AWS Transit Gateway Reference Architectures for Many Amazon VPCs

Agenda

- VPC Connectivity Paradigms
- Inside Transit Gateway
- Transit Gateway Data Flows
- Transit Gateway Reference Architectures

Common Requirements

Interconnect VPCs and their on-prem networks

Globally scale out connectivity across regions

Simplify network configuration

Challenges

Complex point-to-point peering does not scale

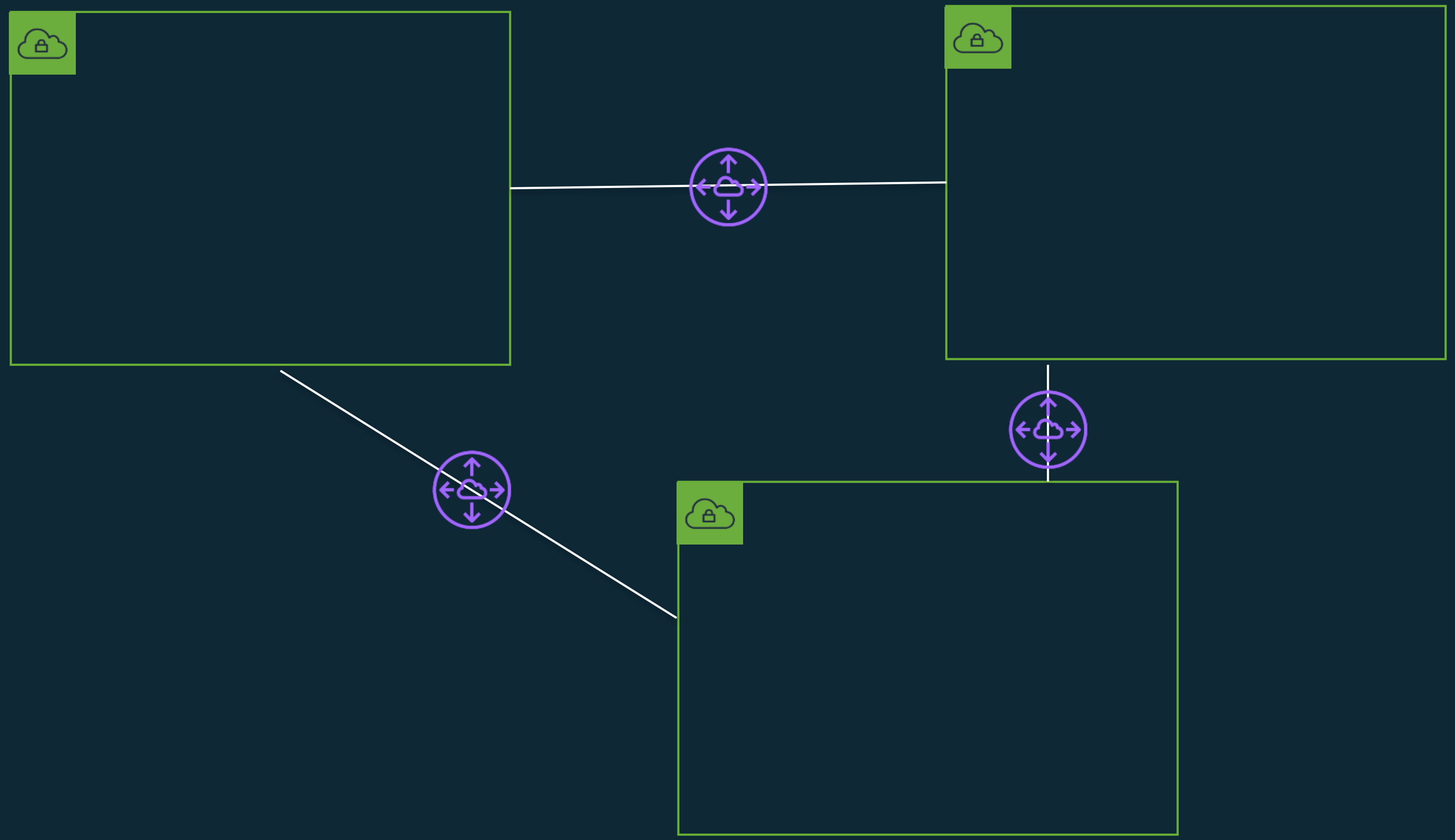
VPN Bandwidth limitations

Monitoring and Management of routing configurations is time consuming

VPC Connectivity Paradigms

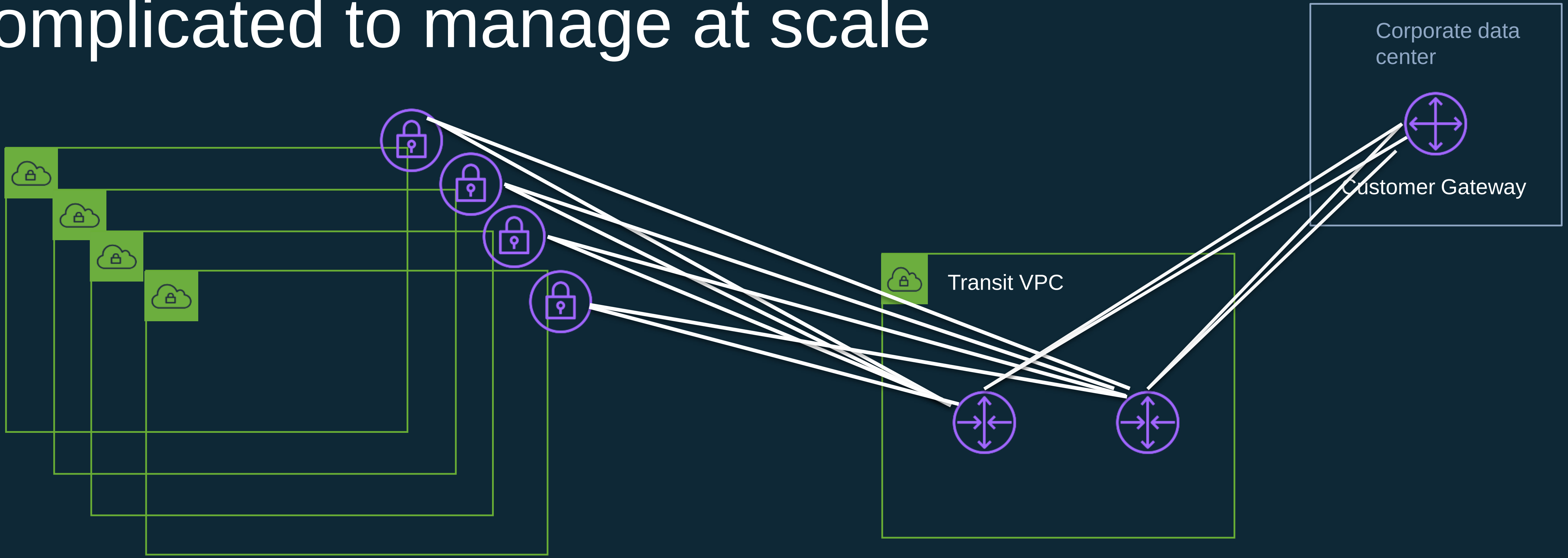
VPC Peering

- Point-to-point connection between VPCs in any region
- Up to 50 peering connections per VPC (can be increased to 125)
- Need full mesh, no transitive routing



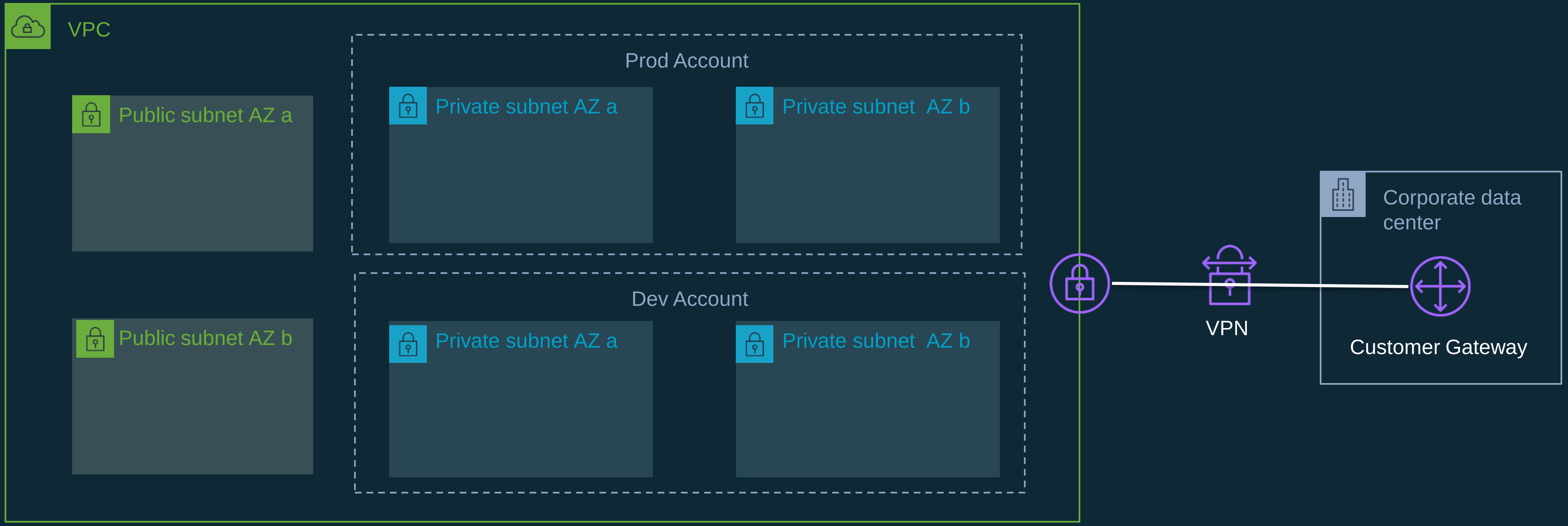
Transit VPC

- Routers in EC2
- More scalable then peering
- Can be complicated to manage at scale



VPC Sharing

- Share subnets across accounts with Resource Access Manager
- Limits (can be increased)
  - 100 Accounts per subnet
  - 100 shared subnets with an account



