Introducing AWS Transit Gateway

Nick Matthews
Principal Solutions Architect
AWS
@nickpowpow

Mohamed Hassan
Senior Product Manager
EC2 Networking, AWS
@mohnader

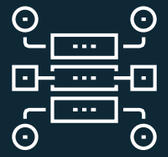
What is Transit Gateway ?

Introducing AWS Transit Gateway

A gateway that provides simple, scalable, and secure connectivity across networks

Regional Gateway

Simple regional gateway to easily manage VPC connectivity



Massive Scale

Attach thousands of VPCs, VPN and Direct Connect connections

Routing Domains

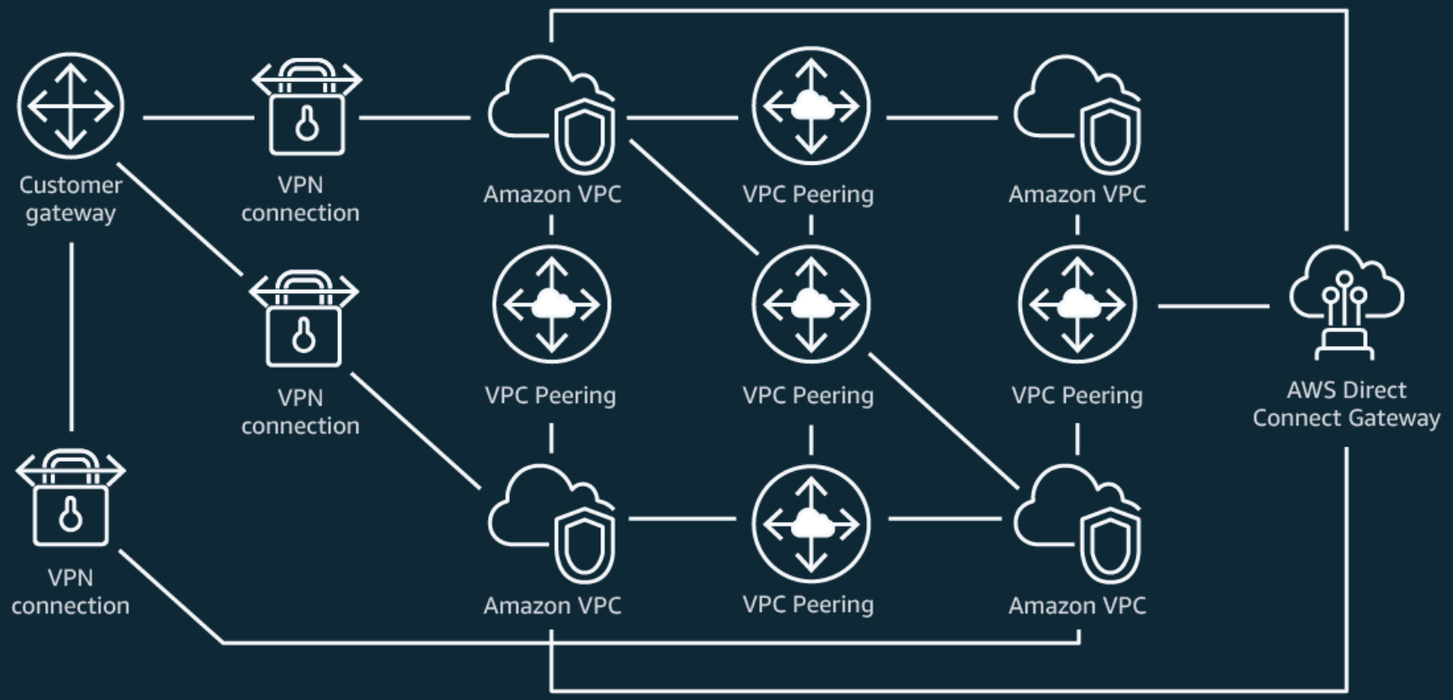
Support for routing domains, allowing per-attachment routing

