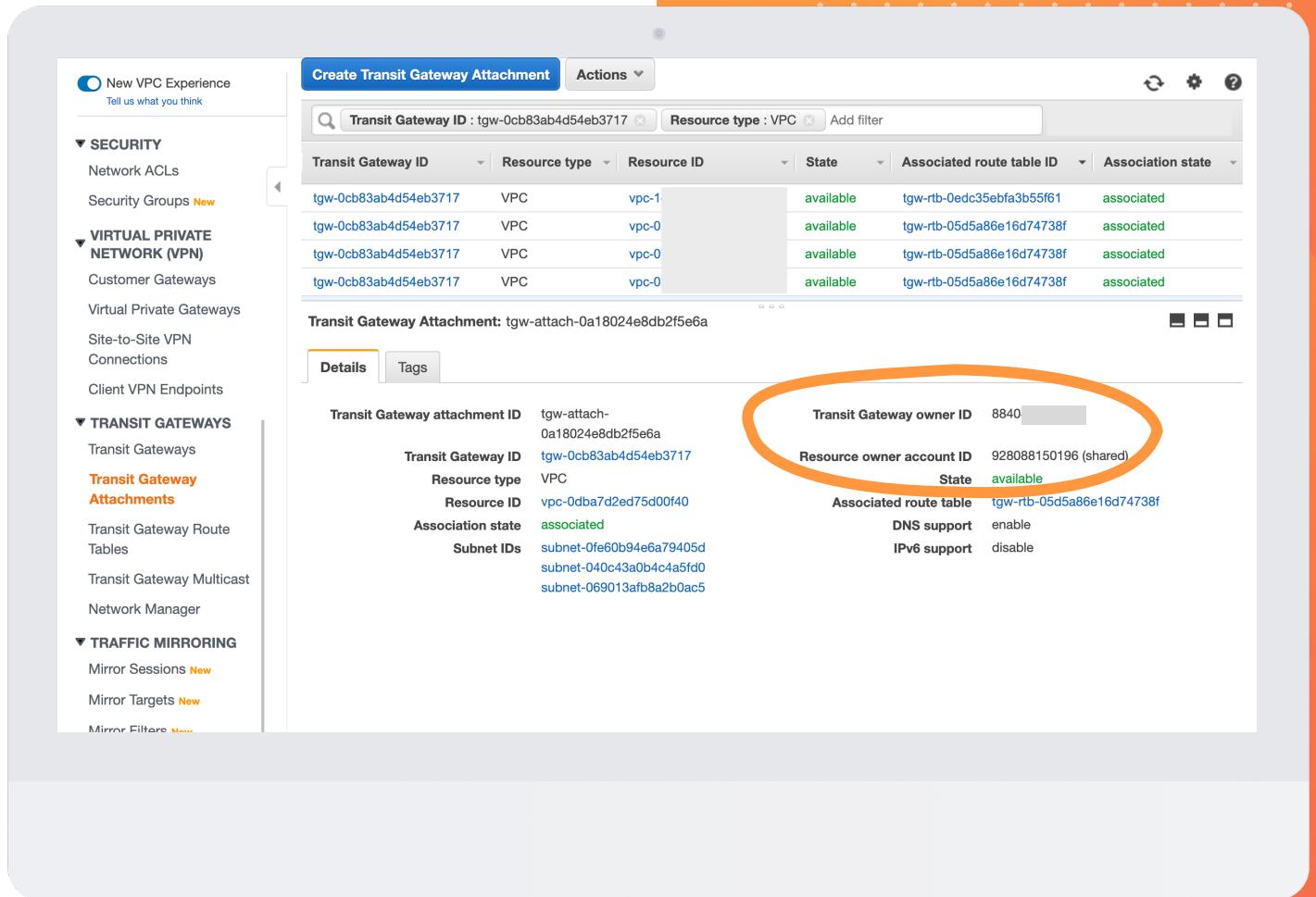
Name	Transit Gateway ID	Owner ID	Status
emnify Cloud Native Connectivity	tgw-0cb83ab4d54eb3717	8840	available

Below the table, a section titled "Transit Gateway: tgw-0cb83ab4d54eb3717" contains tabs for "Details", "Tags", and "Sharing". The "Sharing" tab is active, highlighted with an orange oval. A callout from the "Sharing" tab points to a sub-section titled "Share Transit Gateway" which lists a single resource share entry:

