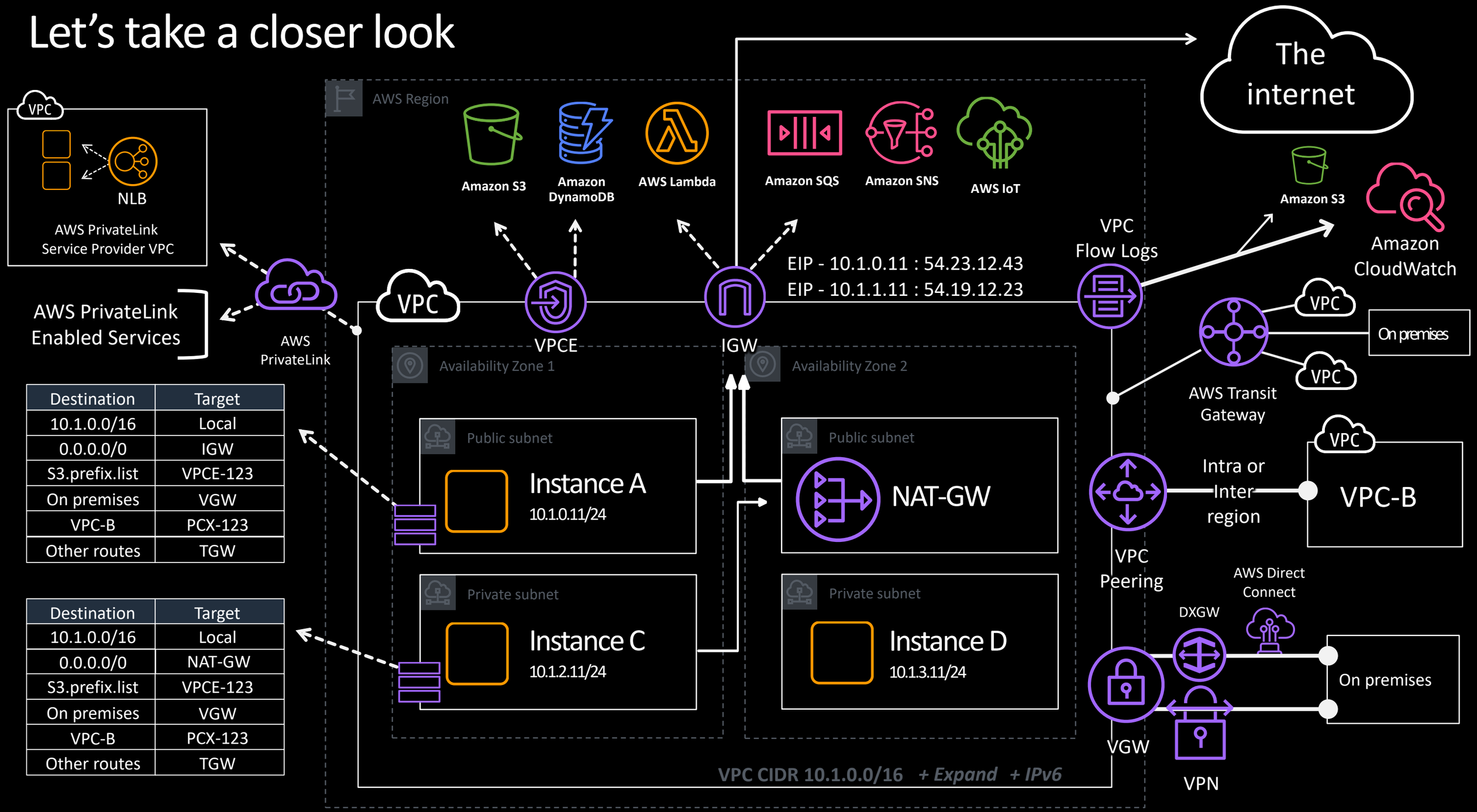
SVC305

# Easily scale your network with AWS Transit Gateway

Bhavin Desai
Senior Solutions Architect
Amazon Web Services

aws SUMMIT

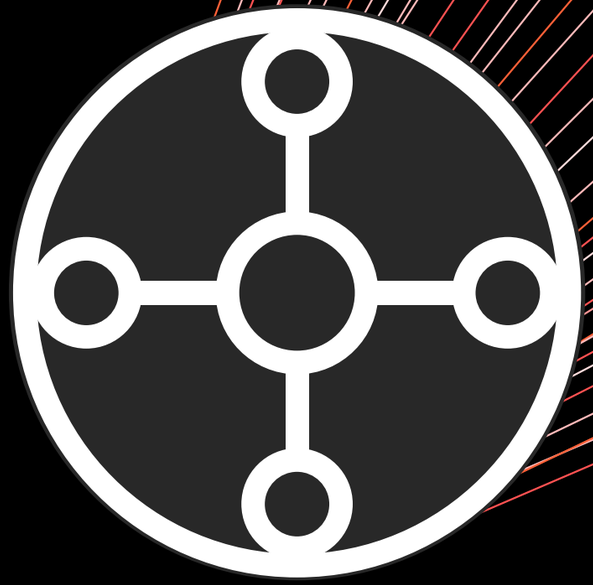
# Let’s take a closer look




| Destination | Target |
|---|---|
| 10.1.0.0/16 | Local |
| 0.0.0.0/0 | IGW |
| S3.prefix.list | VPCE-123 |
| On premises | VGW |
| VPC-B | PCX-123 |
| Other routes | TGW |

| Destination | Target |
|---|---|
| 10.1.0.0/16 | Local |
| 0.0.0.0/0 | NAT-GW |
| S3.prefix.list | VPCE-123 |
| On premises | VGW |
| VPC-B | PCX-123 |
| Other routes | TGW |

# What is the AWS Transit Gateway?

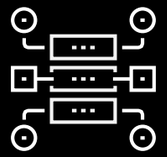


aws SUMMIT

# AWS Transit Gateway

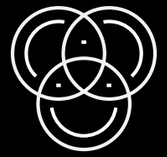
Regional gateway

Simple regional gateway to easily manage VPC connectivity



Massive scale

Ability to attach thousands of VPCs and VPN & AWS Direct Connect connections



Routing domains

Support for routing domains, allowing per-attachment routing

Partner integration

Support for middle-boxing of partner appliances

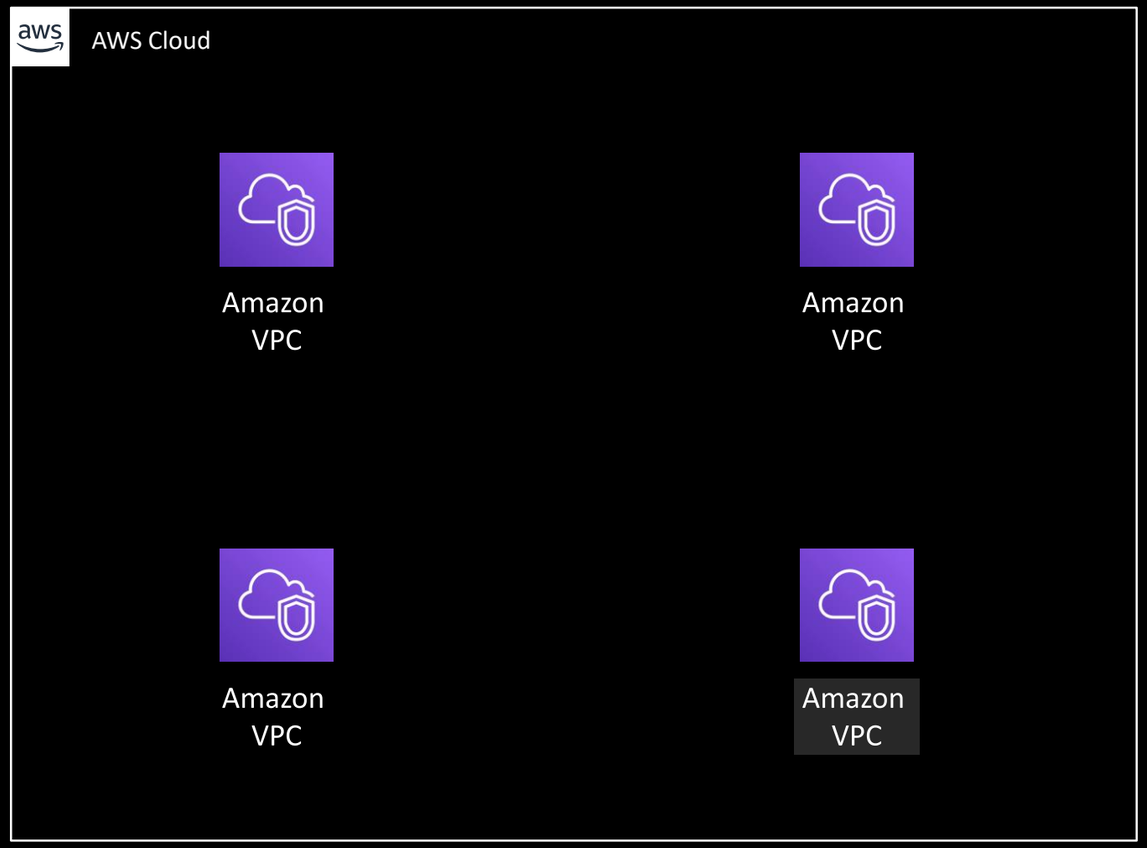
fuze

"AWS Transit Gateway radically evolved and simplified cloud networking. Using AWS Transit Gateway, we reduced the time to interconnect new VPCs and on-premises networks from weeks to minutes while attaining consistent and more reliable network performance!"

