AWS Transit Gateway Reference Architectures for Many Amazon VPCs

James Devine, Senior Specialist Solutions Architect

August 22nd 2019

Agenda

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

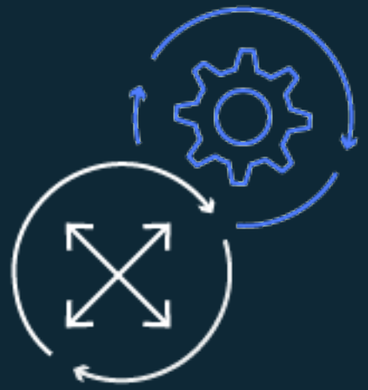
Common Requirements

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

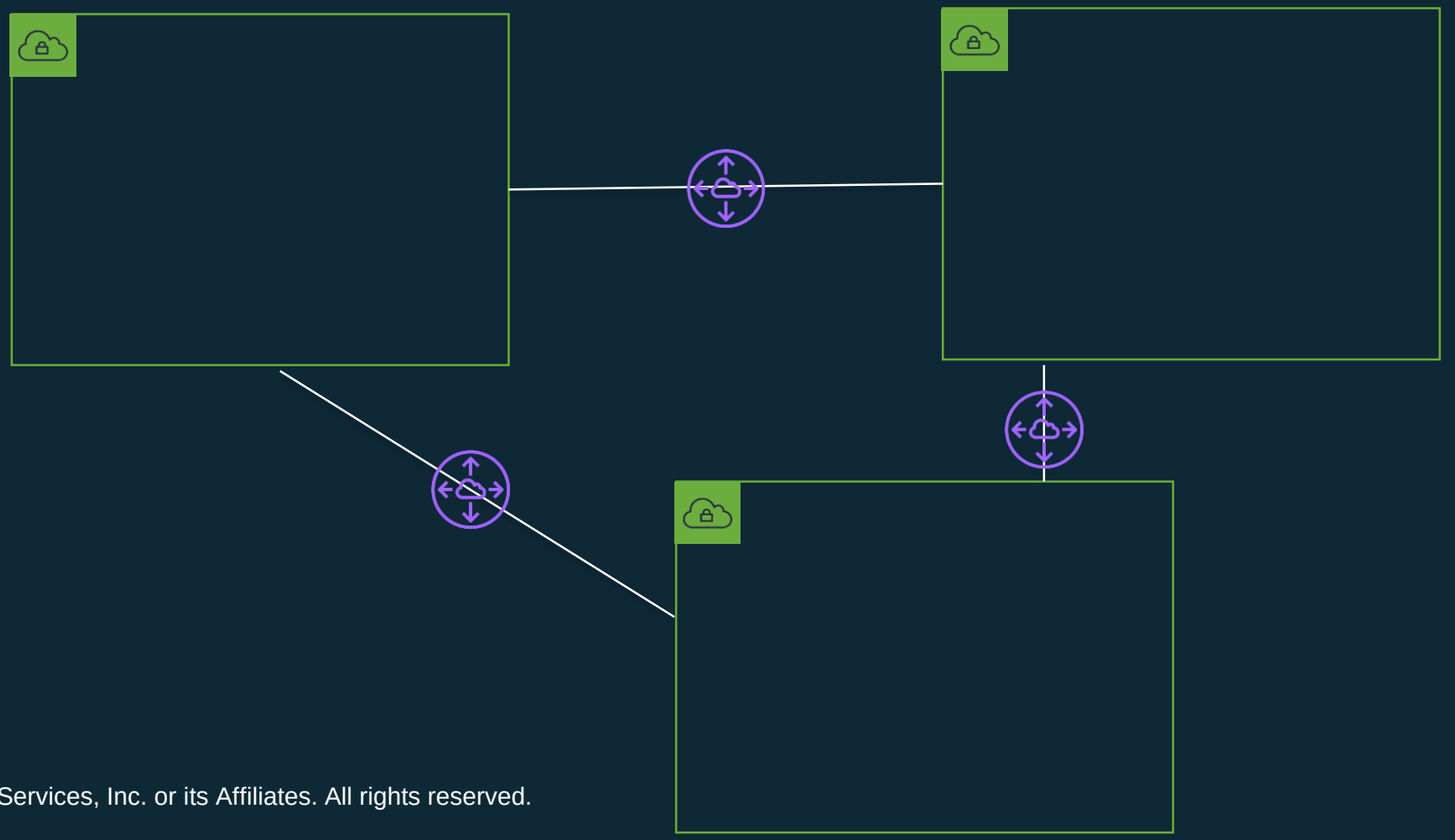
VPN Bandwidth limitations

Monitoring and Management of routing configurations is time consuming

VPC Connectivity Paradigms

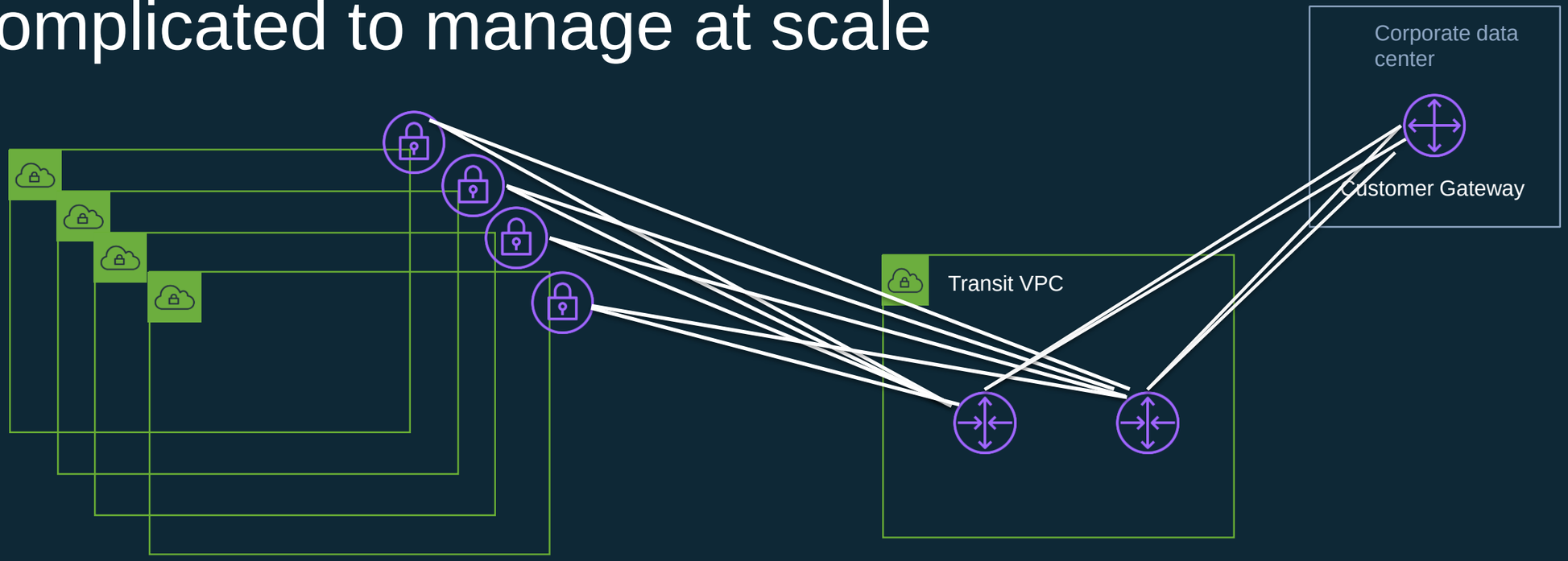
VPC Peering

- 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



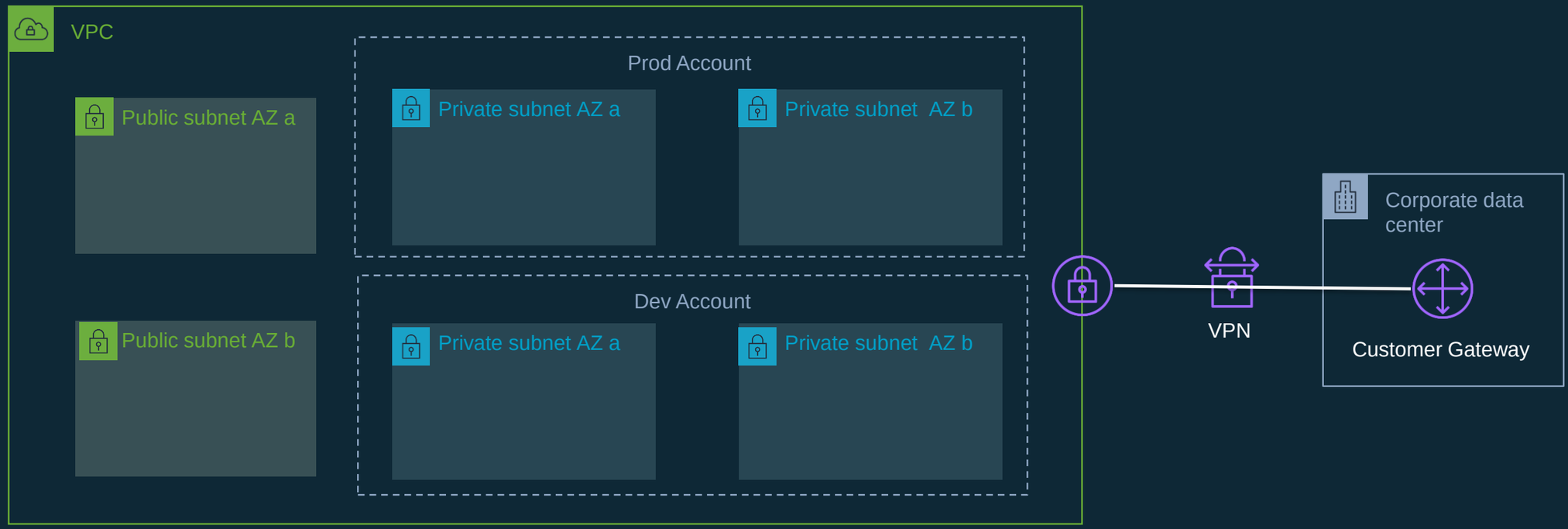
Transit VPC

- 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

