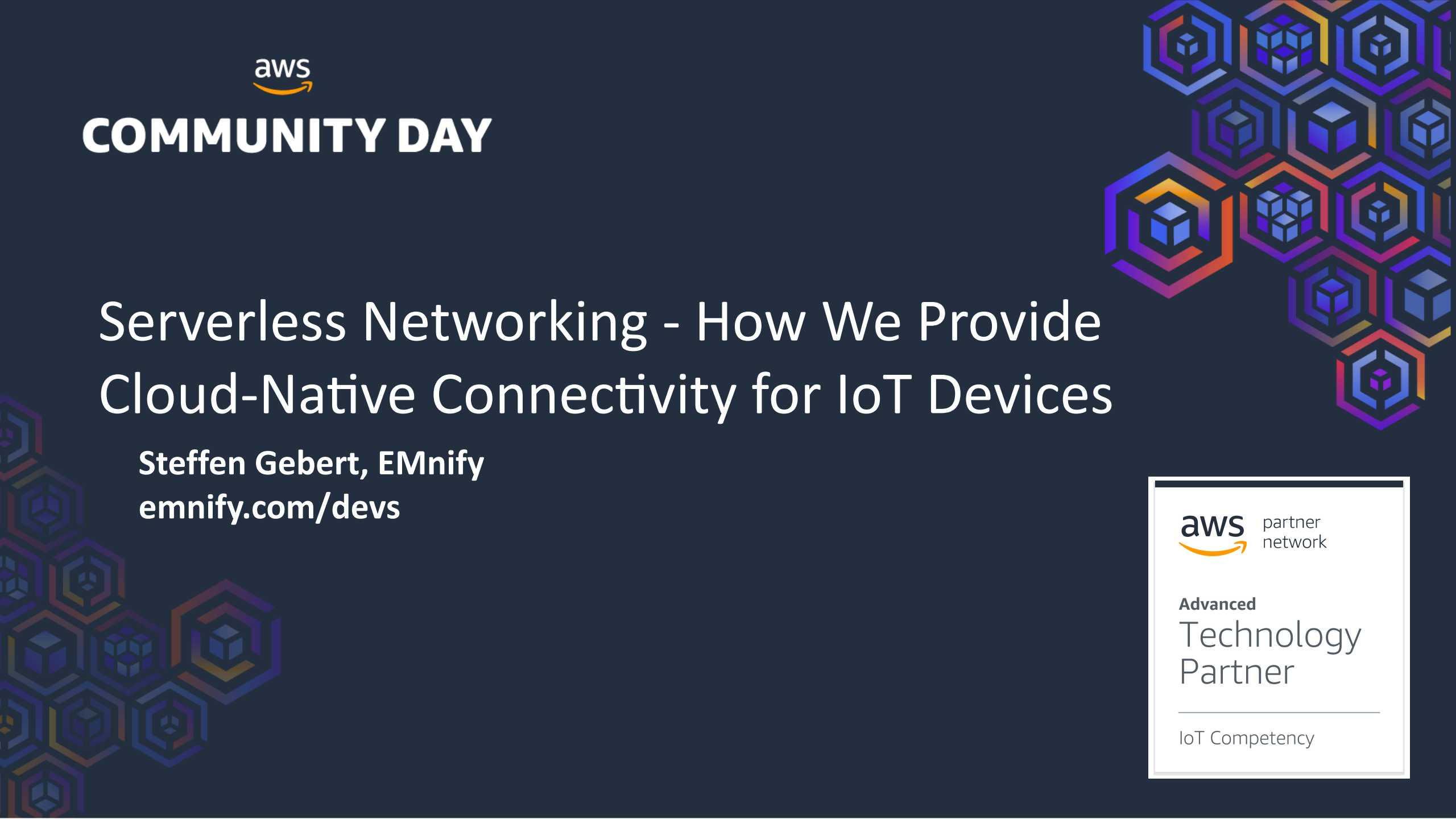
aws

COMMUNITY DAY

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

Steffen Gebert, EMnify
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 in 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.

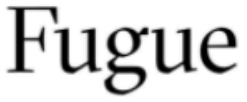
Overall, serverless networking and serverless orchestration allowed us at EMnify to build our new Cloud-Native Connectivity features not only within short time, but with nearly no long-term maintenance efforts.

Thanks to Our Sponsors!

Platinum Sponsor

Gold Sponsors

Silver Sponsors



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

@StGebert

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

The Network

VPC Peering?

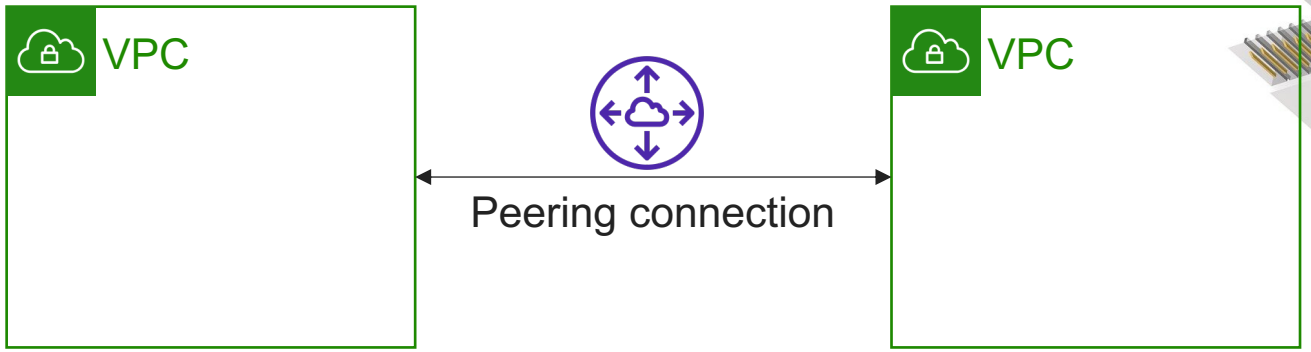
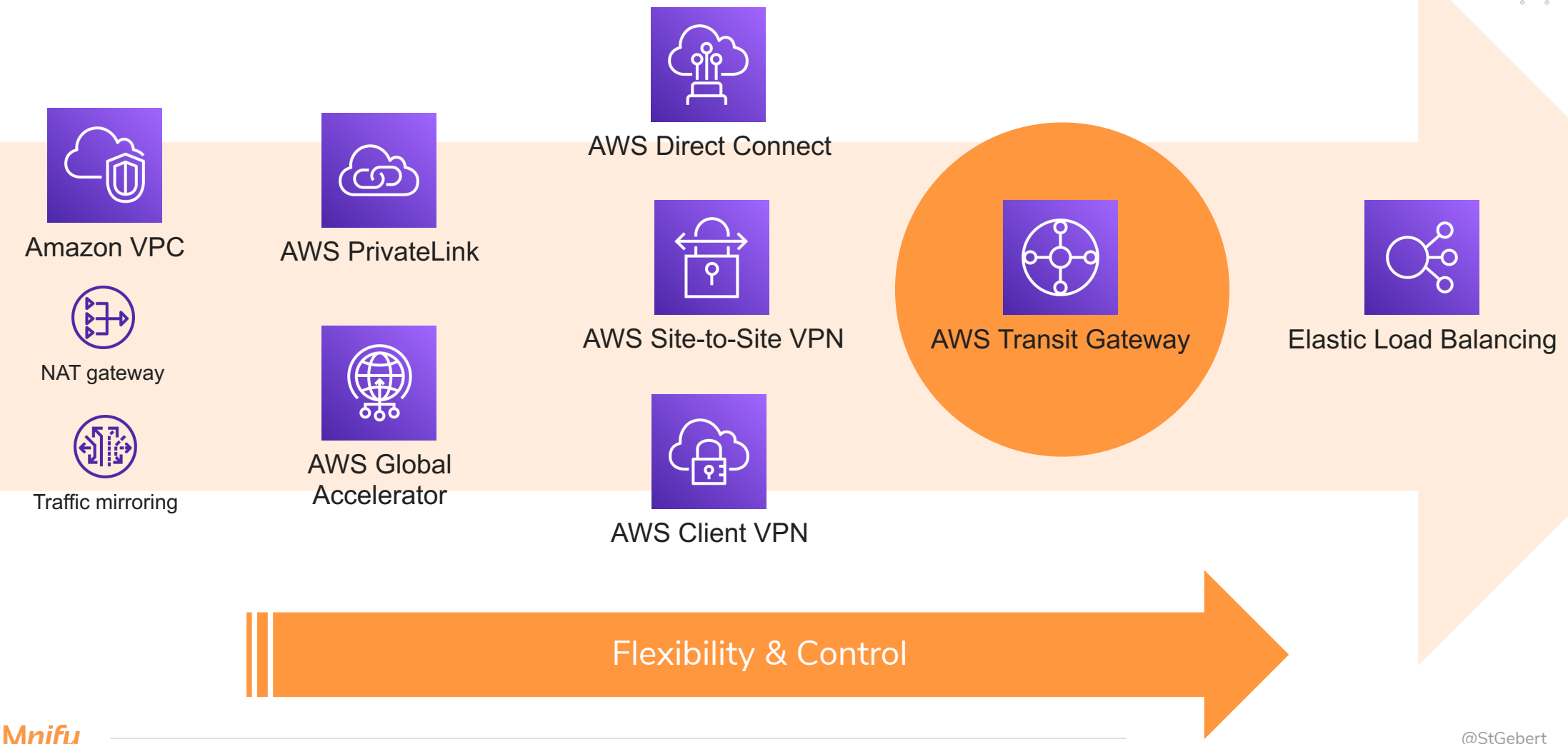


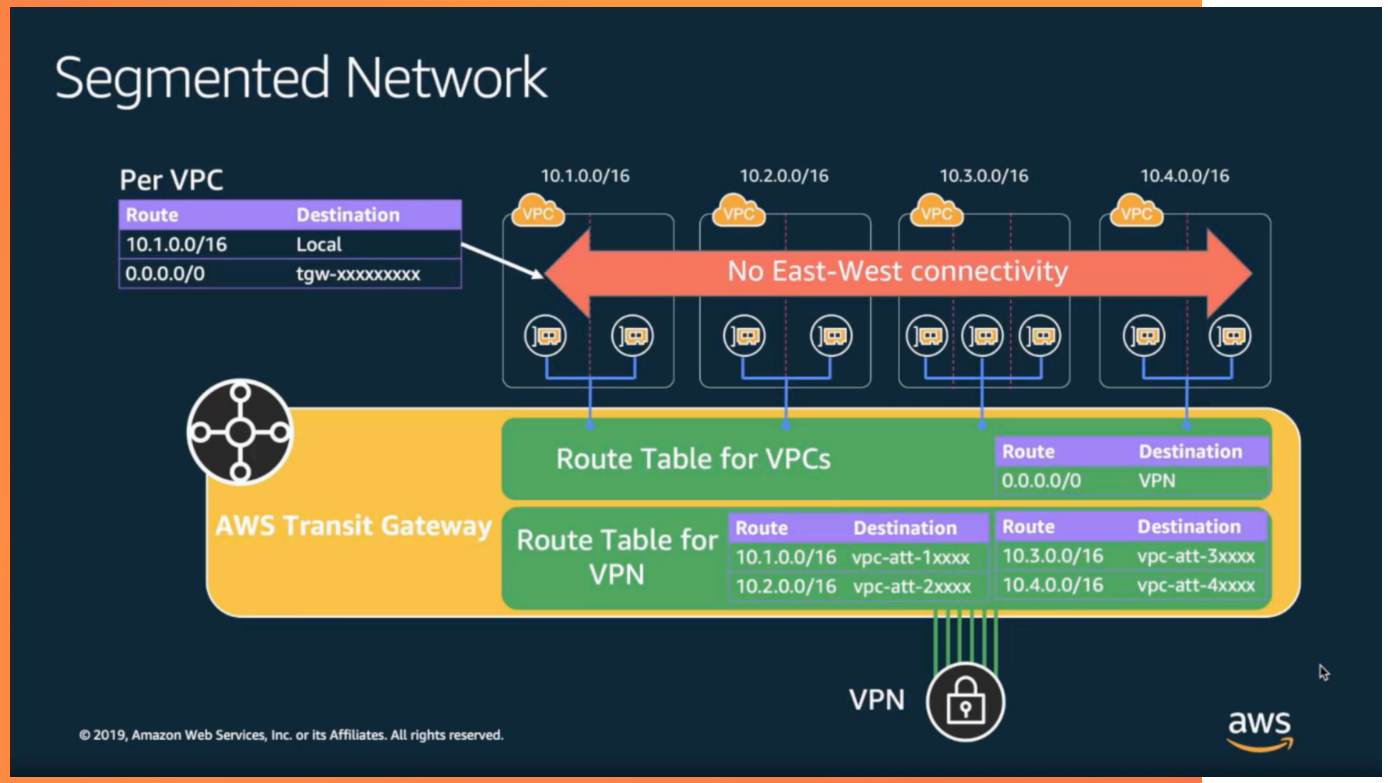
Image Peggy und Marco Lachmann-Anke from Pixabay
https://pixabay.com/users/peggy_marco-1553824