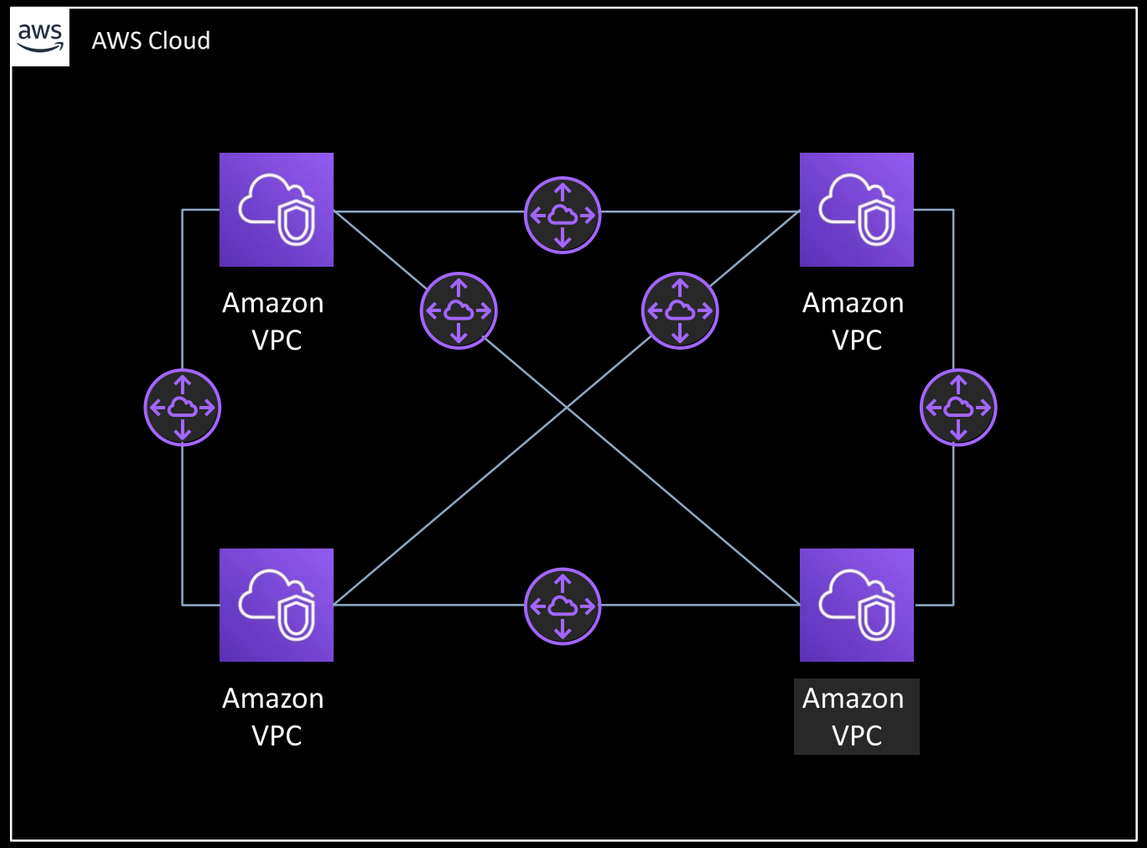
Khoder Shamy
Director, Cloud Platform and Infrastructure
Fuze

aws SUMMIT

# Before AWS Transit Gateway



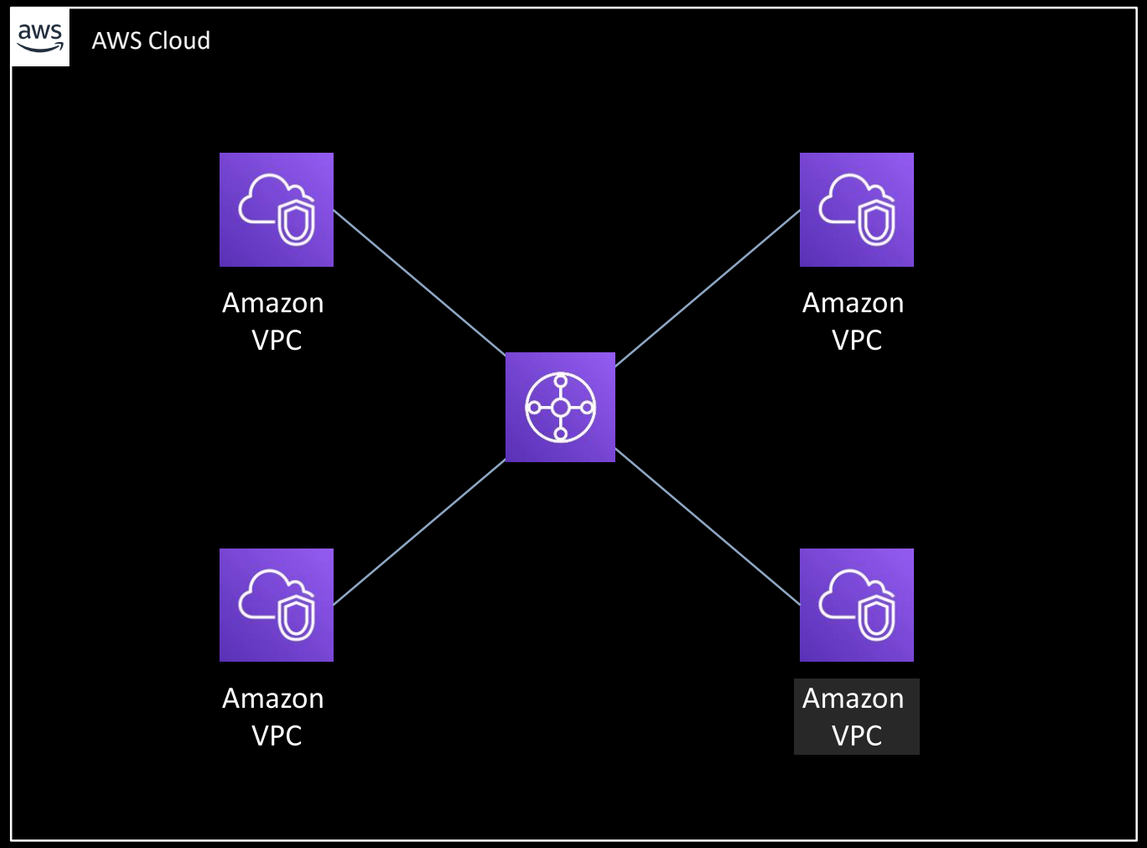
# Interconnecting VPCs at scale: Peering



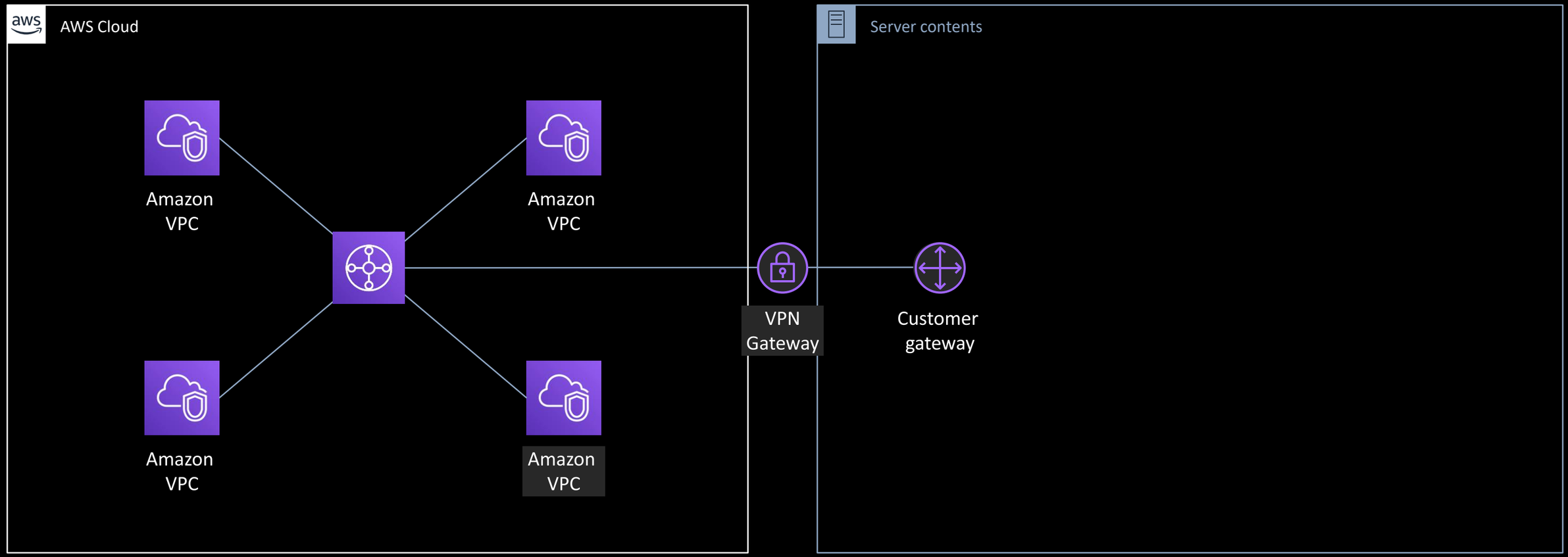

Connecting a large number of VPCs in a mesh is challenging to manage

Connecting on-premises networks to each new VPC can take weeks to months to implement due to customer's internal processes