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

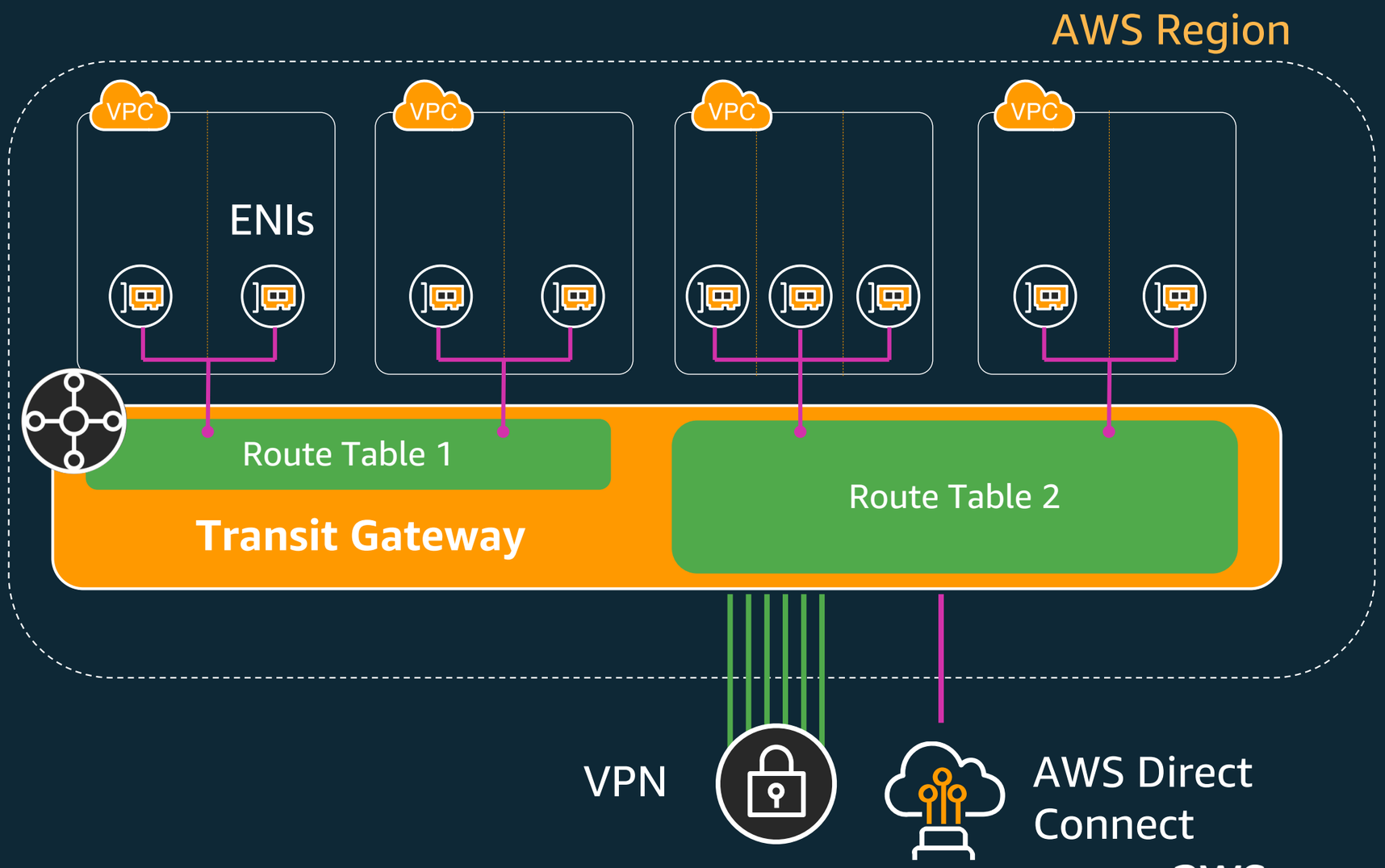
- Centralize VPN and AWS Direct Connect

Scalable

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

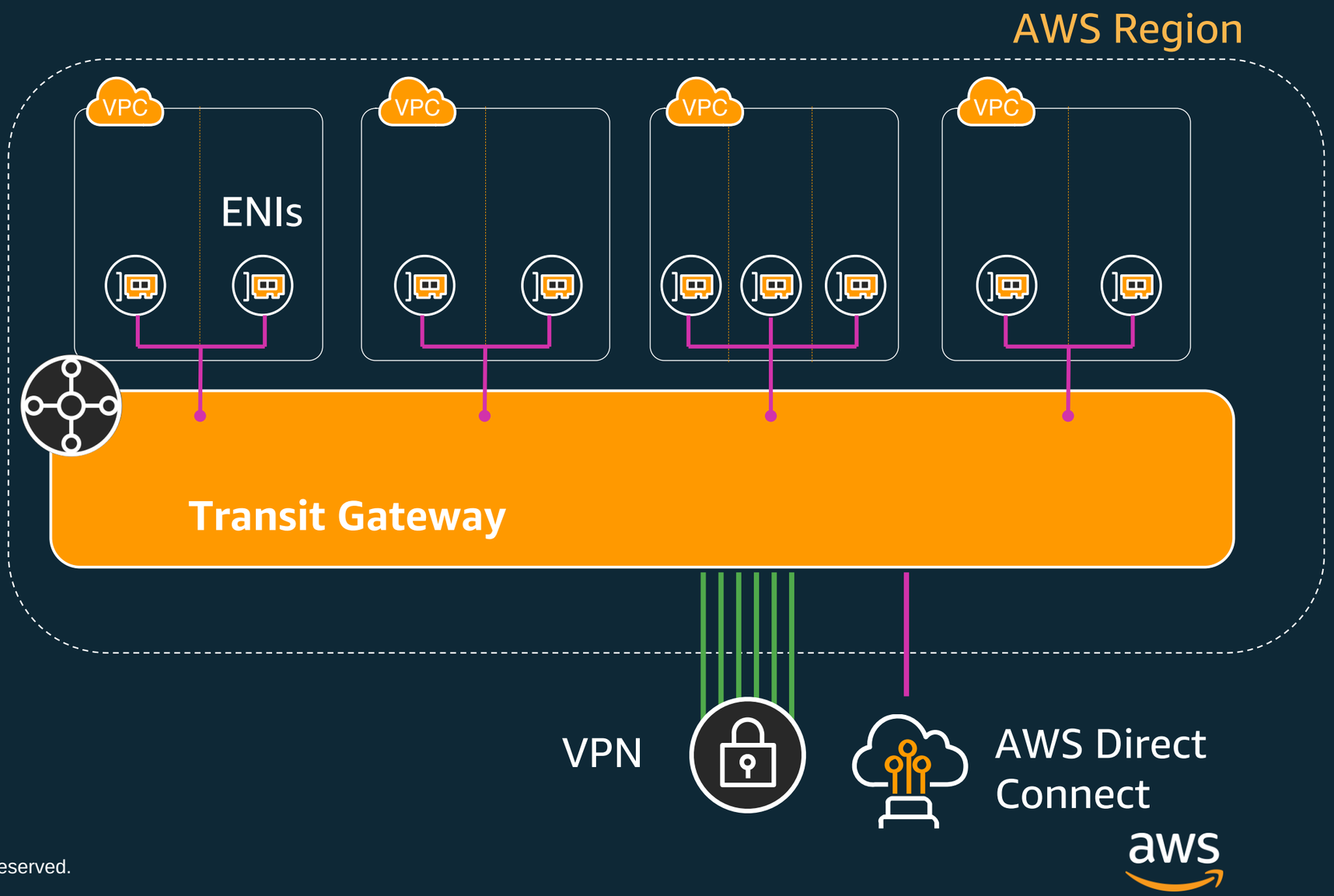
Flexible routing

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



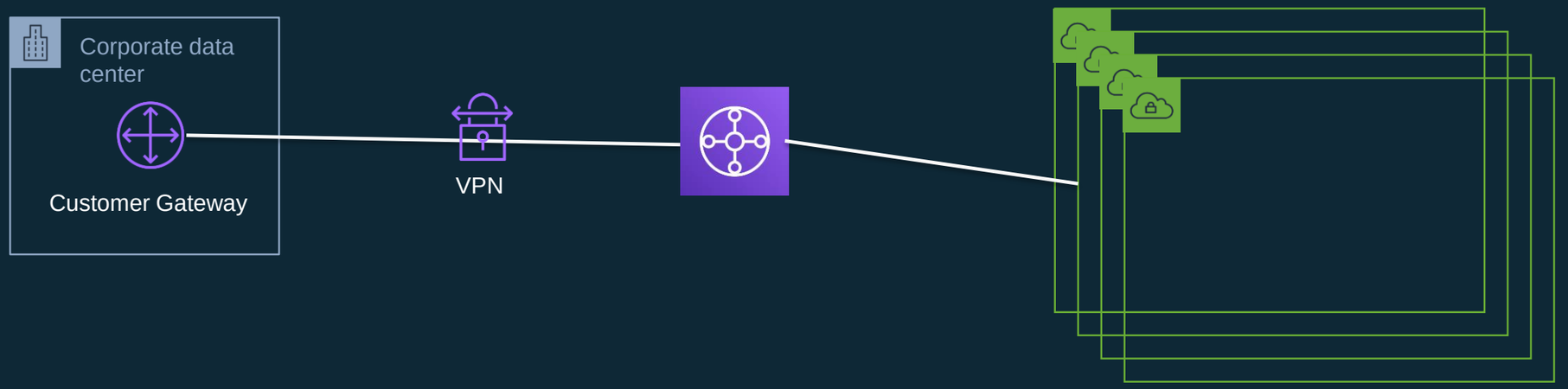
Transit Gateway Attachments

- VPC
- VPN
- Direct Connect

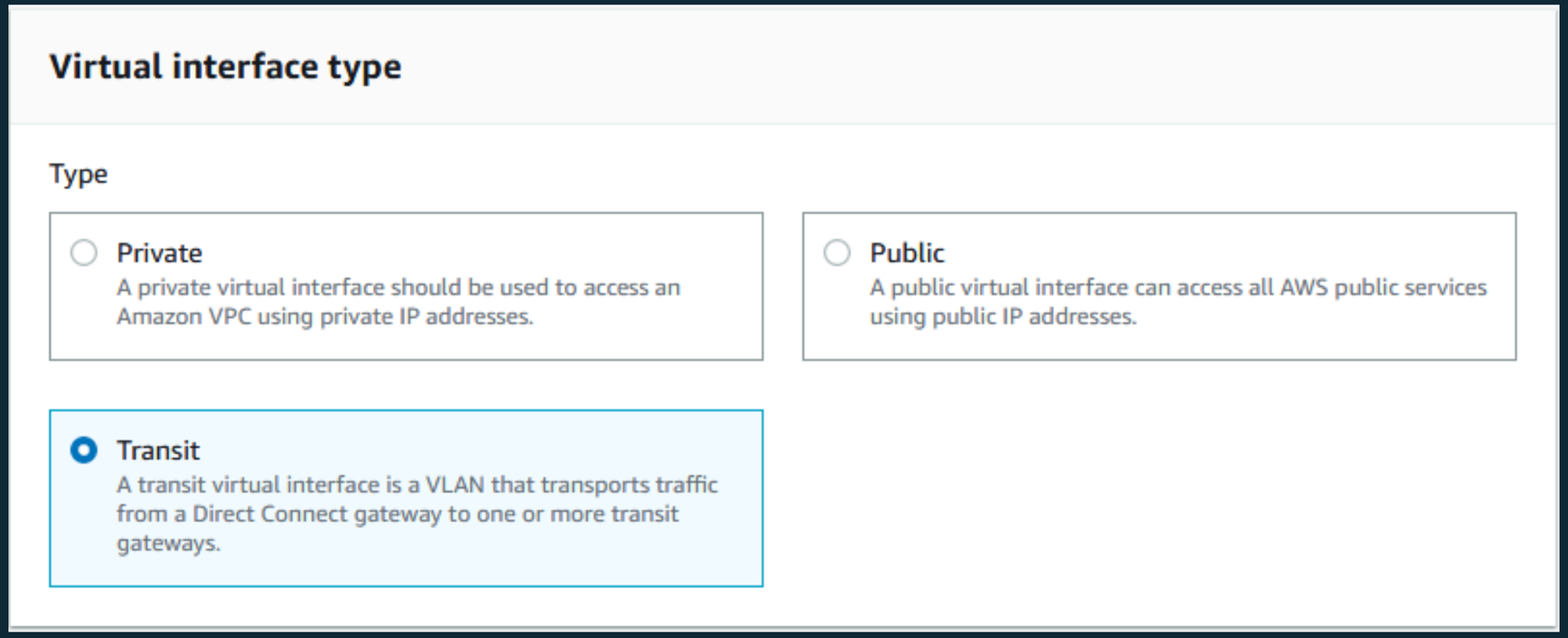


VPN Attachment

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

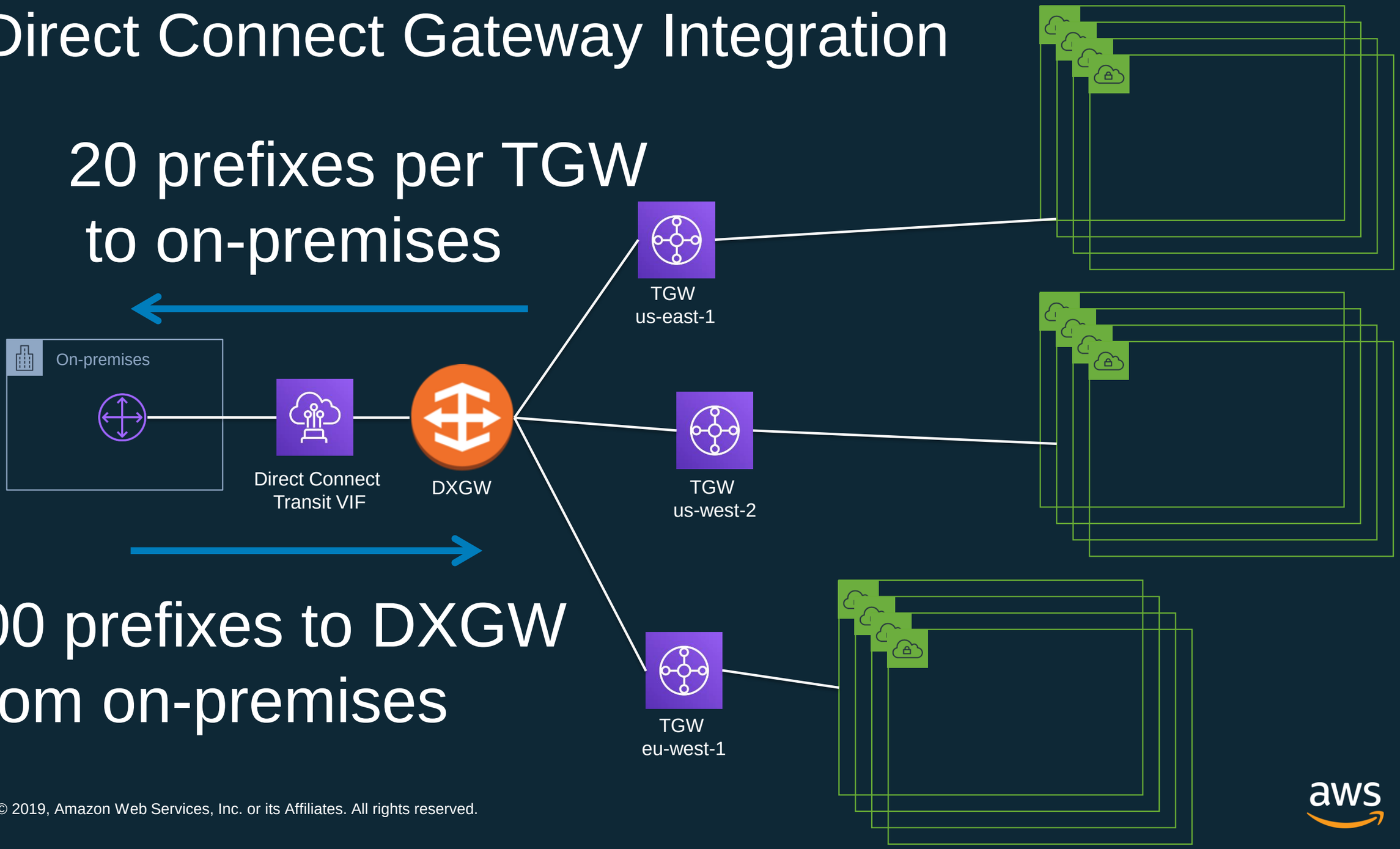


Direct Connect Gateway – Transit VIF



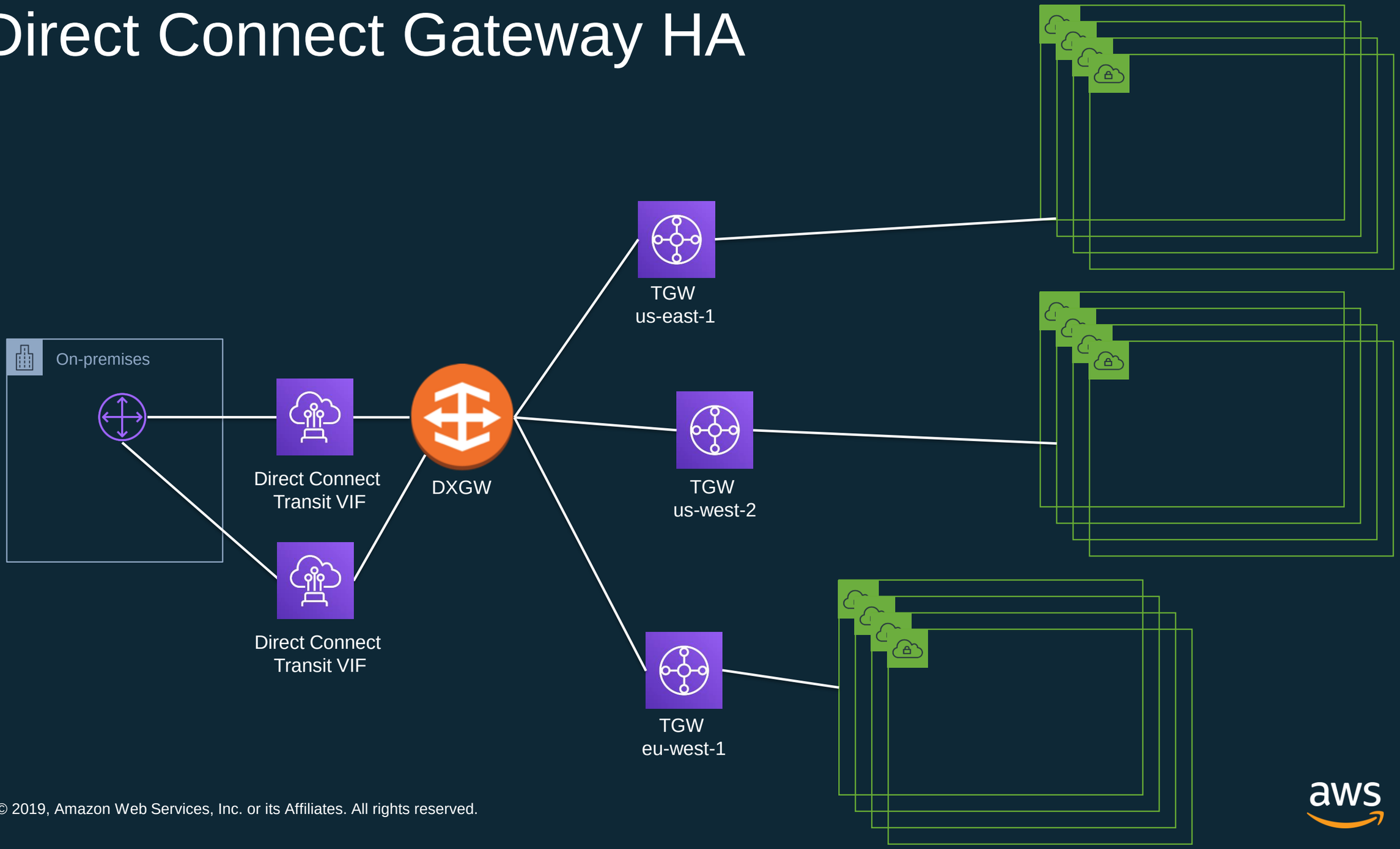
Direct Connect Gateway Integration