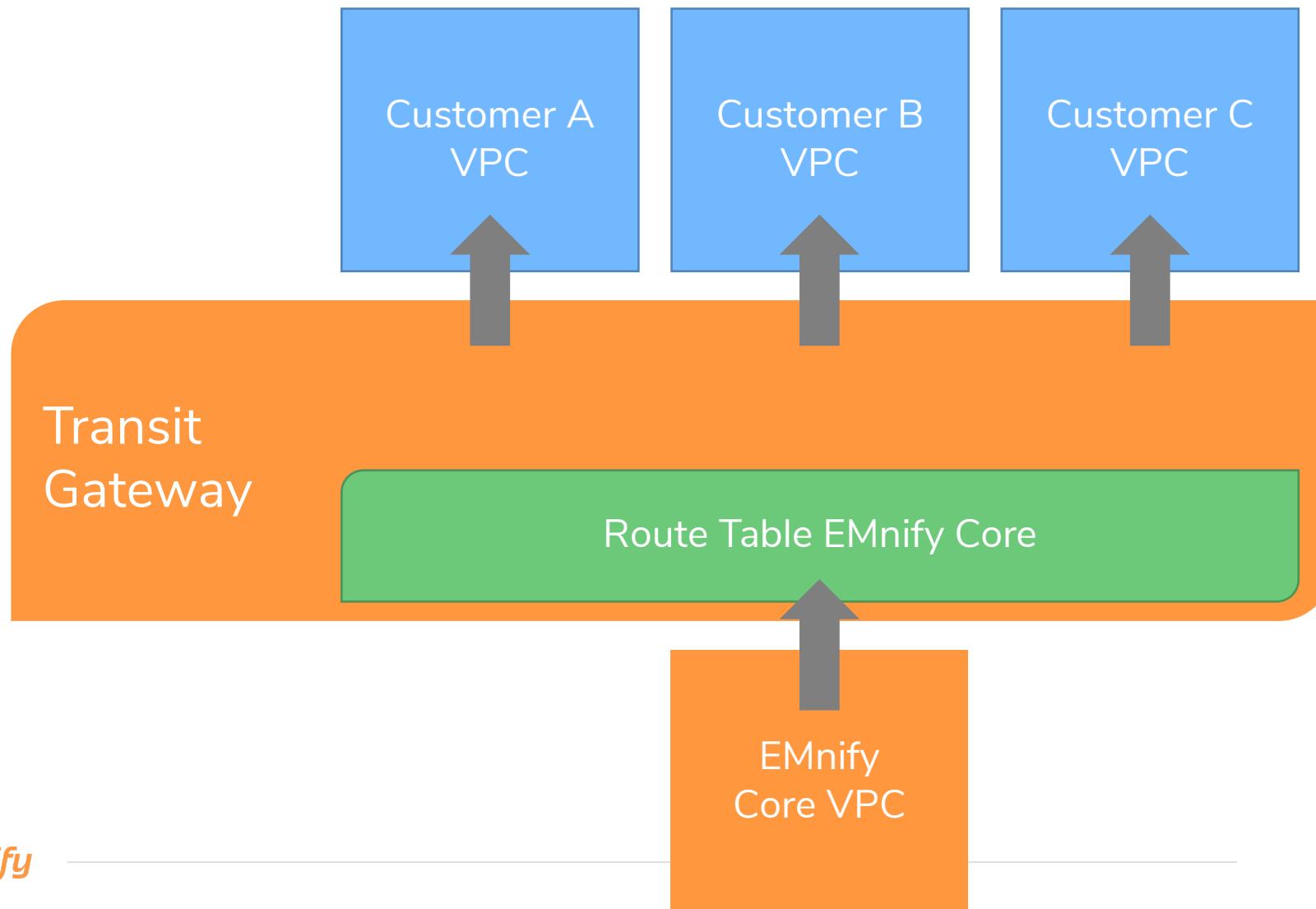
Resource Share Arn	Status
arn:aws:ram:eu-west-1:884047677700:resource-share/8eb593f6-f23c-06cc-41f8-2ce82c31626c	Associated