# Interconnecting VPCs at scale: AWS Transit Gateway



# Single VPN with AWS Transit Gateway



# Introducing AWS Transit Gateway

## Regional service

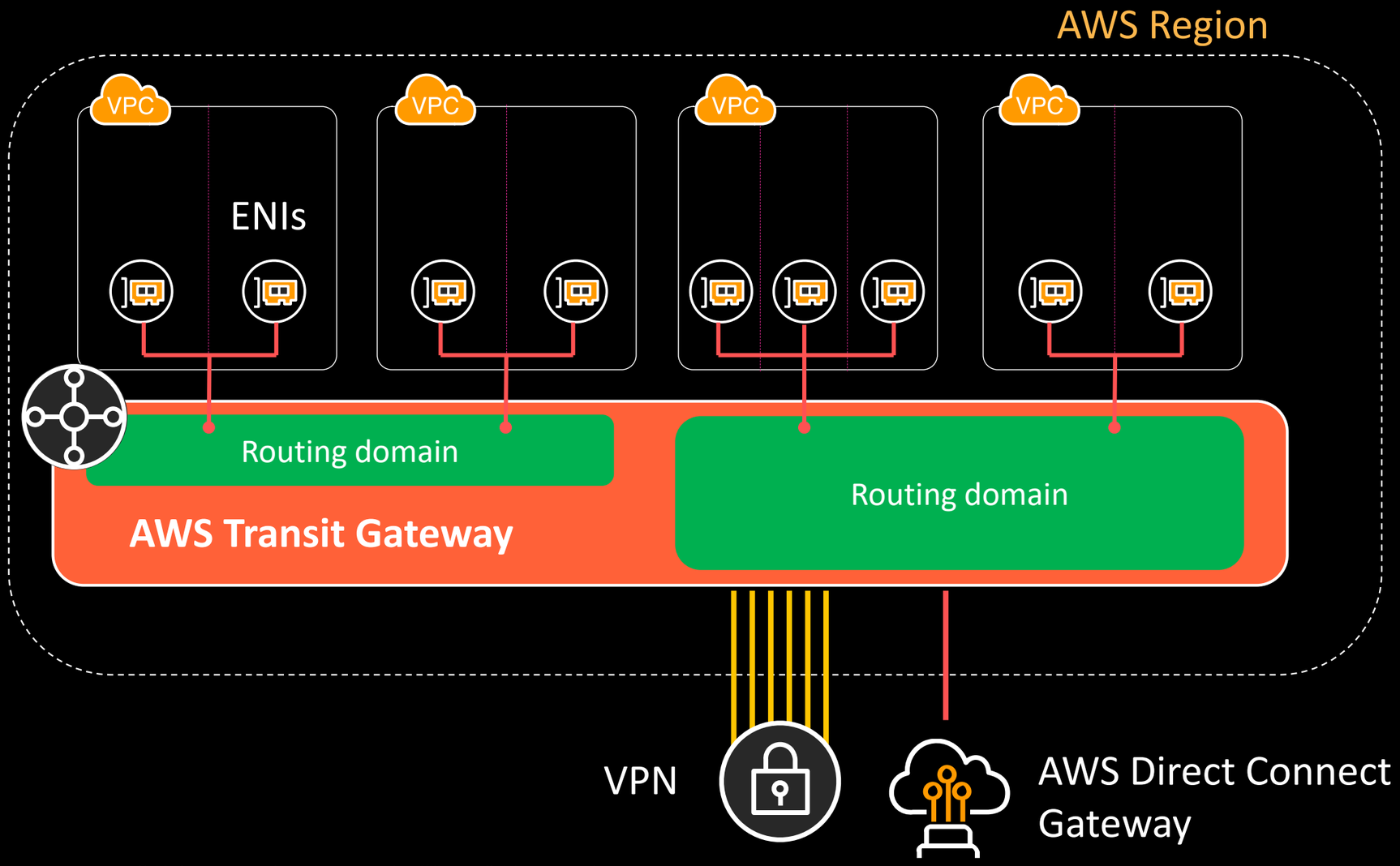
- Centralize VPN and AWS Direct Connect

## Scalable

- Thousands of VPCs across accounts
- Spread traffic over many VPN connections

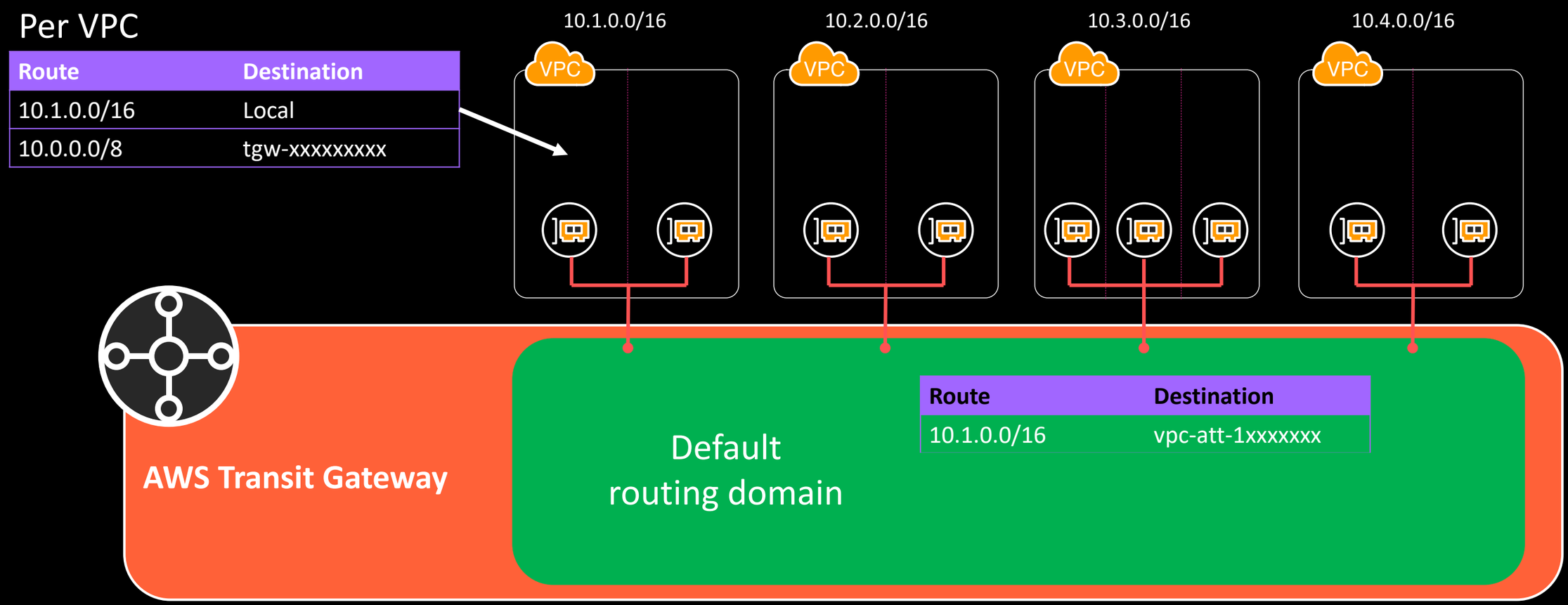
## Flexible routing

- Network interfaces in subnets
- Control segmentation and sharing with routing domains