20 prefixes per TGW
to on-premises

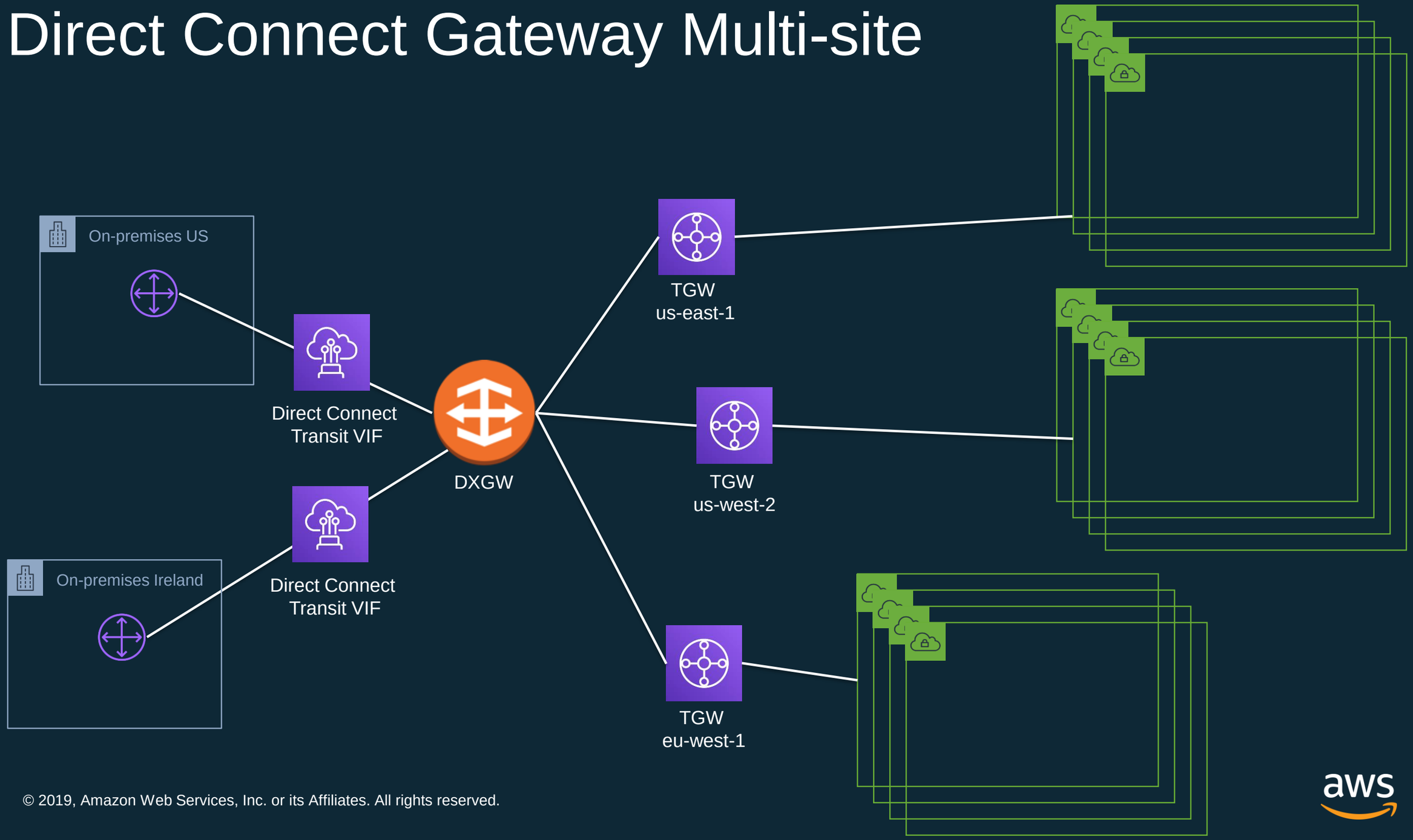


100 prefixes to DXGW
from on-premises

Direct Connect Gateway HA

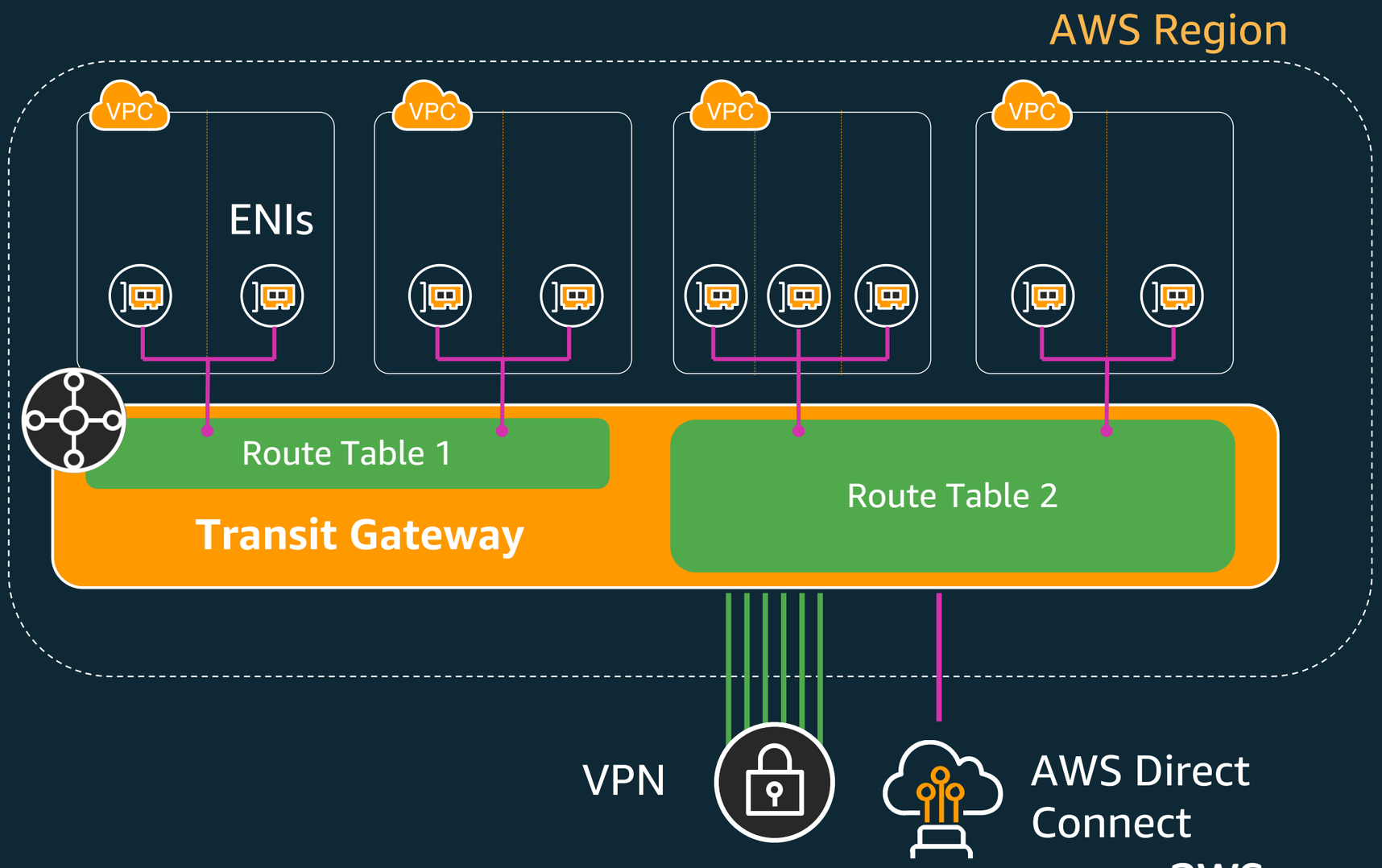


Direct Connect Gateway Multi-site



Transit Gateway Route Tables

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



Transit Gateway Path Selection Behavior

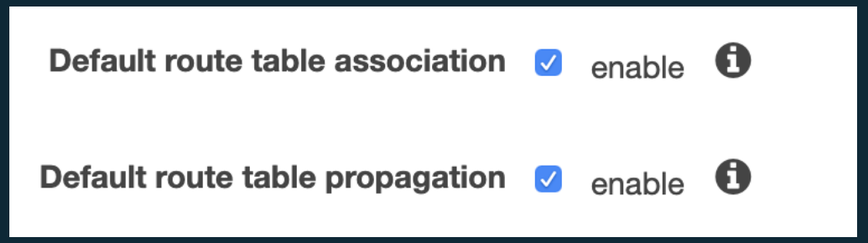
1. Most Specific Route / Longest Prefix Match
2. Static route entries, including static Site-to-Site VPN routes
3. VPC propagated routes
4. BGP propagated routes from AWS Direct Connect gateway
5. BGP propagated routes from AWS Site-to-Site VPN

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)