Network Functions

Serverless'y Network Functions



I AWS Transit Gateway



Source: AWS Transit Gateway Reference Architectures for Many Amazon VPCs

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

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

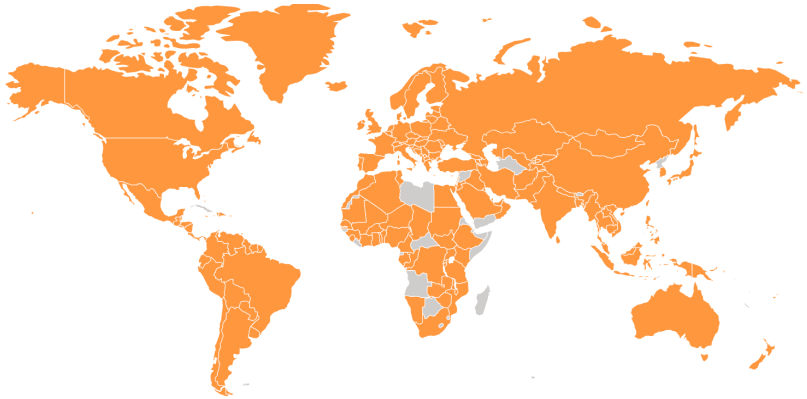
Another fleet of EC2 instances to terminate

STEFFEN

EMnify

Connecting the Internet of Things

Cellular Connectivity Anywhere in the World



movistar · T · airtel · verizon · O2 · vodafone · 中国移动通信 CHINA MOBILE

VimpelCom · Claro · A1 Telekom Austria Group · telenor group · Telia · WIND · 3 · orange

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

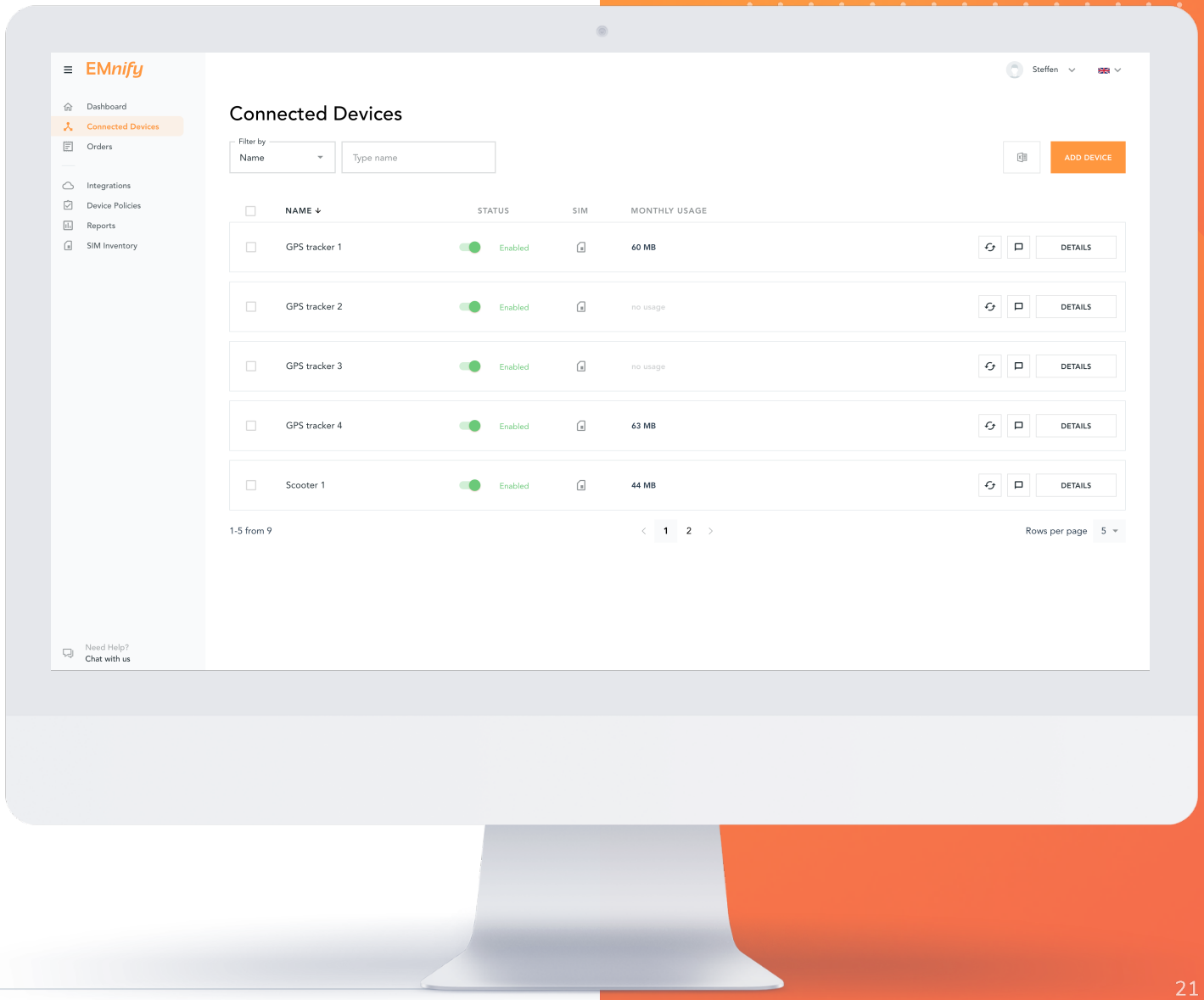
Connectivity Management

Complete Cost & Network Control

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

Real-time Insights

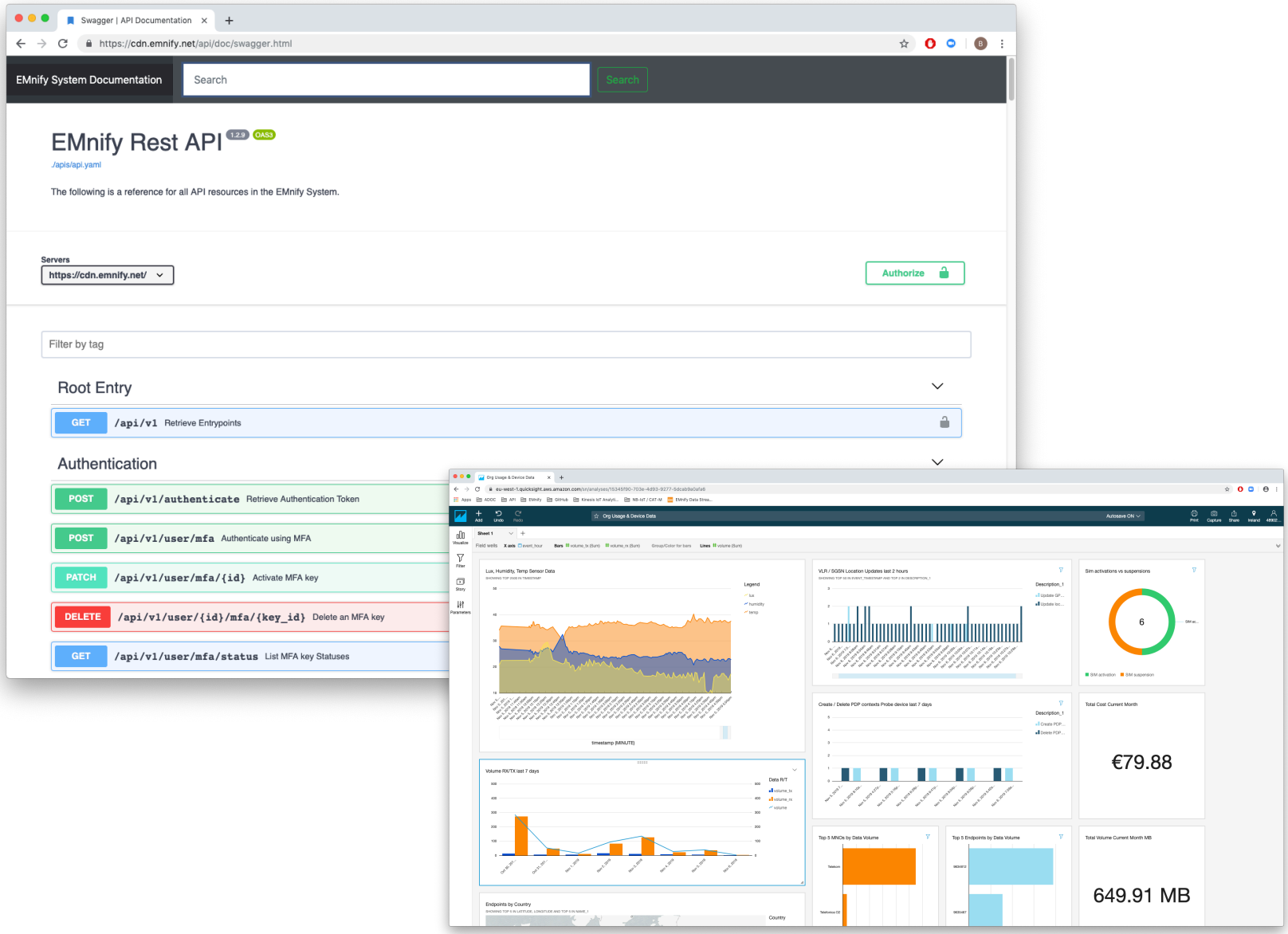
- Visibility and management of networks, devices and connectivity
- Remote Device Access
- Business Reports



Built for Integration

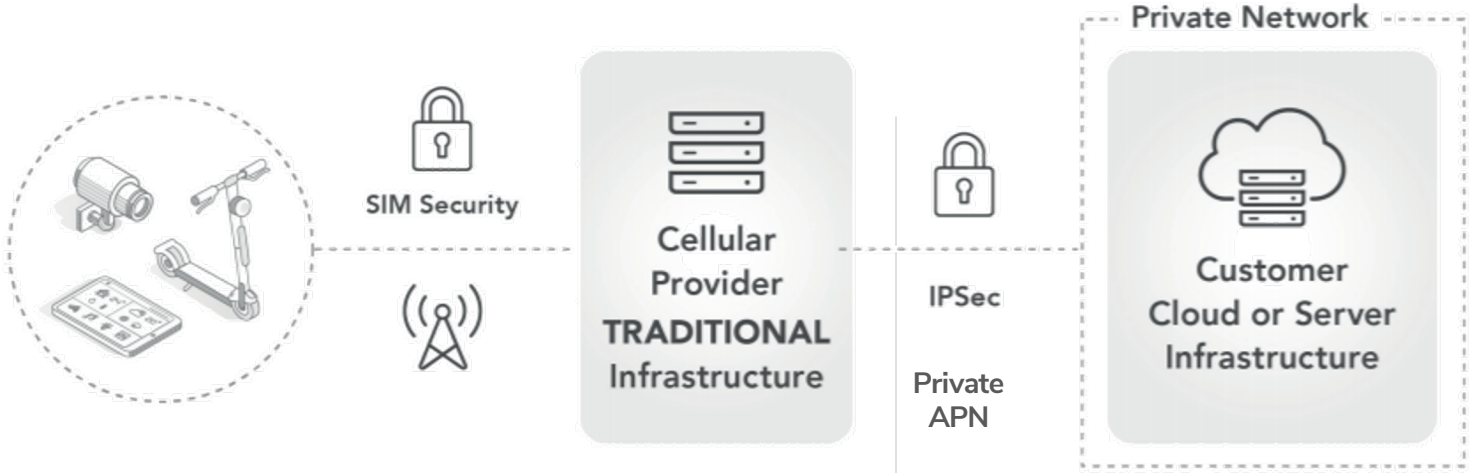
API-First Approach

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



EMnify

Secure Private Network for Cellular IoT



Why required in IoT B2B?