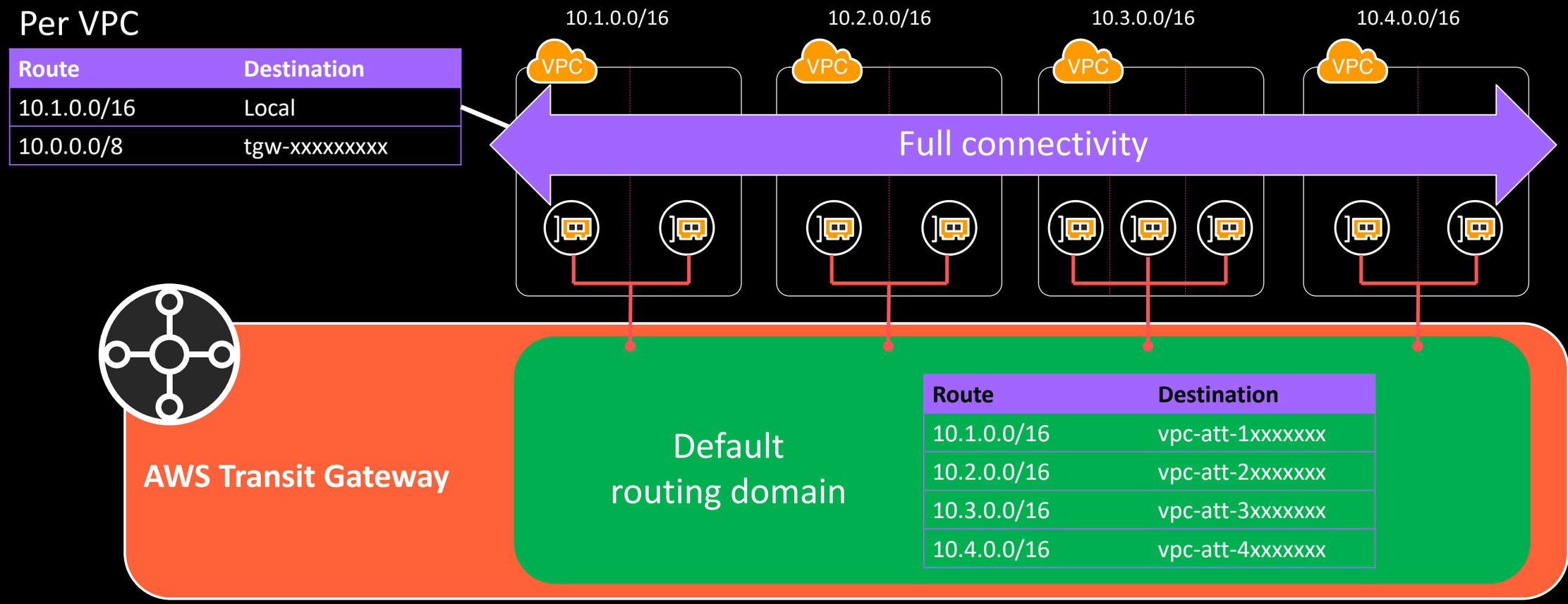



aws SUMMIT

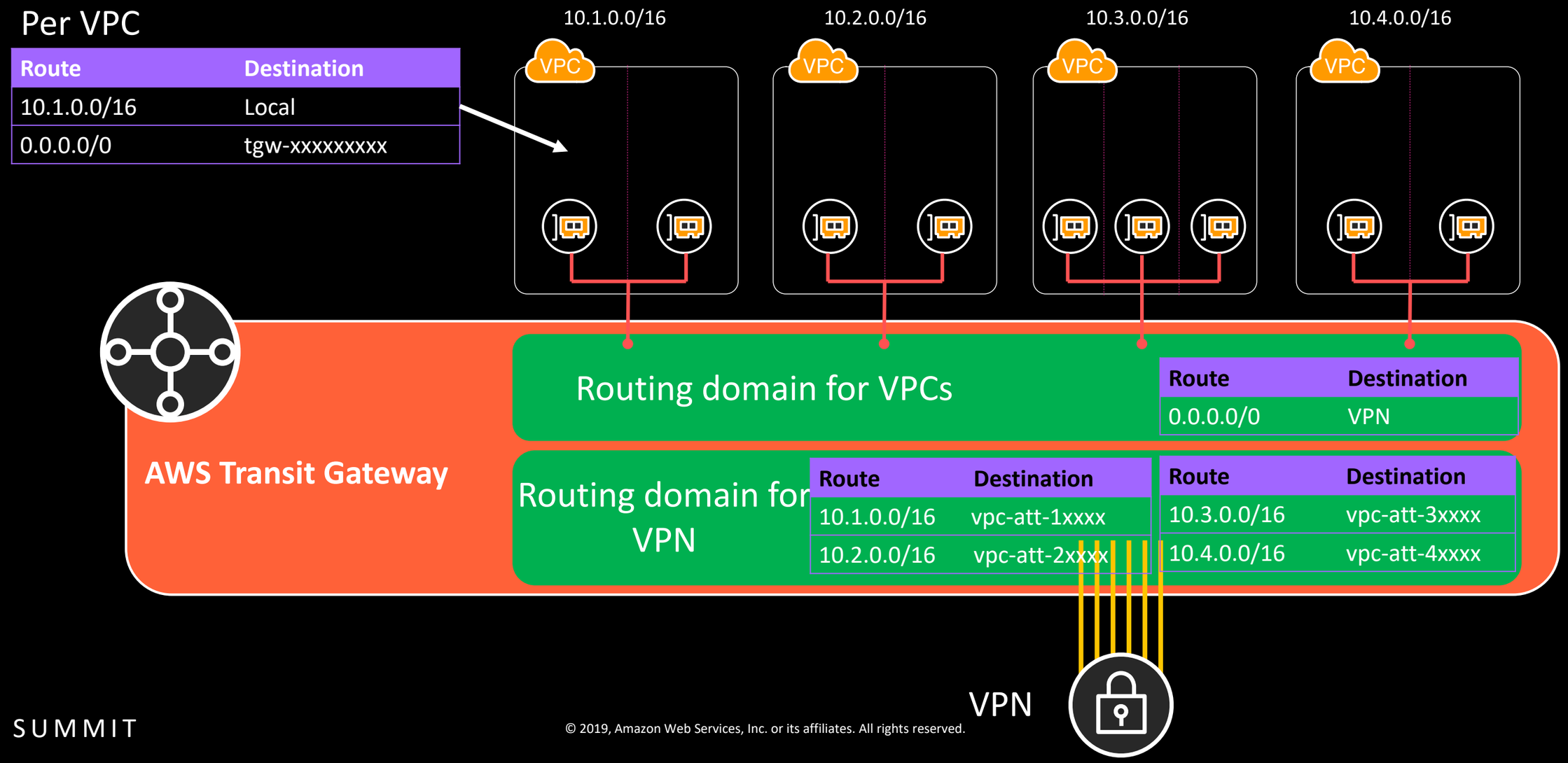
# Flat: AWS Transit Gateway route domains (route tables)



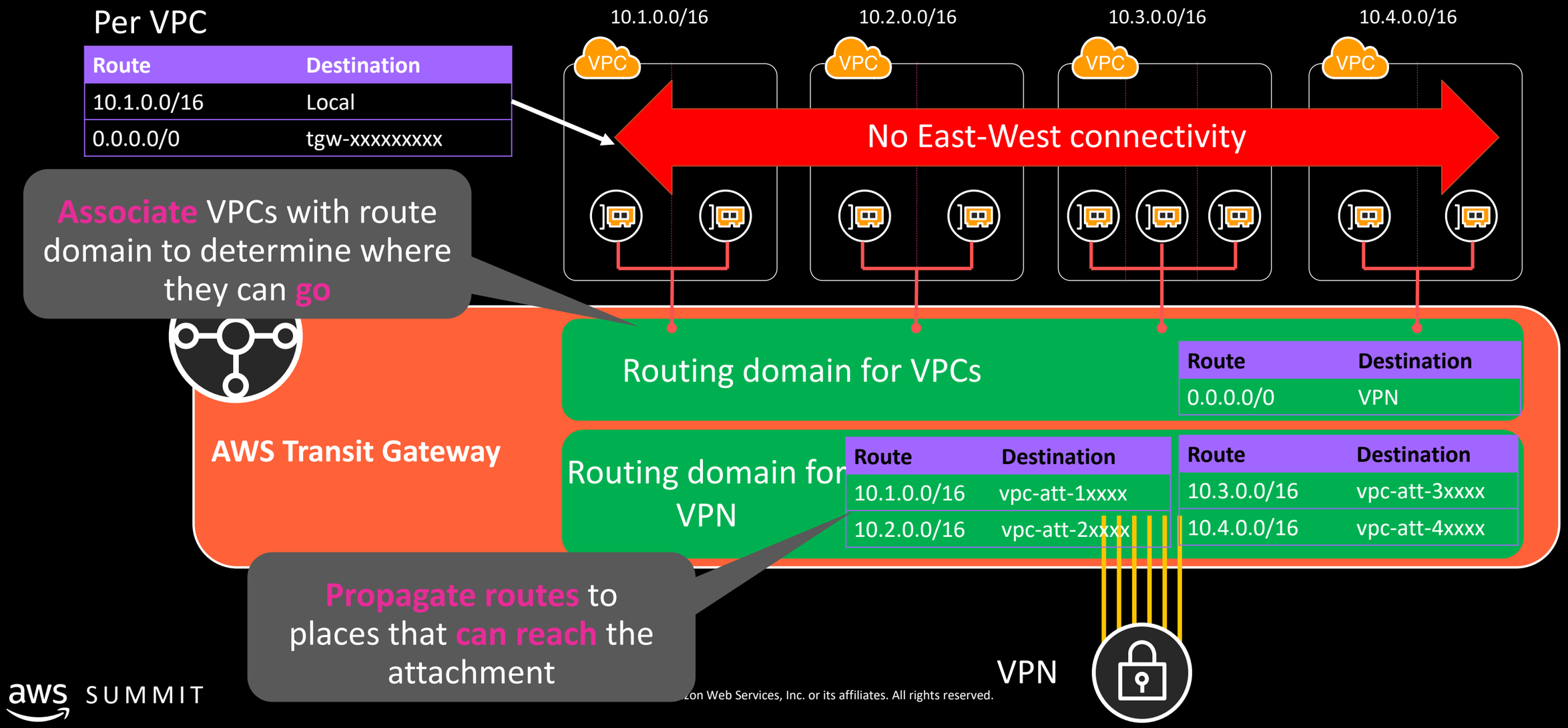
# Flat: AWS Transit Gateway route domains (route tables)