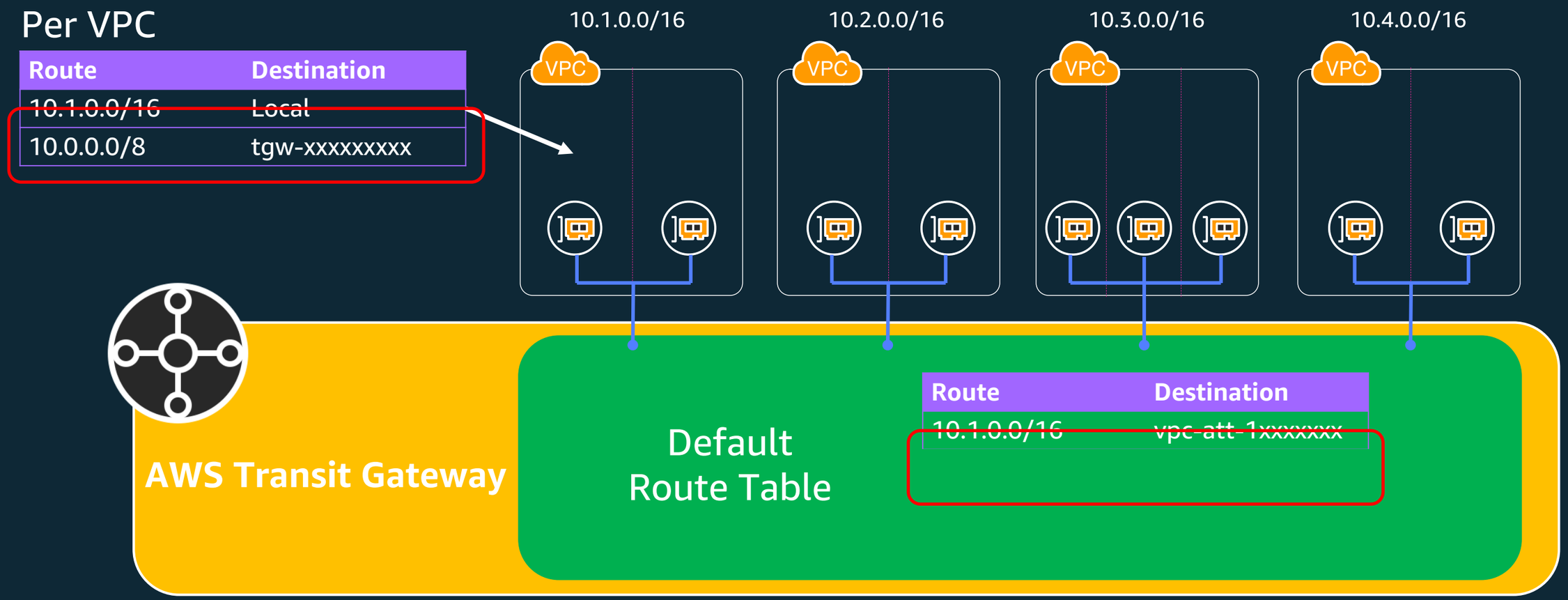
View: All routes

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

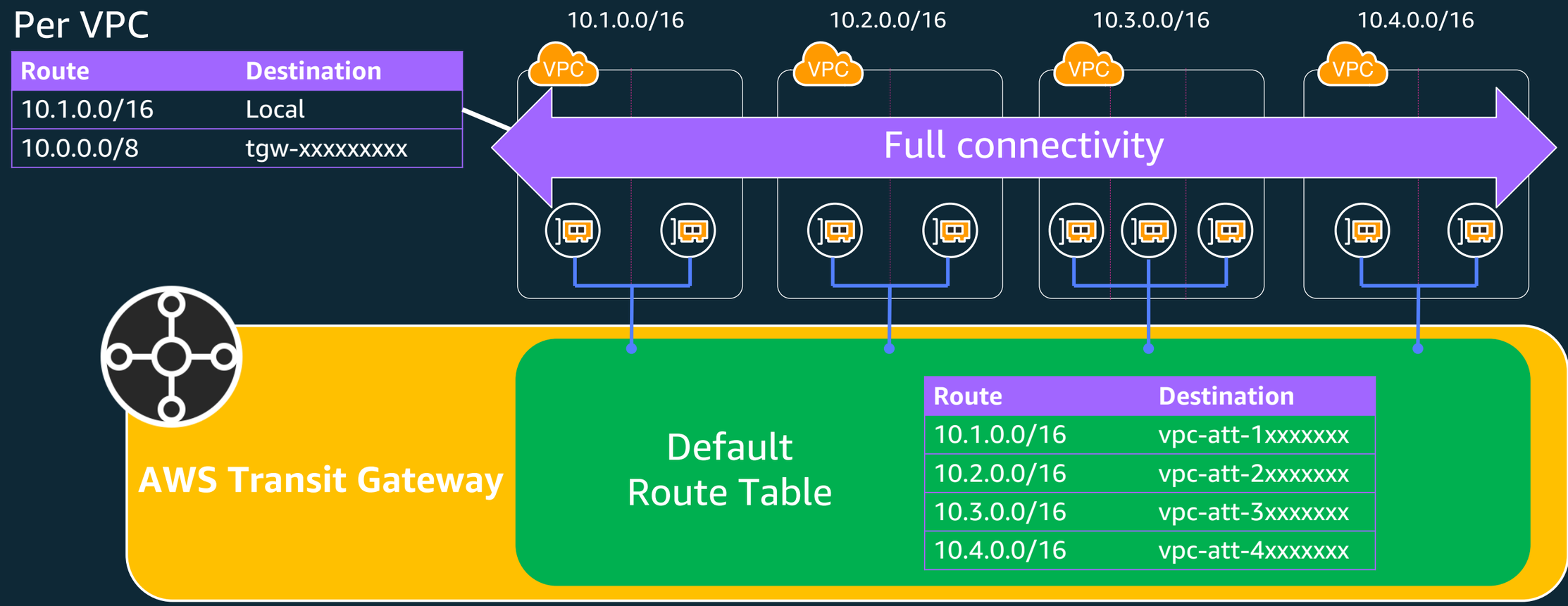
aws

Transit Gateway Data Flows

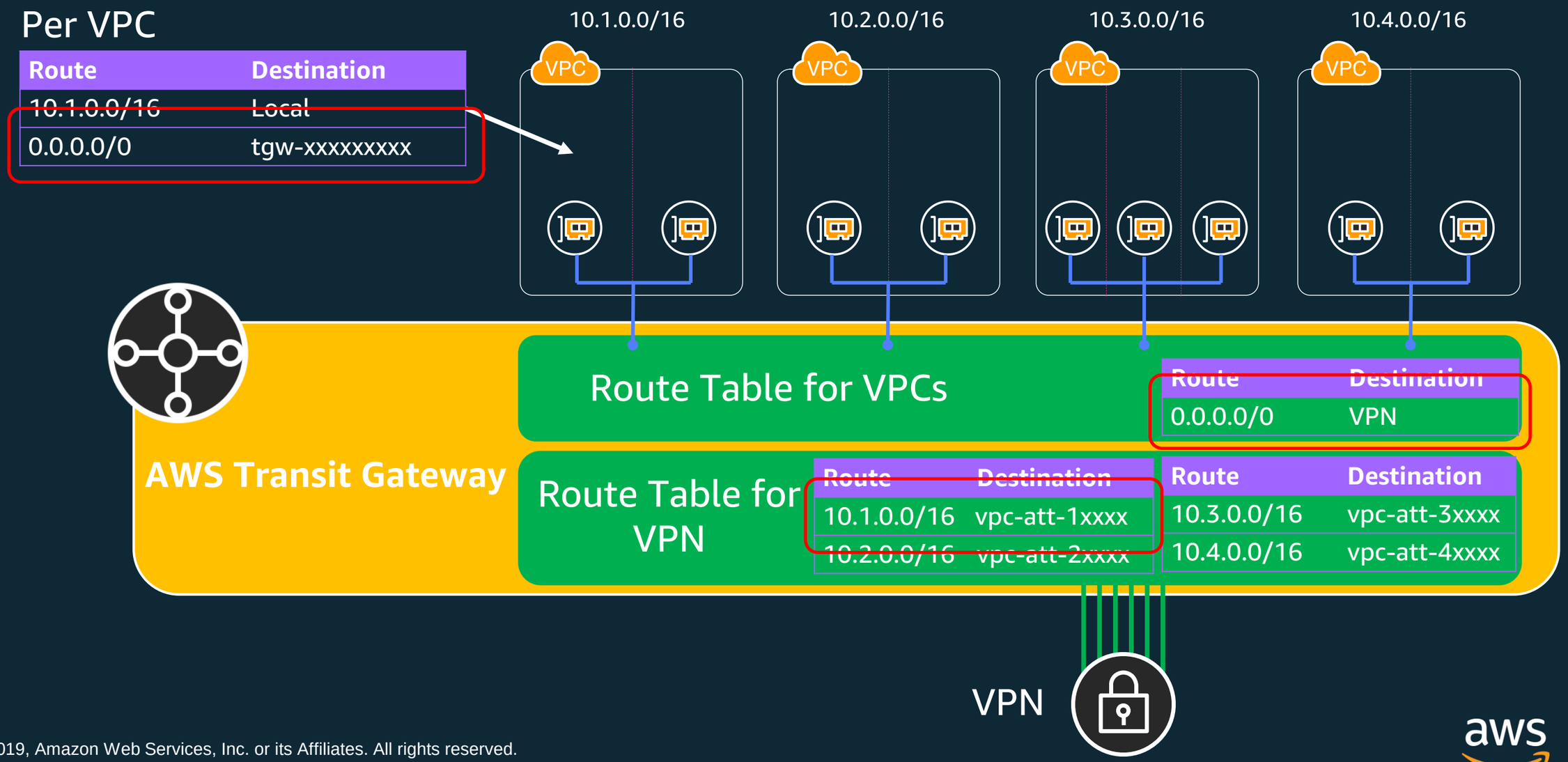