Partner Integration

Support for middle-boxing of partner appliances

aws

Before Transit Gateway

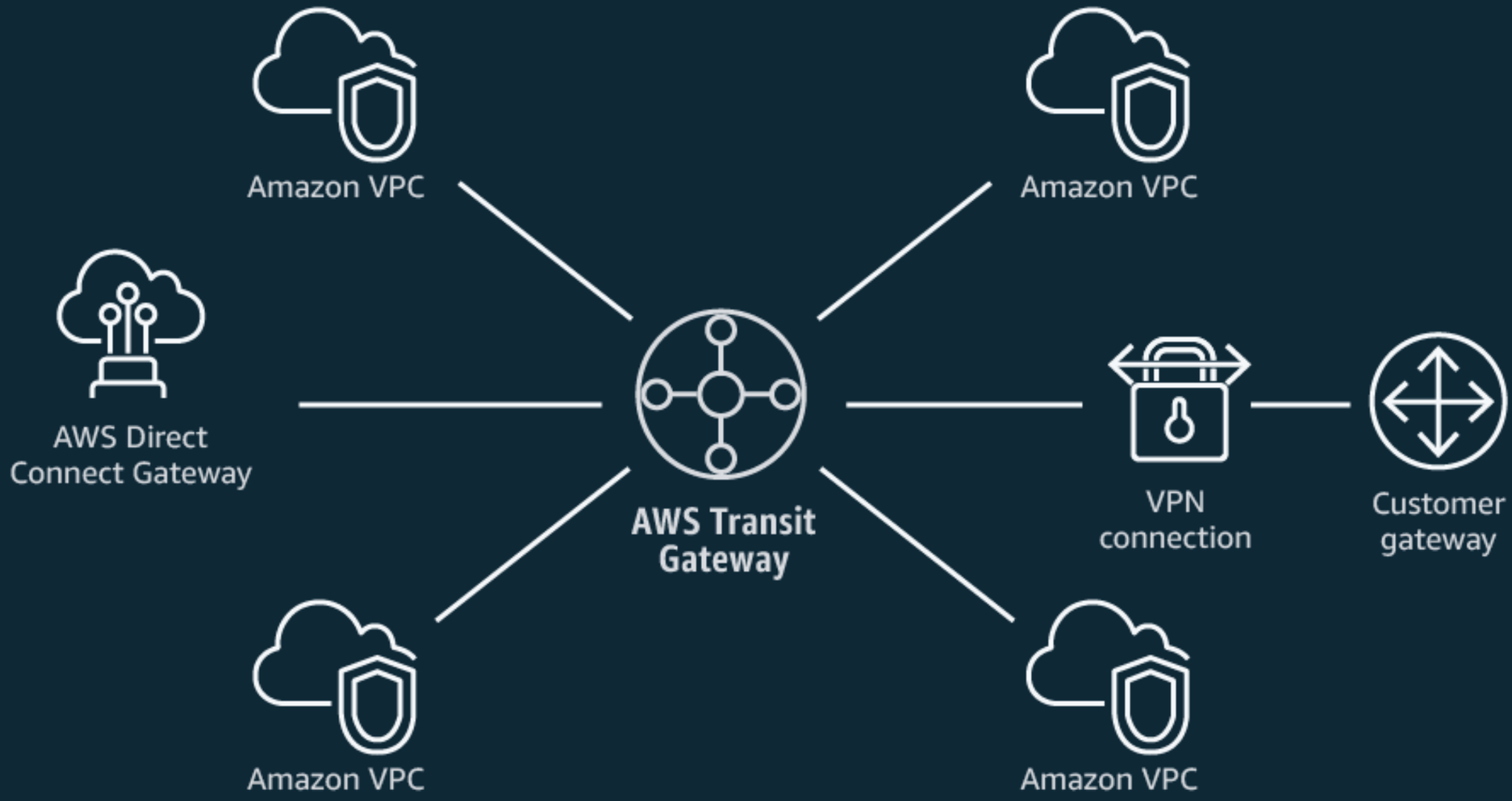


Connecting large number of VPCs in a mesh is challenging to manage

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

Complex configurations are prone to human error

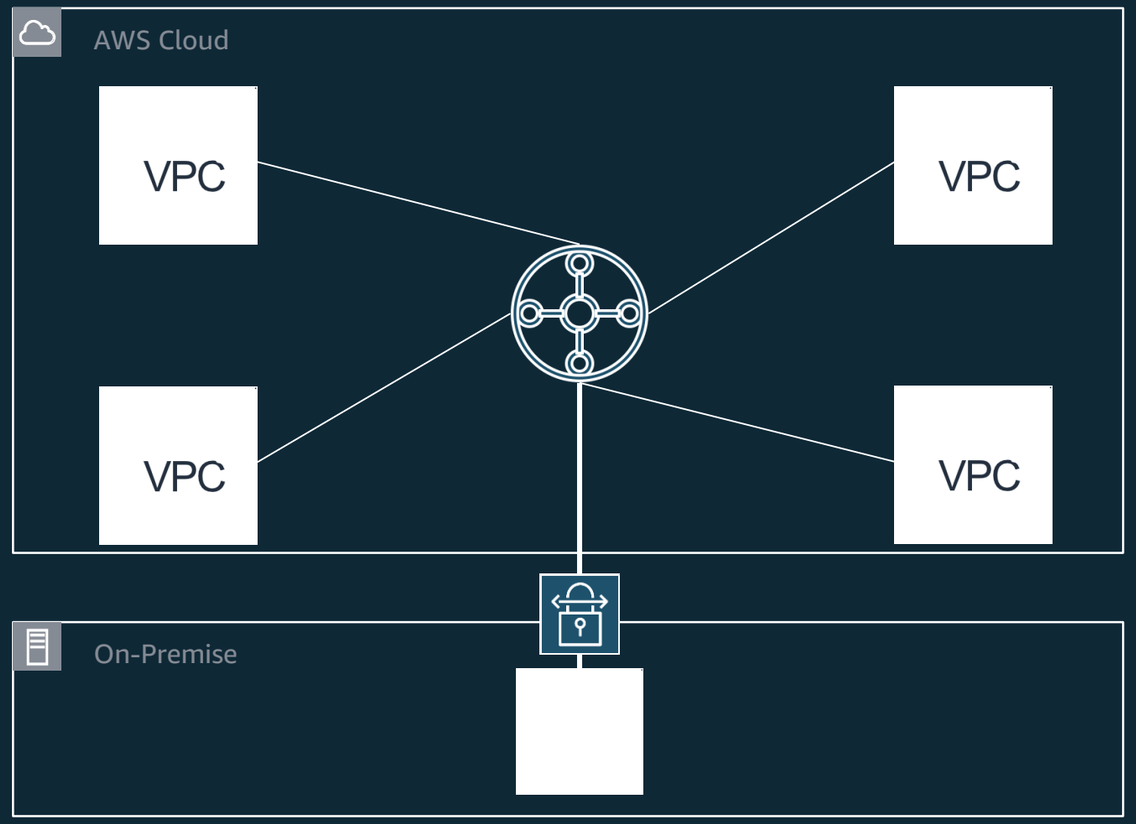
AWS Transit Gateway



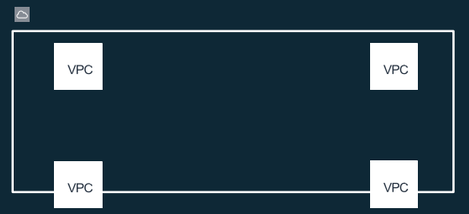
Getting Started with Transit Gateway

Scenario

- Connecting Multiple VPC’s
- Any to any communication
- Sharing a single VPN Connection



Four VPC’s



aws Services Resource Groups

VPC Dashboard

Filter by VPC:

Select a VPC

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

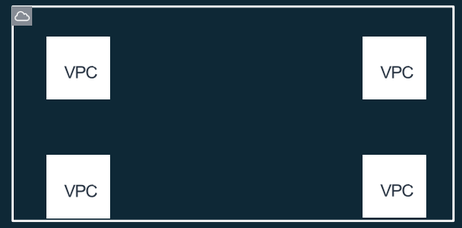
Create VPC | Actions

Filter by tags and attributes or search by keyword

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
VPC-1	vpc-0142574d0fb51ec5d	available	10.1.0.0/16	-
VPC-2	vpc-020b5386c993c588b	available	10.2.0.0/16	-
VPC-3	vpc-0cb9f3ed83dab7f7b	available	10.3.0.0/16	-
VPC-4	vpc-0ef32707c3e17e465	available	10.4.0.0/16	-
--Default VPC--	vpc-c629caaf	available	172.31.0.0/16	-

aws

Create a Transit Gateway



aws Services Resource Groups

Transit Gateways > Create Transit Gateway

Create Transit Gateway

A Transit Gateway (TGW) is a network transit hub that interconnects attachments (VPCs and VPNs) within the same account or across accounts.