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

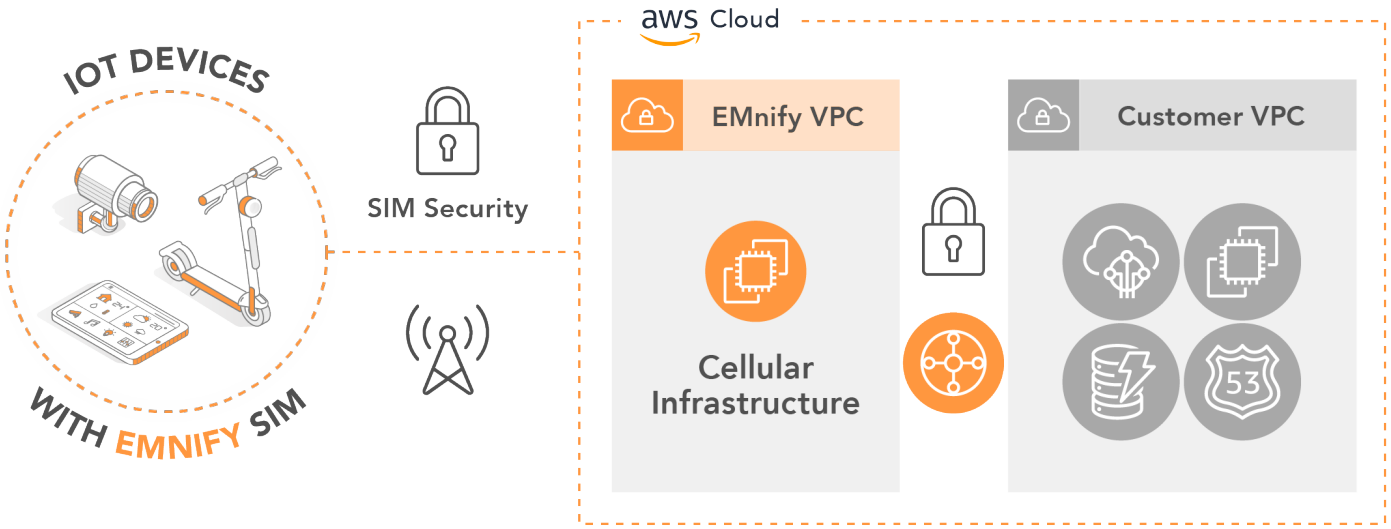
Drawbacks

- 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



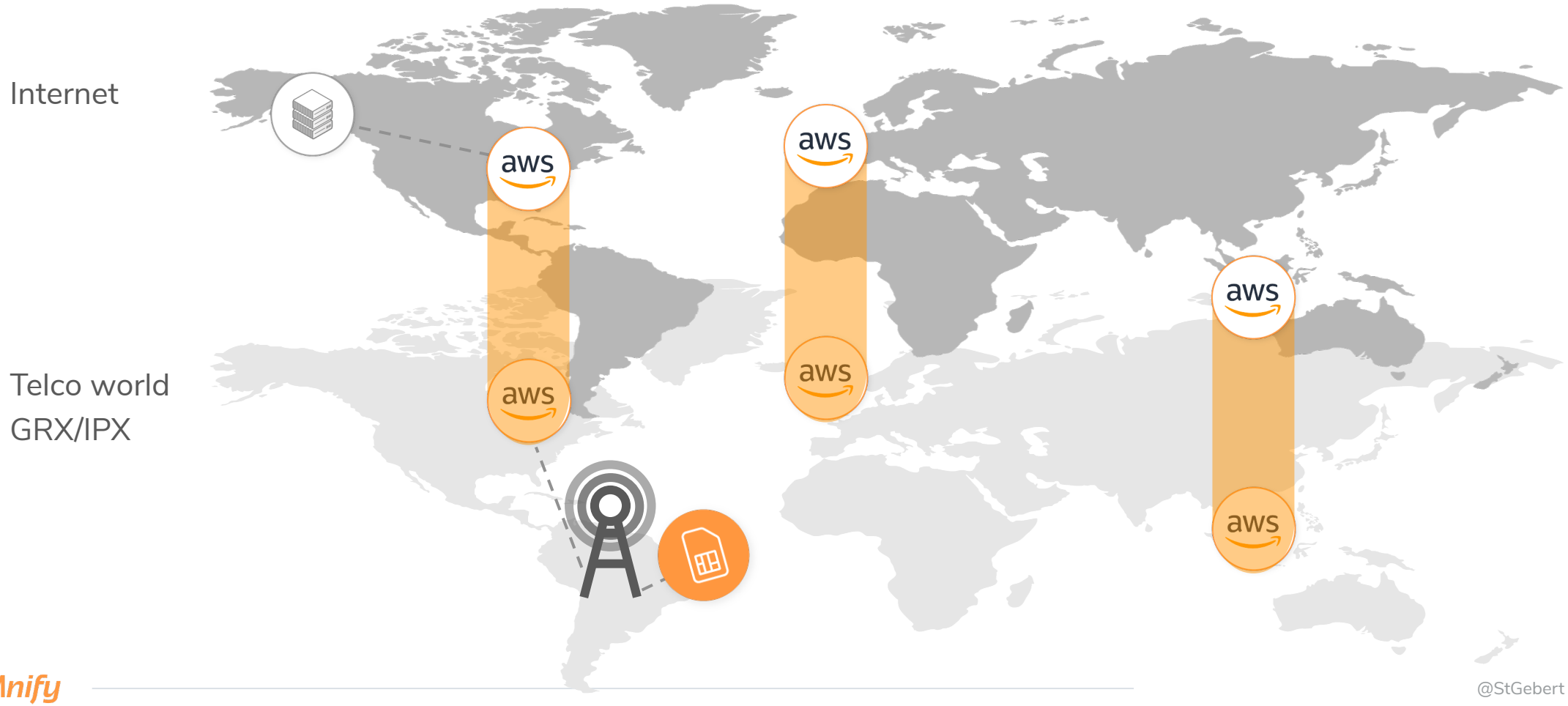
AWS Native Implementation

- 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

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