Flat Network



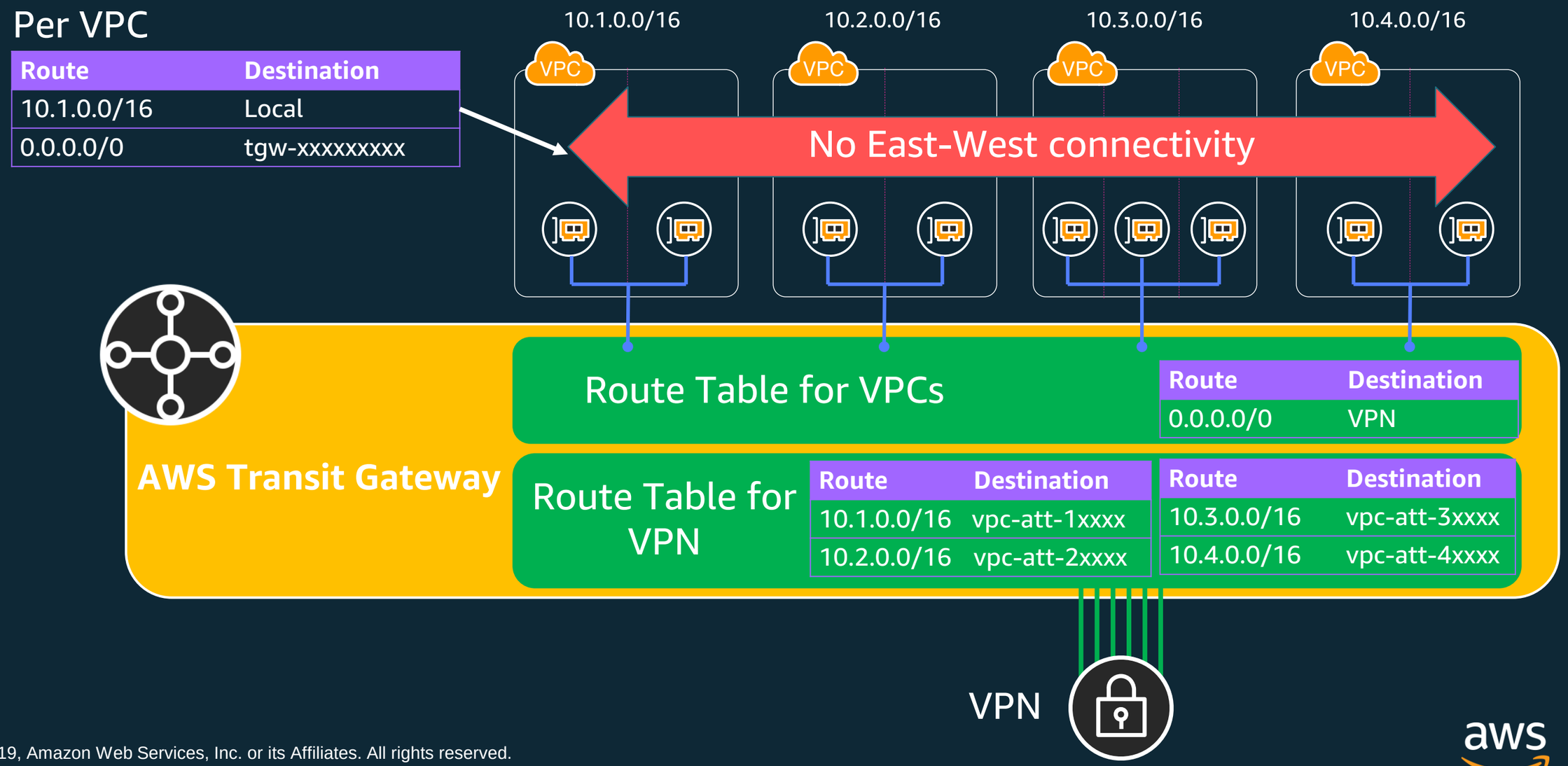
Flat Network



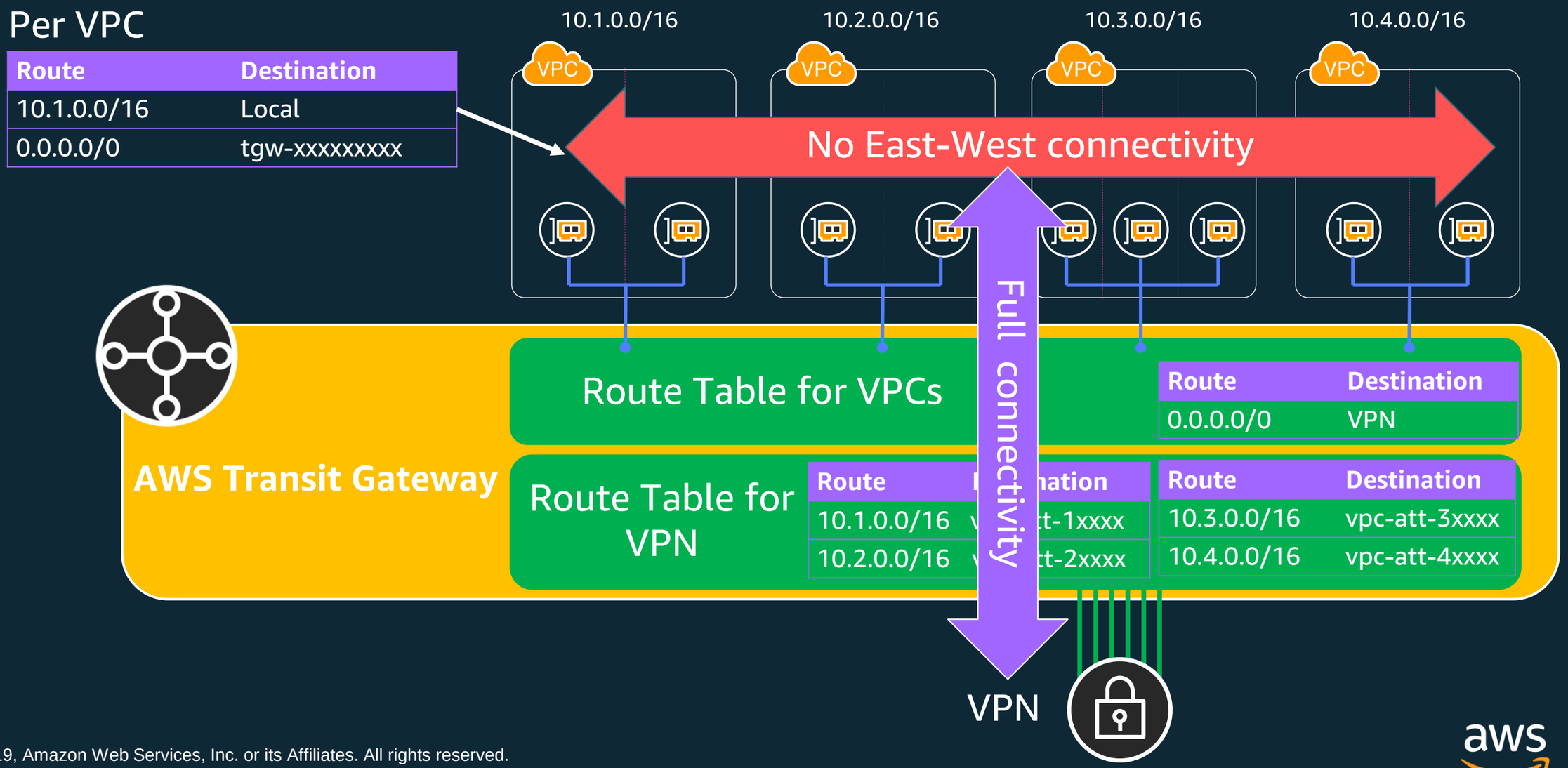
Segmented Network



Segmented Network

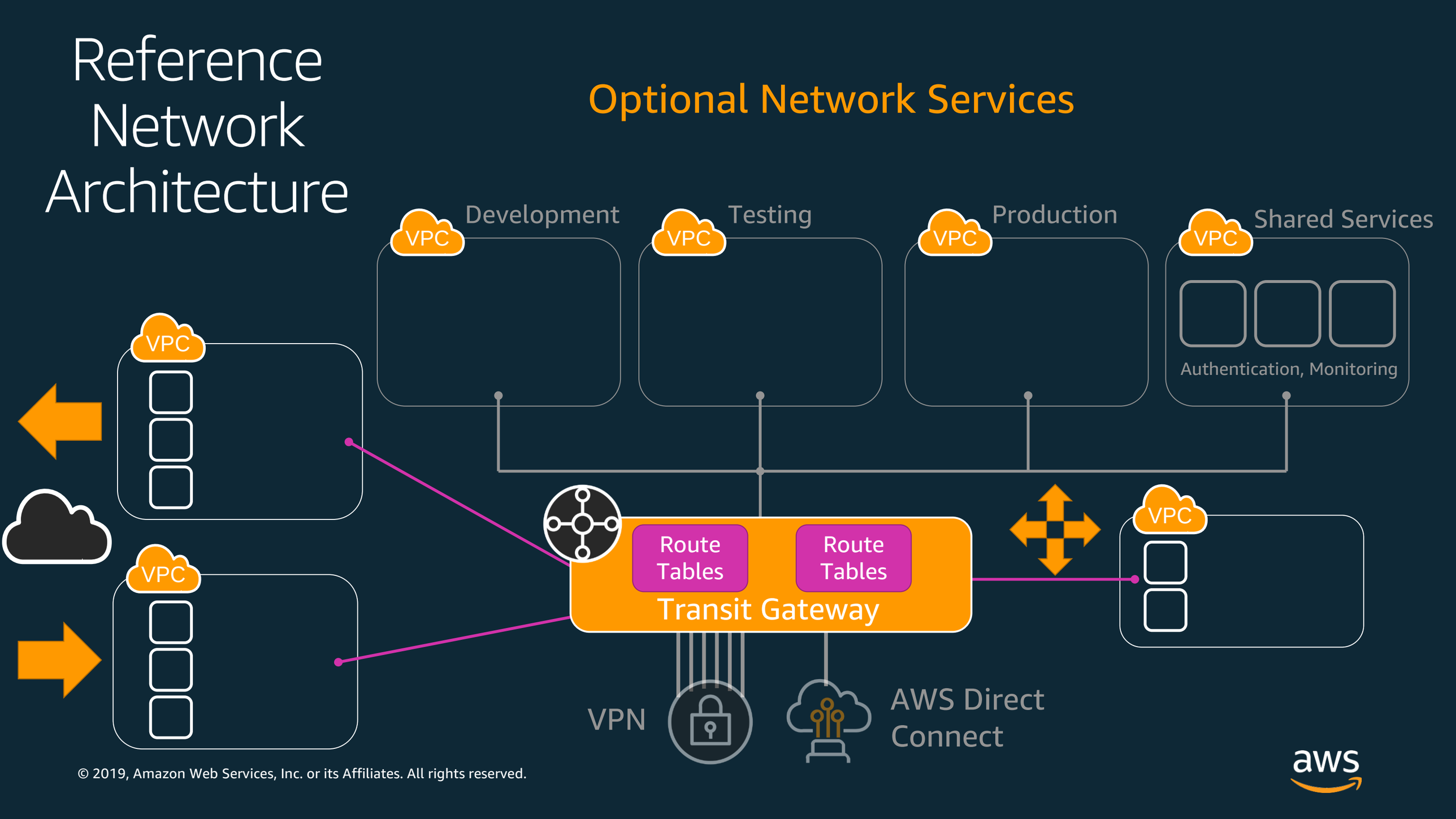