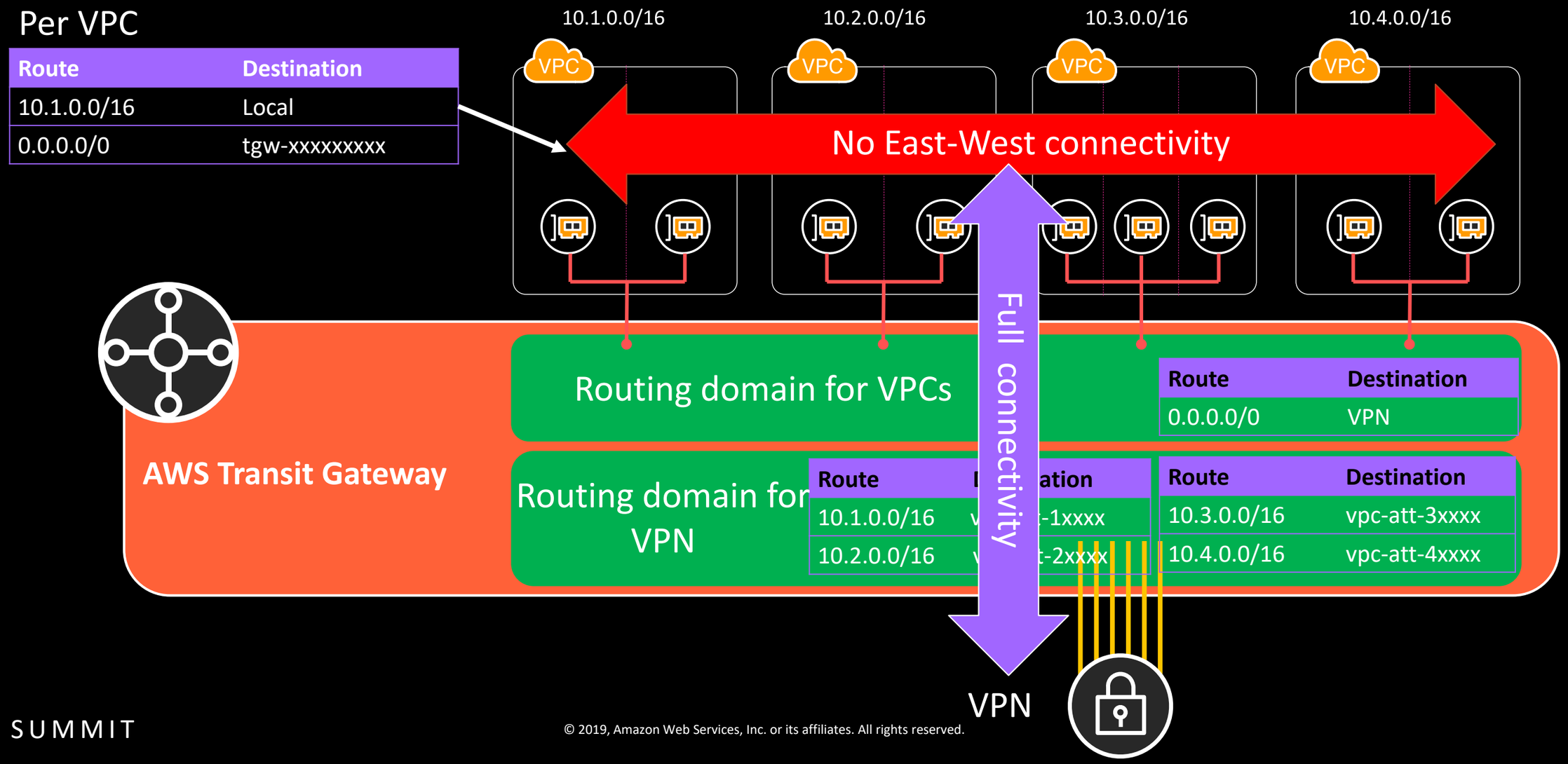
# Isolated: AWS Transit Gateway route domains



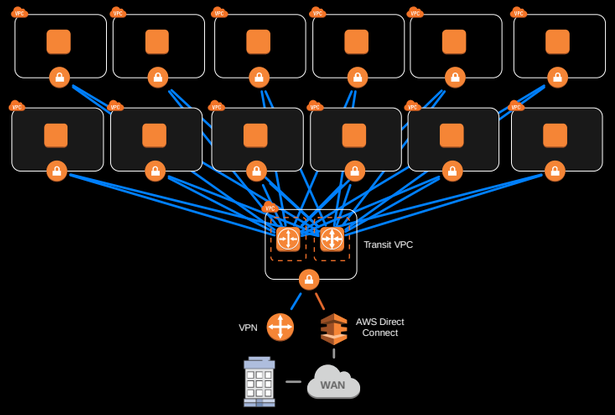
# Isolated: AWS Transit Gateway route domains

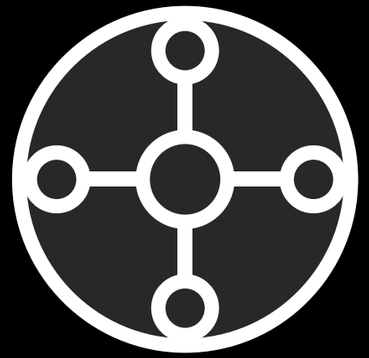


# Isolated: AWS Transit Gateway route domains



# Quick comparison: AWS Transit Gateway and Transit VPC



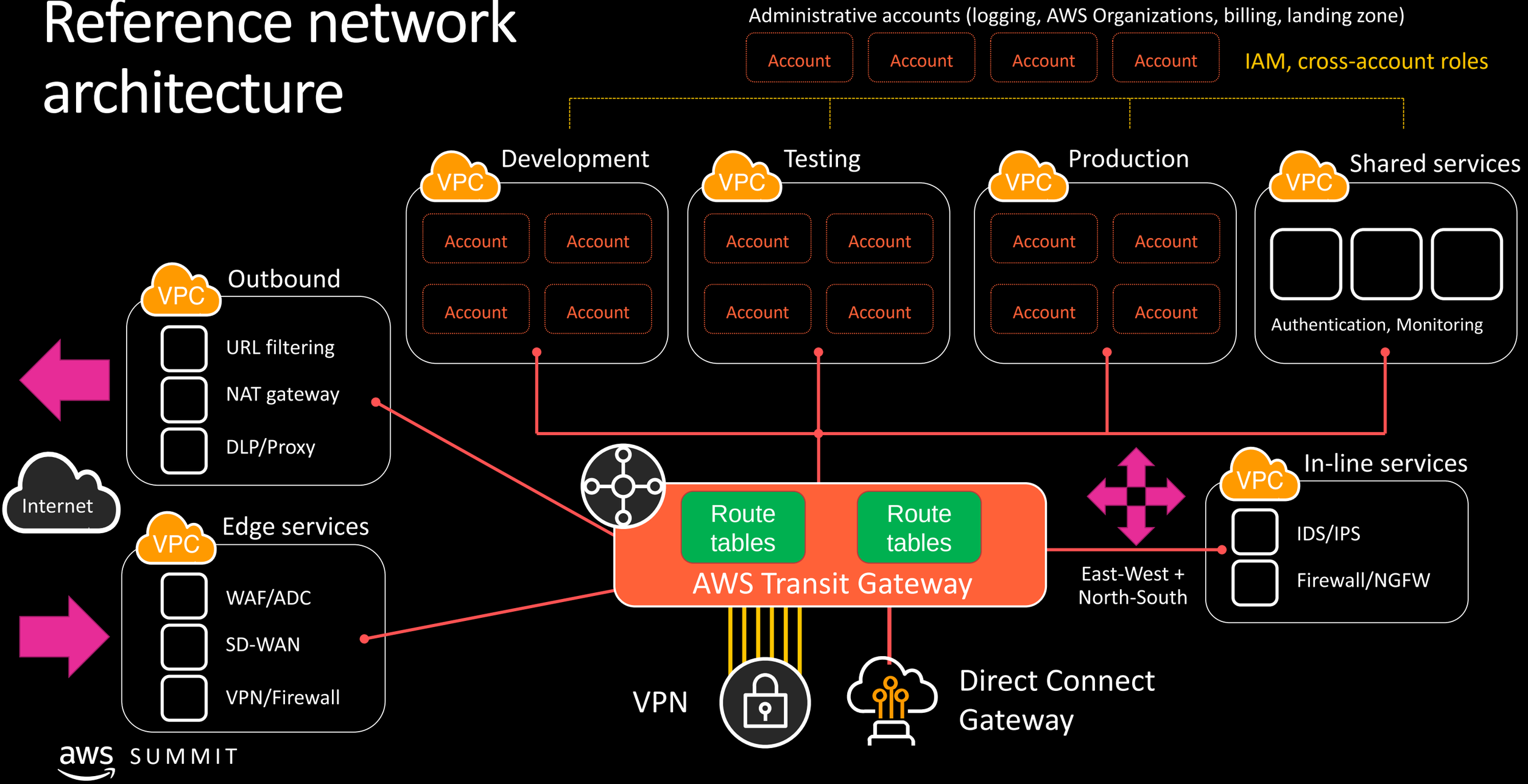
## Transit VPC

- Customer-managed instances
- Uses VPN and virtual private gateways
- Hard to scale and manage
- Difficult to segment

## AWS Transit Gateway

- AWS native service
- Uses elastic network interfaces
- Scales horizontally
- Flexible segmentation