Inside Transit Gateway

AWS Transit Gateway: Key features

AWS Transit Gateway

Centralized routing polices across VPCs and on-premises

Scales to support thousands of VPCs across multi-accounts

Increase connectivity throughput with multiple VPN connections

Flexible segmentation and routing rules

Horizontally scalable

Simplified management

Transit Gateway Overview

Regional router

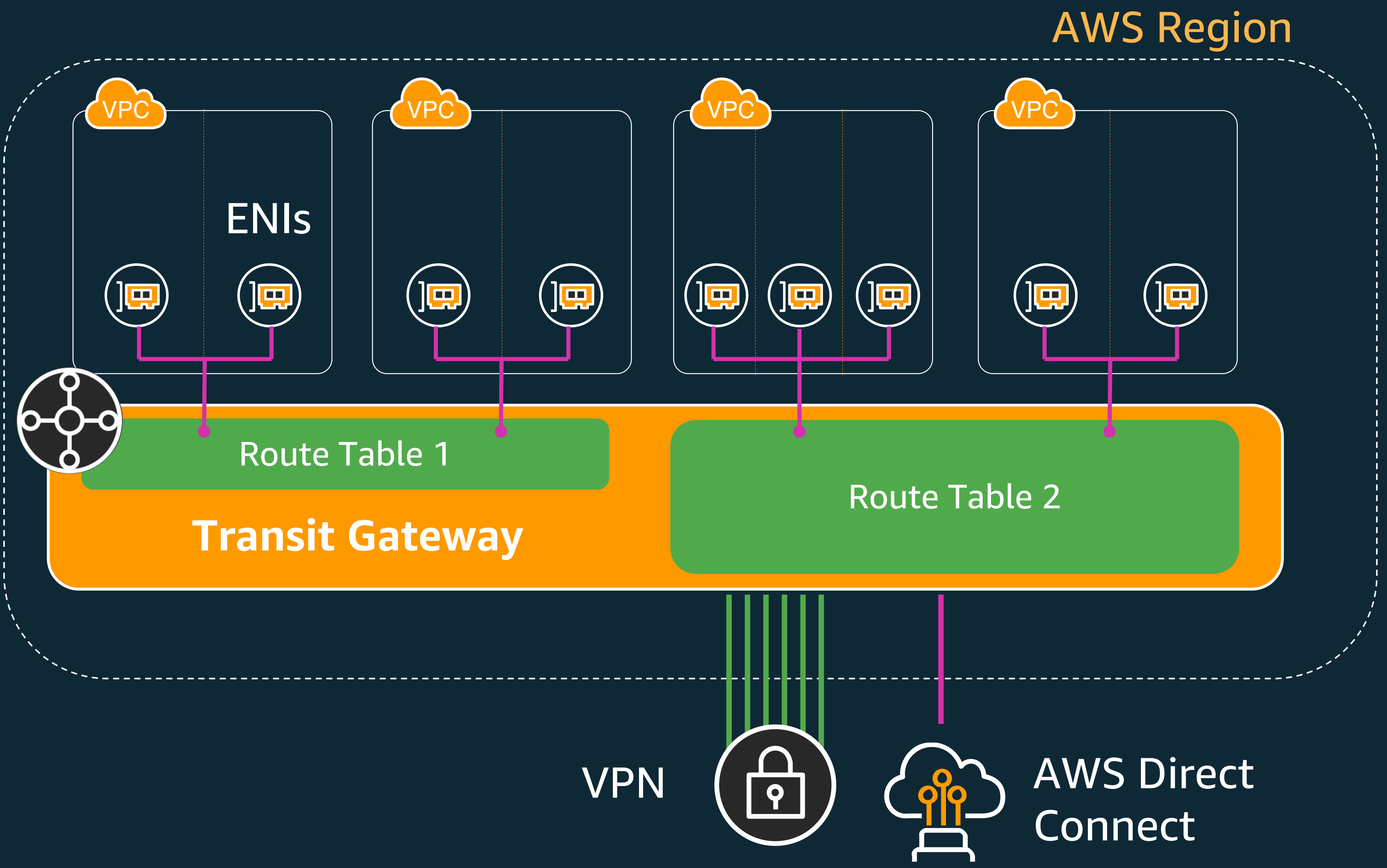
- Centralize VPN and AWS Direct Connect

Scalable

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

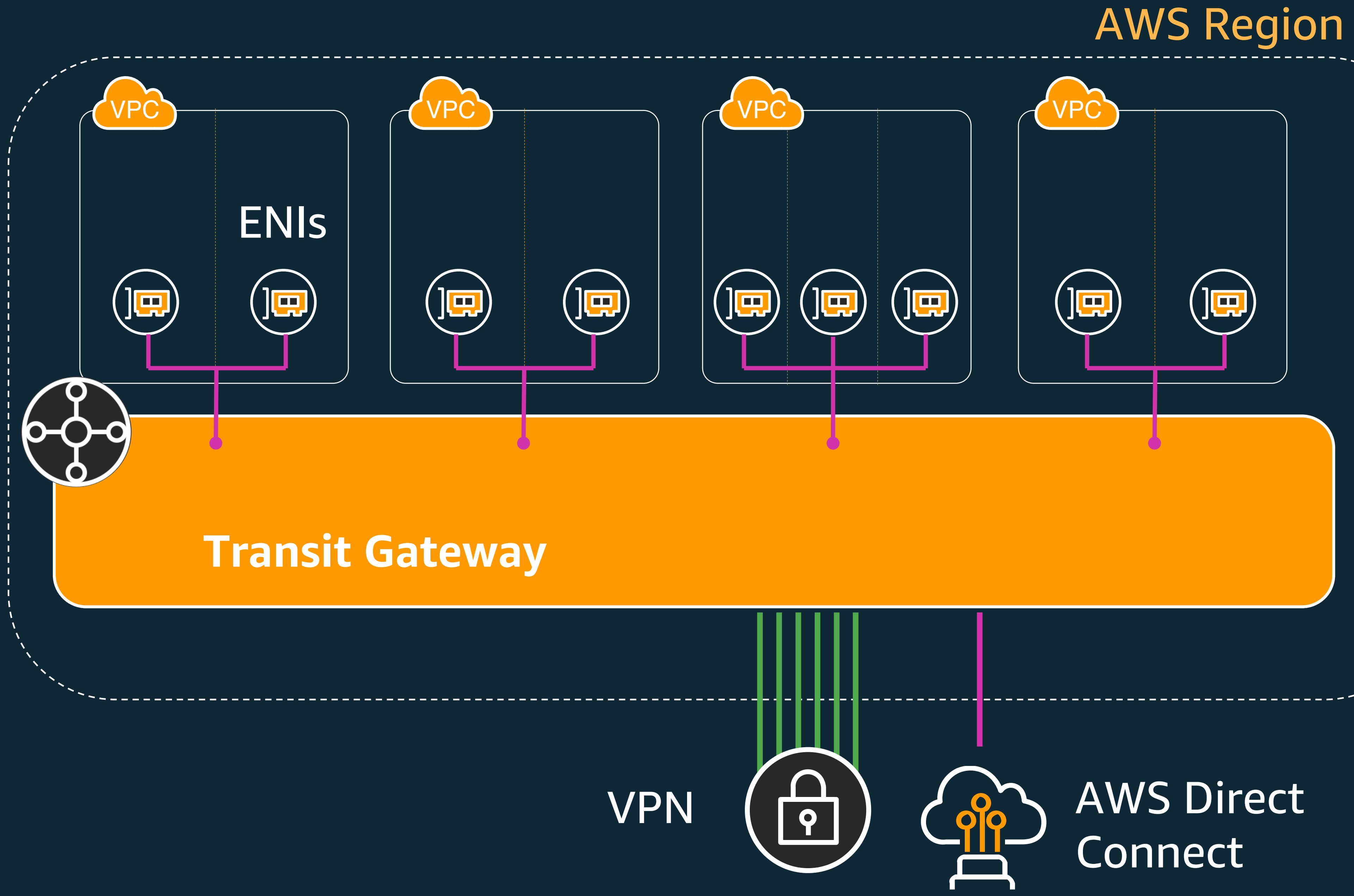
Flexible routing

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



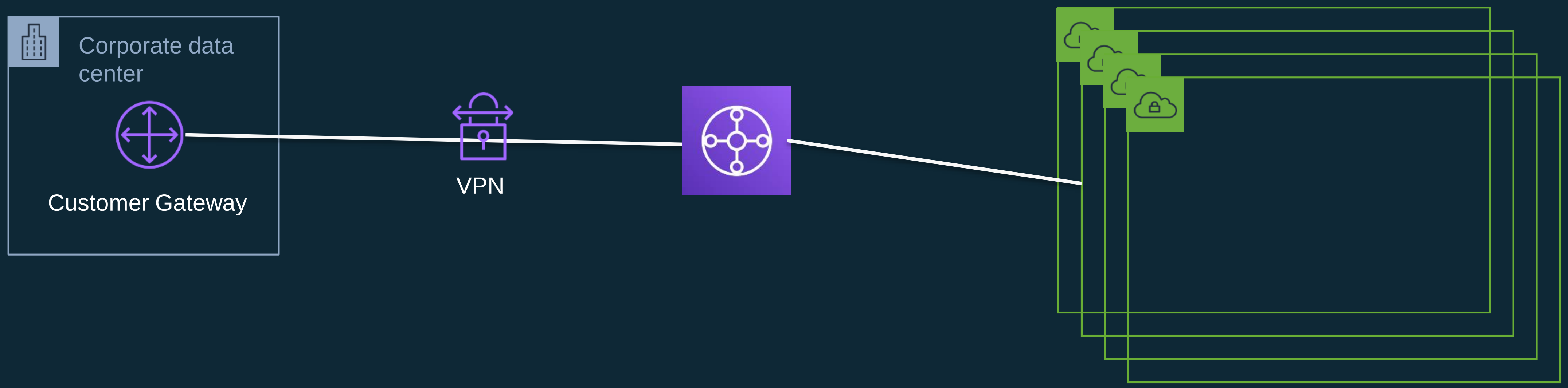
Transit Gateway Attachments

- VPC
- VPN
- Direct Connect

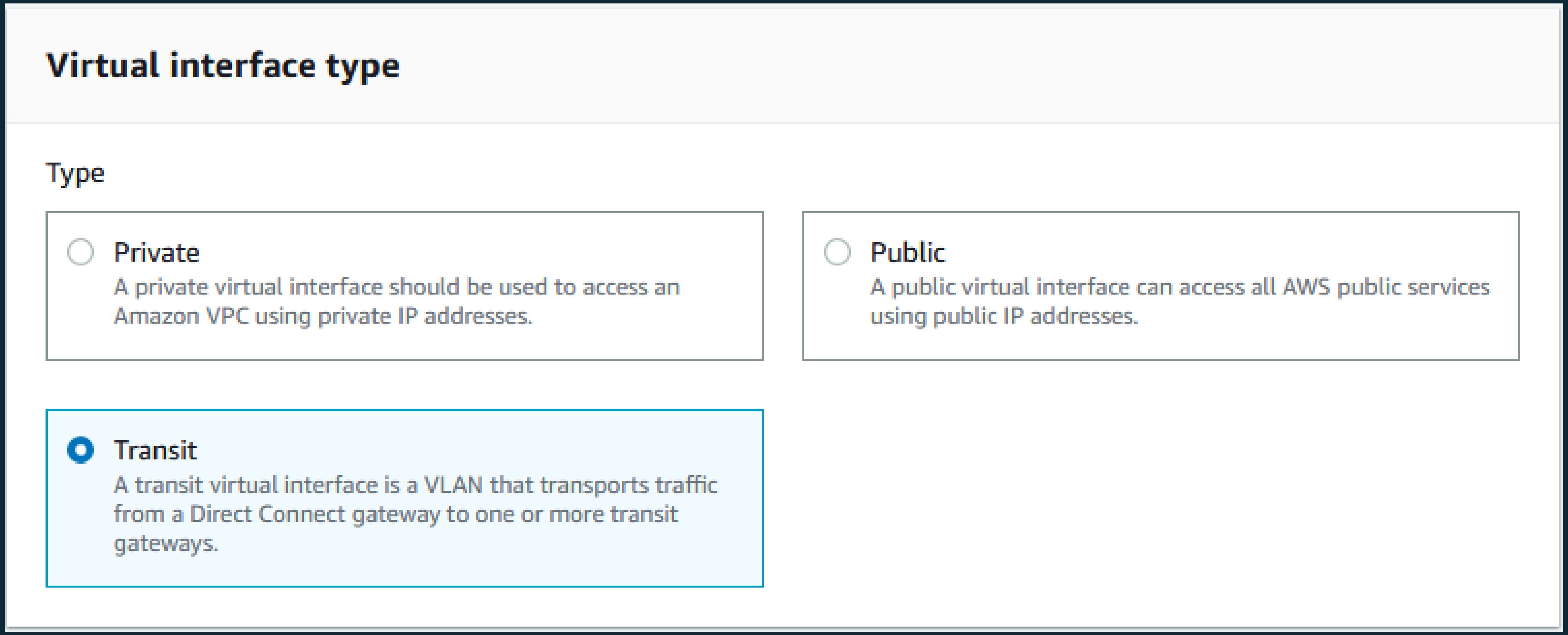


VPN Attachment

- ECMP support
  - Greater availability and throughput (1.25Gbps per VPN attachment)
  - Subject to on-premises customer gateway capabilities



Direct Connect Gateway – Transit VIF



Virtual interface type

Type

○ Private
A private virtual interface should be used to access an Amazon VPC using private IP addresses.