Segmented Network

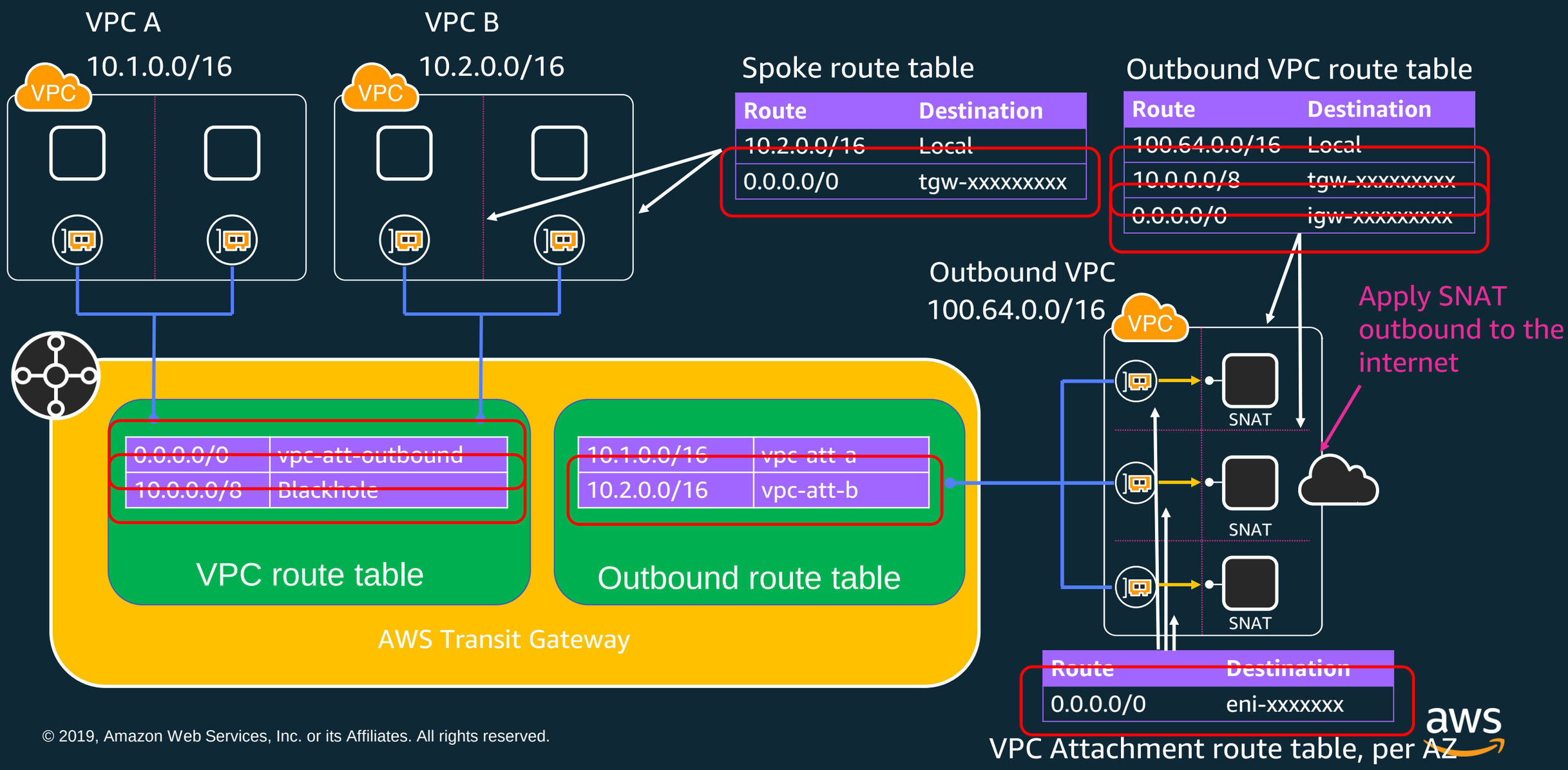


Transit Gateway Reference Architectures

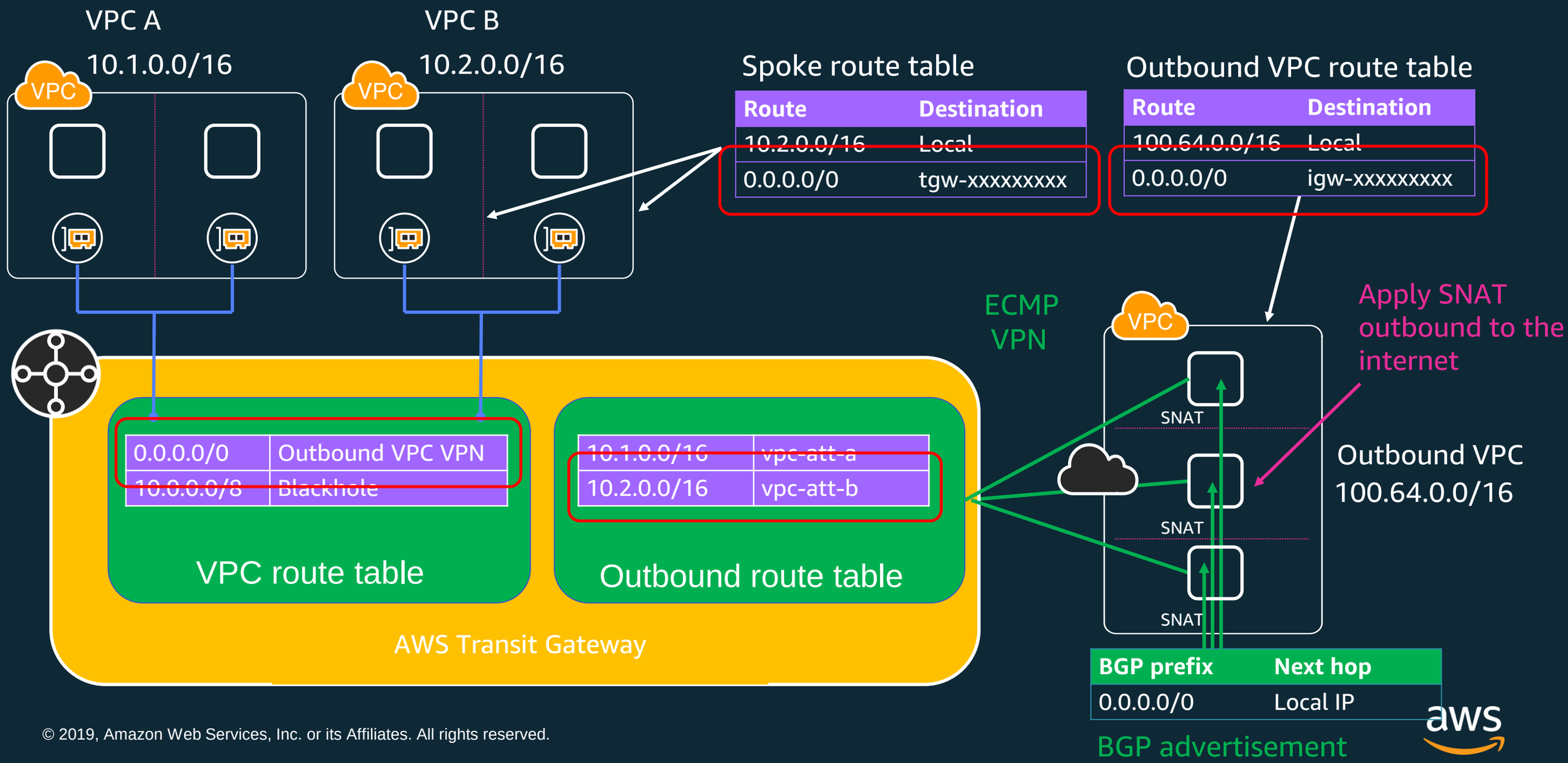
Reference Network Architecture



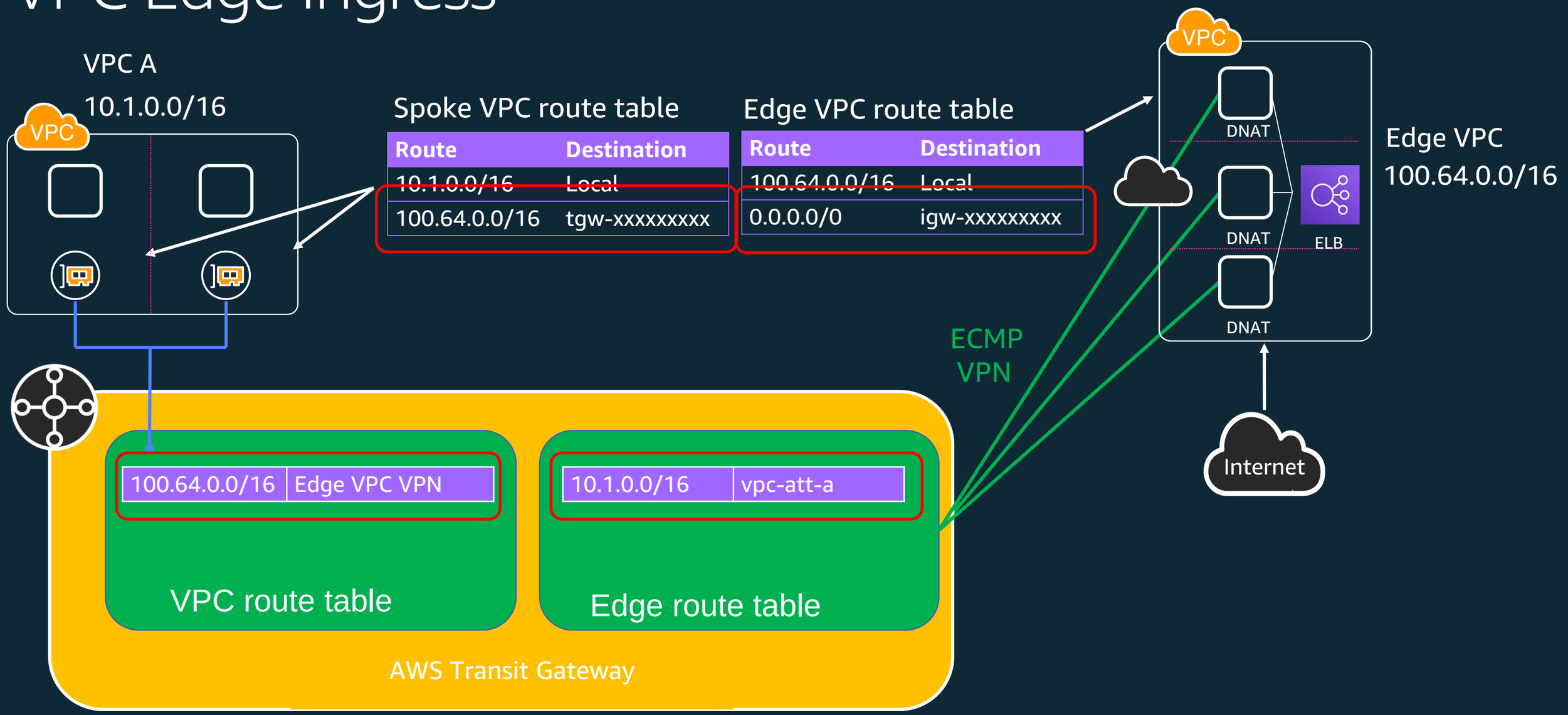