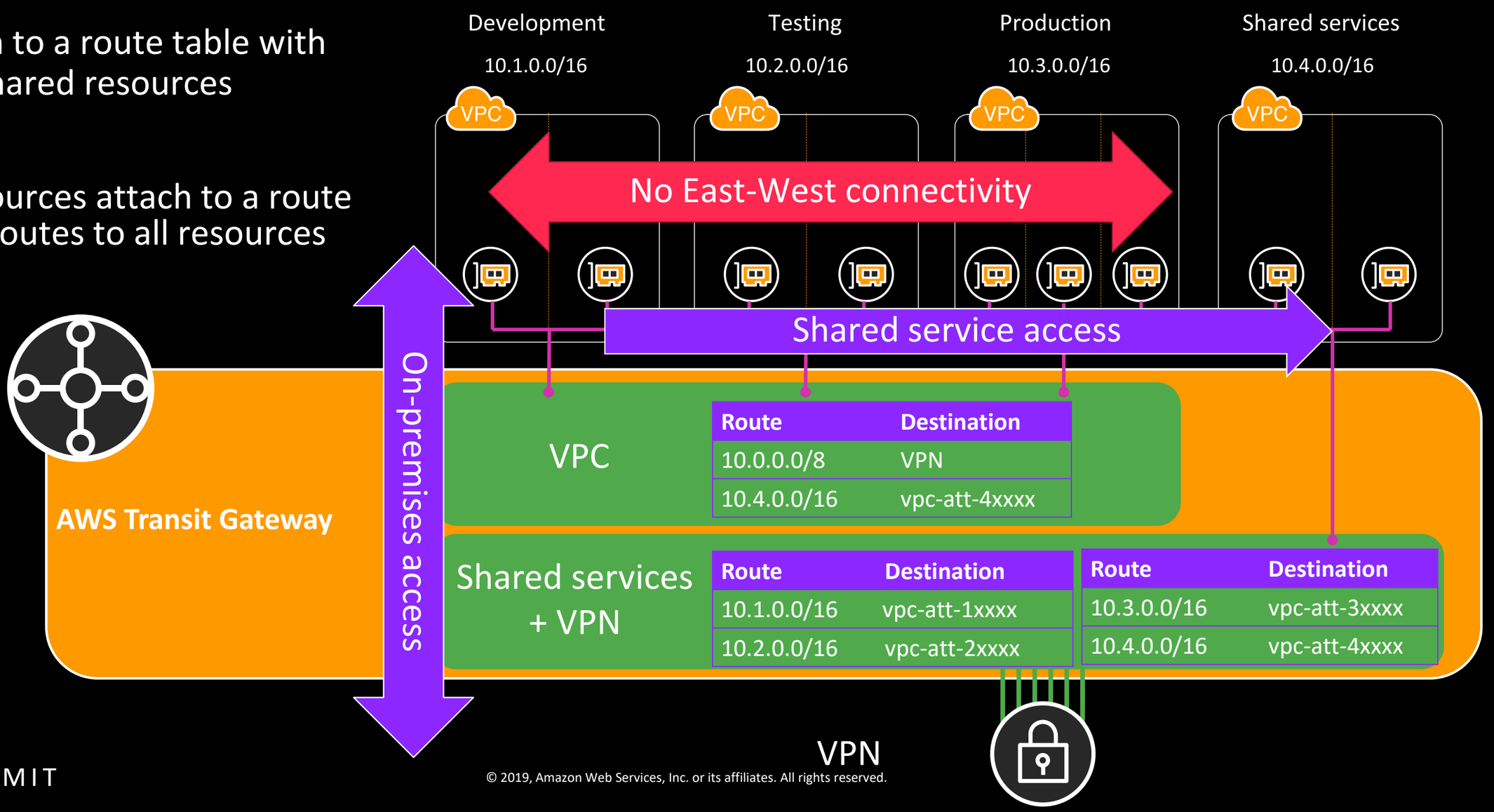
# Reference network architecture



# Use case 1: Shared services with AWS Transit Gateway

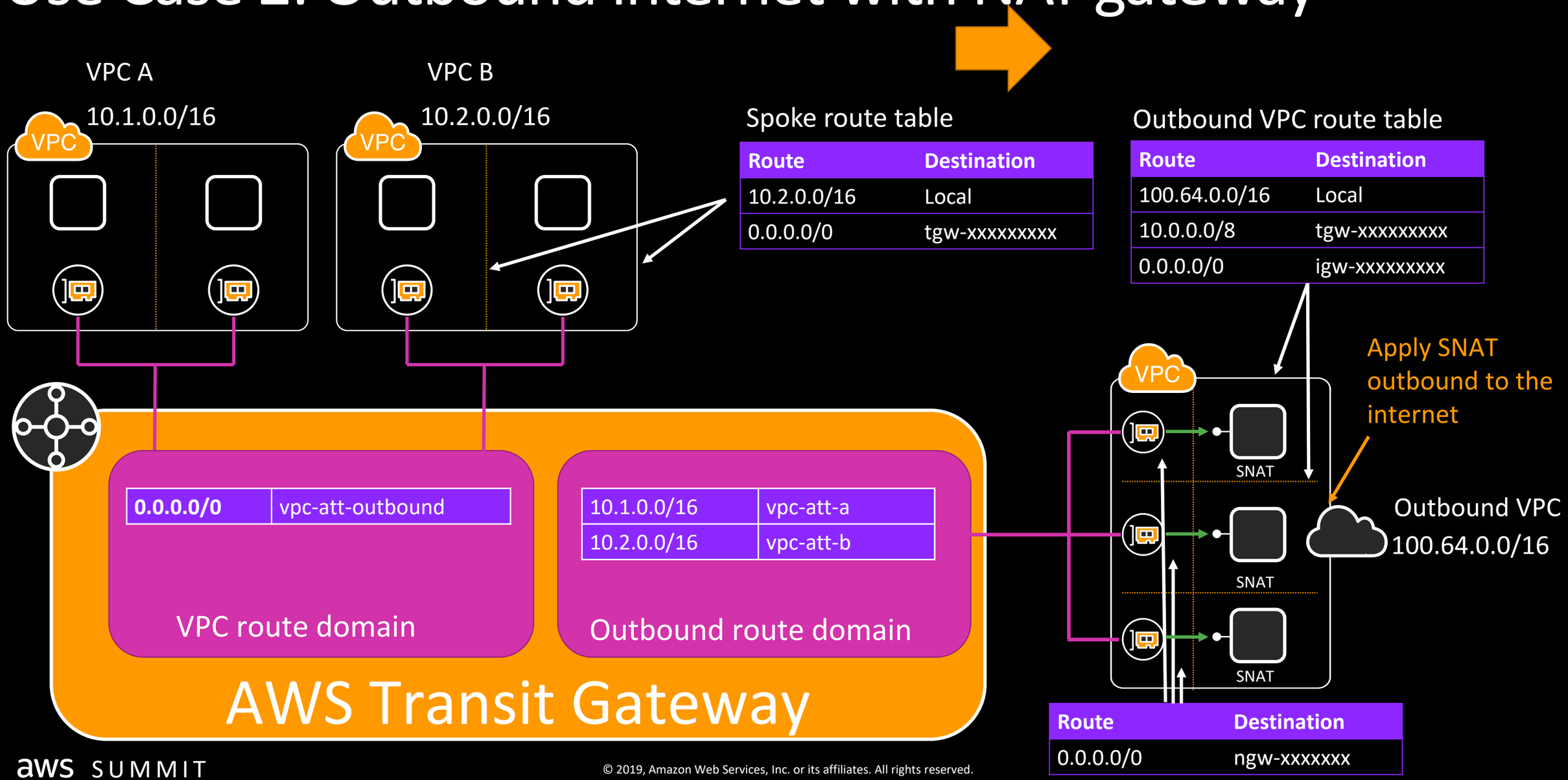
VPCs attach to a route table with routes to shared resources