Limits scale

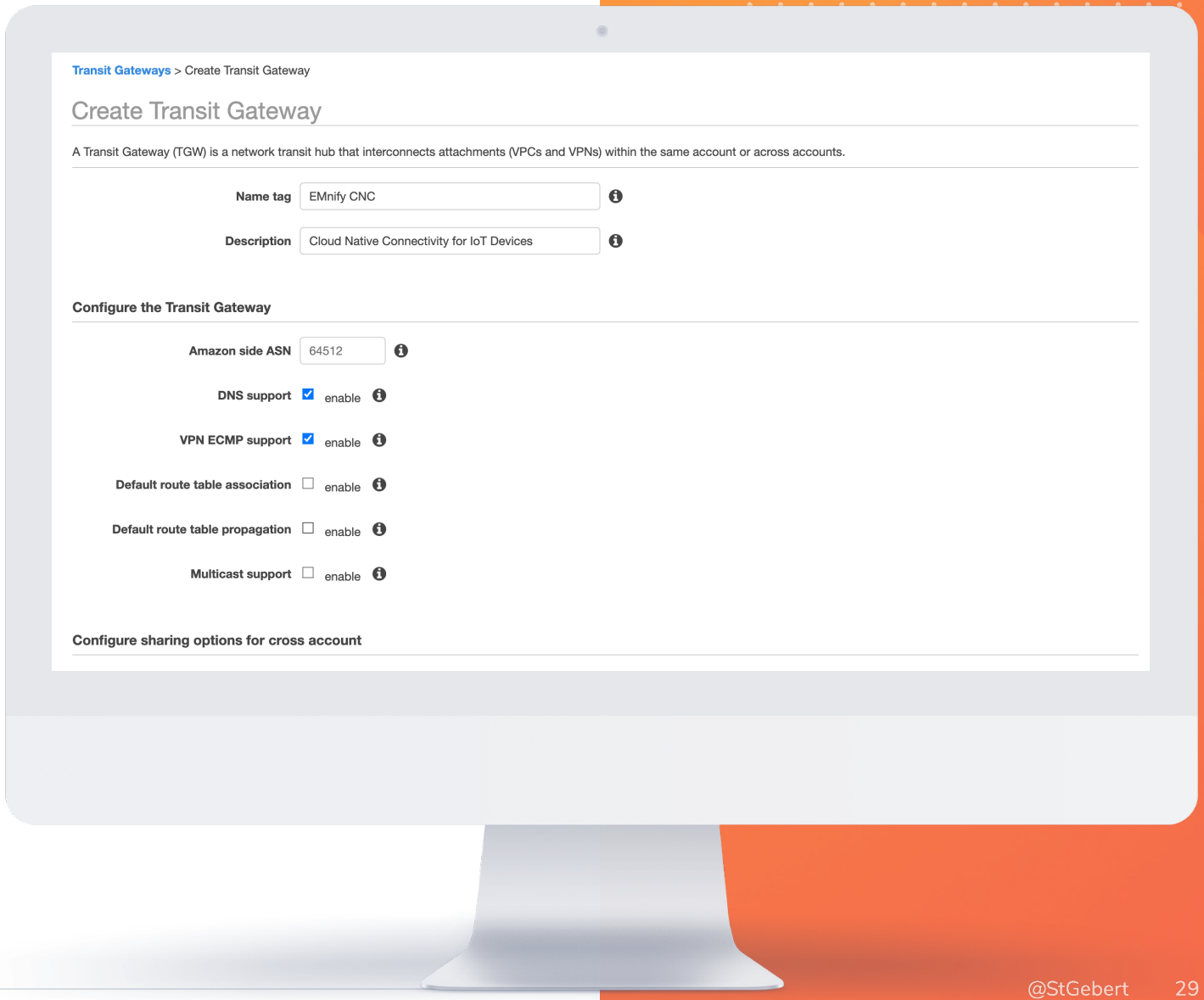
👍

CNC Transit Gateway Setup

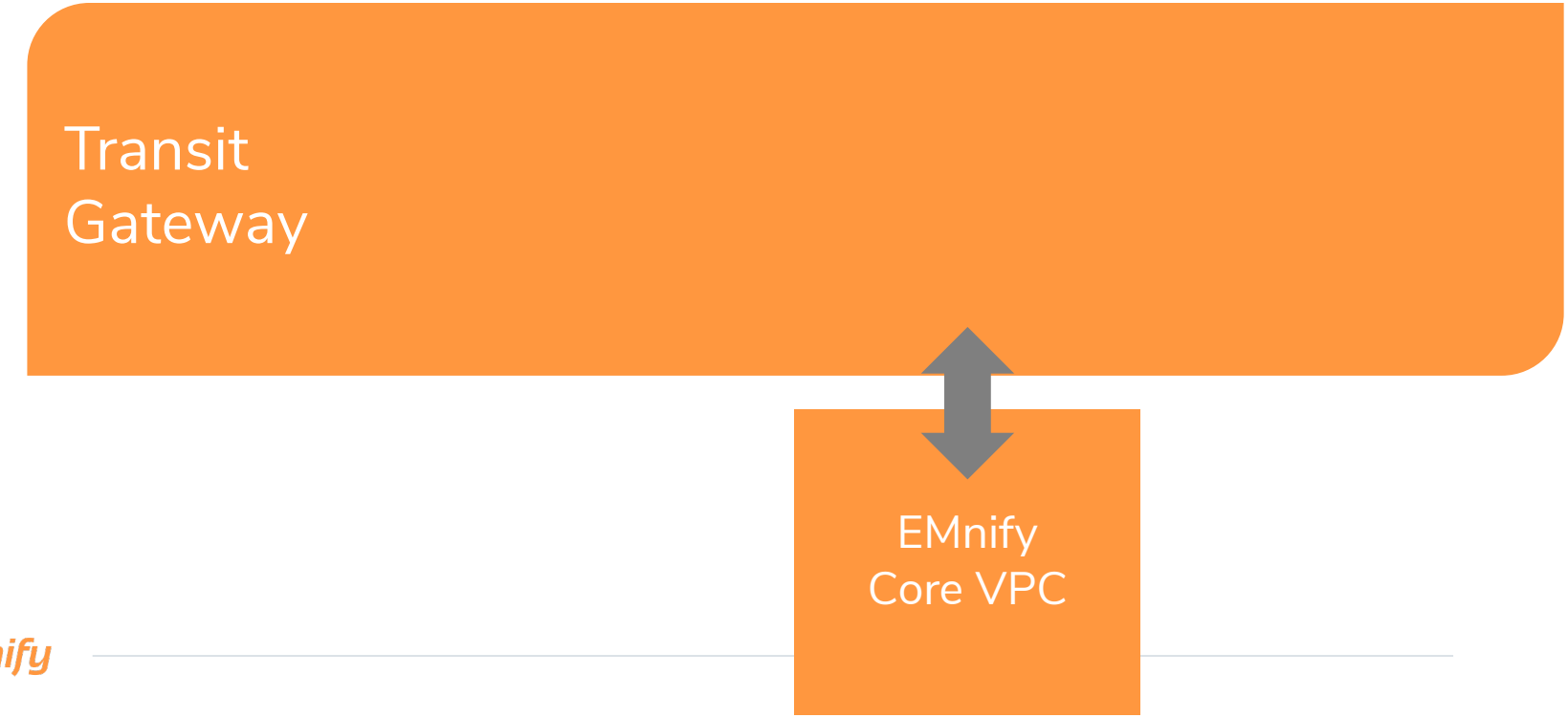
Transit
Gateway

TGW Creation

- Regional resource
- Automatically available in all AZs

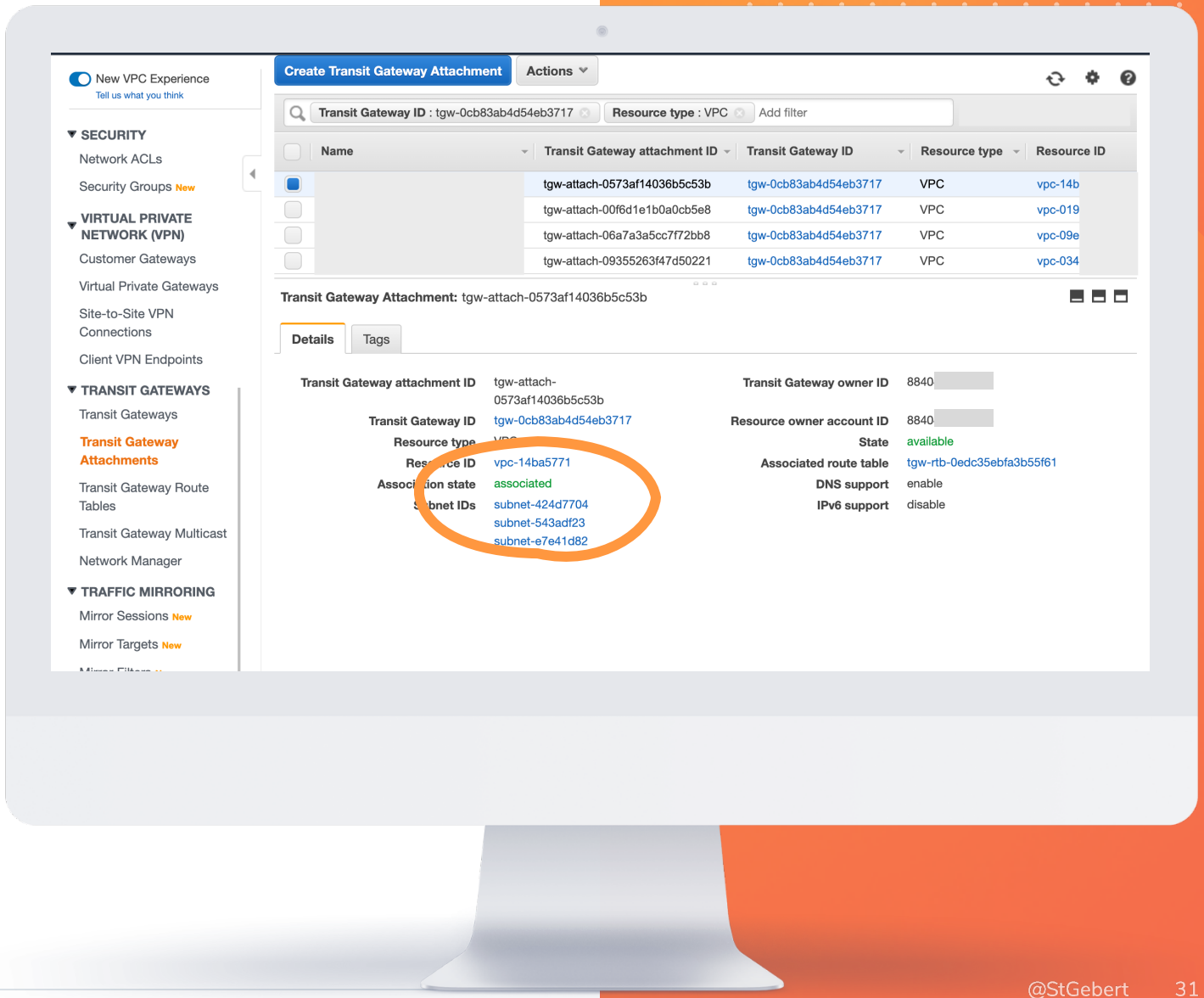


CNC Transit Gateway Setup

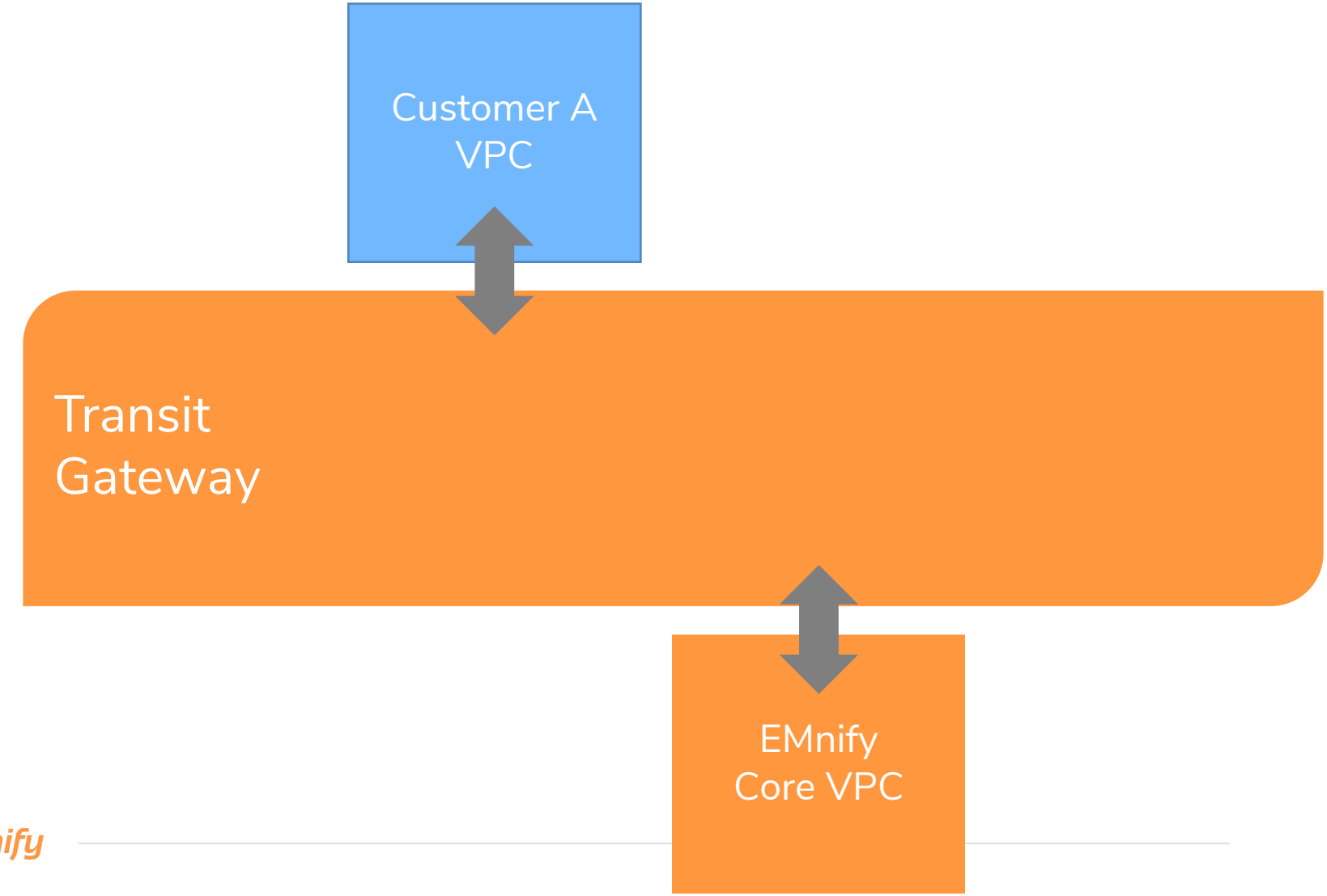


Attachment EMnify Core VPC