Centralized NAT



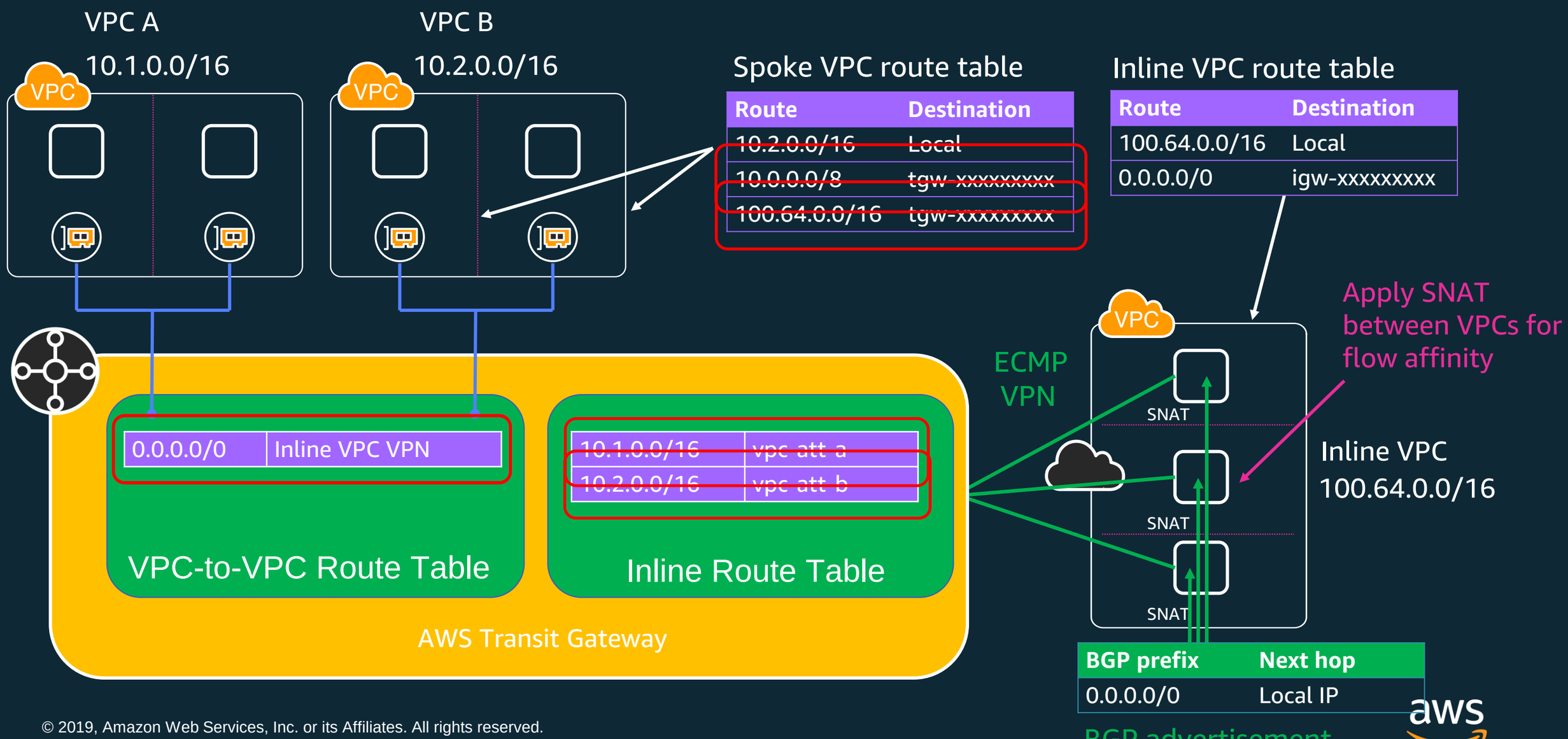
Centralized NAT



VPC Edge Ingress



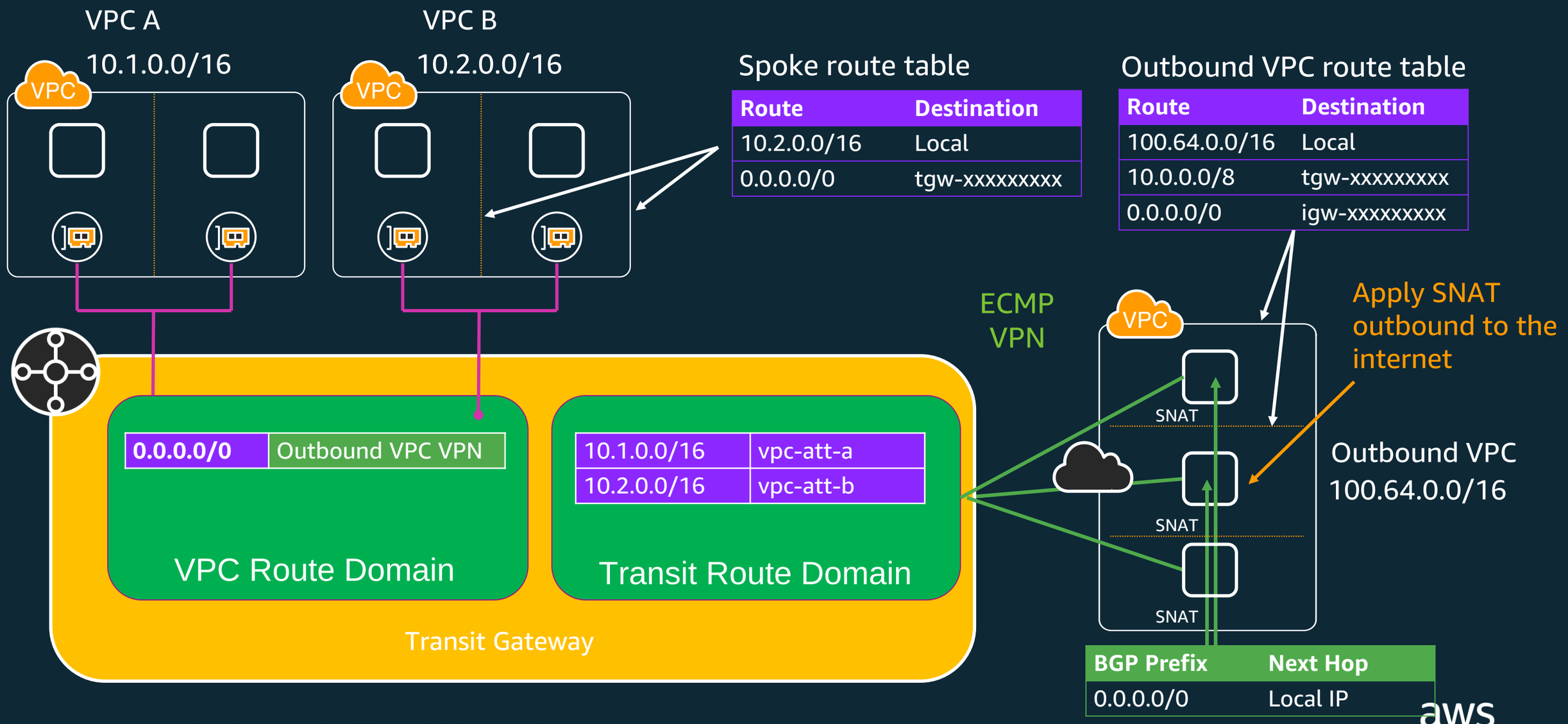
VPC to VPC Inspection



Outbound VPC Services

Use Cases:

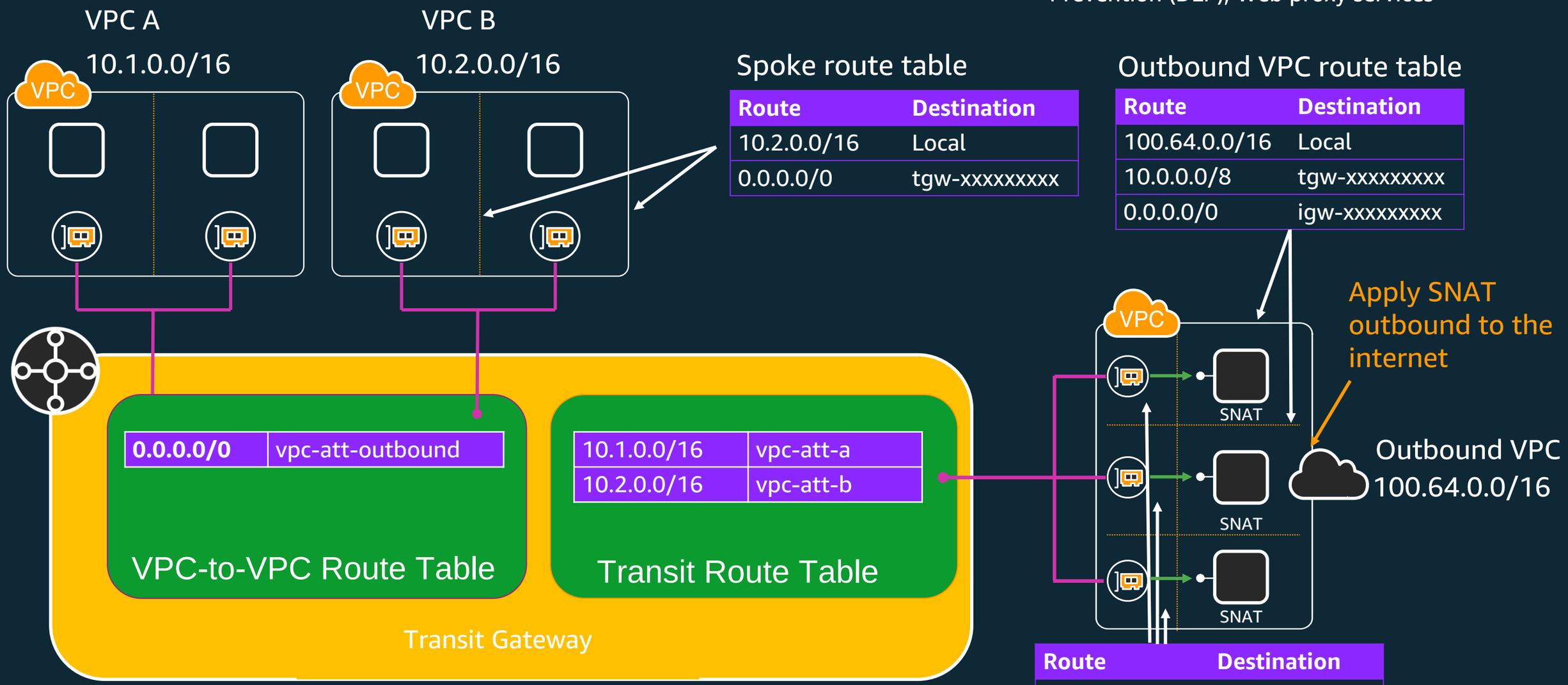
URL filtering, NAT gateway, Data-loss Prevention (DLP), Web proxy services



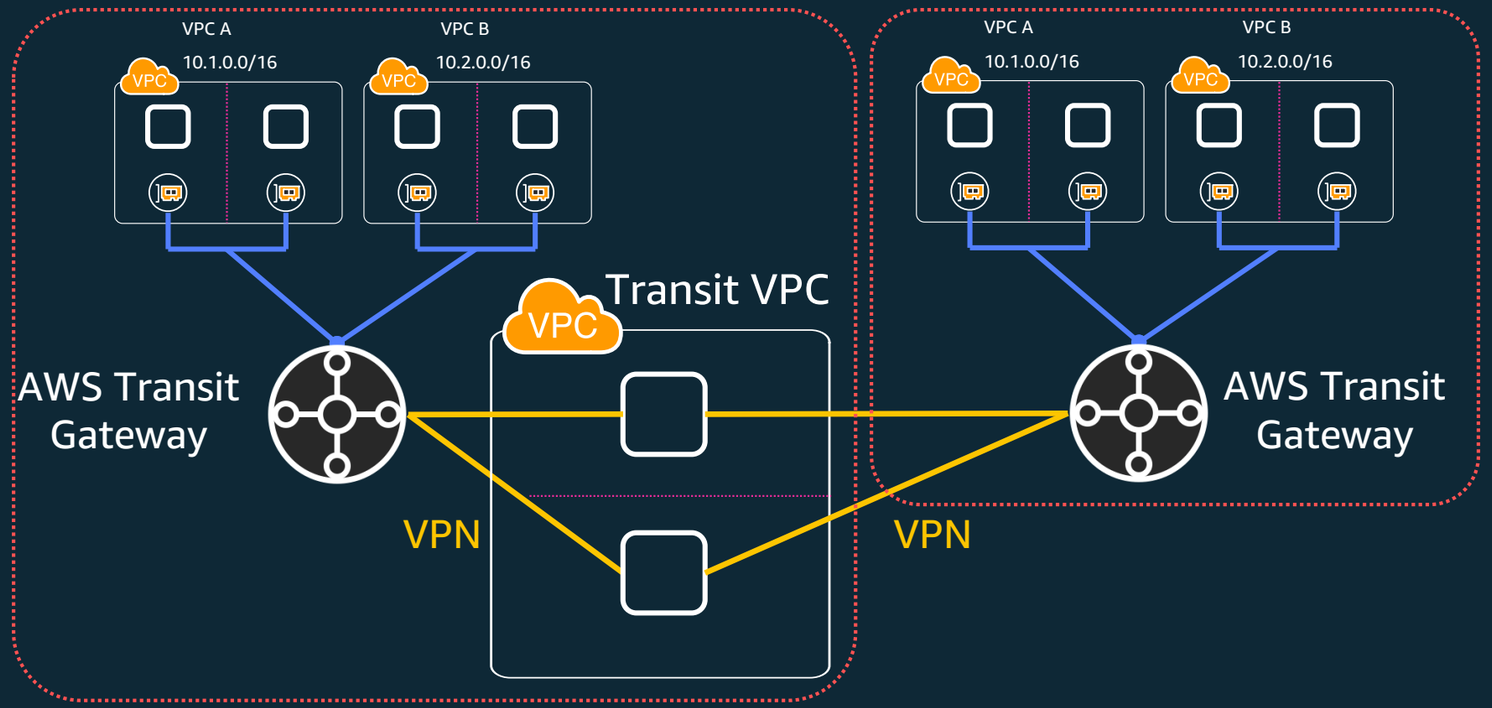
Outbound VPC Services – No VPN

Use Cases:

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



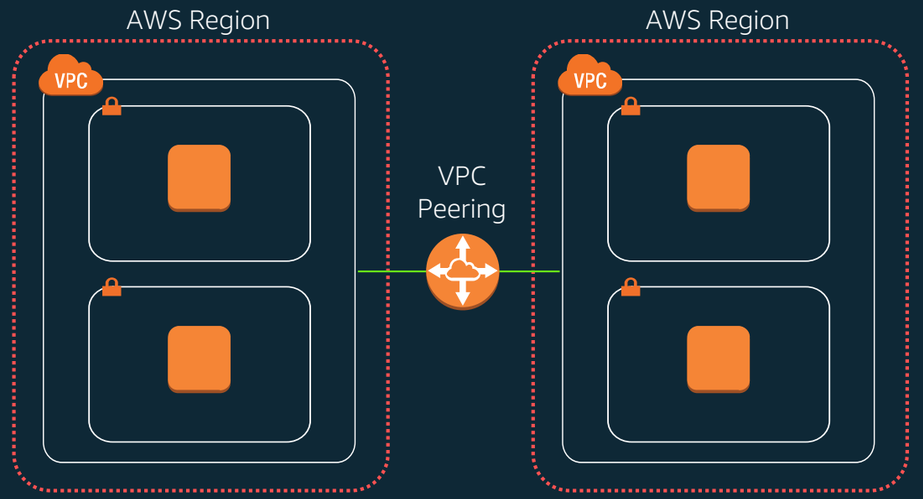
AWS Transit Gateway in multiple Regions



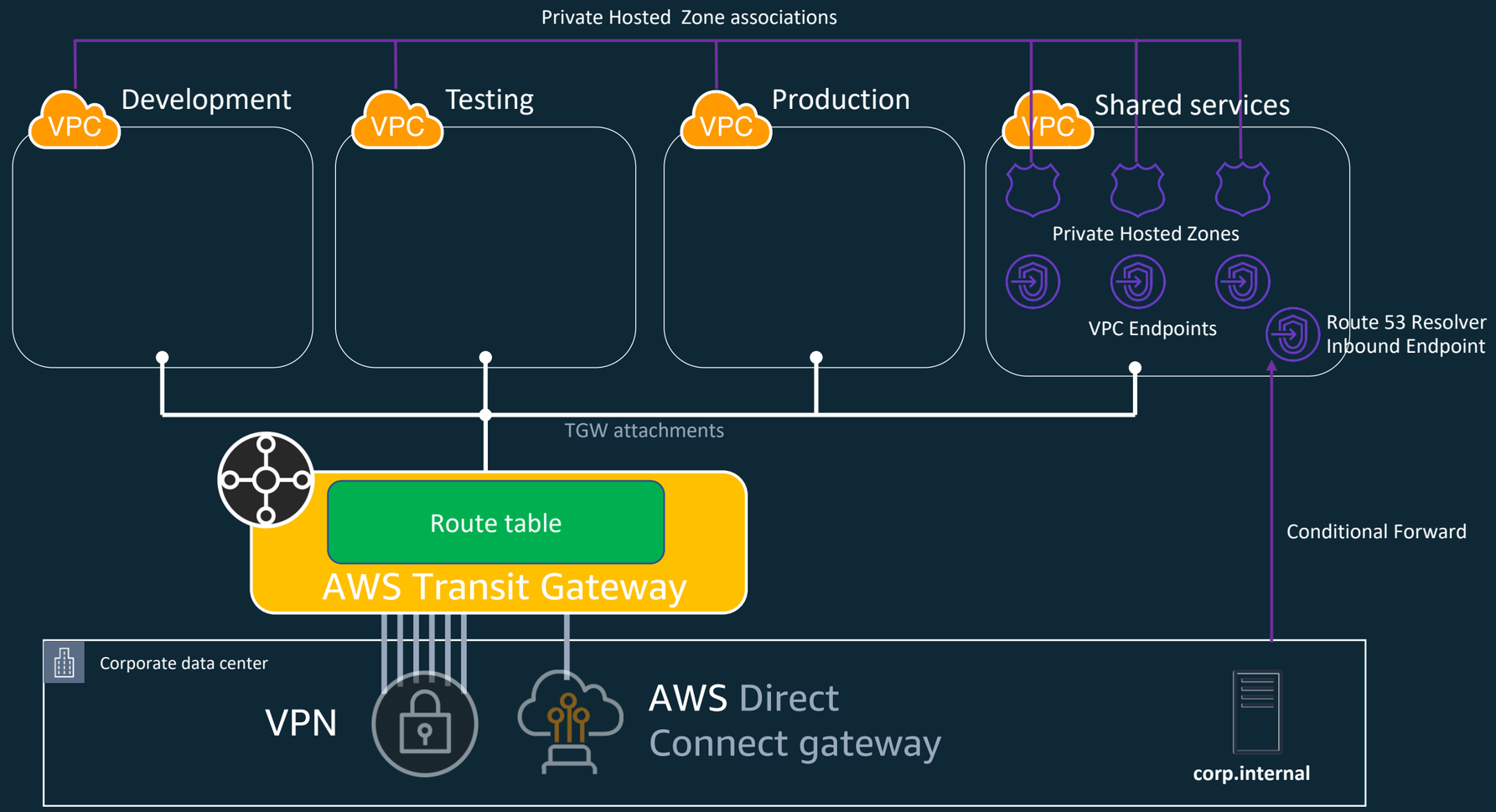
Connecting Regions with VPN

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?