Shared resources attach to a route table with routes to all resources



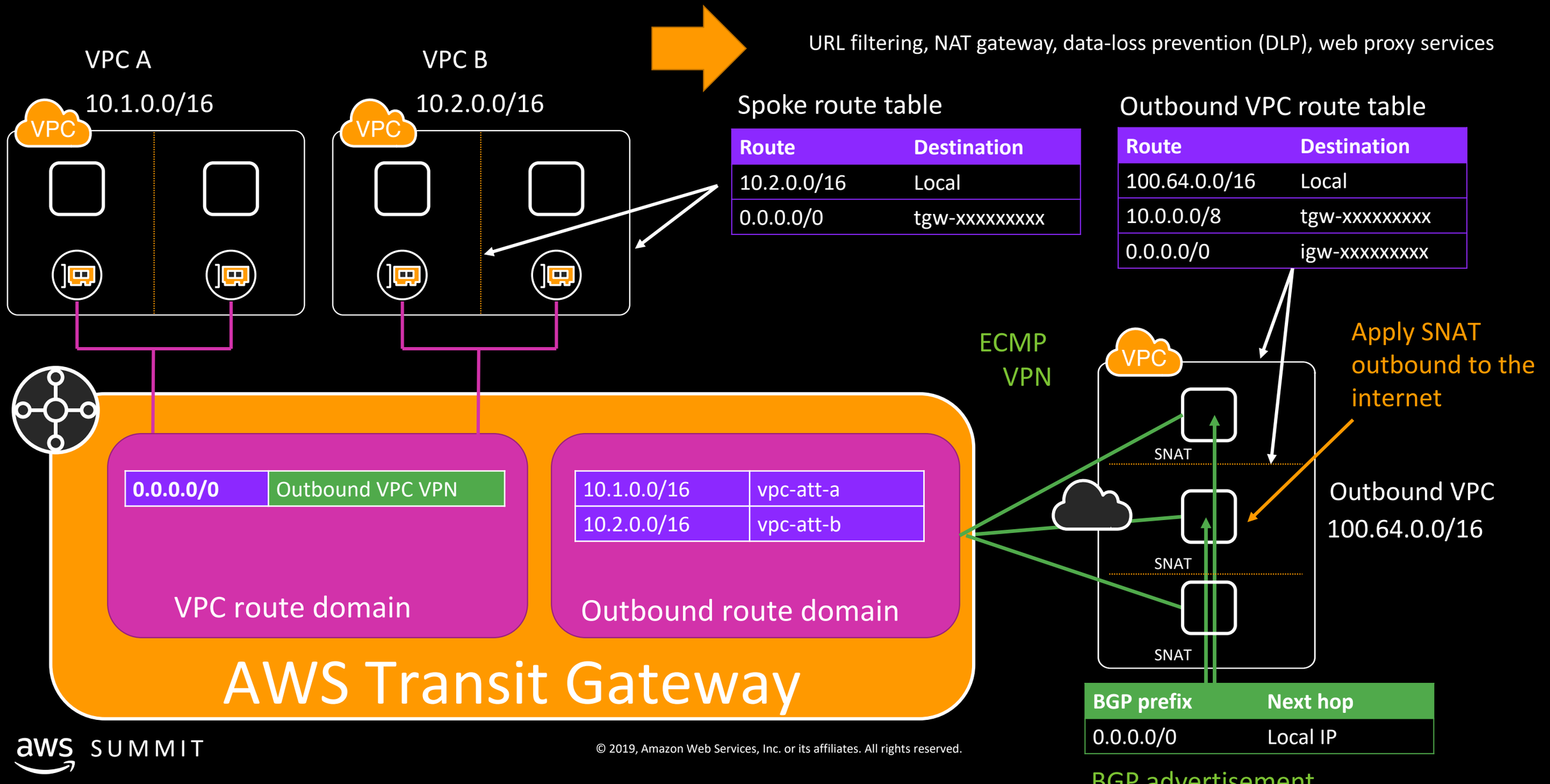

aws SUMMIT

# Use Case 2: Outbound internet with NAT gateway




aws SUMMIT

# Use Case 3: Outbound services VPC

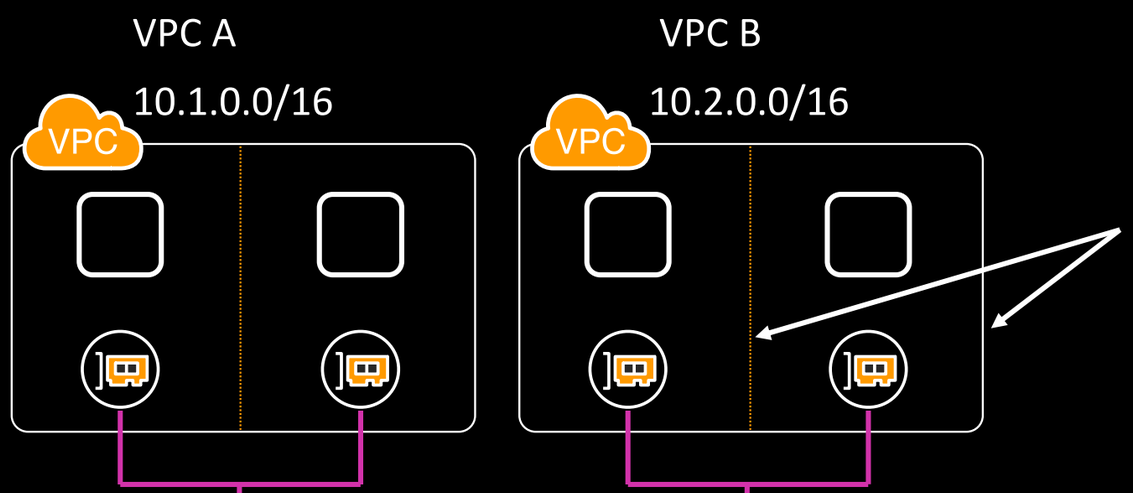



aws SUMMIT

# VPC to VPC service insertion

Use cases:

Intrusion detection/prevention (IDS/IPS), firewalls, next-gen firewalls (NGFWs), unified threat management (UTM)




Spoke route table

| Route | Destination |
|---|---|
| 10.2.0.0/16 | Local |
| 0.0.0.0/0 | tgw-xxxxxxxxx |
| 100.64.0.0/16 | tgw-xxxxxxxxx |

VPCs will traffic as originated from the in-line VPC CIDR

Outbound VPC route table

| Route | Destination |
|---|---|
| 100.64.0.0/16 | Local |
| 10.0.0.0/8 | tgw-xxxxxxxxx |
| 0.0.0.0/0 | igw-xxxxxxxxx |

Apply SNAT between VPCs for flow affinity

ECMP VPN

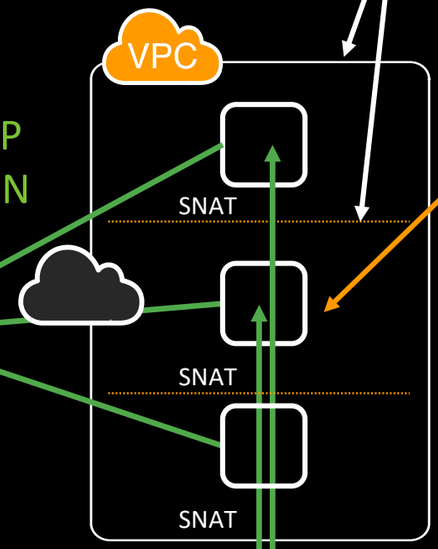
| 0.0.0.0/0 | Outbound VPC VPN |
|---|---|

VPC route domain

| 10.1.0.0/16 | vpc-att-a |
|---|---|
| 10.2.0.0/16 | vpc-att-b |

Outbound route domain

AWS Transit Gateway




In-line VPC
100.64.0.0/16

| BGP prefix | Next hop |
|---|---|
| 0.0.0.0/0 | Local IP |

BGP advertisement

aws SUMMIT

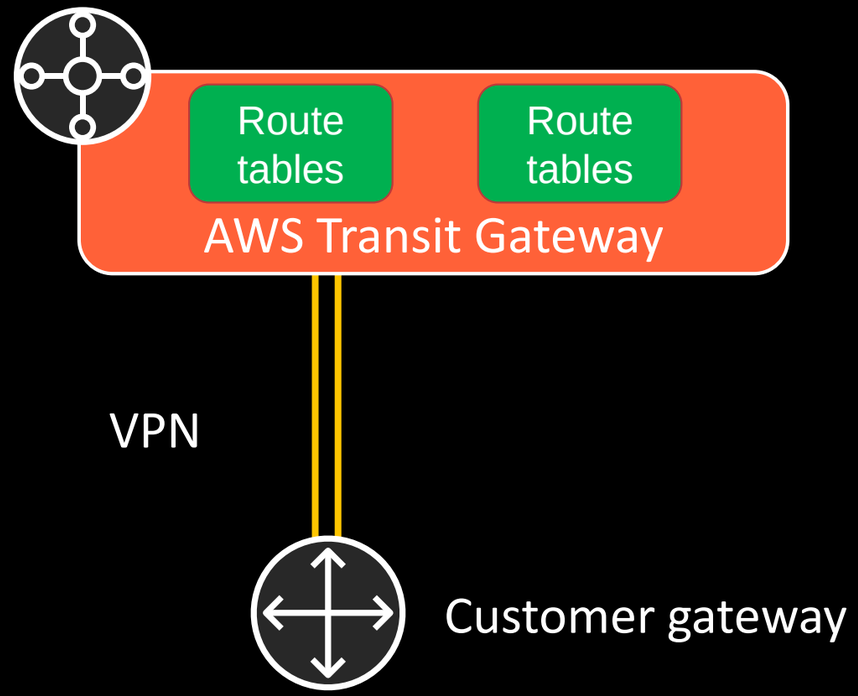
# VPN with AWS Transit Gateway

Consolidate VPN at the transit gateway (TGW)

- VPN acts similar to the virtual private gateway (VGW)
  - Bandwidth, configuration, APIs, cost, and experience
  - VPN is attached to a TGW instead of a VGW
  - Same 1.25 Gbps bandwidth per tunnel applies

Encryption to the edge of many VPCs

- Traffic is encrypted until it’s inside the VPC
- Does not natively encrypt traffic between VPCs
  - Inter-region VPC peering does



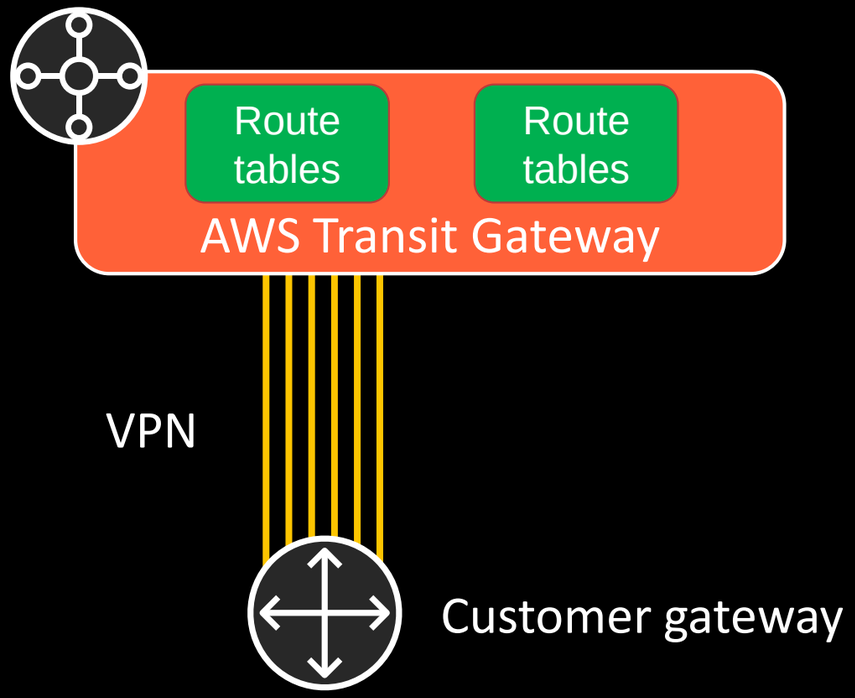
# VPN with AWS Transit Gateway: Add more bandwidth

Support for spreading traffic across many tunnels

- Equal-cost multi-path (ECMP) support with BGP multi-path
- Tested up to 50 Gbps of traffic
- Split traffic into smaller flows, multi-part uploads, etc.