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



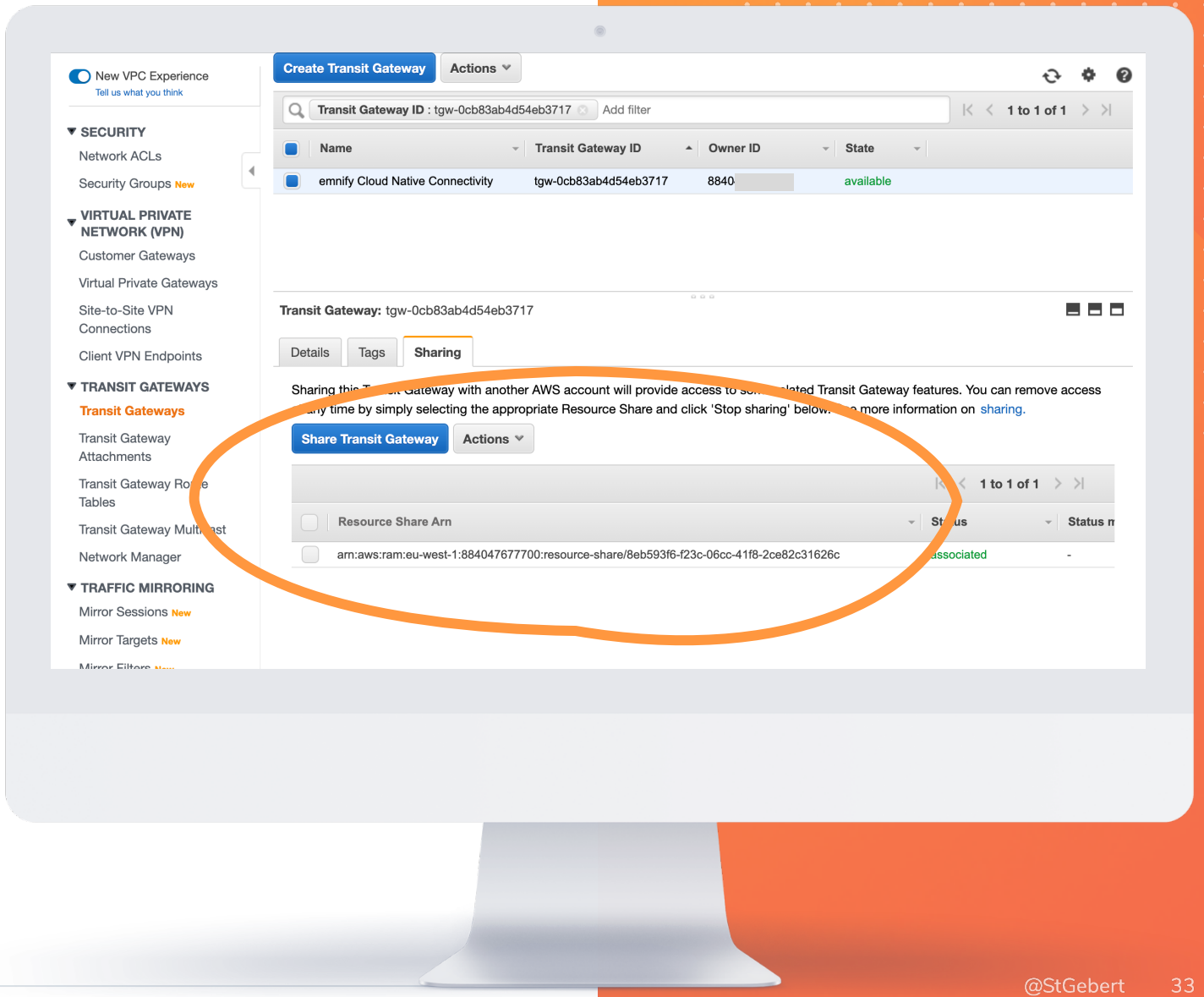
CNC Transit Gateway Setup



Resource Share

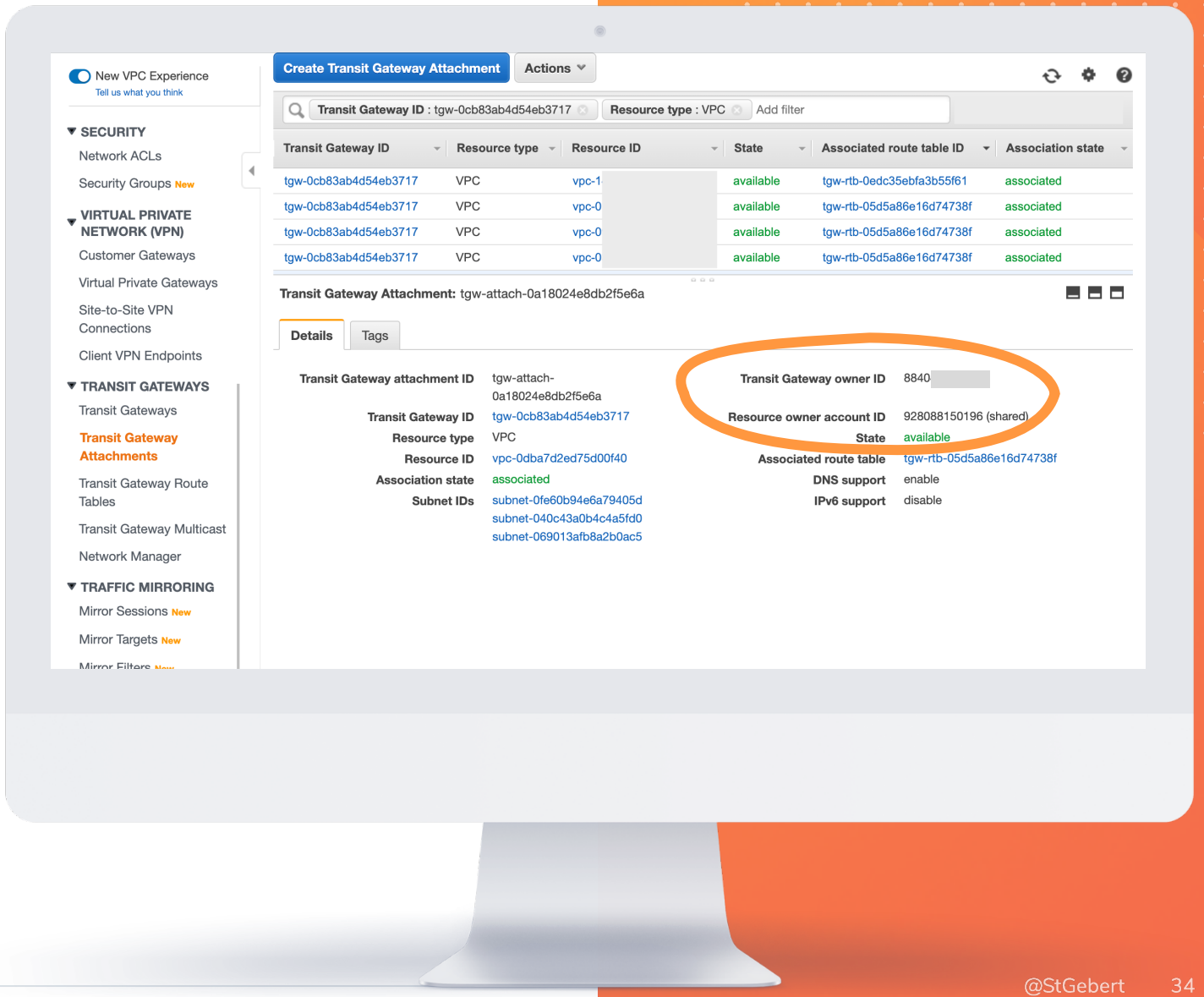
AWS Resource Access Manager

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

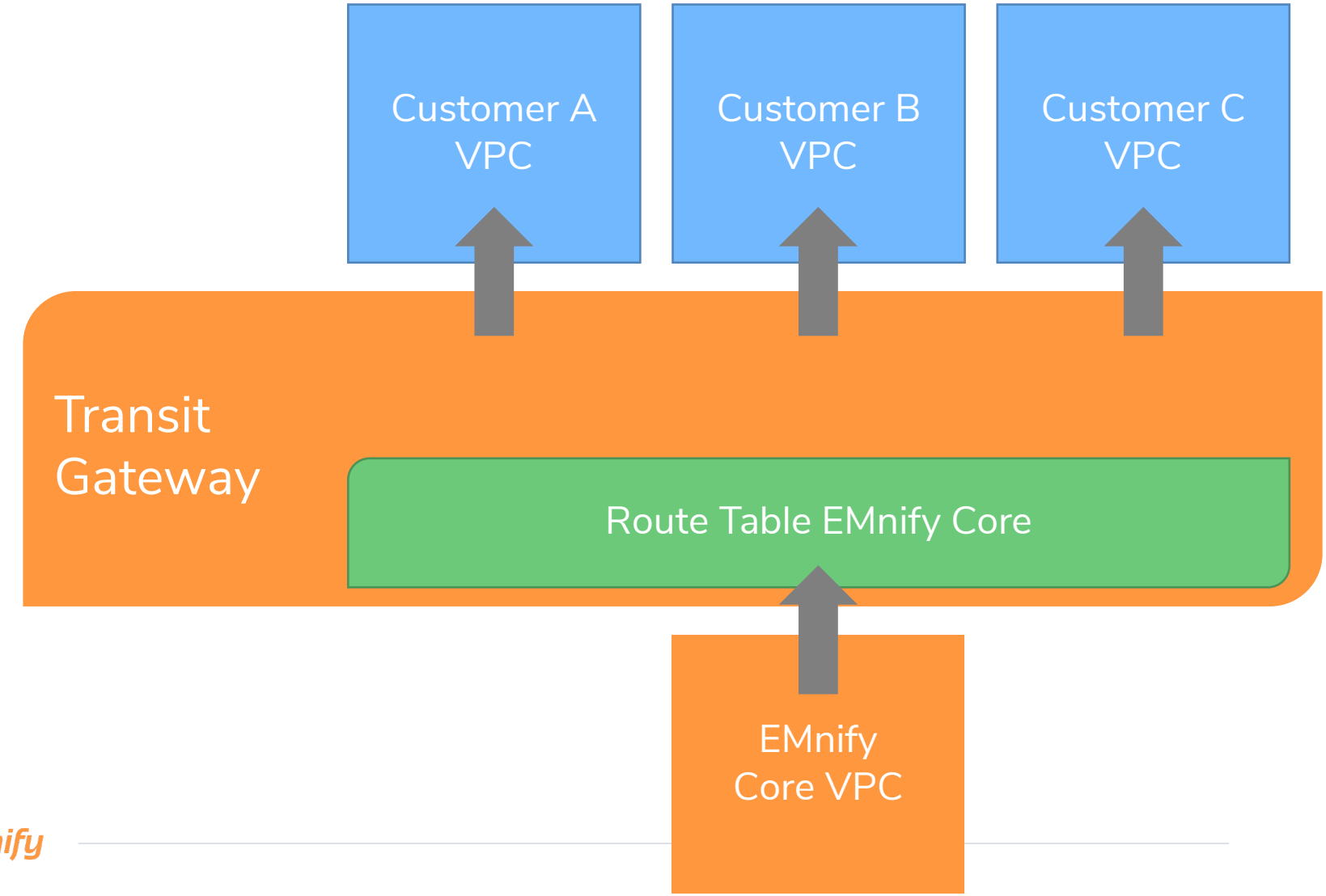


Attachment Customer VPC