Name tag OHIO-TGW-1

Description OHIO-TGW-1

Configure the Transit Gateway

Amazon side ASN 64512

DNS support enable

ECMP support enable

Default route table association enable

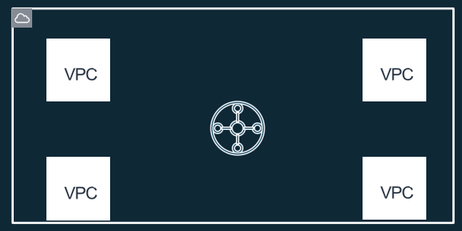
Default route table propagation enable

Configure sharing options for cross account

Automatically accept attachments enable

aws

Create a Transit Gateway



aws Services Resource Groups

- Endpoint Services
- NAT Gateways
- Peering Connections

Security

- Network ACLs
- Security Groups

VPN Connections

- Customer Gateways
- Virtual Private Gateways
- VPN Connections

Transit Gateways

- Transit Gateways
- Transit Gateway Attachments
- Transit Gateway Route Tables

Create Transit Gateway | **Actions**

Filter by tags and attributes or search by keyword

Description	Transit Gateway ID	State	Amazon ASN	DNS support	Default association route table	Default propagation route table
OHIO-TGW-1	tgw-0174e65e24e6ed02e	available	64512	enable	enable	enable

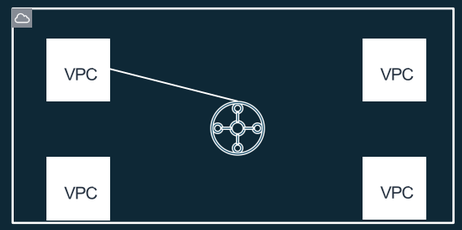
Transit Gateway: tgw-0174e65e24e6ed02e

Details | Tags

Transit Gateway ID	tgw-0174e65e24e6ed02e	**Owner account ID**	[redacted]
State	available	**Amazon ASN**	64512
DNS support	enable	**ECMP support**	-
Auto approve shared attachments	disable	**Default association route table**	enable
Association route table ID	tgw-rtb-05c844b0ae308a214	**Default propagation route table**	enable
Propagation route table ID	tgw-rtb-05c844b0ae308a214		

aws

Create VPC Attachments



aws Services Resource Groups

Transit Gateway attachments > Create Transit Gateway attachment

Create Transit Gateway attachment

Create a VPC or VPN attachment to a Transit Gateway.

Transit Gateway ID* tgw-0174e65e24e6ed02e

Attachment Type (•) VPC ( ) VPN

VPC Attachment

Select a VPC that you would like to attach to the Transit Gateway.