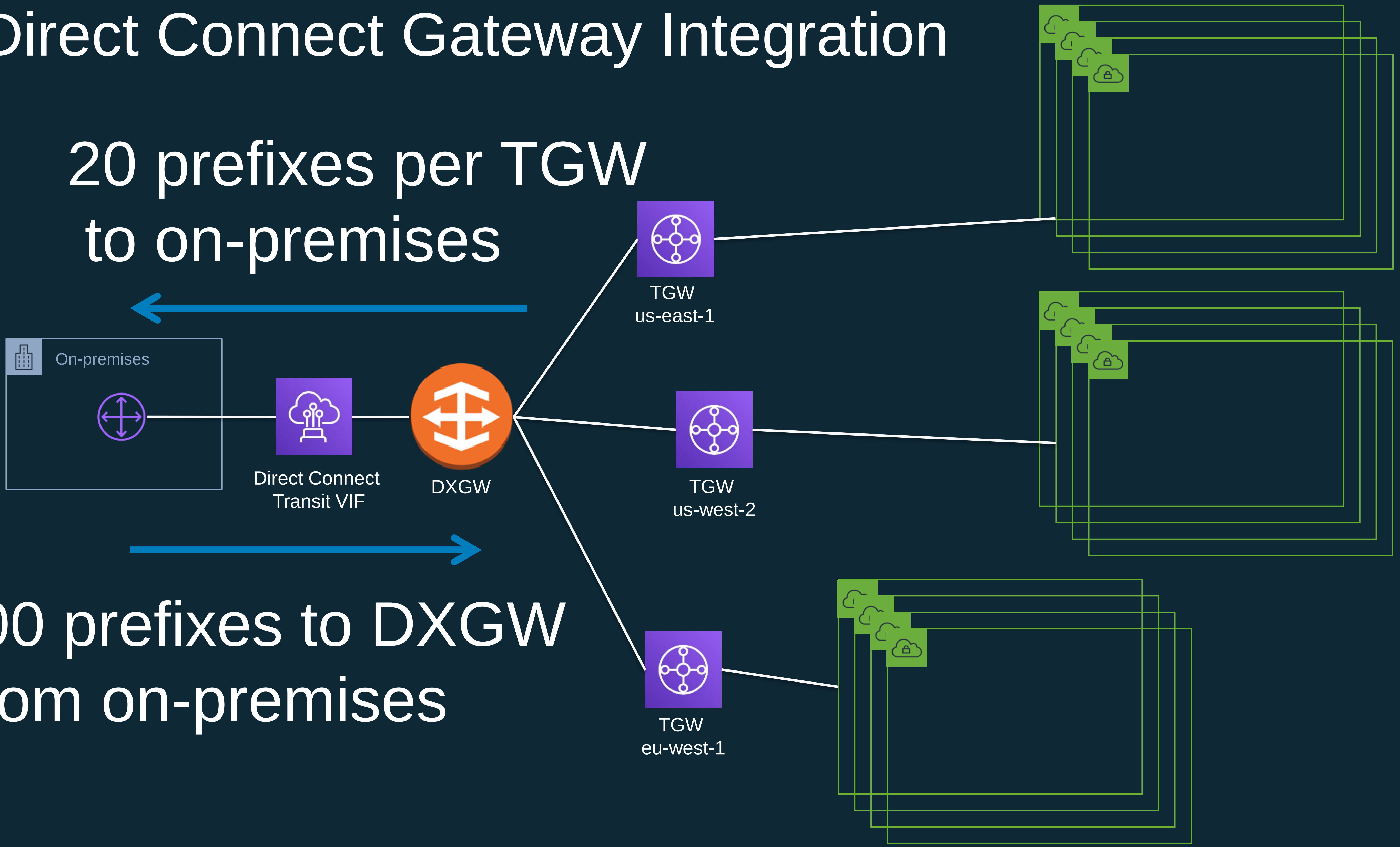
○ Public
A public virtual interface can access all AWS public services using public IP addresses.

● Transit
A transit virtual interface is a VLAN that transports traffic from a Direct Connect gateway to one or more transit gateways.

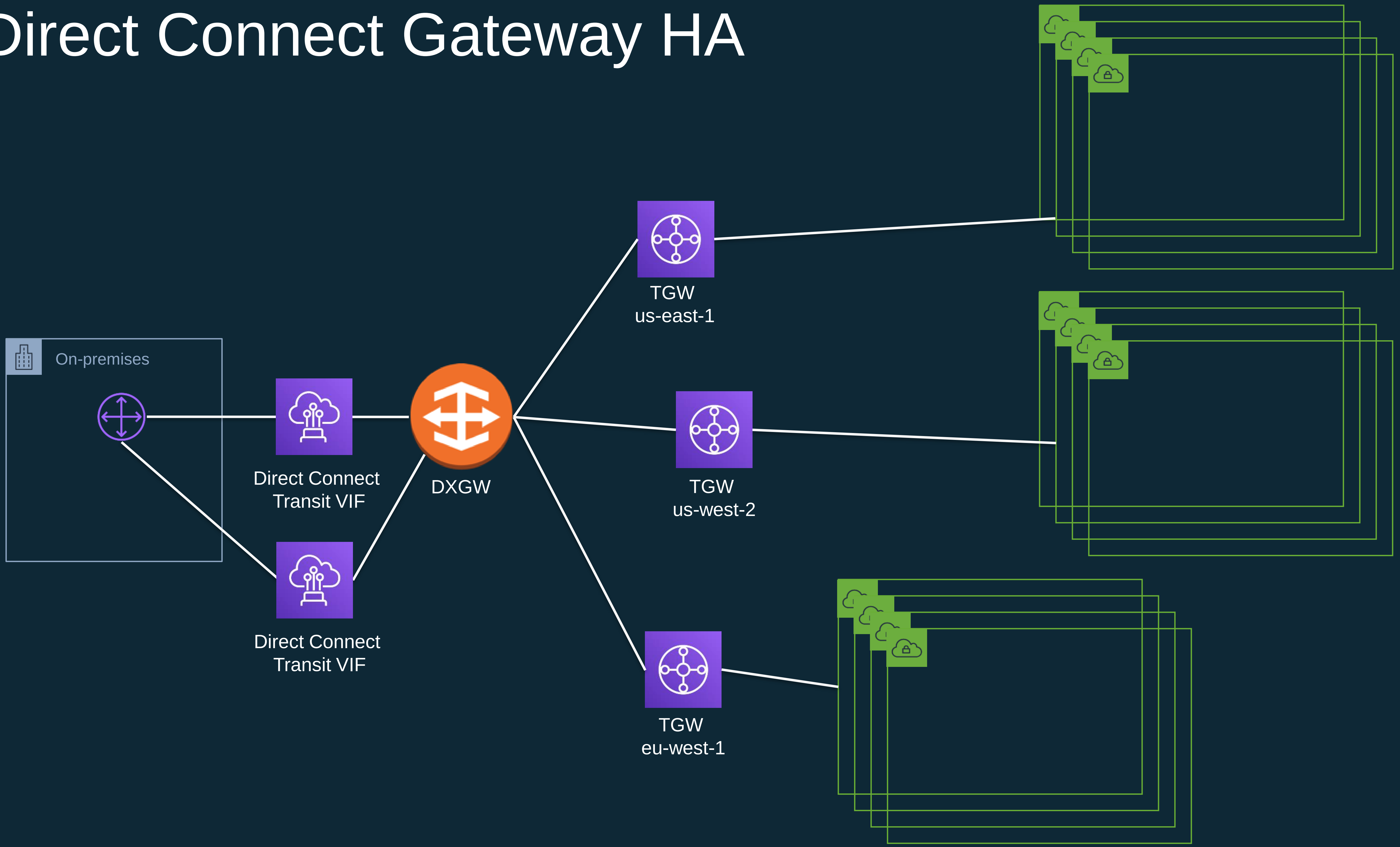
Direct Connect Gateway Integration

20 prefixes per TGW to on-premises

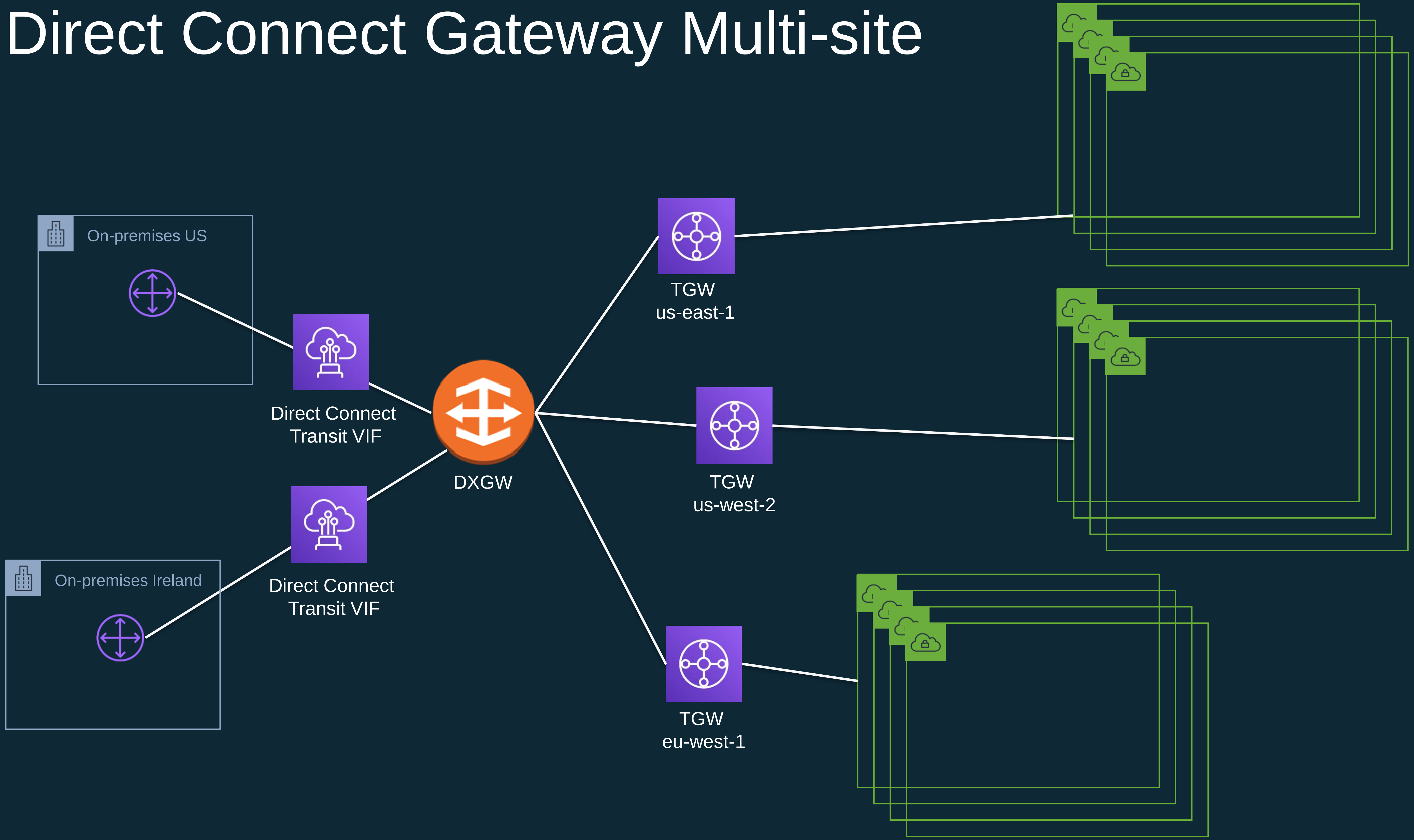
100 prefixes to DXGW from on-premises



Direct Connect Gateway HA

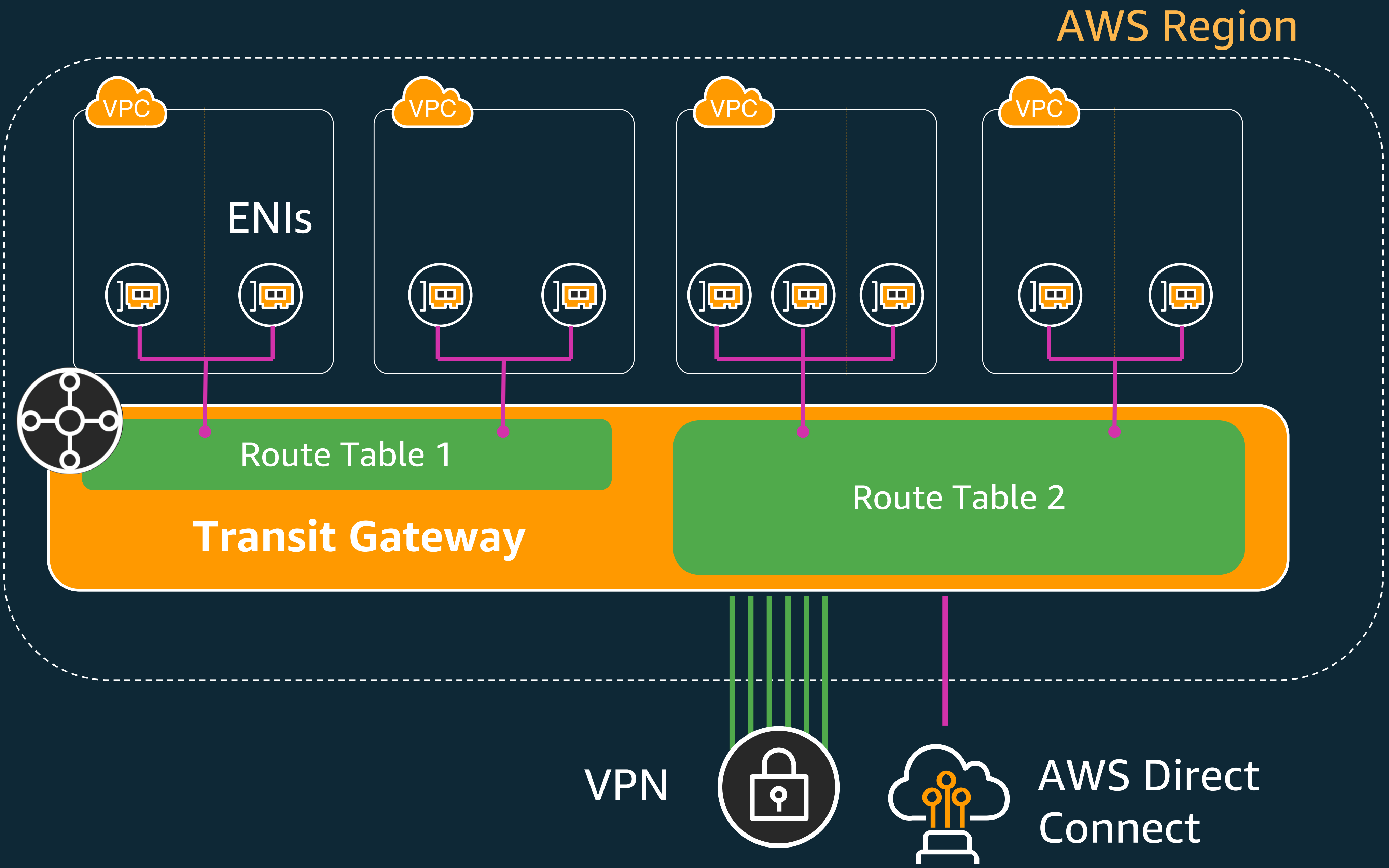


Direct Connect Gateway Multi-site



Transit Gateway Route Tables

- Control routing between attachments
- 20 route table limit per TGW
- Can have blackhole routes