- Triggered by customer side

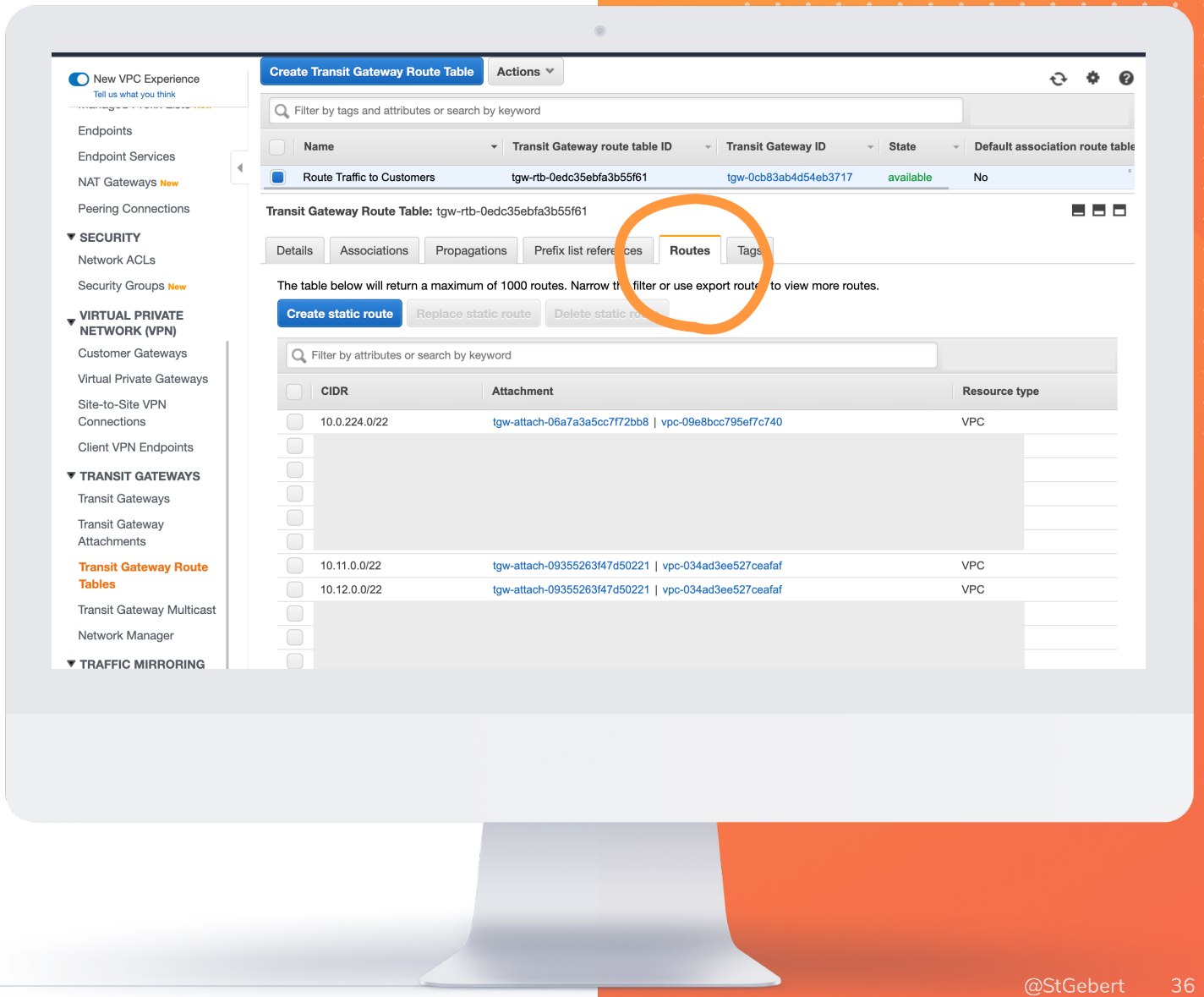


CNC Transit Gateway Setup



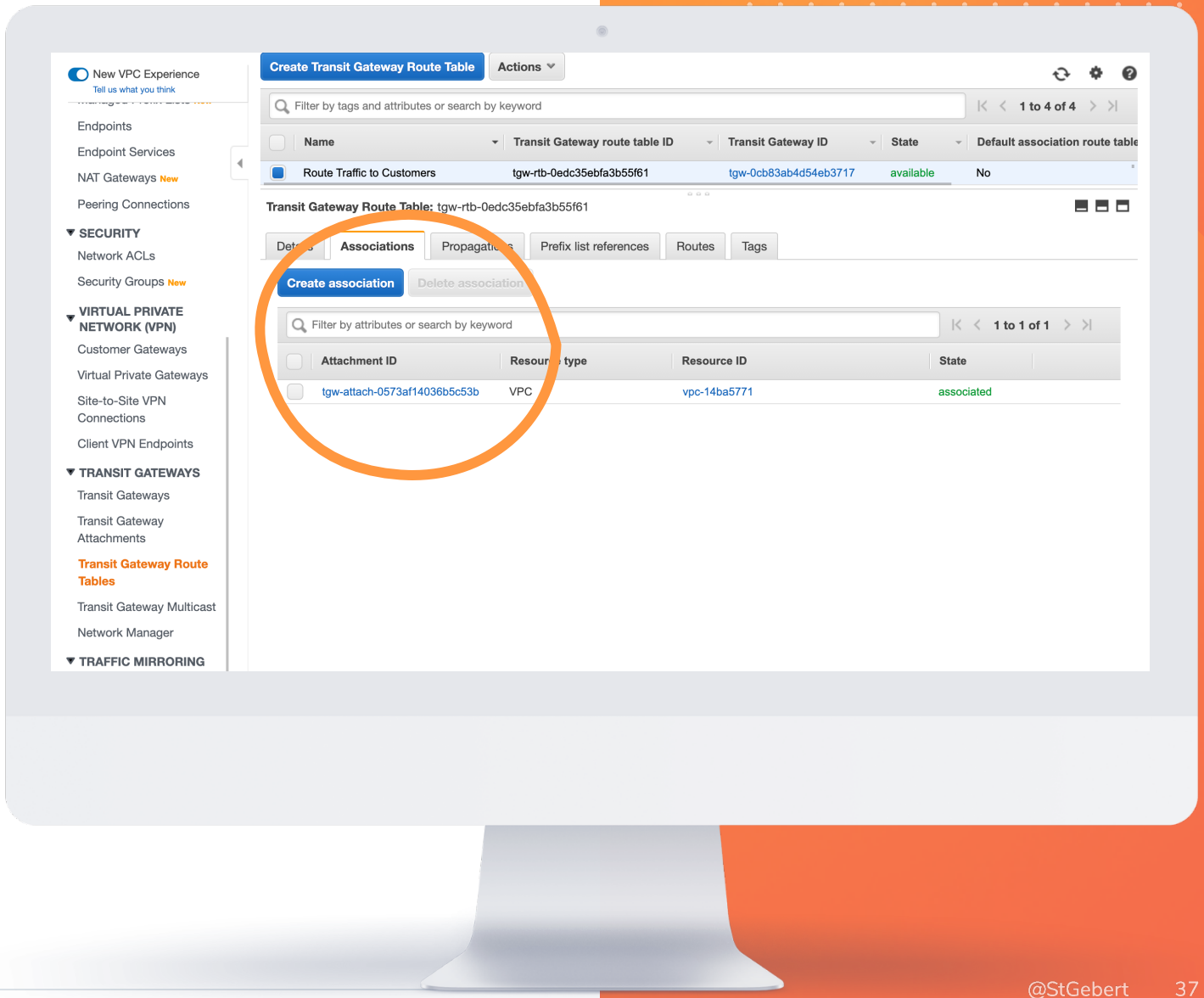
Route Tables

- Static routes to customer VPCs

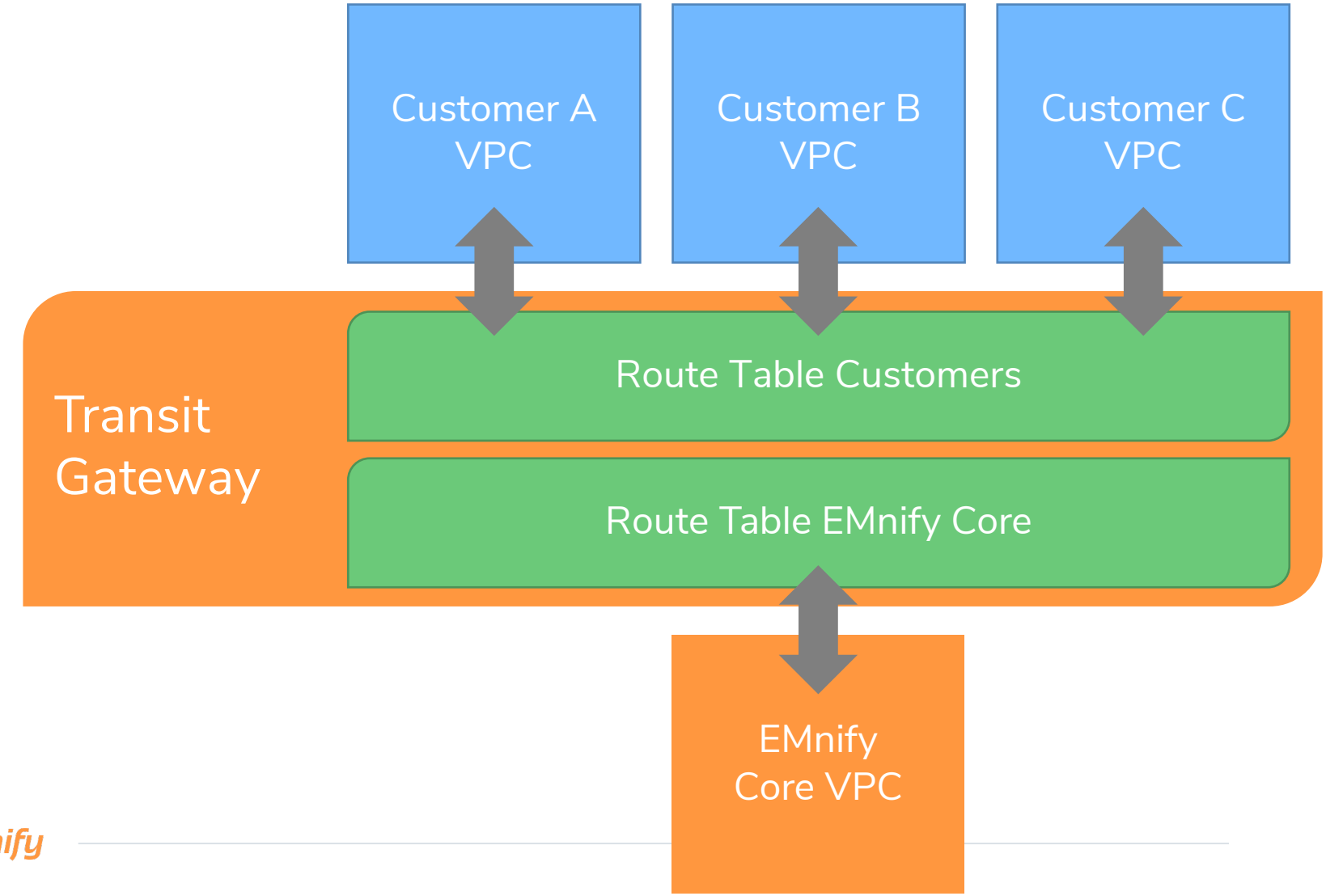


Route Tables

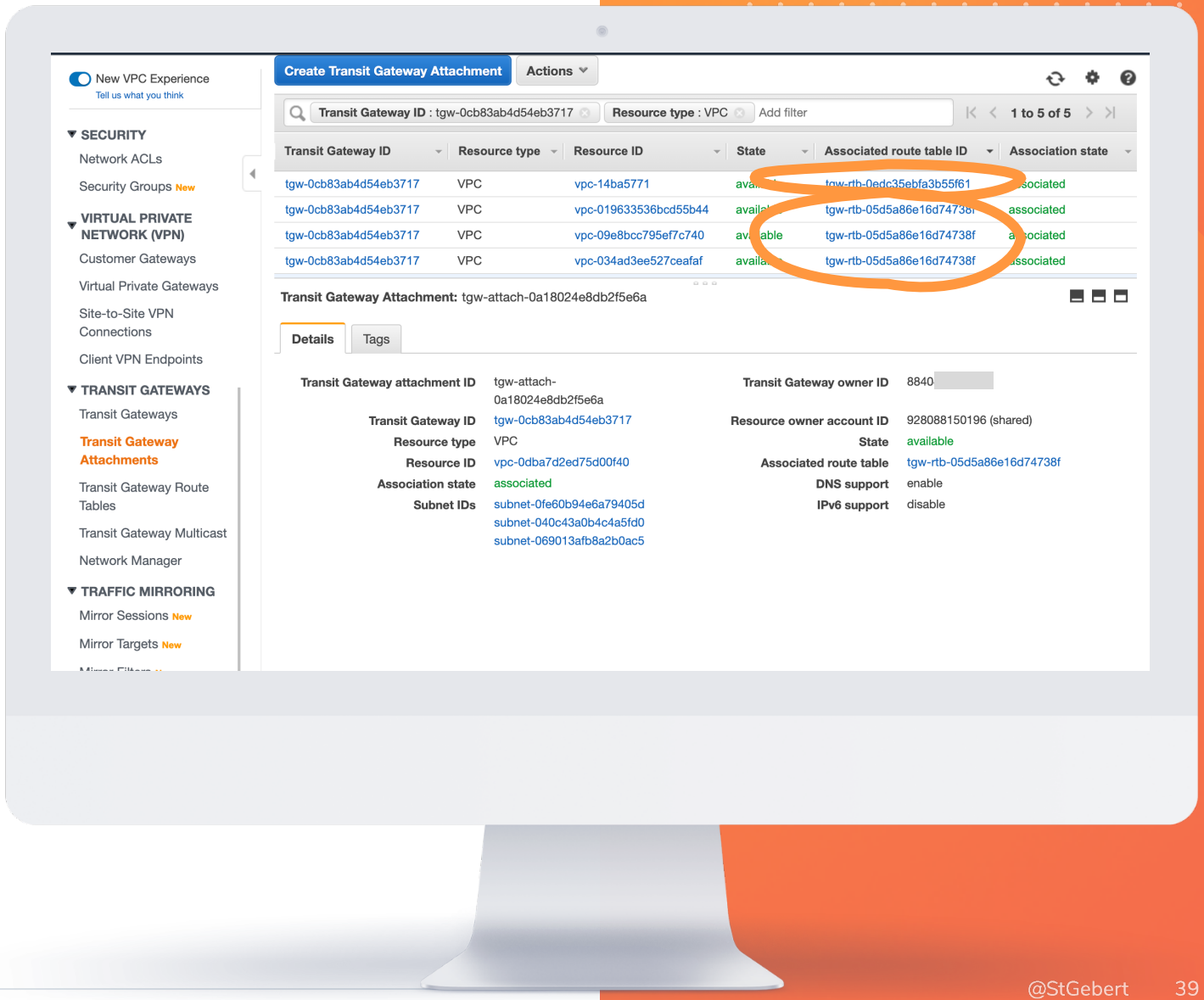
- Associated with our VPC only (egress traffic from our PoV)