# Attachment Customer VPC

- Triggered by customer side

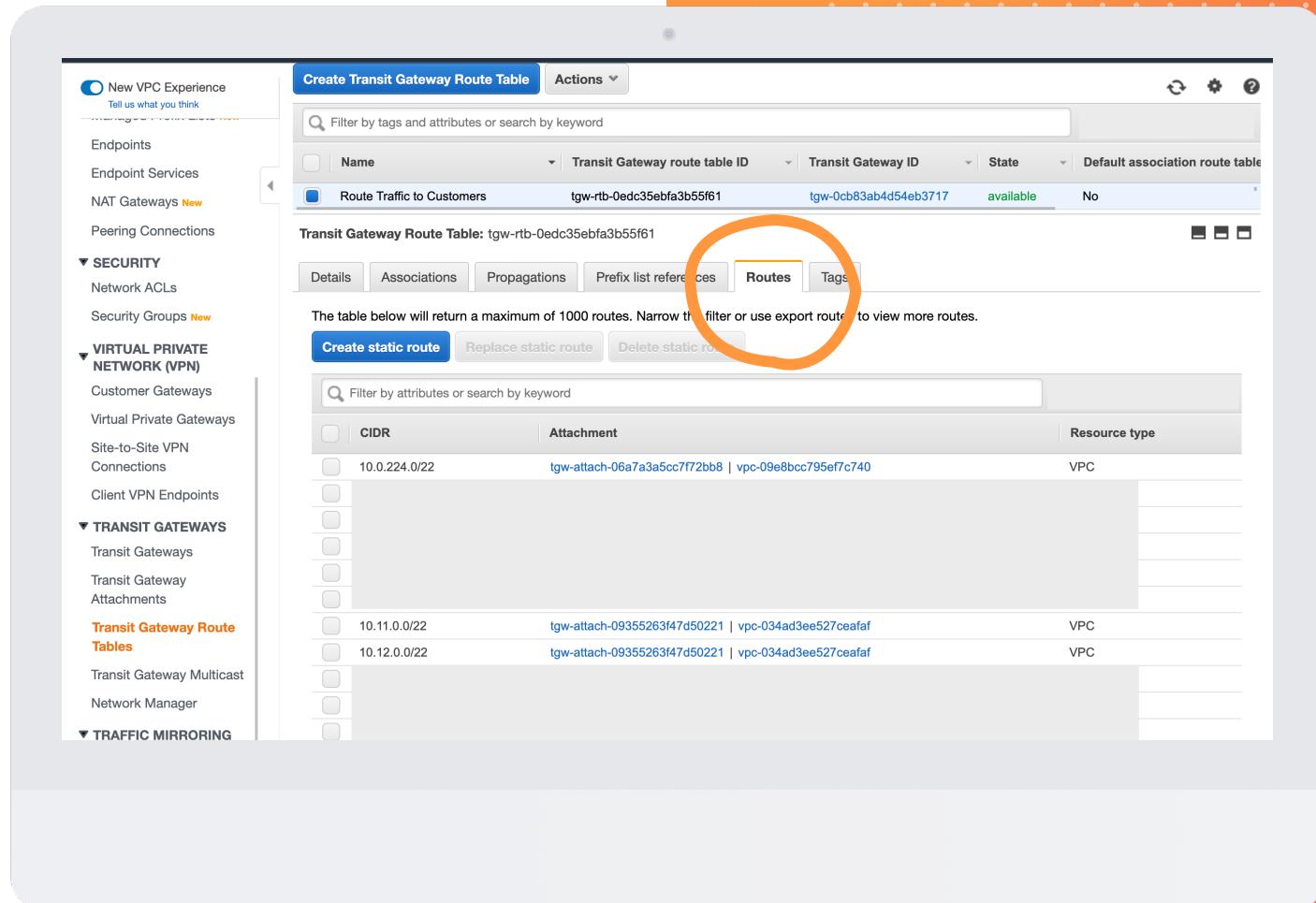


# CNC Transit Gateway Setup



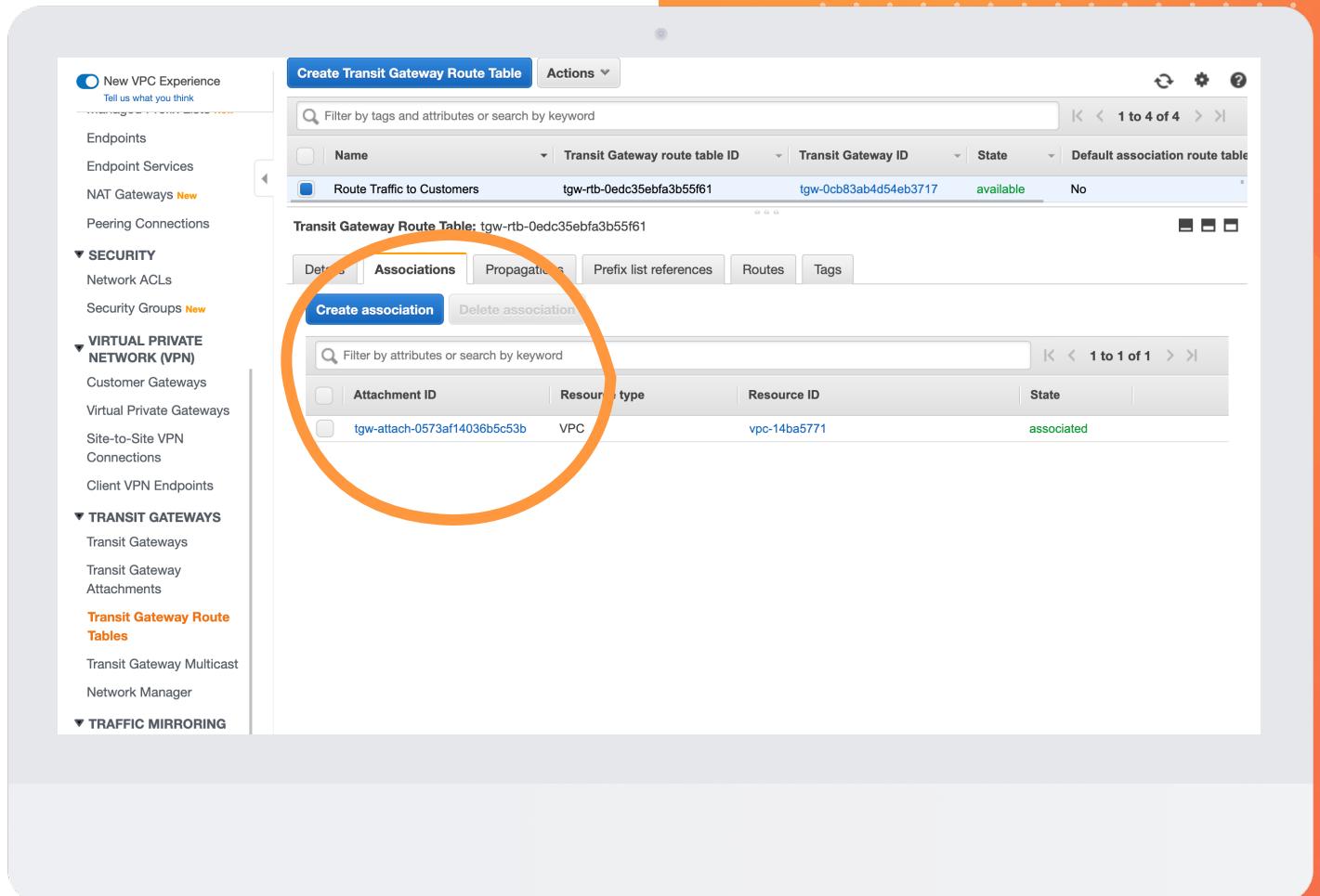
# Route Tables

- Static routes to customer VPCs

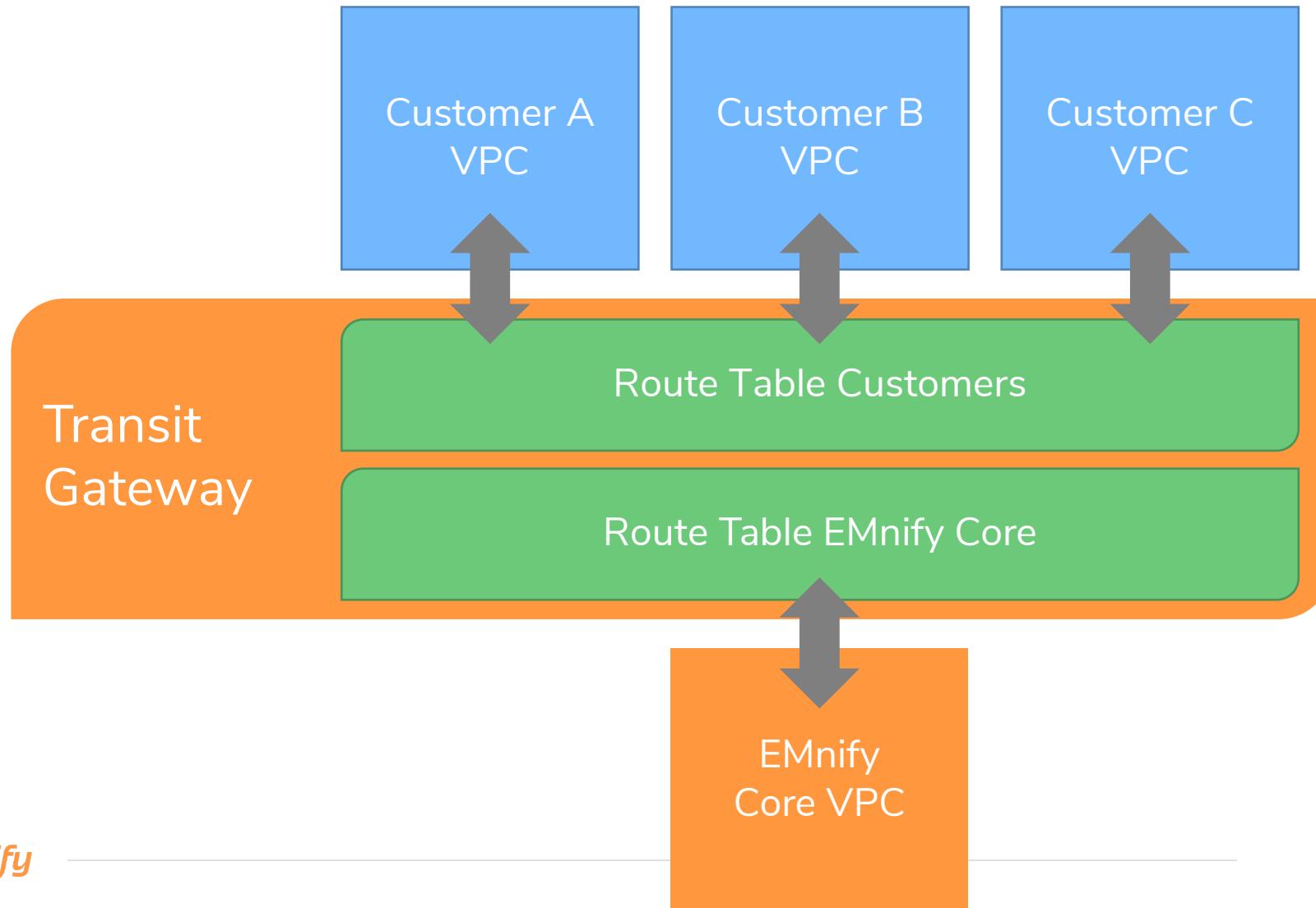


# Route Tables

- Associated with our VPC only  
(egress traffic from our PoV)



# CNC Transit Gateway Setup



# Route Tables

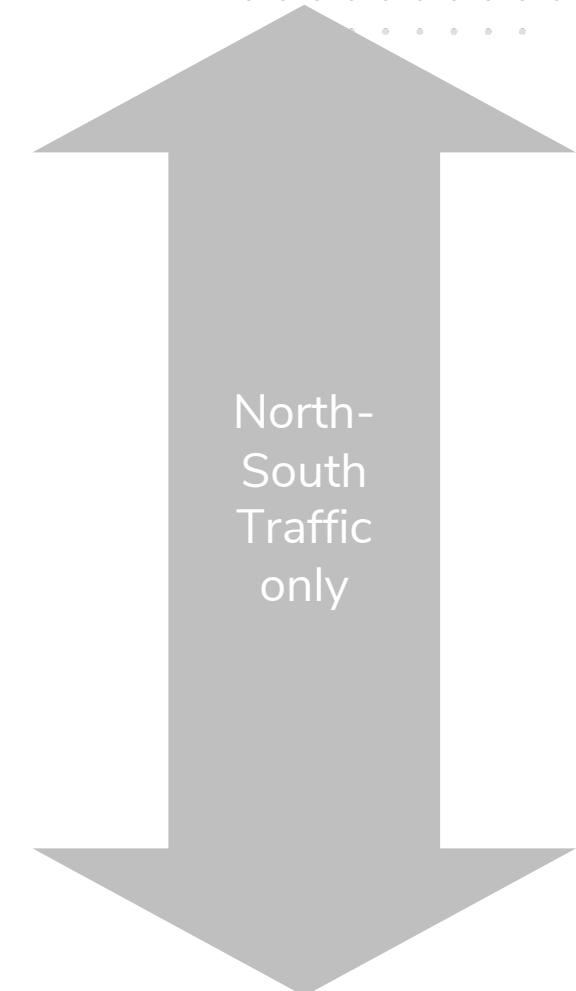
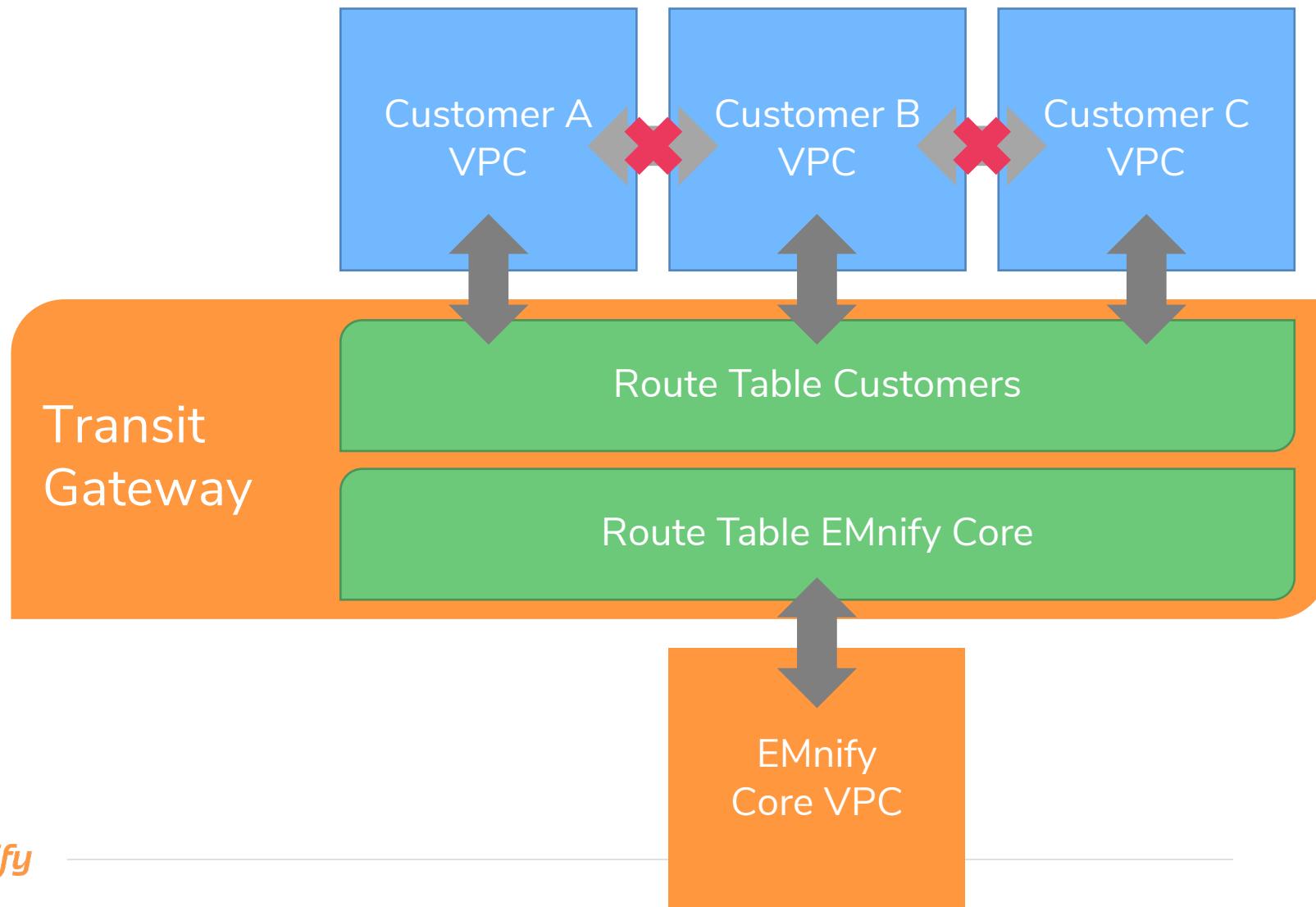
The screenshot shows the AWS CloudFormation console with the 'Create Transit Gateway Attachment' page open. The left sidebar includes sections for SECURITY (Network ACLs, Security Groups), VIRTUAL PRIVATE NETWORK (VPN) (Customer Gateways, Virtual Private Gateways, Site-to-Site VPN Connections, Client VPN Endpoints), TRANSIT GATEWAYS (Transit Gateways, **Transit Gateway Attachments**, Transit Gateway Route Tables, Transit Gateway Multicast, Network Manager), and TRAFFIC MIRRORING (Mirror Sessions, Mirror Targets). The main content area displays a table of Transit Gateway Attachments:

Transit Gateway ID	Resource type	Resource ID	State	Associated route table ID	Association state
tgw-0cb83ab4d54eb3717	VPC	vpc-14ba5771	available	tgw-rtb-0edc35ebfa3b55f61	associated
tgw-0cb83ab4d54eb3717	VPC	vpc-019633536bcd55b44	available	tgw-rtb-05d5a86e16d74738f	associated
tgw-0cb83ab4d54eb3717	VPC	vpc-09e8bcc795ef7c740	available	tgw-rtb-05d5a86e16d74738f	associated
tgw-0cb83ab4d54eb3717	VPC	vpc-034ad3ee527ceafaf	available	tgw-rtb-05d5a86e16d74738f	associated

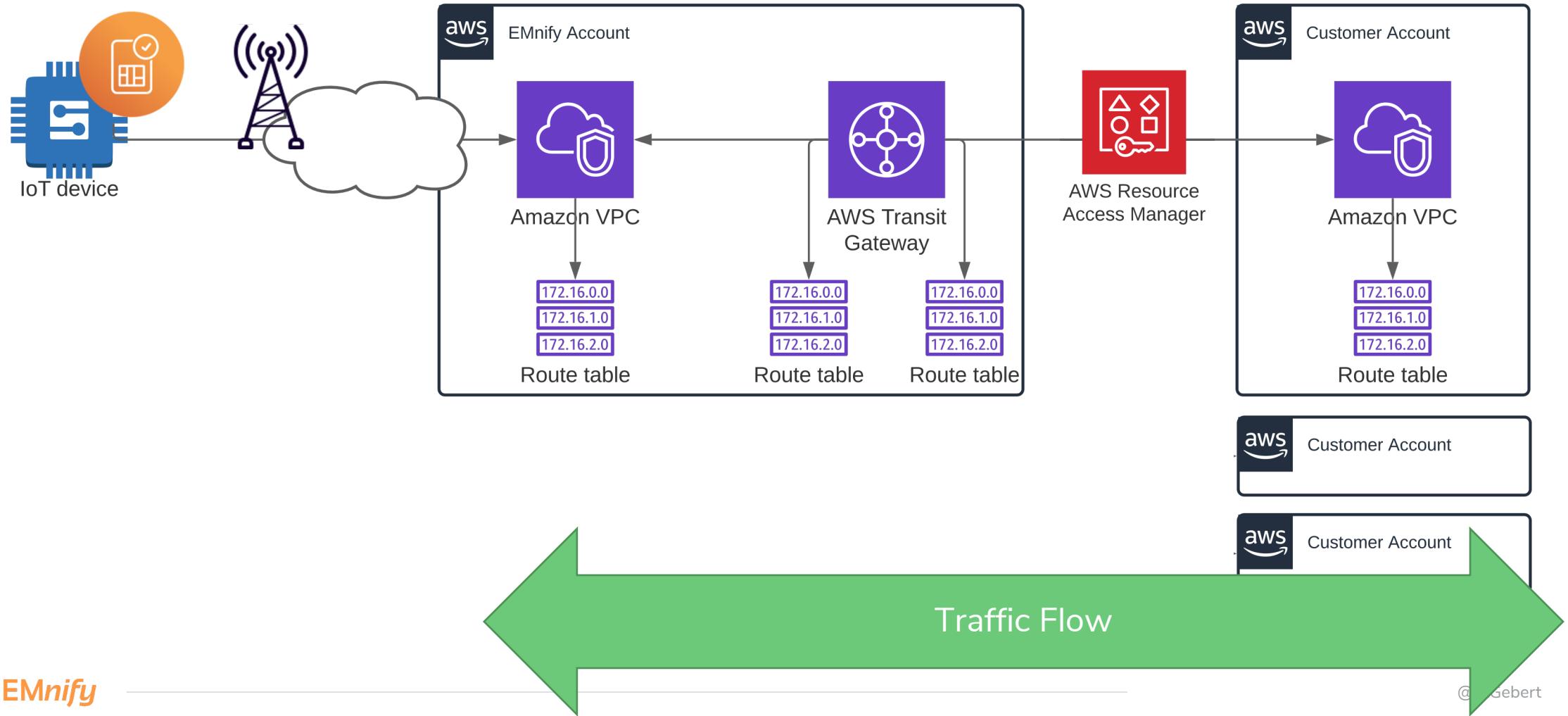
Below the table, the 'Transit Gateway Attachment' details are shown:

Transit Gateway attachment ID	tgw-attach-0a18024e8db2f5e6a	Transit Gateway owner ID	8840 [REDACTED]
Transit Gateway ID	tgw-0cb83ab4d54eb3717	Resource owner account ID	928088150196 (shared)
Resource type	VPC	State	available
Resource ID	vpc-0dba7d2ed75d00f40	Associated route table	tgw-rtb-05d5a86e16d74738f
Association state	associated	DNS support	enable
Subnet IDs	subnet-0fe60b94e6a79405d subnet-040c43a0b4c4a5fd0 subnet-069013afb8a2b0ac5	IPv6 support	disable

# CNC Transit Gateway Setup



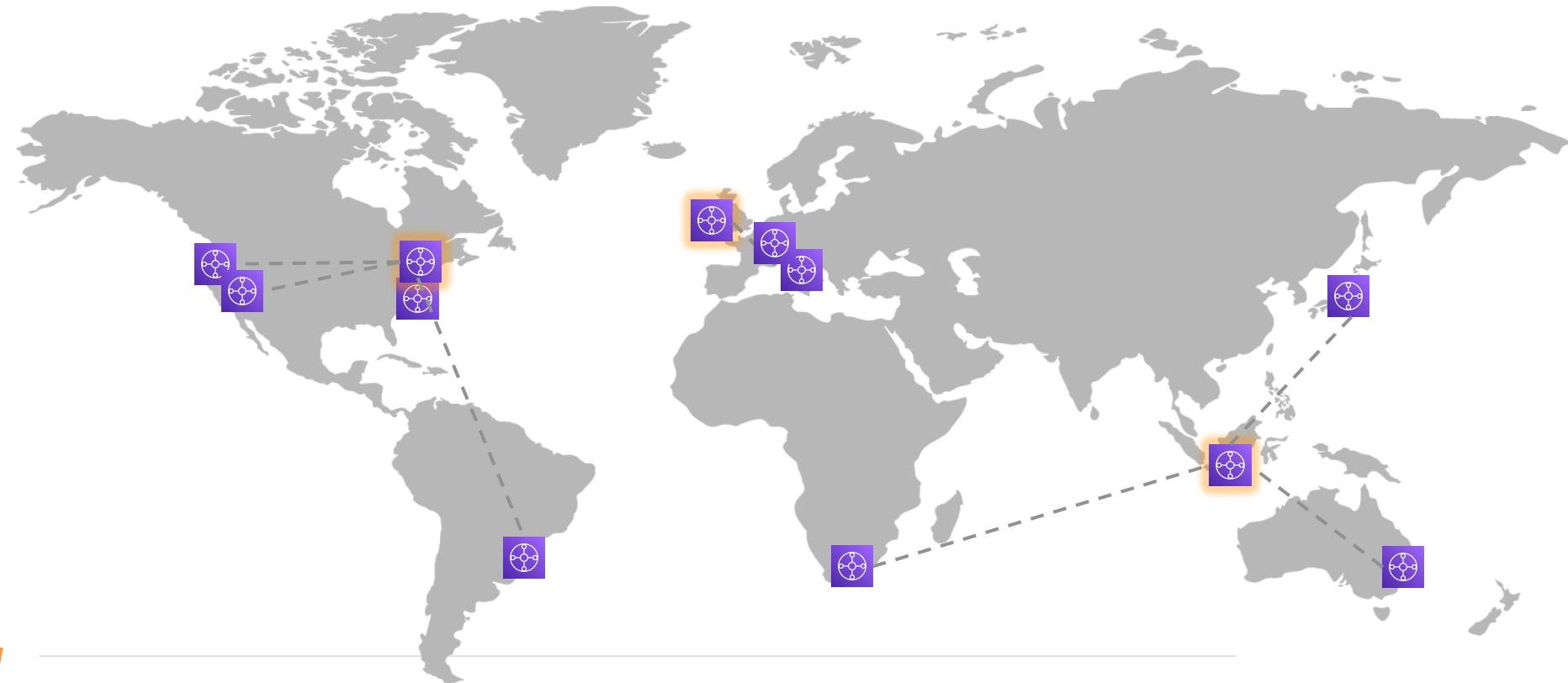
# Data Plane



# TGW Bonus Points

# Cross-Region TGW Peering

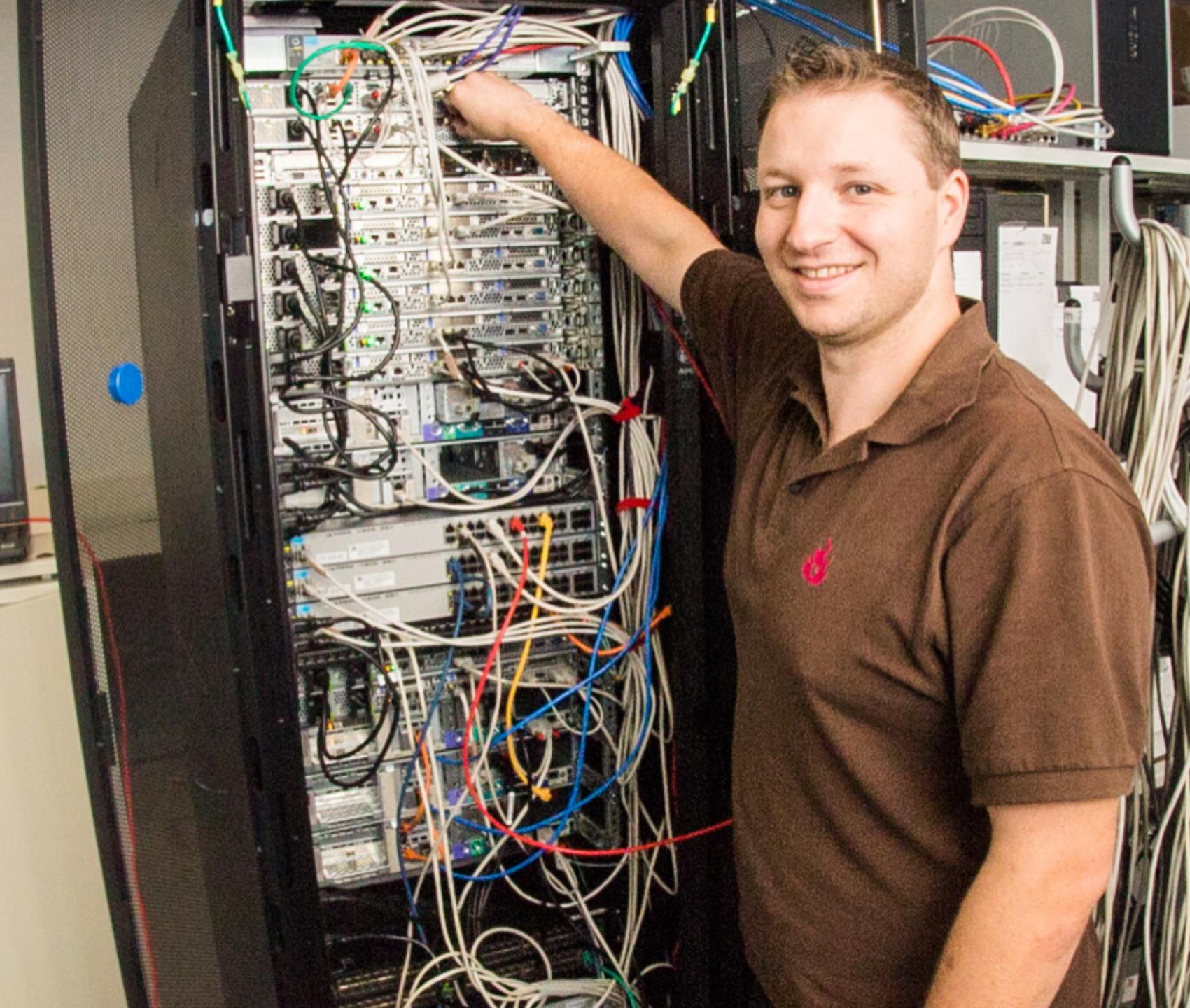
Independence of our core network deployment regions