Transit Gateway Path Selection Behavior

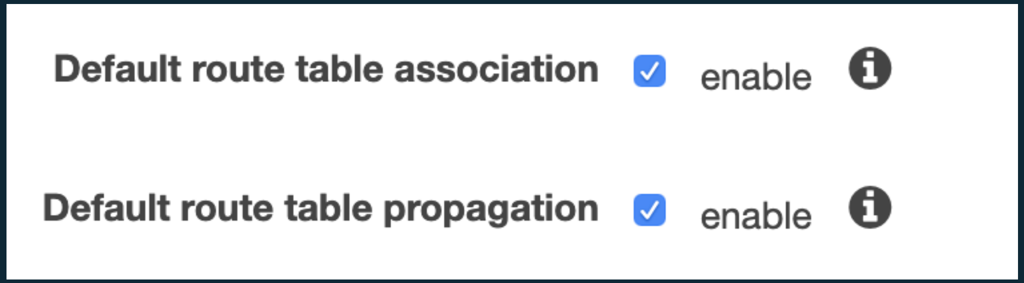
1. Most Specific Route / Longest Prefix Match
2. Static route entries, including static Site-to-Site VPN routes
3. VPC propagated routes
4. BGP propagated routes from AWS Direct Connect gateway
5. BGP propagated routes from AWS Site-to-Site VPN

Notes on ASNs

- Private ASN are used with DXGW, TGW, and VPNs
- Each TGW should have a unique ASN (if you want to connect them)
- DXGW and TGW require unique ASNs

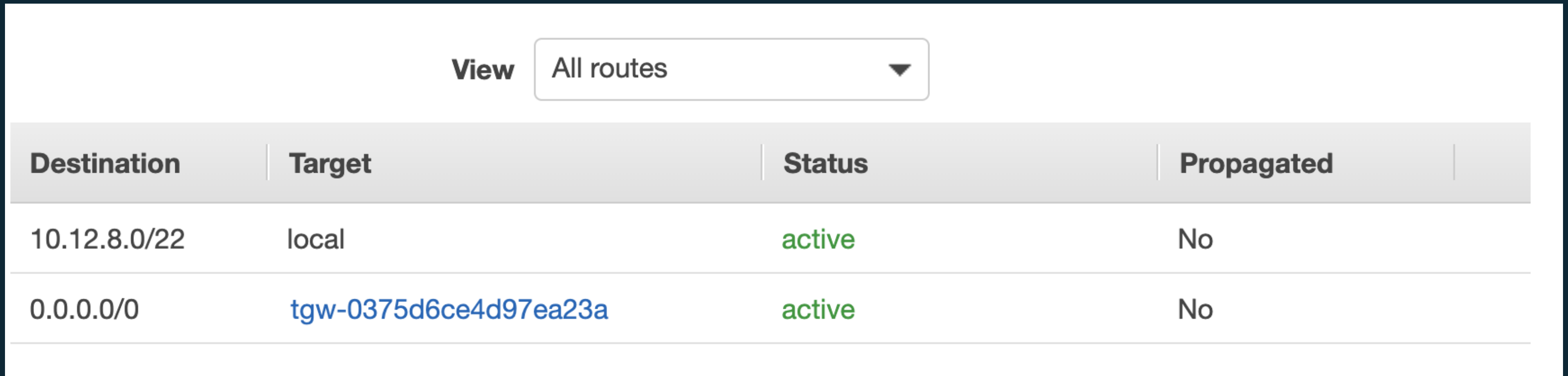
Propagations

- By default learned routes are propagated to TGW route table
- Routes don't propagate to VPC route table (can use default route to TGW)



Default route table association ☑ enable

Default route table propagation ☑ enable

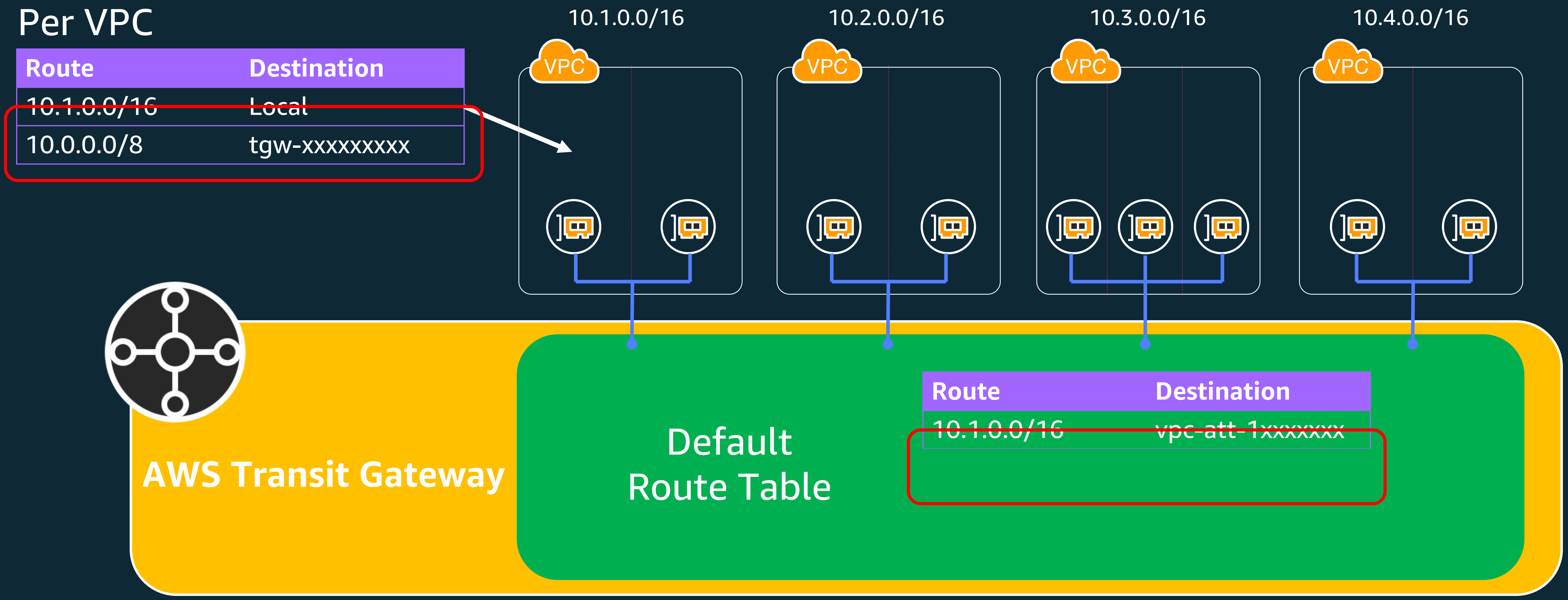


View: All routes

Destination	Target	Status	Propagated
10.12.8.0/22	local	active	No
0.0.0.0/0	tgw-0375d6ce4d97ea23a	active	No