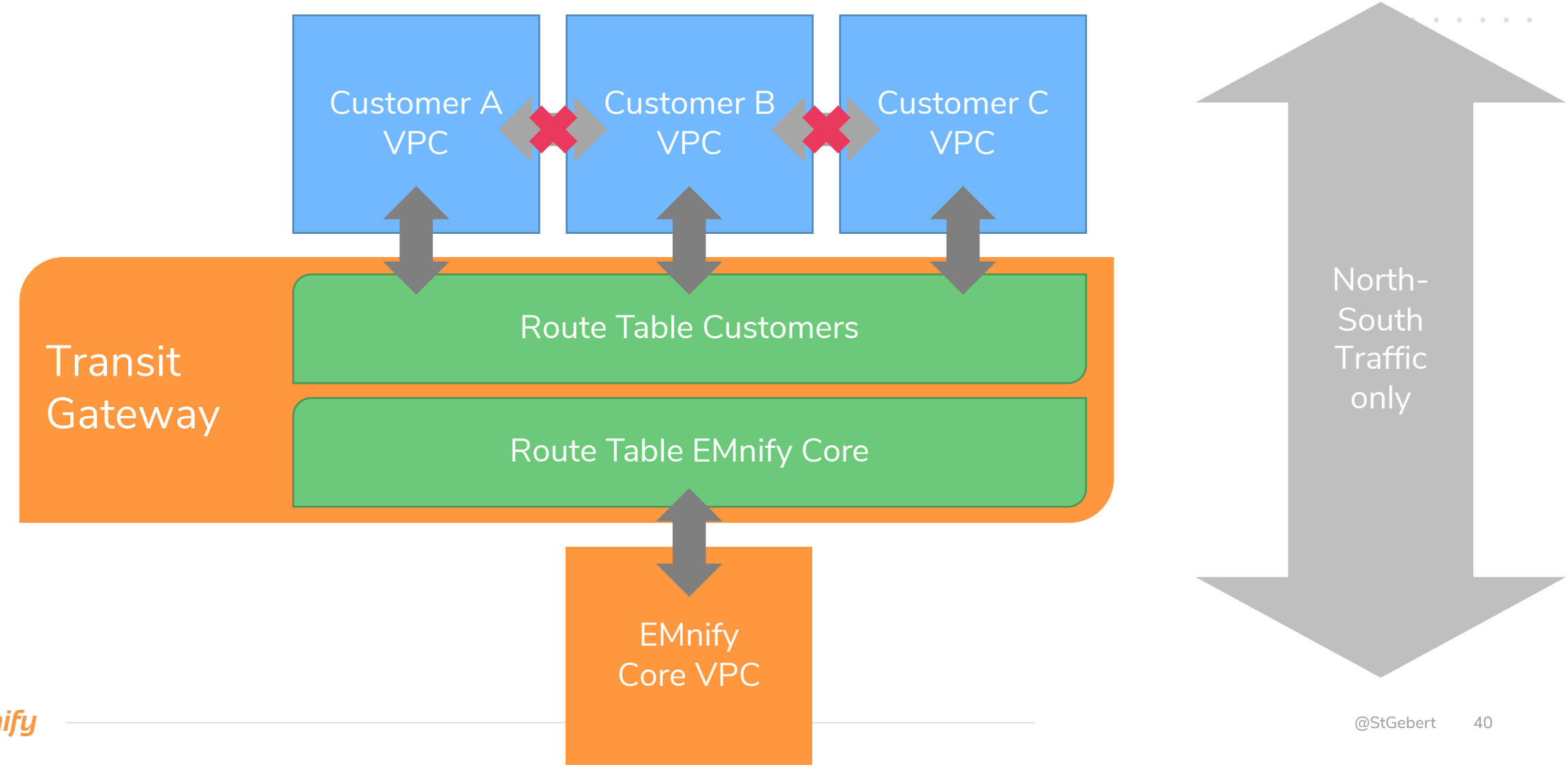
CNC Transit Gateway Setup



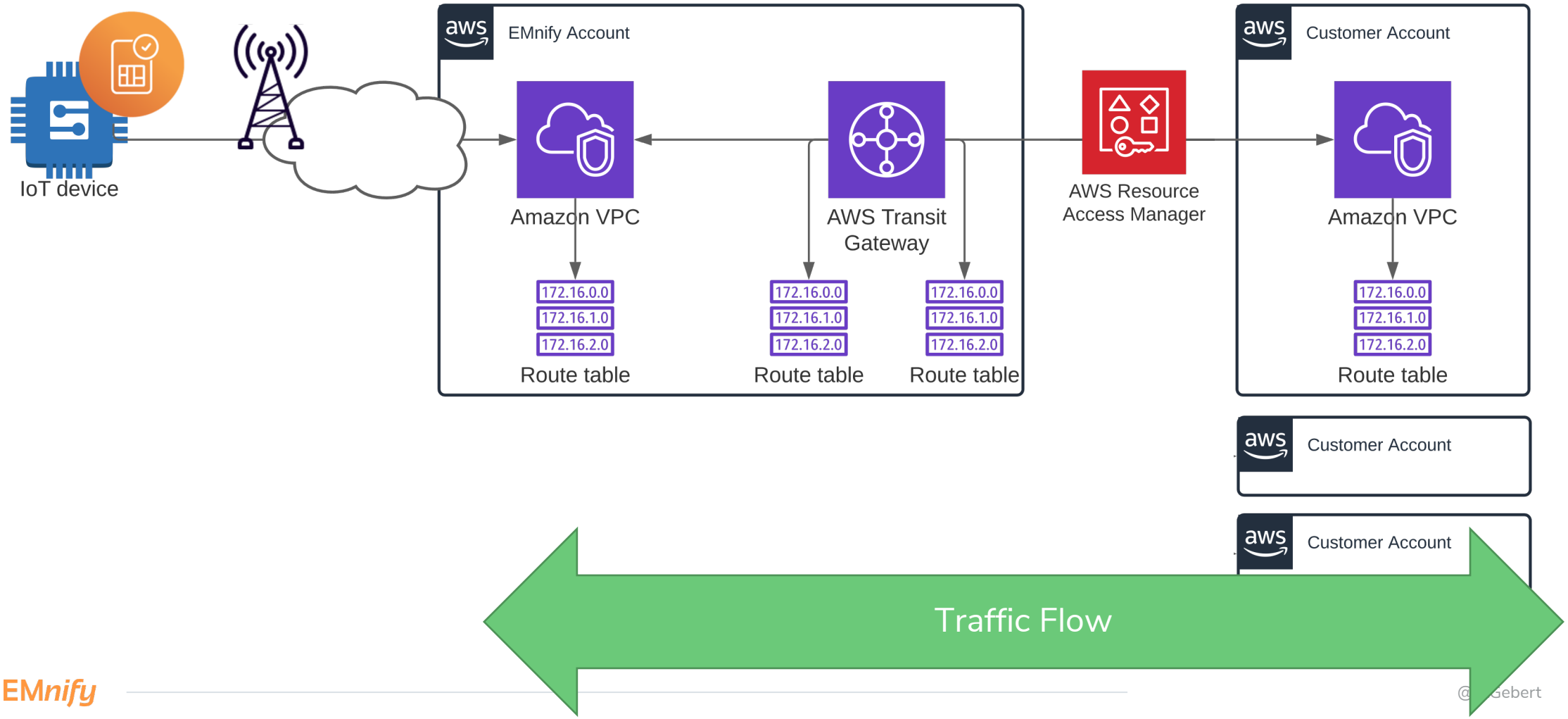
Route Tables



CNC Transit Gateway Setup



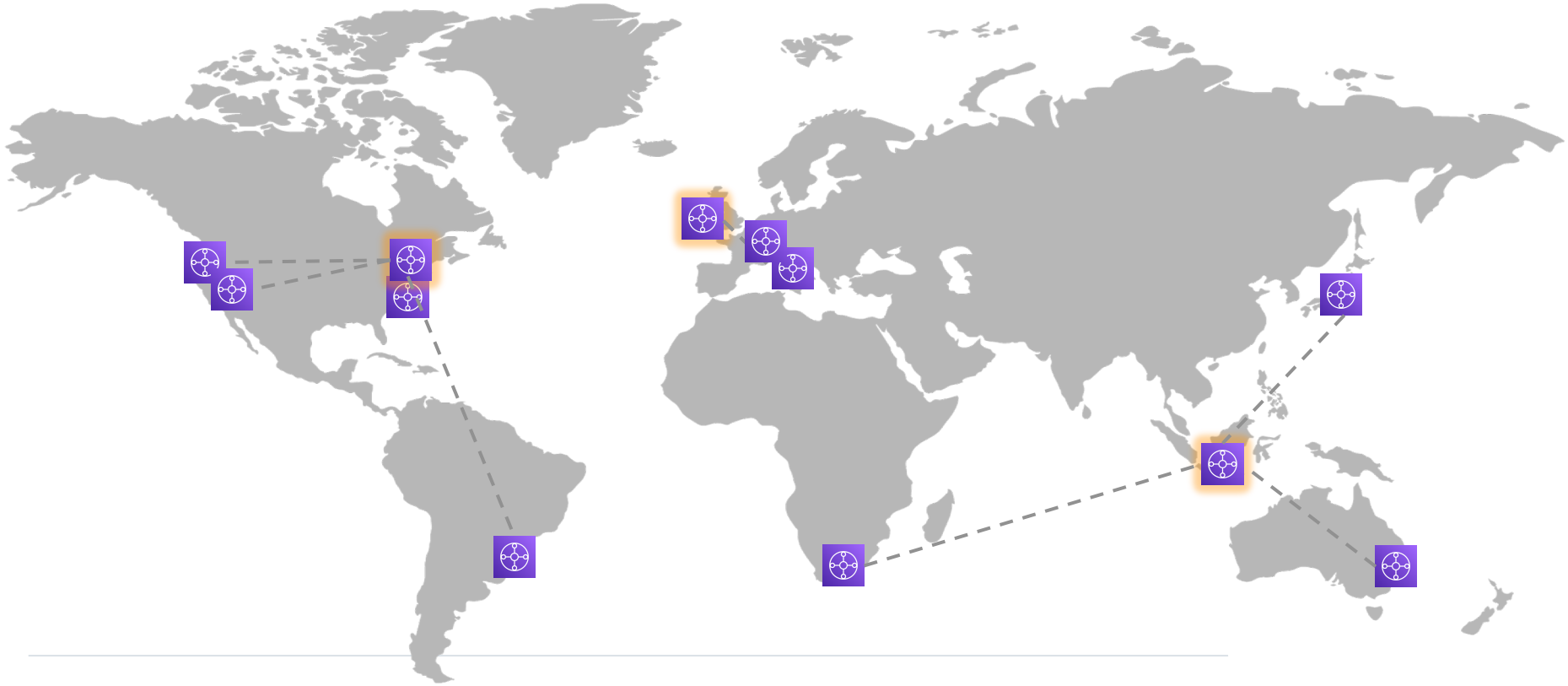
Data Plane


IoT device
aws
EMnify Account
Amazon VPC
AWS Transit Gateway
AWS Resource Access Manager
aws
Customer Account
Amazon VPC
172.16.0.0
172.16.1.0
172.16.2.0
Route table
Route table
Route table
Route table
aws
Customer Account
aws
Customer Account
Traffic Flow