# IPsec VPN

## ＼(ツ)／

- Replacing custom IPsec setups with managed AWS Site-to-Site VPN
- Advantages
  - API
  - Highly available (BGP)
  - Somebody else fixes it



EMnify

# Demo



Your VPCs | VPC Management

eu-west-1.console.aws.amazon.com/vpc/home?region=eu-west-1#vpcs:

aws Services

EMnify - Steffen Gebert - Test

cdn.emnify.net/#/endpoints

Start Dashboard Endpoints SIMs Service Profiles Tariff Profiles Data Packages Stats Billing Users

Filter Name Enter name... + Create endpoint

ID	Name	ICCID	MSISDN	IP	IMEI	Service Profile	Tariff Profile
8429305	✓ Steffen's Test Phone	8988303000000099589	423663999953772	100.67.212.3	3596780953439431	CNC	Internal Test Tariff
9926741	✓ Test EMNLI-only	898830300000269928	423663910039941	100.67.212.2	3596780953439416	Default SP	Internal Test Tariff
9949752	✓ Test B-only	898830300000614461	423663910233471	100.67.212.4	3557480920471701	Default SP	Generic Tariff Profile
9950563	✓ Test EMNLI-only 2	898830300000614449	423663910233459	100.67.212.5	3557480920471701	Default SP	Generic Tariff Profile
10410312	✓ PJ Test	898830300000495179	423663910152739	100.67.212.1	8625360453326600	Default SP	Internal Test Tariff
10420185	✓ LTE-Stick FritzBox	898830300004858763	423663920199232	100.67.212.6	8601120210368100	Default SP	Generic Tariff Profile
10420530	✓ bq Aquaris X	898830300004858764	423663920199233	100.67.212.7	8638930403739607	Default SP	Internal Test Tariff
10420572	✓ iPhone	898830300004858765	423663920199234	100.67.212.8	3548260961935638	Default SP	Generic Tariff Profile
10424551	✓ LTE-Stick, well not	898830300004858766	423663920199235	100.67.212.9	3586250832547836	Default SP	Generic Tariff Profile

Support

Pixel 3a

	State
5d00f40	✓ Available

15:23

Fri, Nov 13

98% • Charging rapidly (4 min until full)