Transit Gateway Data Flows

Flat Network

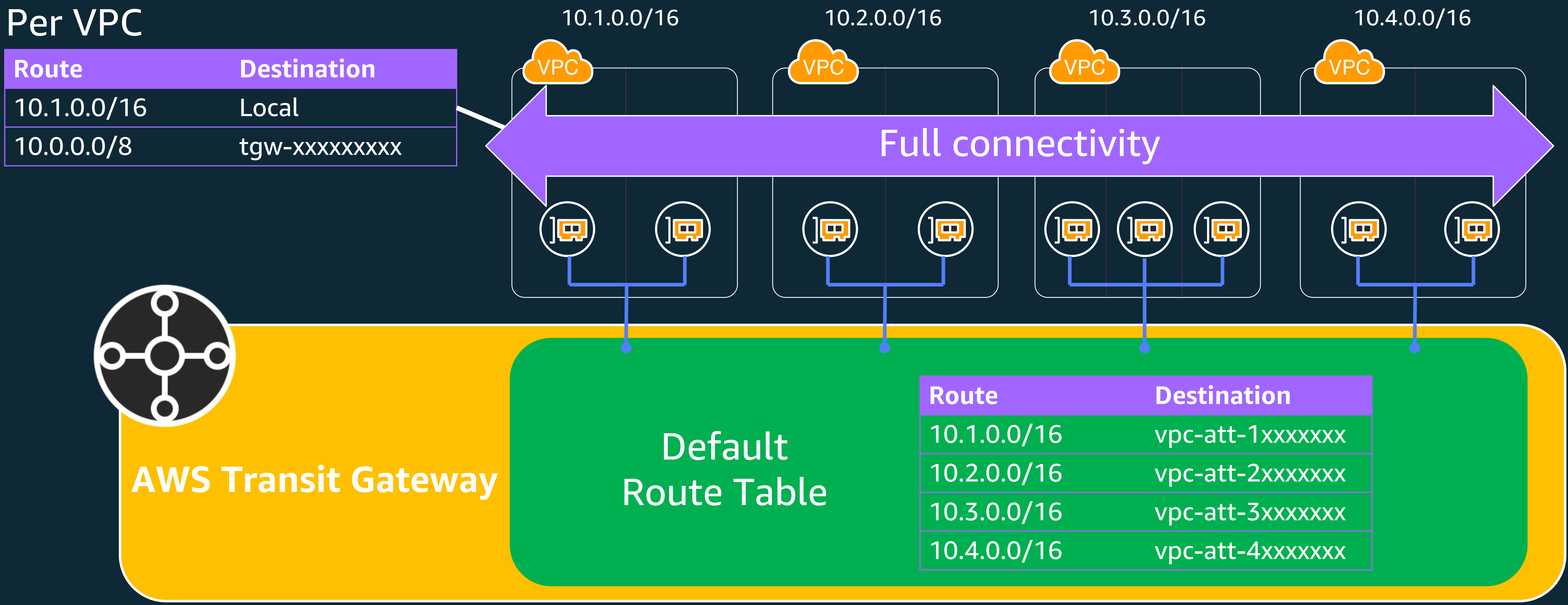


Per VPC

Route	Destination
10.1.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx

Route	Destination
10.1.0.0/16	vpc-att-1xxxxxxx

Flat Network

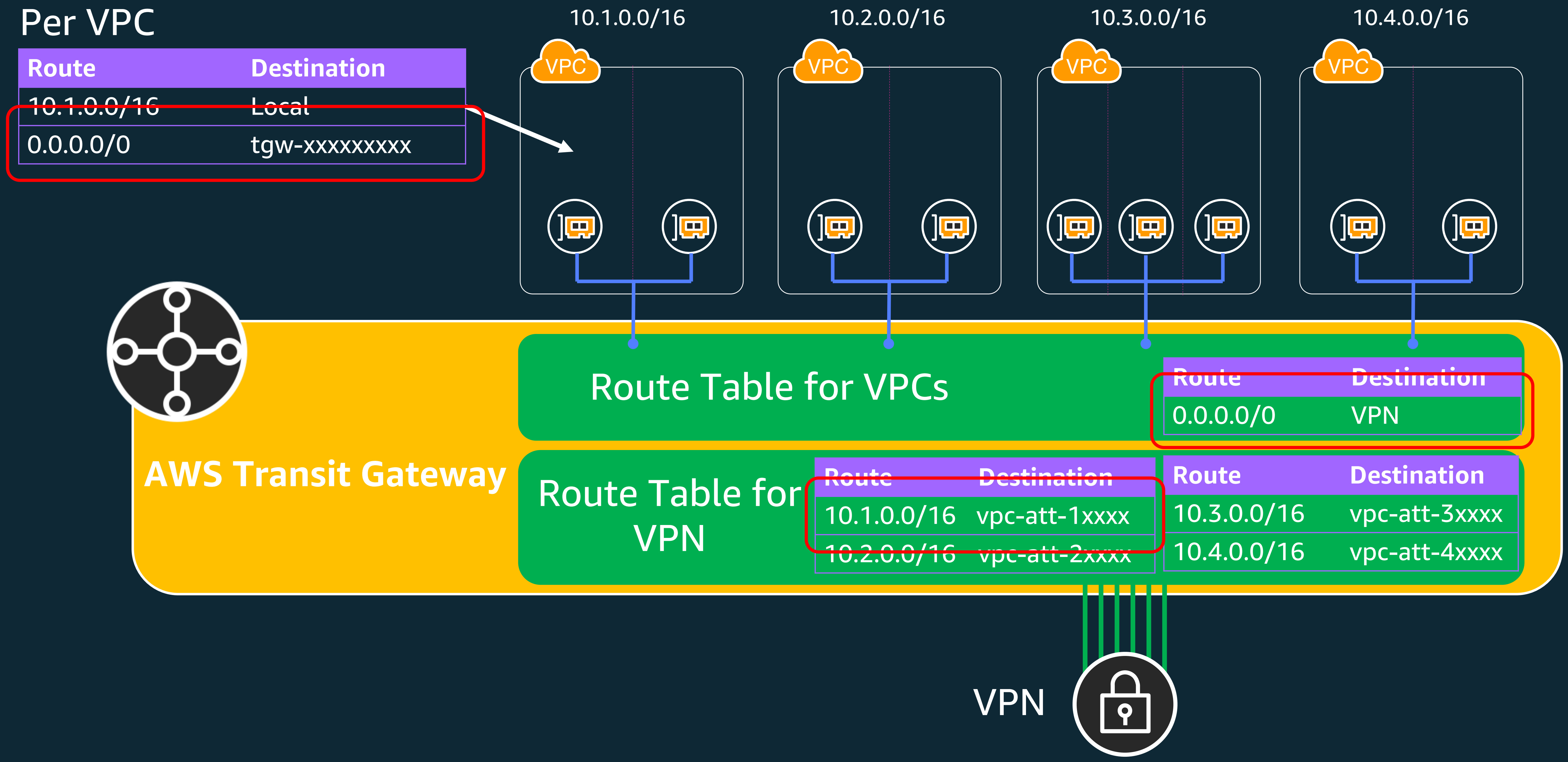


Per VPC

Route	Destination
10.1.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx

Route	Destination
10.1.0.0/16	vpc-att-1xxxxxxx
10.2.0.0/16	vpc-att-2xxxxxxx
10.3.0.0/16	vpc-att-3xxxxxxx
10.4.0.0/16	vpc-att-4xxxxxxx

Segmented Network



Per VPC

Route	Destination
10.1.0.0/16	Local
0.0.0.0/0	tgw-xxxxxxxxx

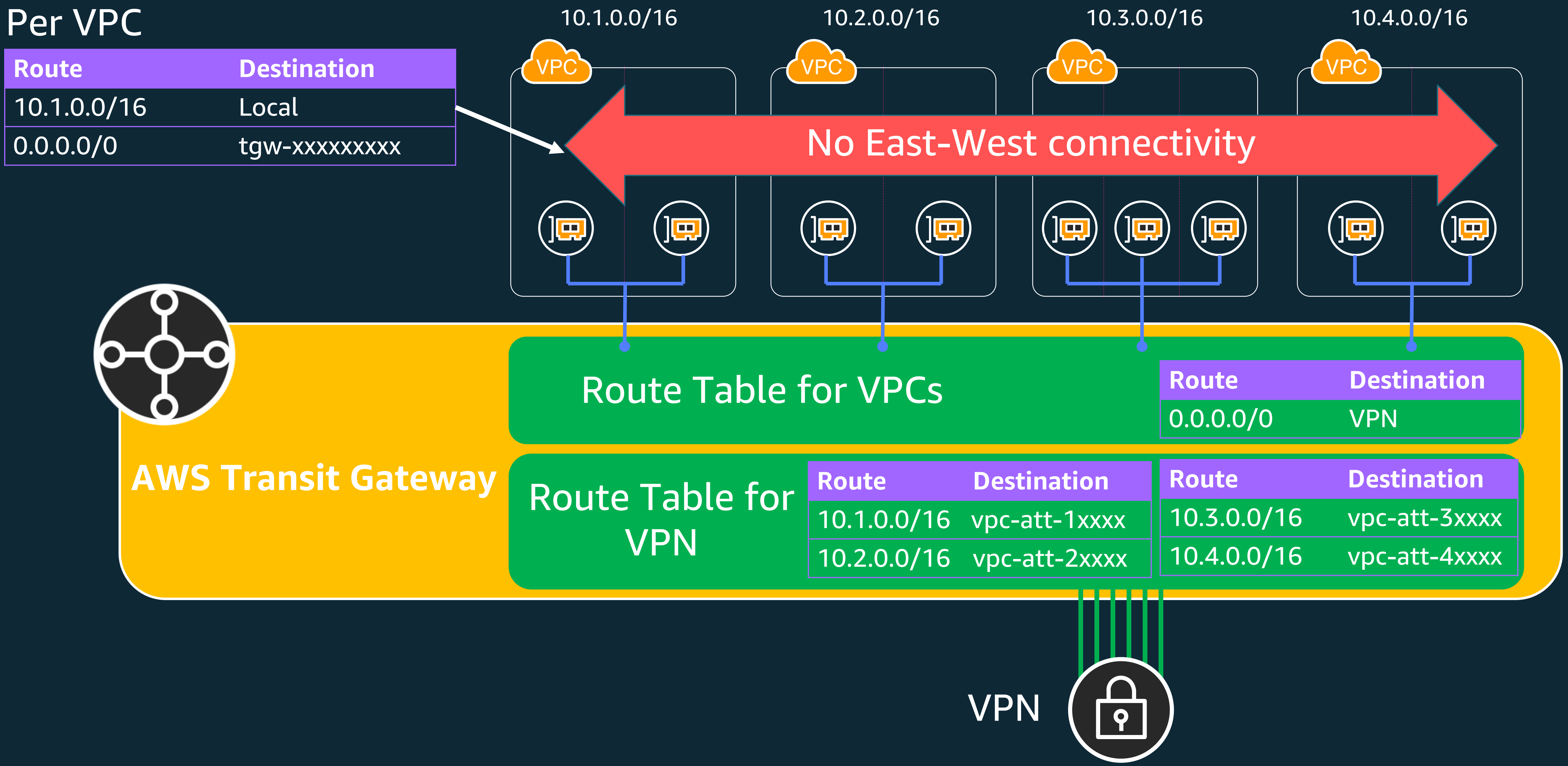
Route Table for VPCs

Route	Destination
0.0.0.0/0	VPN

Route Table for VPN

Route	Destination
10.1.0.0/16	vpc-att-1xxxx
10.2.0.0/16	vpc-att-2xxxx
10.3.0.0/16	vpc-att-3xxxx
10.4.0.0/16	vpc-att-4xxxx

Segmented Network



Per VPC

Route	Destination
10.1.0.0/16	Local
0.0.0.0/0	tgw-xxxxxxxxx

Route Table for VPCs

Route	Destination
0.0.0.0/0	VPN

Route Table for VPN

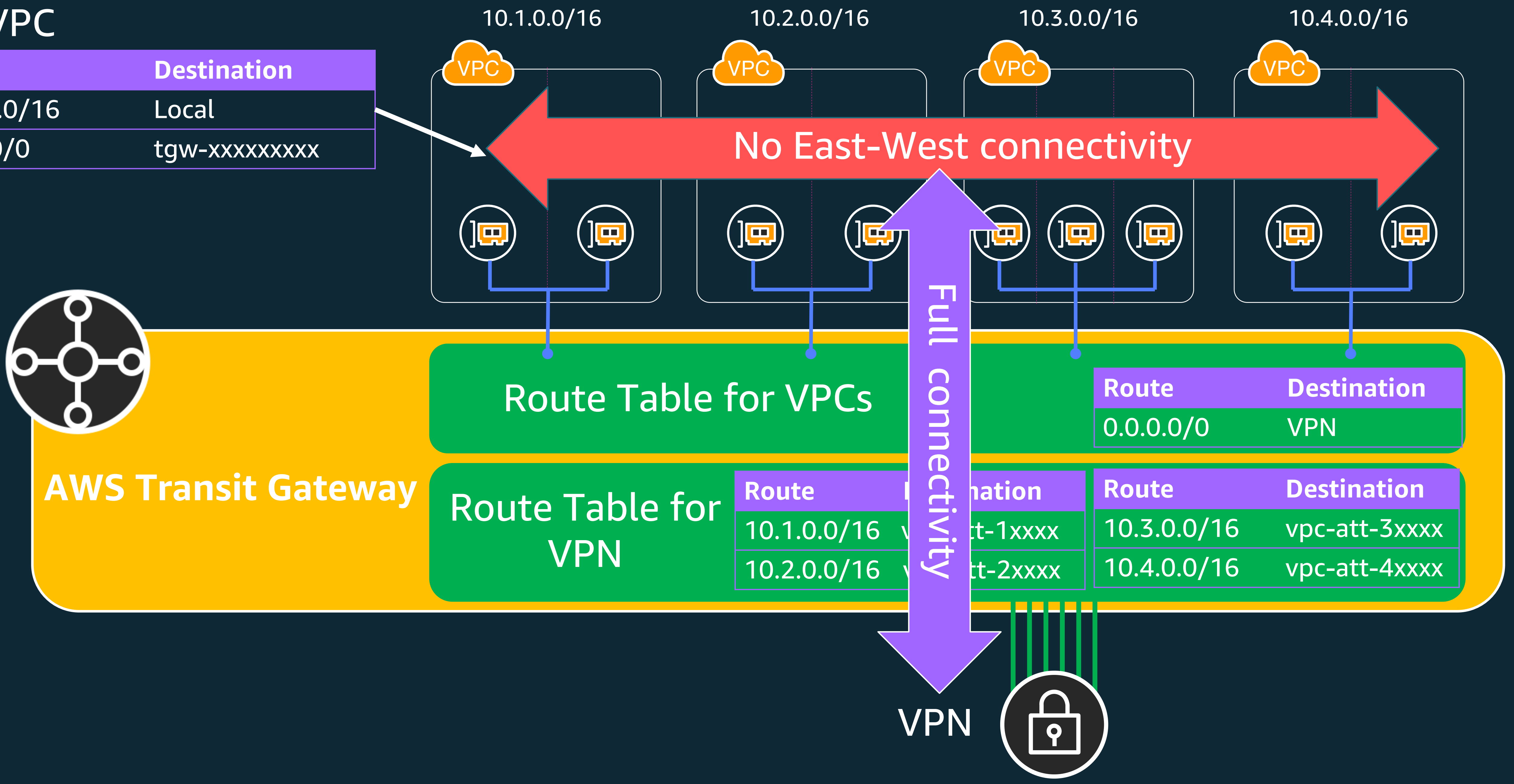
Route	Destination
10.1.0.0/16	vpc-att-1xxxx
10.2.0.0/16	vpc-att-2xxxx