TGW Bonus Points

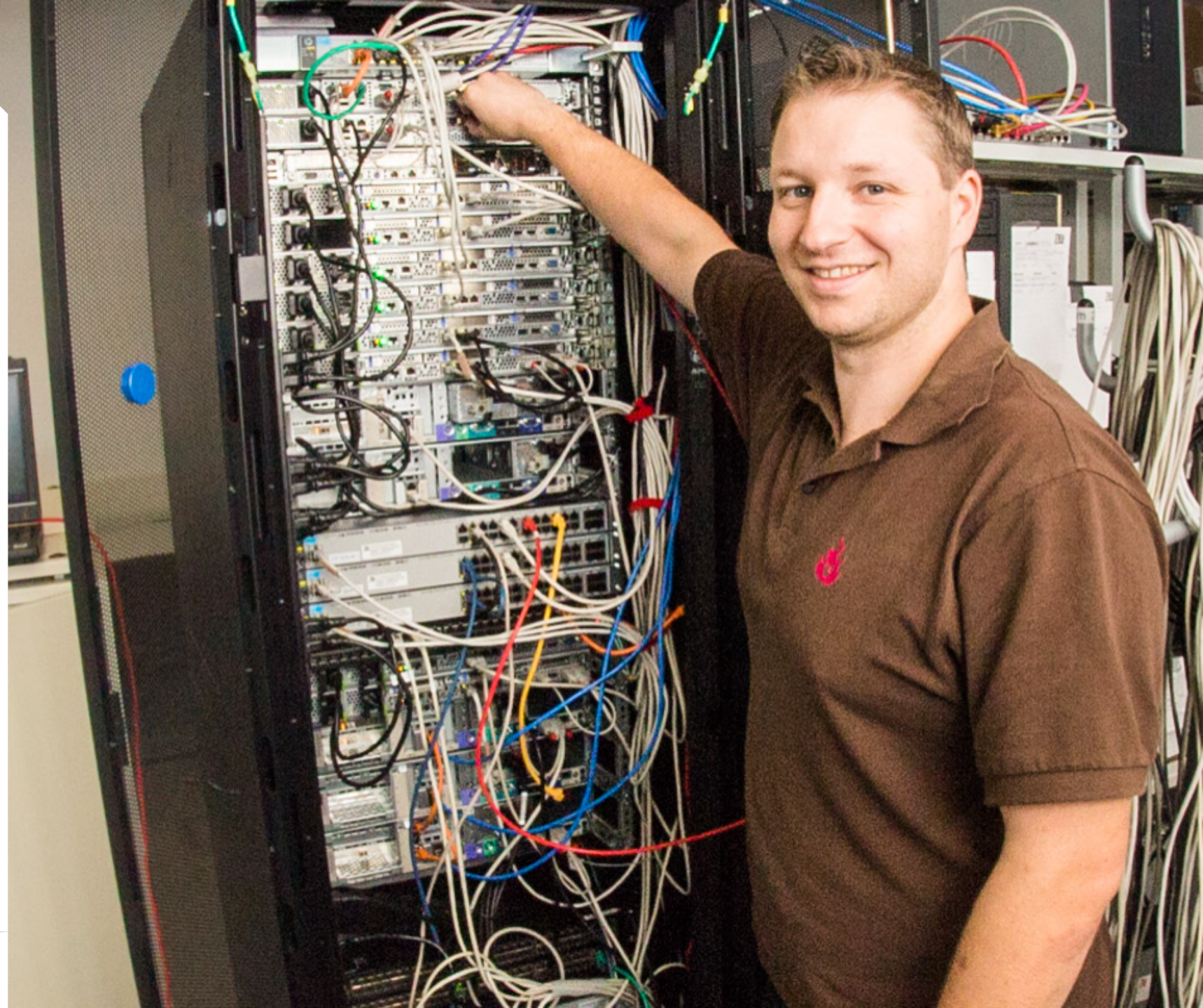
Cross-Region TGW Peering

Independence of our core network deployment regions



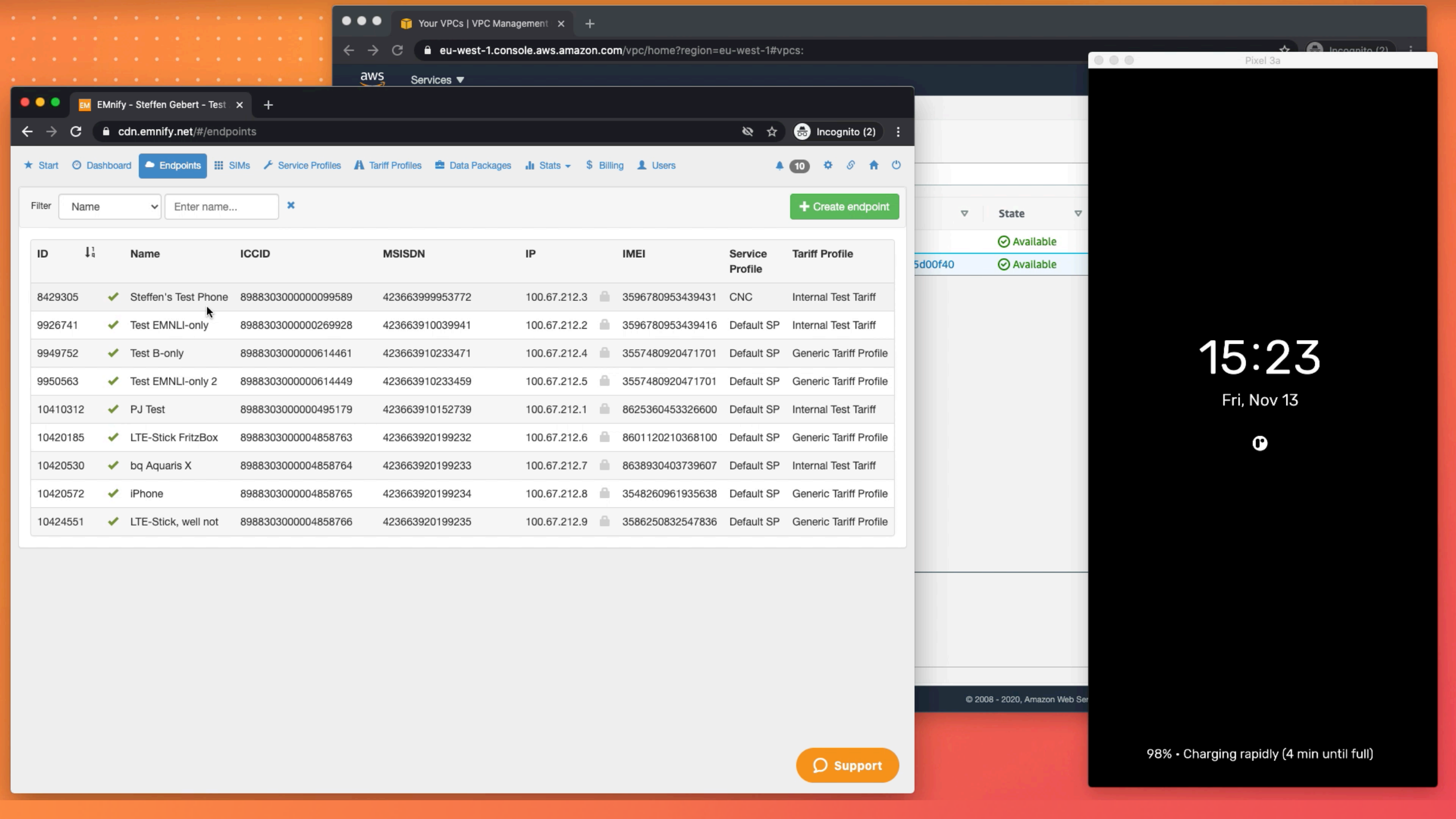
IPsec VPN ¯_(ツ)_/¯

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



EMnify

Demo

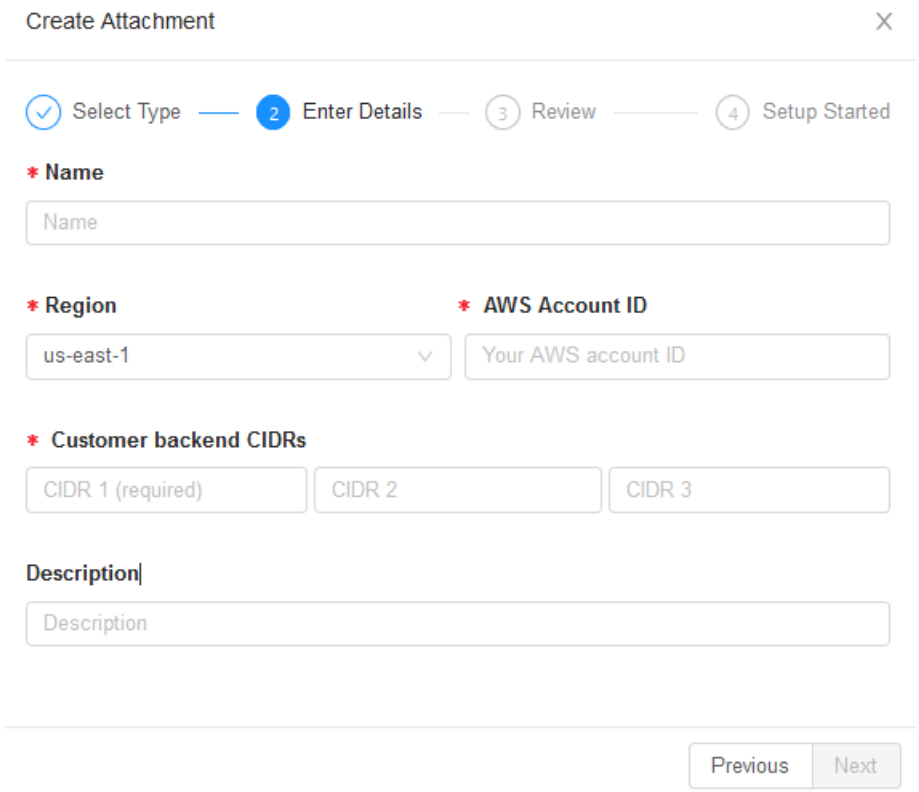

Your VPCs | VPC Management
eu-west-1.console.aws.amazon.com/vpc/home?region=eu-west-1#vpcs:
aws
Services
Incognito (2)
Pixel 3a
15:23
Fri, Nov 13
98% • Charging rapidly (4 min until full)
EMnify - Steffen Gebert - Test
cdn.emnify.net/#/endpoints
Incognito (2)
Start
Dashboard
Endpoints
SIMs
Service Profiles
Tariff Profiles
Data Packages
Stats
Billing
Users
10
Filter
Name
Enter name...
Create endpoint
State
Available
Available
5d00f40
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 8988303000000269928 423663910039941 100.67.212.2 3596780953439416 Default SP Internal Test Tariff
9949752 Test B-only 8988303000000614461 423663910233471 100.67.212.4 3557480920471701 Default SP Generic Tariff Profile
9950563 Test EMNLI-only 2 8988303000000614449 423663910233459 100.67.212.5 3557480920471701 Default SP Generic Tariff Profile
10410312 PJ Test 8988303000000495179 423663910152739 100.67.212.1 8625360453326600 Default SP Internal Test Tariff
10420185 LTE-Stick FritzBox 8988303000004858763 423663920199232 100.67.212.6 8601120210368100 Default SP Generic Tariff Profile
10420530 bq Aquaris X 8988303000004858764 423663920199233 100.67.212.7 8638930403739607 Default SP Internal Test Tariff
10420572 iPhone 8988303000004858765 423663920199234 100.67.212.8 3548260961935638 Default SP Generic Tariff Profile
10424551 LTE-Stick, well not 8988303000004858766 423663920199235 100.67.212.9 3586250832547836 Default SP Generic Tariff Profile
Support
© 2008 - 2020, Amazon Web Ser

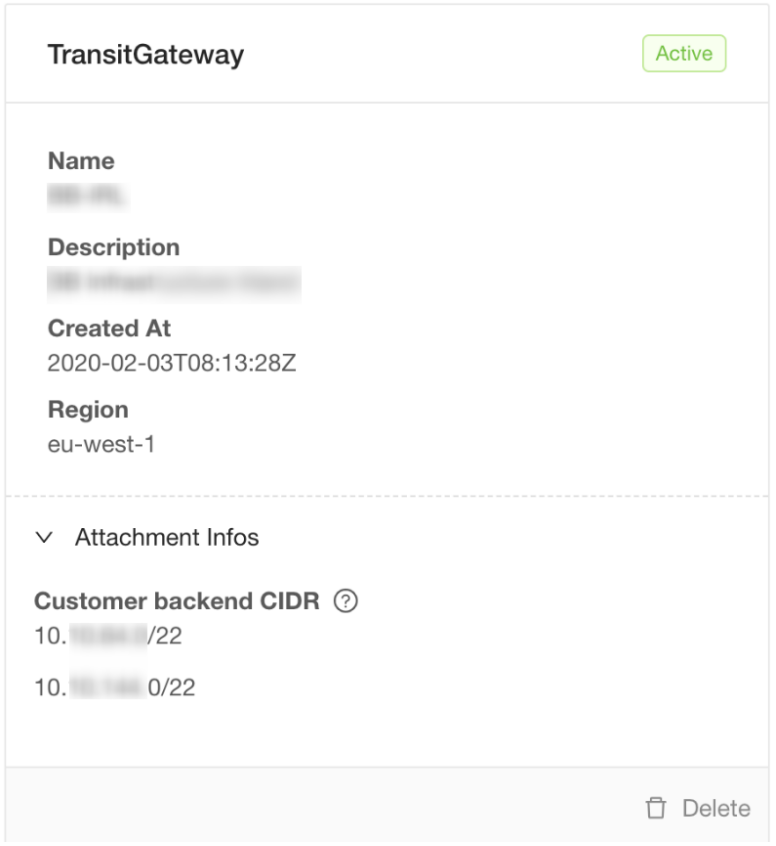
EMnify

Control Plane

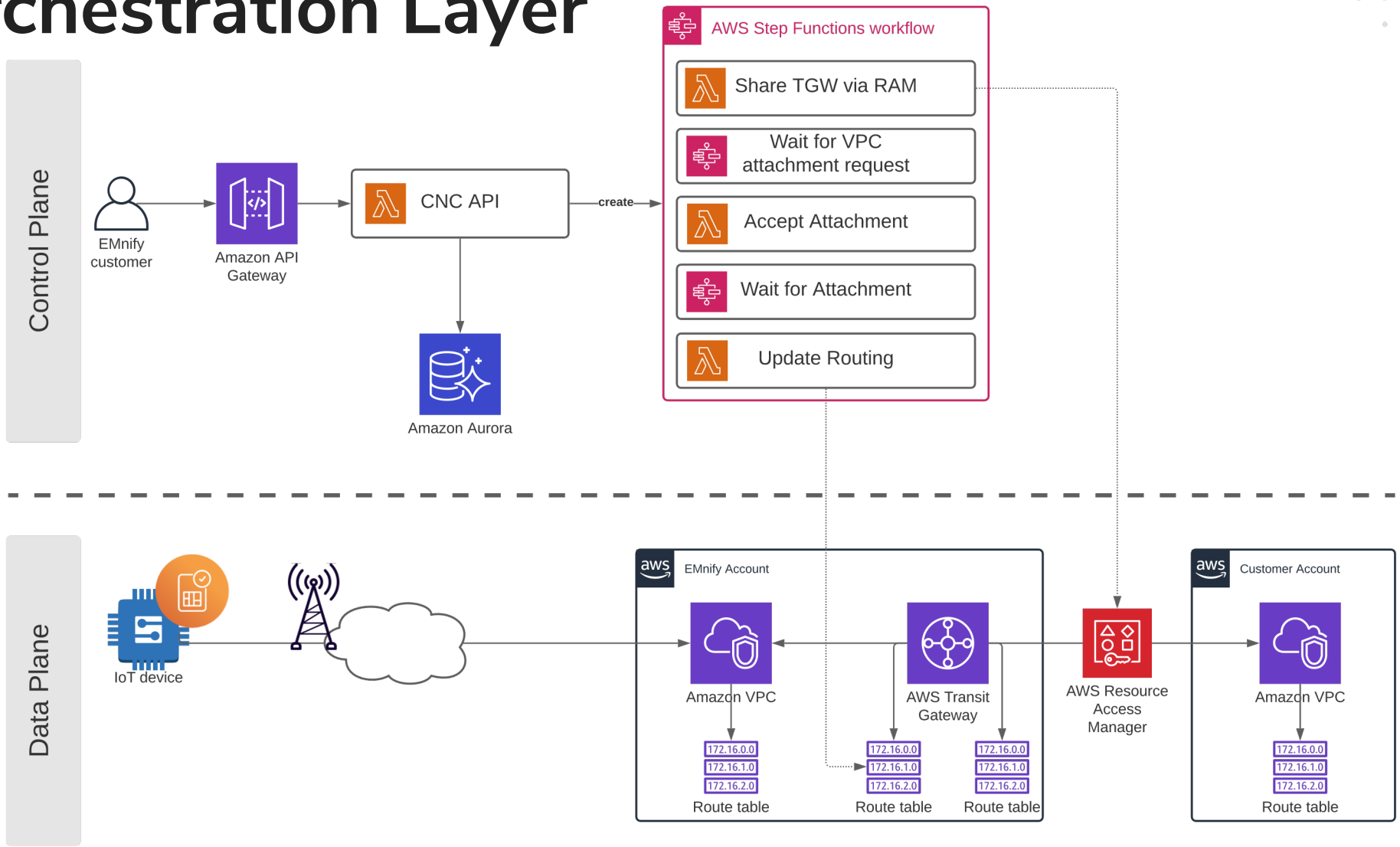
Enabling Self-Service

- Customer portal / REST API





Orchestration Layer



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**