Check your on-premises configuration

- Multi-path BGP
- ECMP support, amount of equal paths, reverse-path forwarding/spoofing checks
- Only supported with BGP, not static routing



# AWS Direct Connect with AWS Transit Gateway

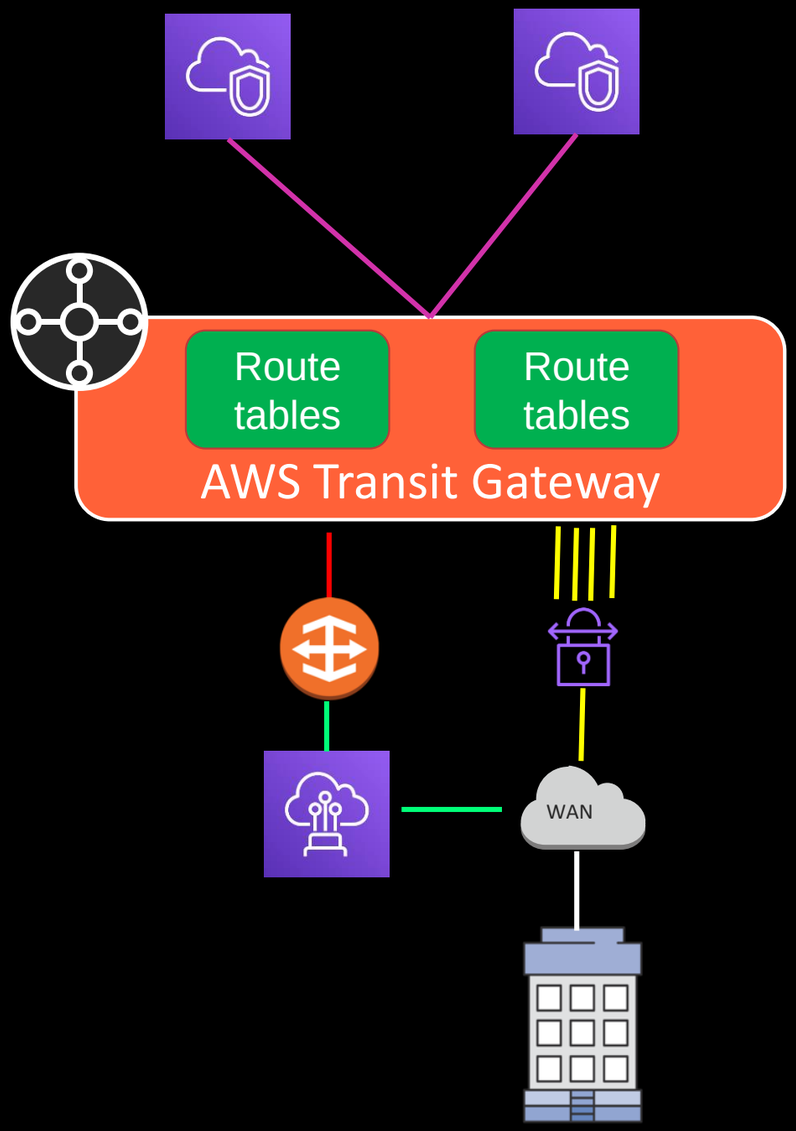
New

## AWS Direct Connect gateway attachment

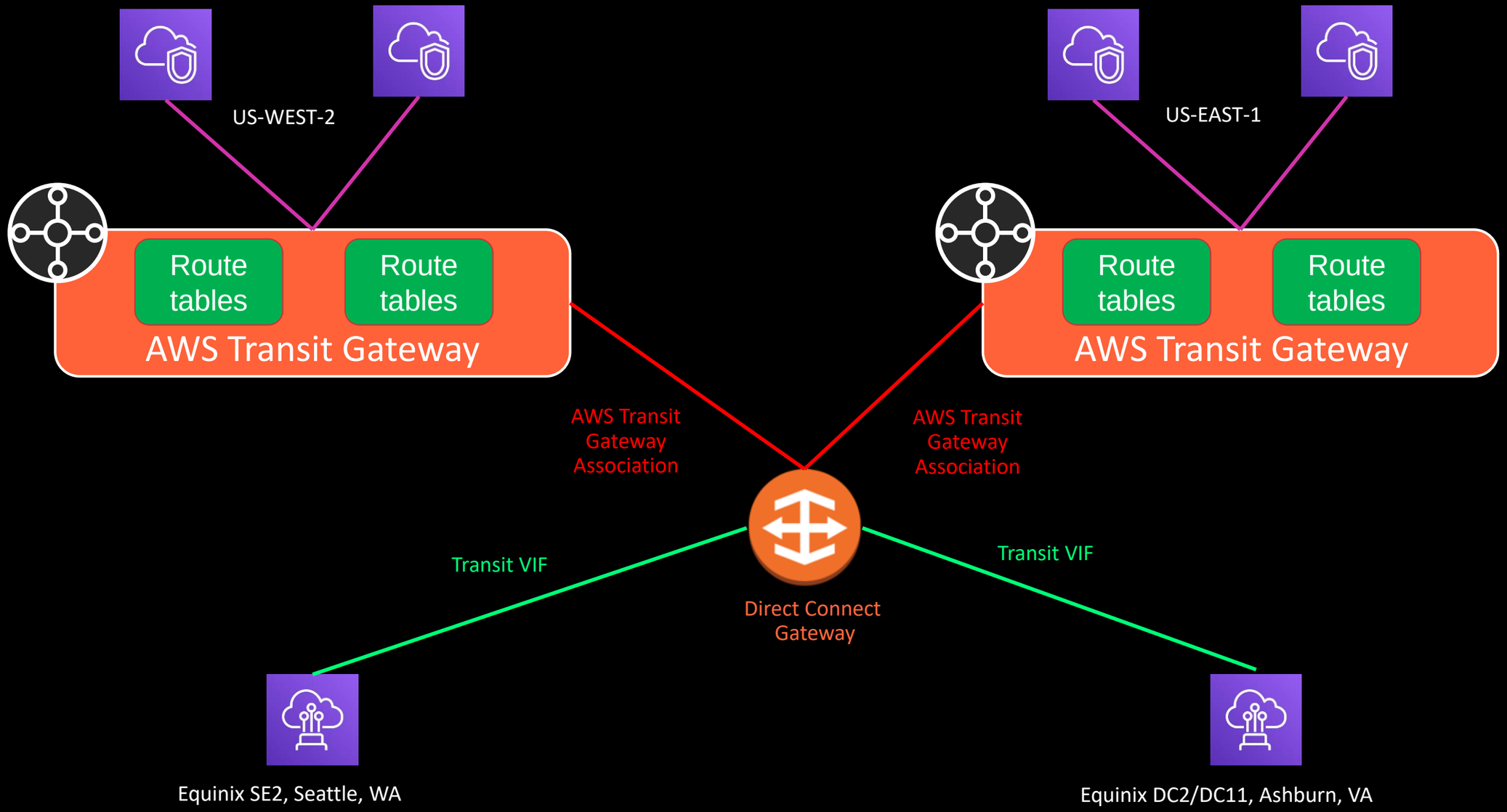
- Direct Connect gateway (DXGW)
- Attach transit virtual interface (VIF) to DXGW
- Associate AWS Transit Gateway to Direct Connect gateway
  - List the network prefixes that you want to advertise to on premises

## Benefits

- Use dedicated high bandwidth of 1G and 10G AWS Direct Connect connections
- Failover between AWS Direct Connect and AWS site-to-site VPN
- Connectivity from AWS Direct Connect co-locations



# Direct Connect gateway and AWS Transit Gateway



# Conclusions

# Takeaways

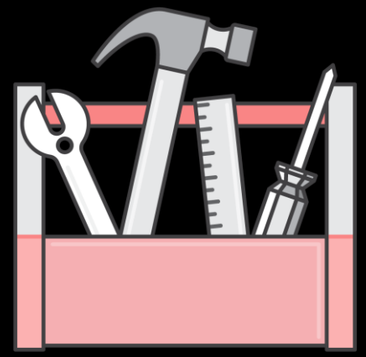
We have tools and architectures that horizontally scale to many VPCs

There’s wiggle room for your specific use cases

Use services in combination to meet scale and security requirements

# Advice

- Networking changes fast; no more crystal balls.
- Start simple! Stay simple. Reduce complexity to smaller scopes.
- Segment and modify as needed.
- Experiment and test.



# Thank you!

Bhavin Desai
bhavind@amazon.com

aws SUMMIT