Route	Destination
10.3.0.0/16	vpc-att-3xxxx
10.4.0.0/16	vpc-att-4xxxx

Segmented Network

Per VPC

Route	Destination
10.1.0.0/16	Local
0.0.0.0/0	tgw-xxxxxxxxx



Route	Destination
0.0.0.0/0	VPN

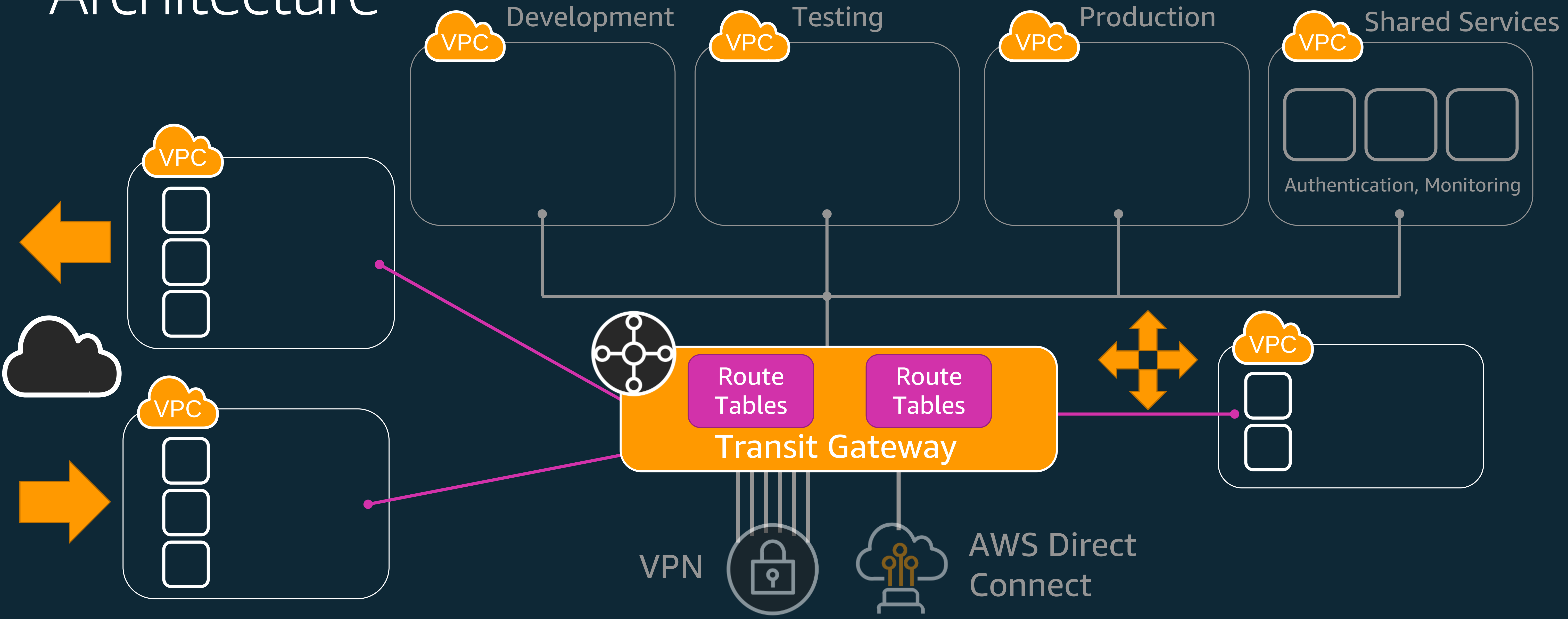
Route	I nation
10.1.0.0/16	v tt-1xxxx
10.2.0.0/16	v tt-2xxxx