EMnify

# Control Plane



# | Enabling Self-Service

- Customer portal / REST API

### Create Attachment

1 Select Type — 2 Enter Details — 3 Review — 4 Setup Started

**\* Name**

**\* Region**

us-east-1
▼

**\* AWS Account ID**

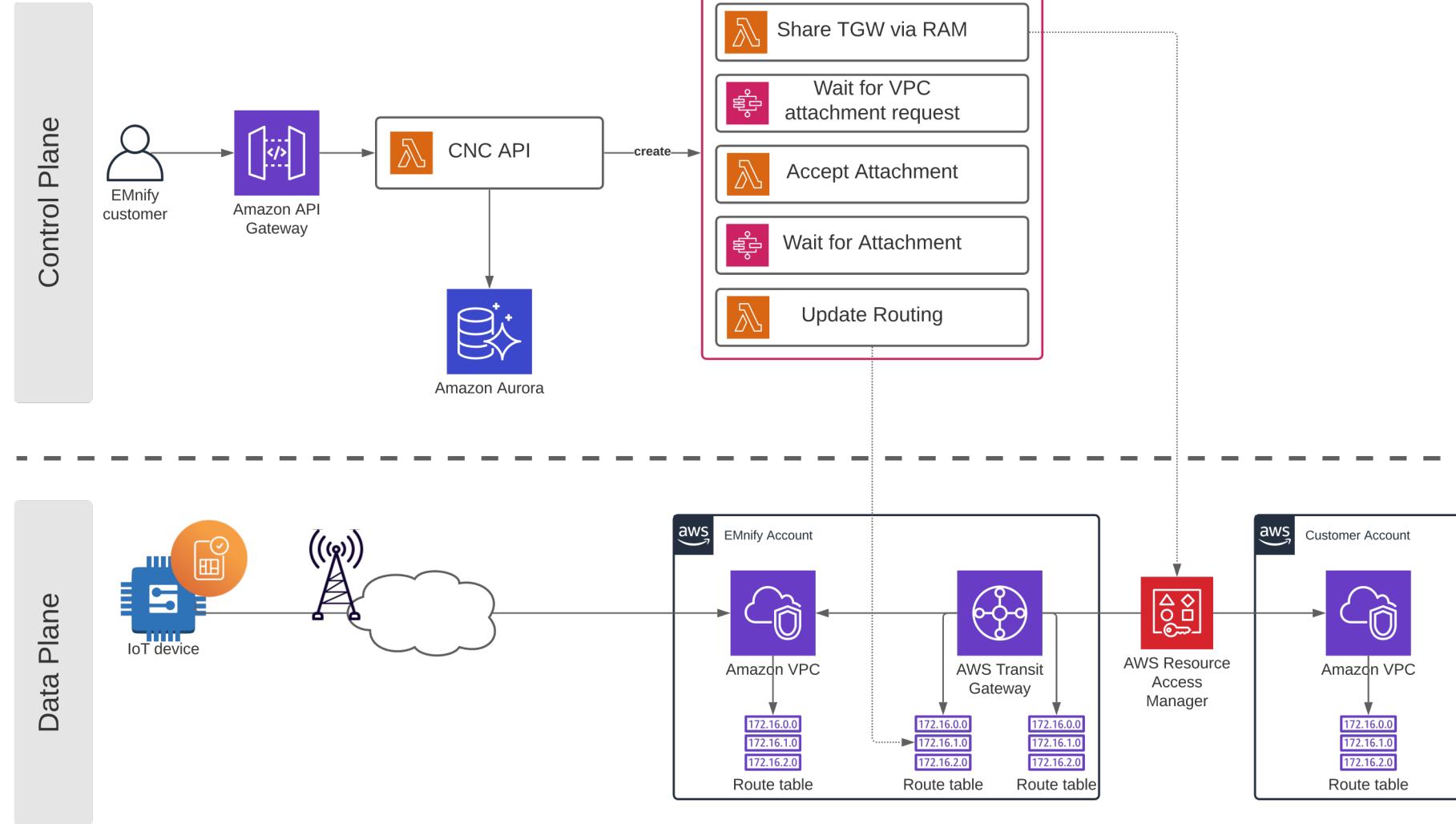
**\* Customer backend CIDRs**

**Description**

Previous Next

TransitGateway	
	Active
<b>Name</b>	[REDACTED]
<b>Description</b>	[REDACTED]
<b>Created At</b>	2020-02-03T08:13:28Z
<b>Region</b>	eu-west-1
<hr/>	
▼ Attachment Infos	
<b>Customer backend CIDR</b>	?
10. [REDACTED] /22	
10. [REDACTED] 0/22	
<hr/>	
<input type="button" value="Delete"/>	Delete

# Orchestration Layer



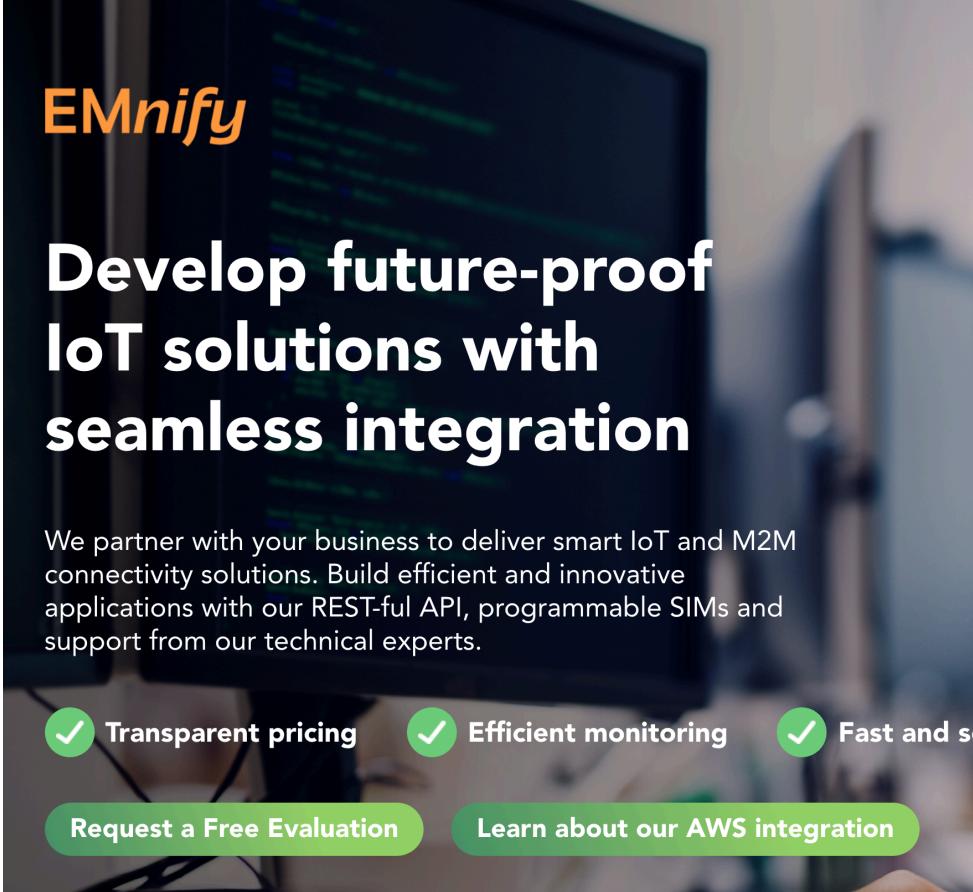
# I Conclusion

- More and more serverless network functions in AWS
- New use cases possible “the serverless way” through TGW
  - Data path taken care of by AWS
  - Control plane accessible via APIs
- EMnify’s Connectivity Platform for the IoT
  - Cloud Native Connectivity implementation using TGW
  - Fully serverless data plane and control plane
  - Shorter delivery time, better stability

EMnify

# Need a Lockdown Project?

Go to [emnify.com/devs](https://emnify.com/devs)



**EMnify**

**Develop future-proof  
IoT solutions with  
seamless integration**

We partner with your business to deliver smart IoT and M2M connectivity solutions. Build efficient and innovative applications with our RESTful API, programmable SIMs and support from our technical experts.

 Transparent pricing    Efficient monitoring    Fast and secure

[Request a Free Evaluation](#)   [Learn about our AWS integration](#)



Advanced  
Technology  
Partner

IoT Competency