Route	Destination
10.3.0.0/16	vpc-att-3xxxx
10.4.0.0/16	vpc-att-4xxxx

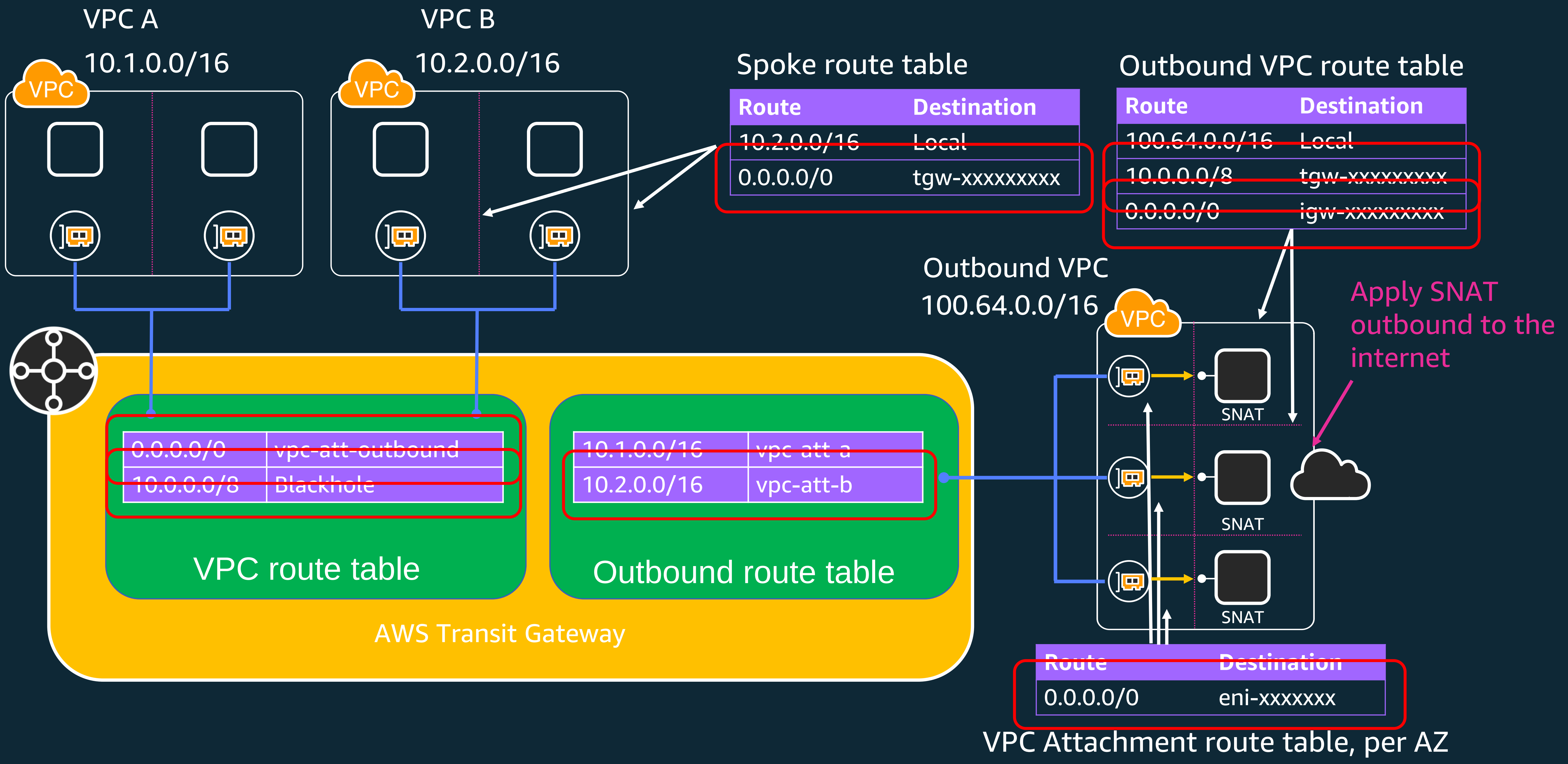
Transit Gateway Reference Architectures

Reference Network Architecture

Optional Network Services



Centralized NAT



VPC A

10.1.0.0/16

VPC B

10.2.0.0/16

Spoke route table

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

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

Outbound VPC

100.64.0.0/16

Apply SNAT outbound to the internet

0.0.0.0/0	vpc-att-outbound
10.0.0.0/8	Blackhole

VPC route table

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

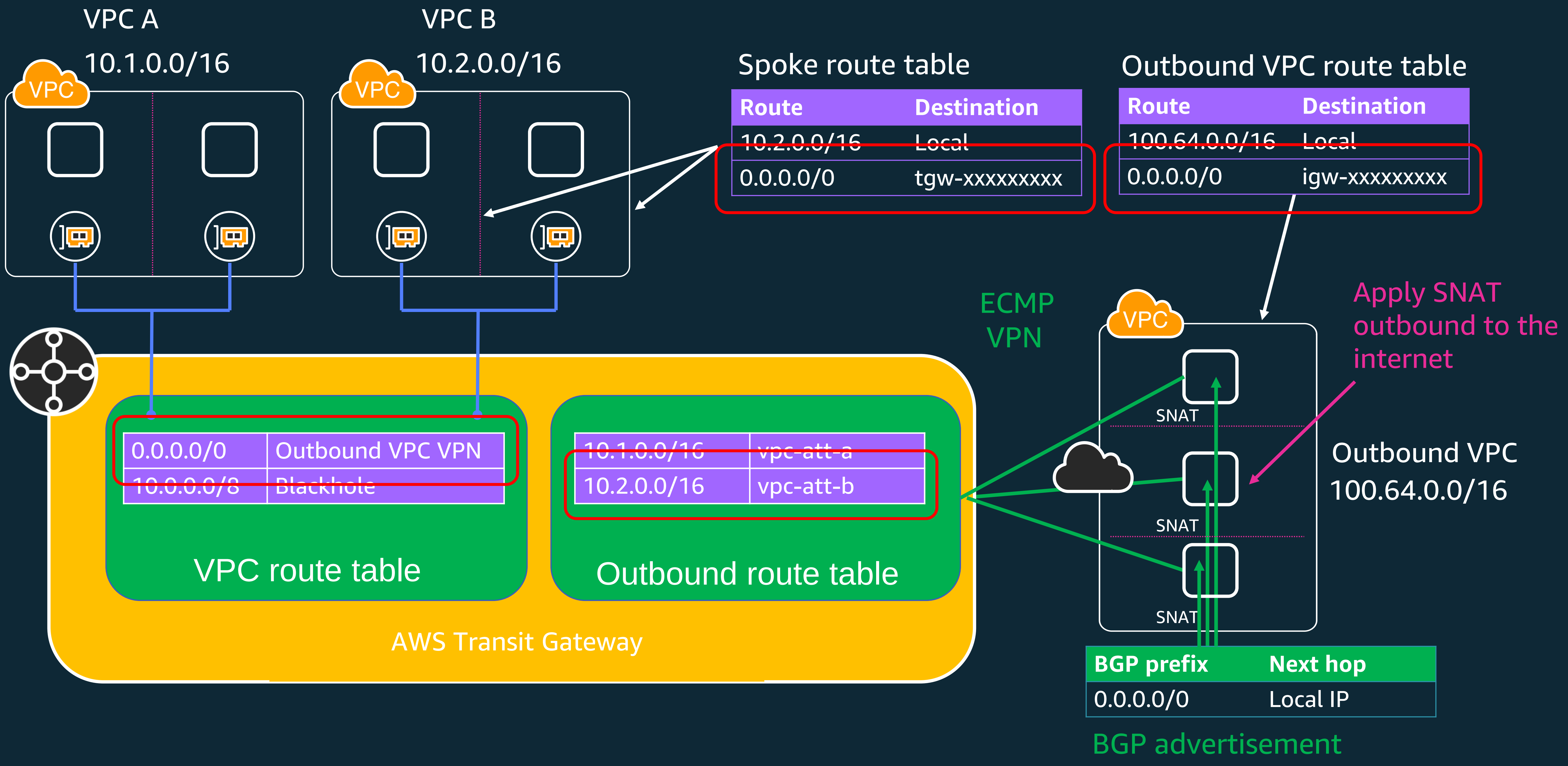
Outbound route table

AWS Transit Gateway

Route	Destination
0.0.0.0/0	eni-xxxxxxx

VPC Attachment route table, per AZ

Centralized NAT



Spoke route table

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

Outbound VPC route table

Route	Destination
100.64.0.0/16	Local
0.0.0.0/0	igw-xxxxxxxxx

VPC route table

0.0.0.0/0	Outbound VPC VPN
10.0.0.0/8	Blackhole

Outbound route table

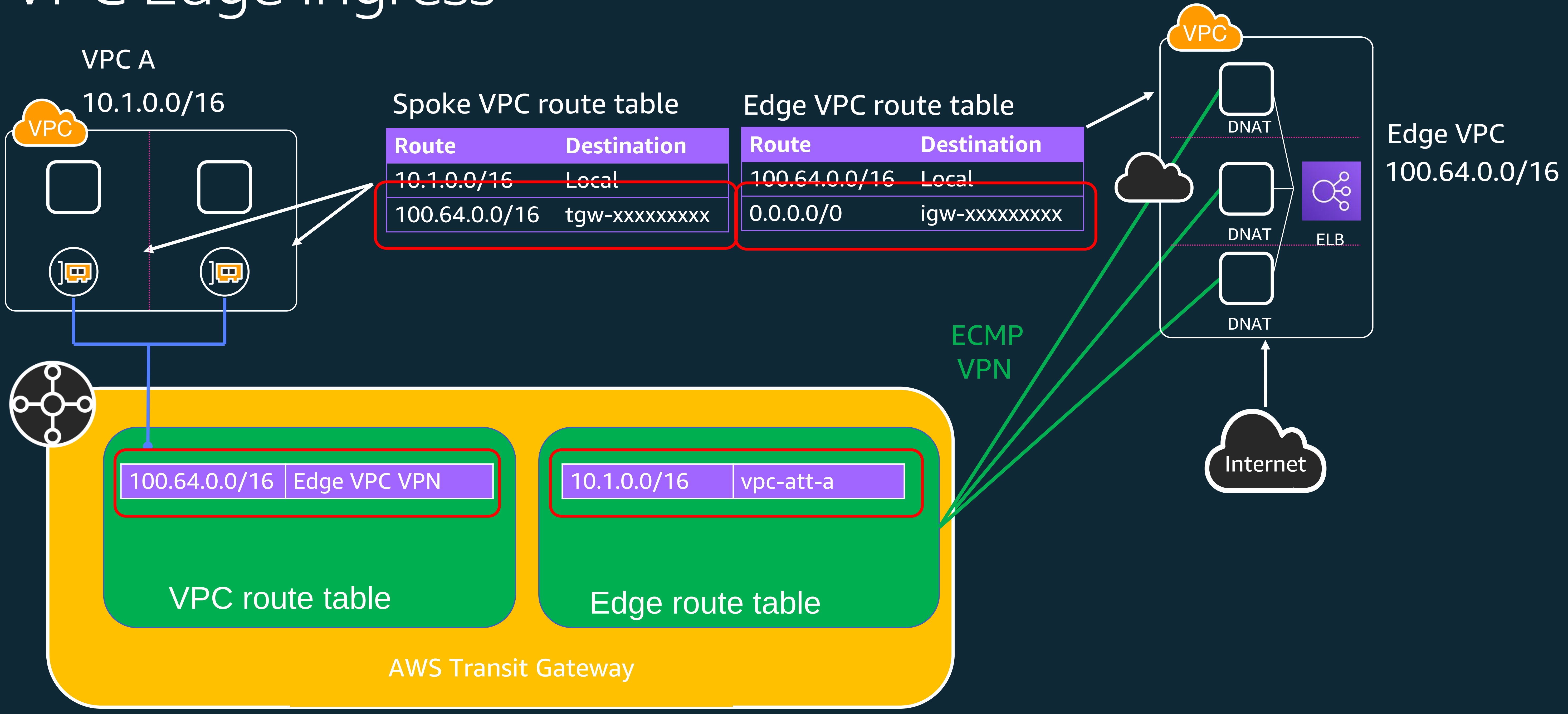
10.1.0.0/16	vpc-att-a
10.2.0.0/16	vpc-att-b

BGP advertisement

BGP prefix	Next hop
0.0.0.0/0	Local IP

VPC Edge Ingress

BGP prefix	Next hop
100.64.0.0/16	Local IP



Spoke VPC route table

Route	Destination
10.1.0.0/16	Local
100.64.0.0/16	tgw-xxxxxxxxx

Edge VPC route table

Route	Destination
100.64.0.0/16	Local
0.0.0.0/0	igw-xxxxxxxxx

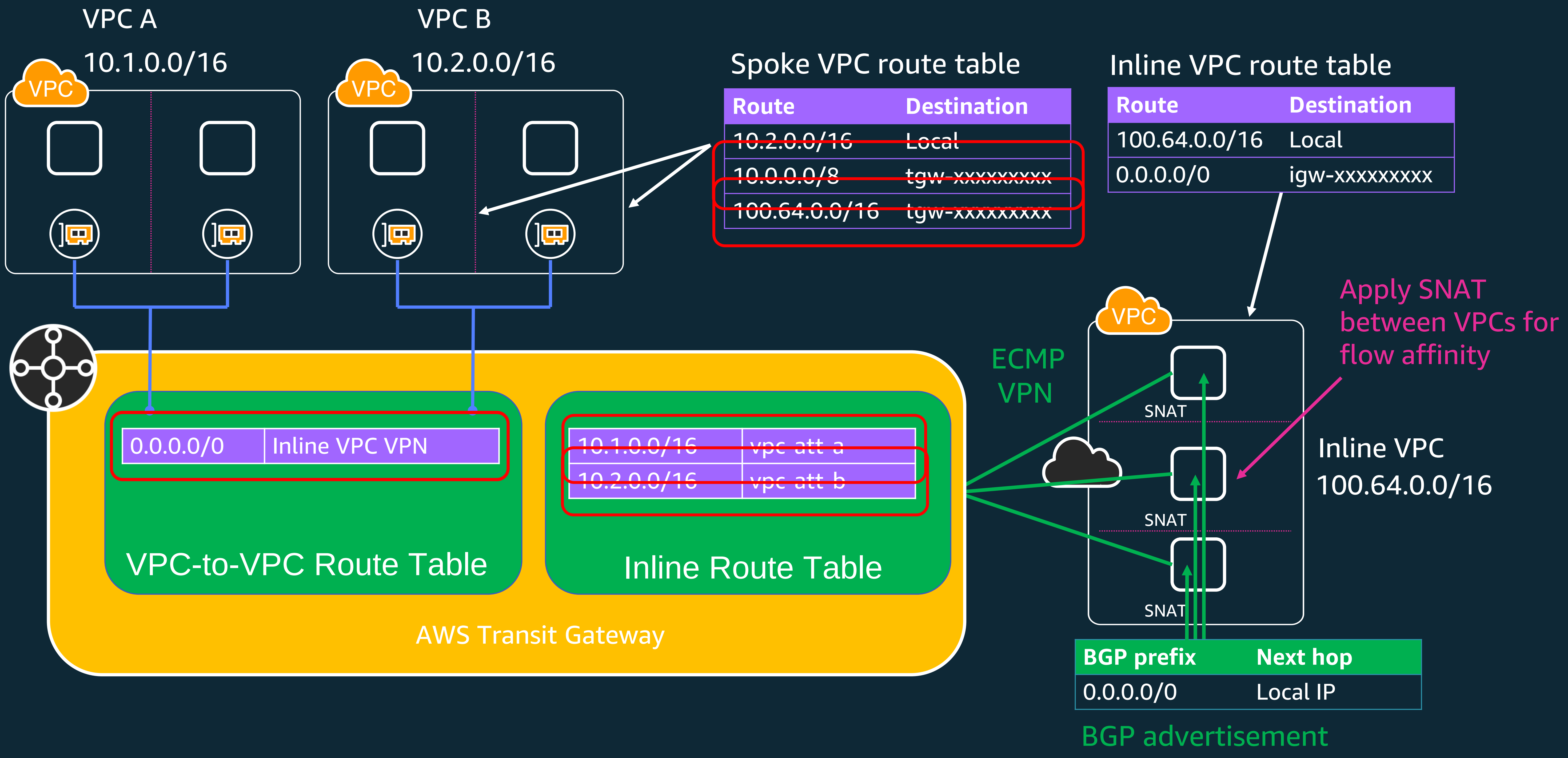
VPC route table

100.64.0.0/16	Edge VPC VPN

Edge route table

10.1.0.0/16	vpc-att-a

VPC to VPC Inspection



Spoke VPC route table

Route	Destination
10.2.0.0/16	Local
10.0.0.0/8	tgw-xxxxxxxxx
100.64.0.0/16	tgw-xxxxxxxxx

Inline VPC route table

Route	Destination
100.64.0.0/16	Local
0.0.0.0/0	igw-xxxxxxxxx

VPC-to-VPC Route Table

0.0.0.0/0	Inline VPC VPN

Inline Route Table

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

Apply SNAT between VPCs for flow affinity

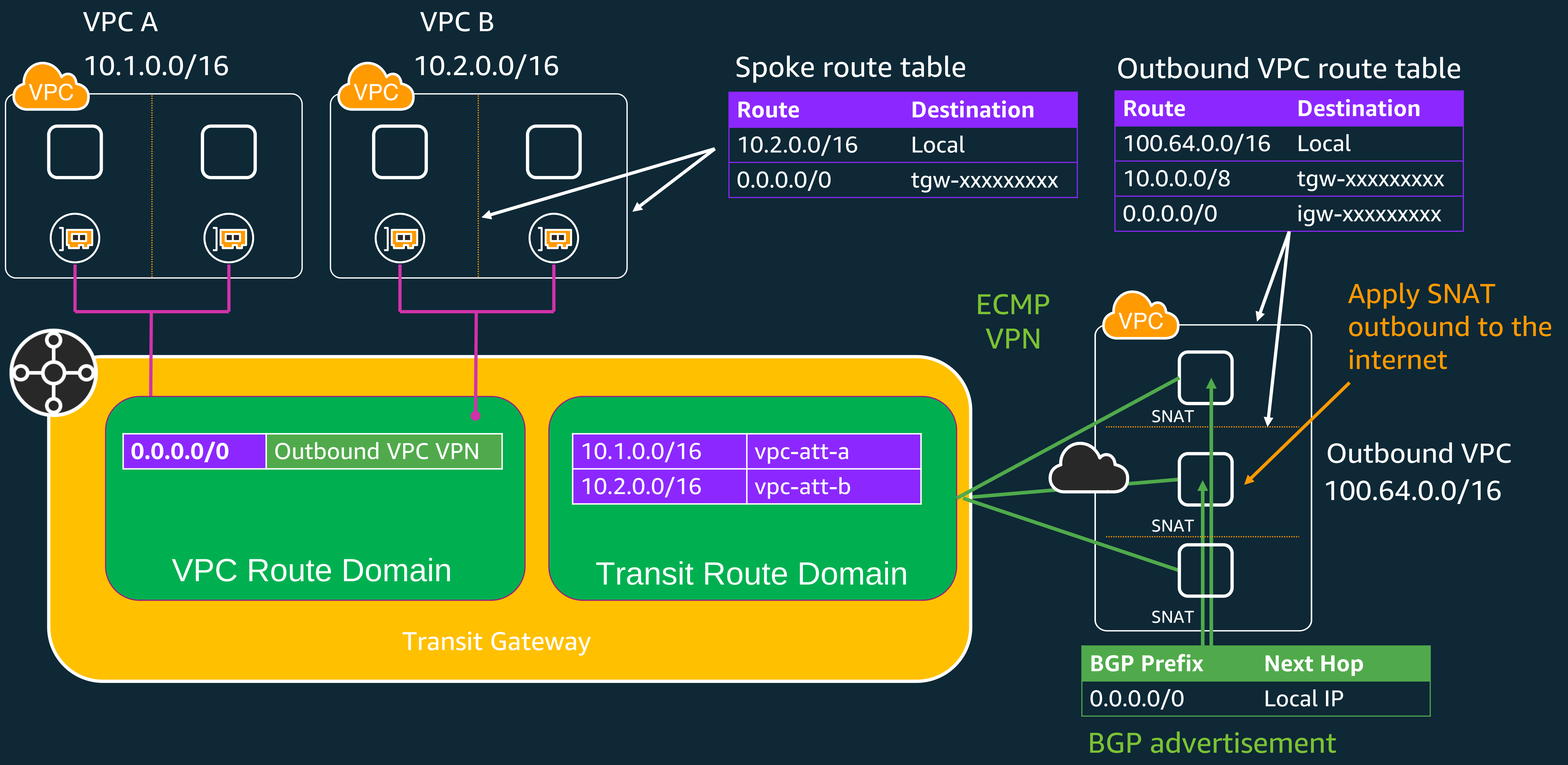
BGP prefix	Next hop
0.0.0.0/0	Local IP

BGP advertisement

Outbound VPC Services

Use Cases:

URL filtering, NAT gateway, Data-loss Prevention (DLP), Web proxy services



Spoke route table

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

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

0.0.0.0/0	Outbound VPC VPN

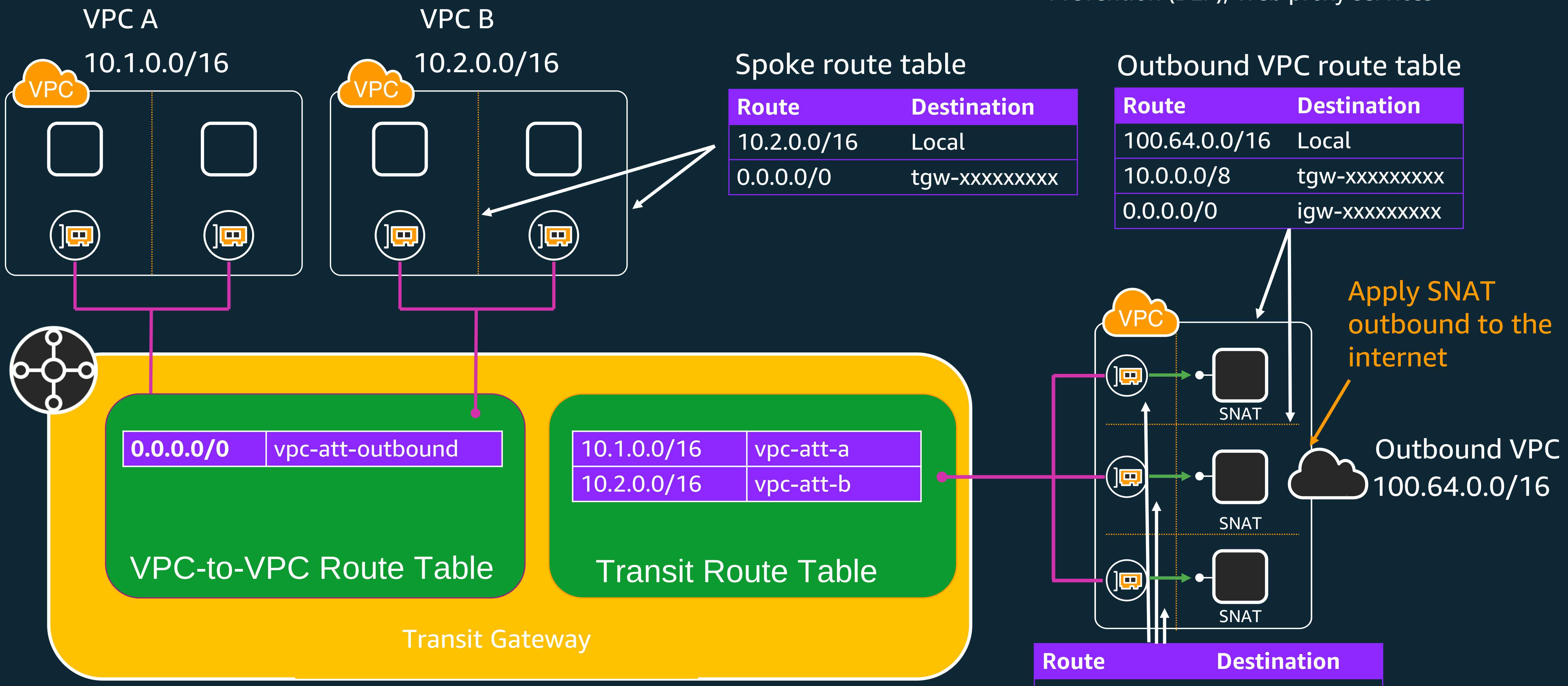
10.1.0.0/16	vpc-att-a
10.2.0.0/16	vpc-att-b

BGP Prefix	Next Hop
0.0.0.0/0	Local IP

Outbound VPC Services – No VPN

Use Cases:

URL filtering, NAT gateway, Data-loss Prevention (DLP), Web proxy services



Apply SNAT outbound to the internet

Spoke route table

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

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

VPC-to-VPC Route Table

0.0.0.0/0	vpc-att-outbound

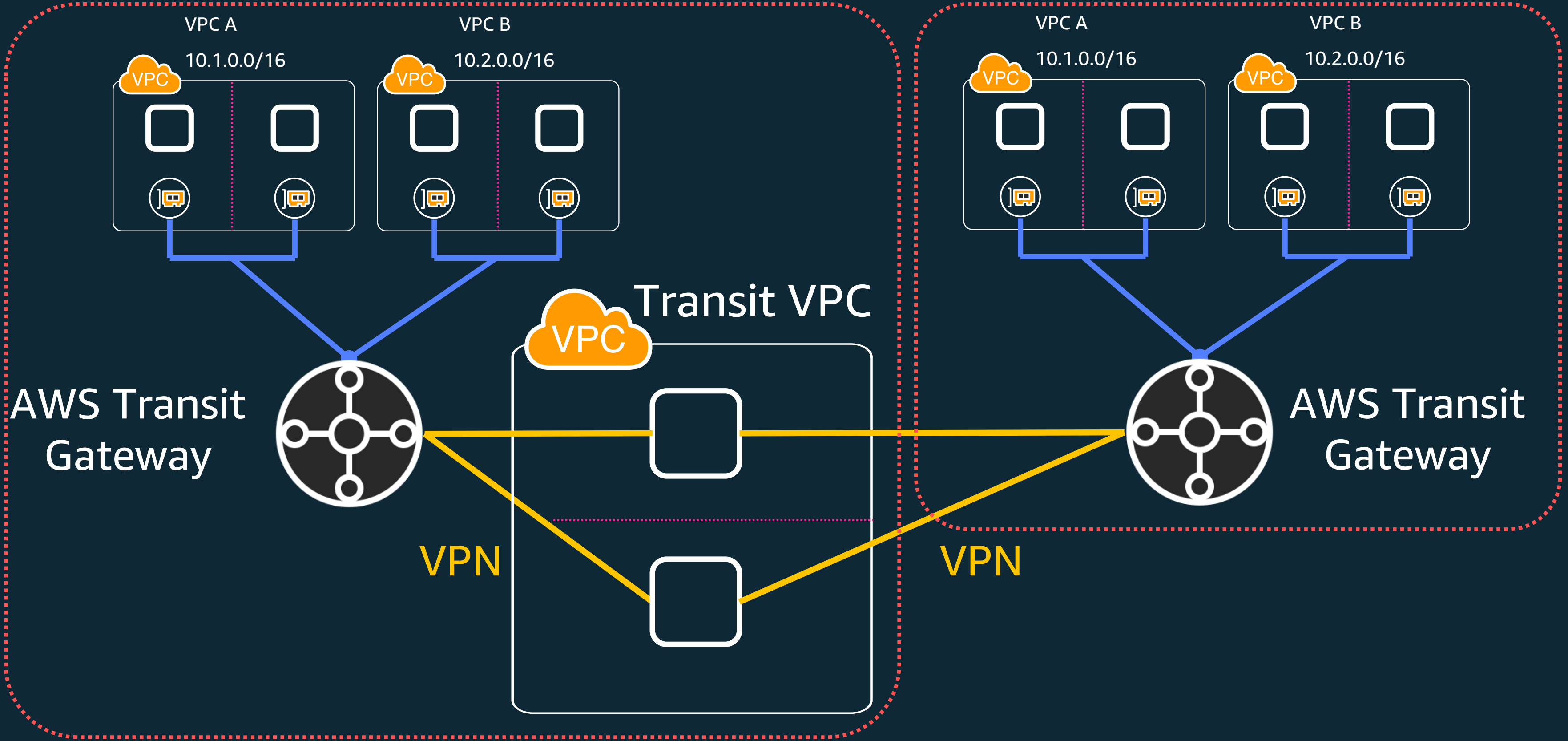
Transit Route Table

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

Route	Destination
0.0.0.0/0	eni-xxxxxxx

Ingress route table, per AZ

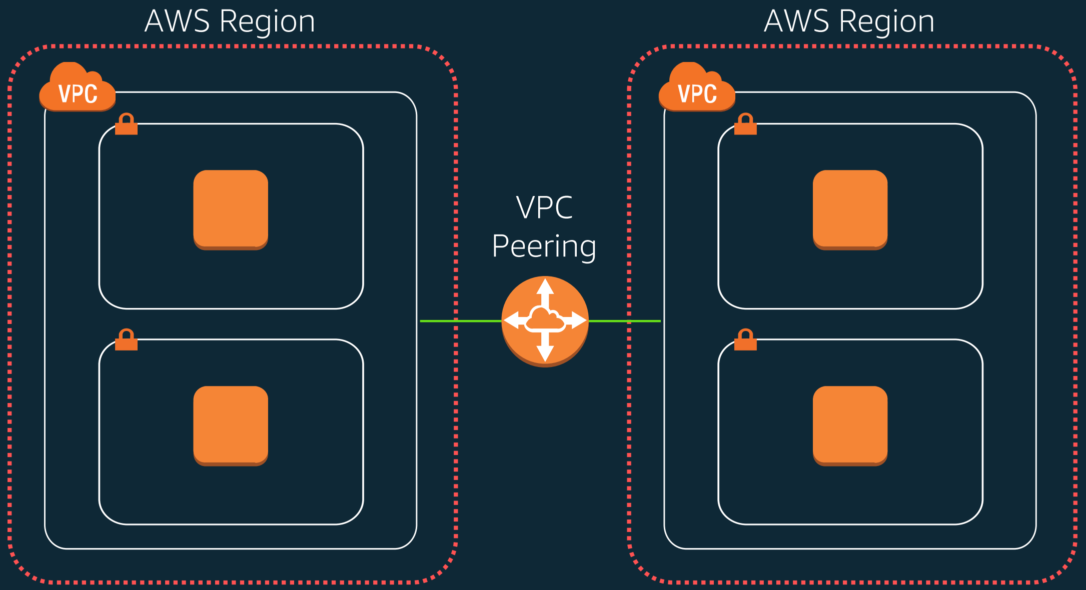
AWS Transit Gateway in multiple Regions



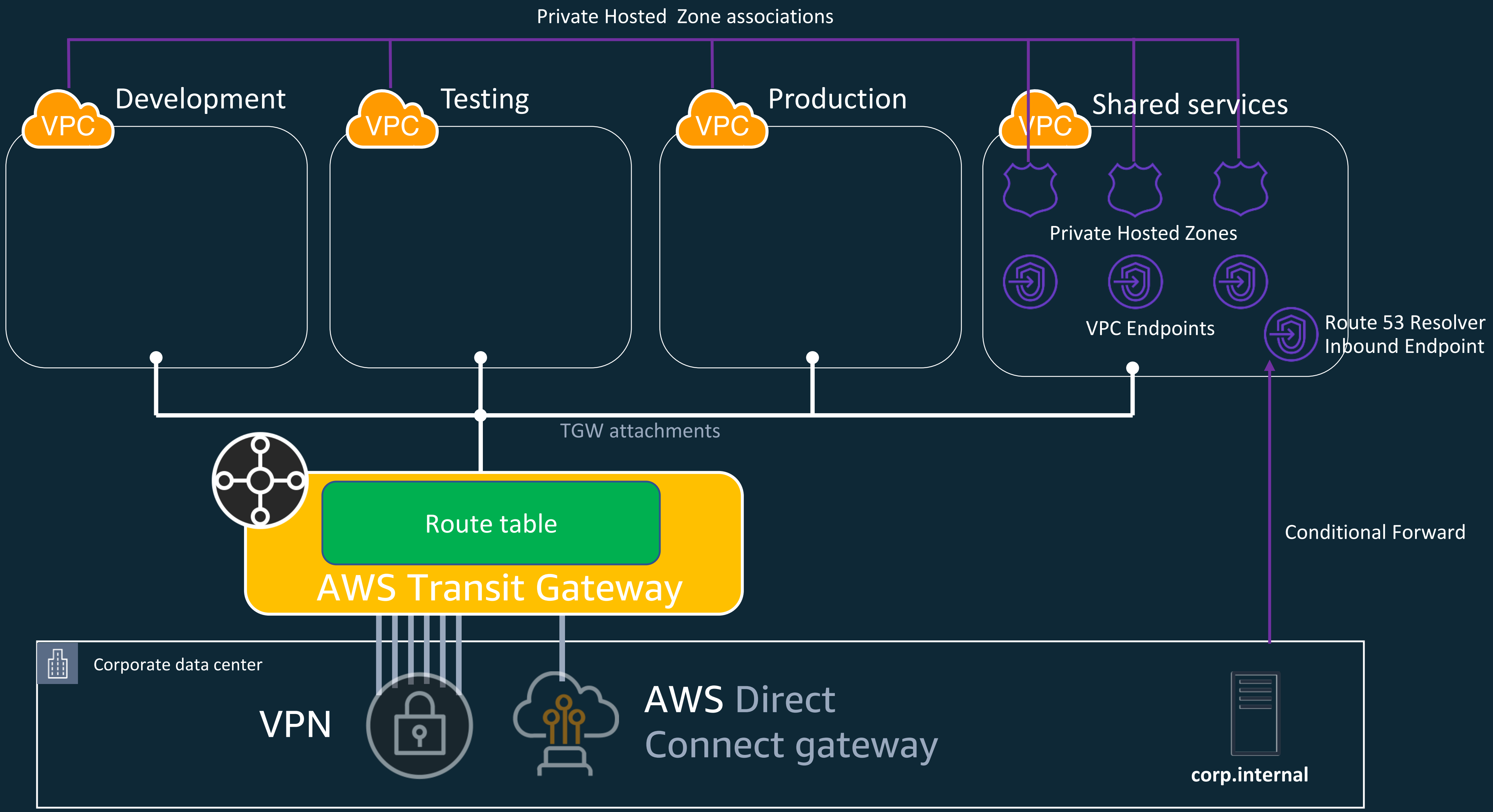
Connecting Regions with VPN

AWS Transit Gateway inter-region support coming soon!

Inter-region peering



Centralized PrivateLink with Hybrid Cloud



Take Away

- There are a number of ways to interconnect VPCs on AWS and to/from on-premises (peering, transit gateway, transit VPC, VPC sharing, etc.)
    - No single ”right way”
- Transit gateway is an AWS native service greatly improving on the transit VPC design pattern
- We’re here to help!
    - Talk to your account team – they can bring in specialists

Questions?