Name tag VPC-1-ATT

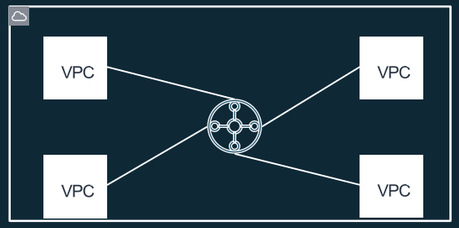
VPC ID vpc-0142574d0fb51ec5d

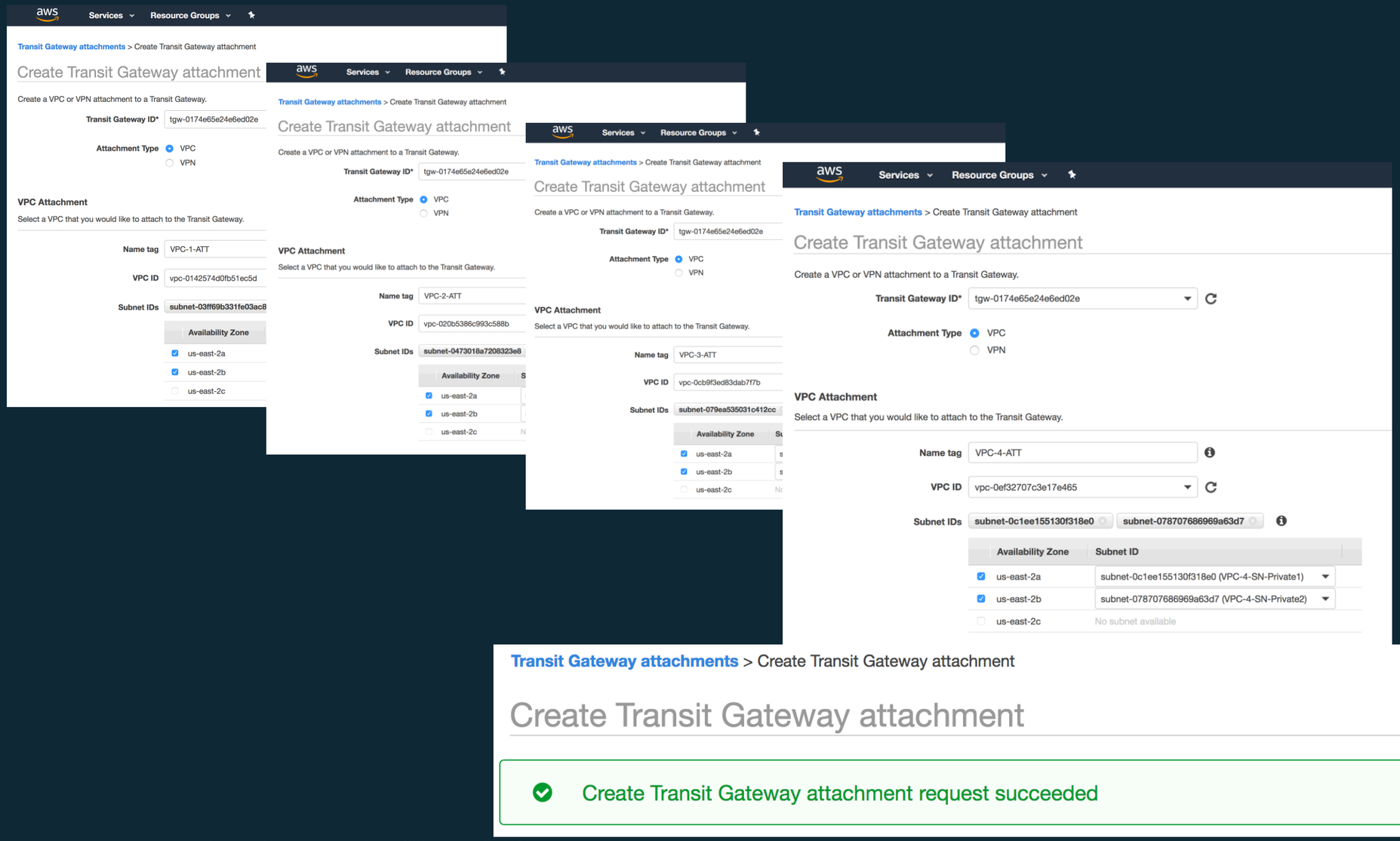
Subnet IDs subnet-03ff69b331fe03ac8 subnet-01a7781b44eb10568

	Availability Zone	Subnet ID
☑	us-east-2a	subnet-03ff69b331fe03ac8 (VPC-1-SN-Private1)
☑	us-east-2b	subnet-01a7781b44eb10568 (VPC-1-SN-Private2)
☐	us-east-2c	No subnet available

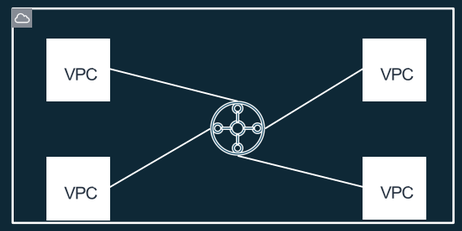
aws

Create VPC Attachments





View VPC Attachments



aws Services Resource Groups

Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections

Security
Network ACLs
Security Groups

VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections

Transit Gateways
Transit Gateways
Transit Gateway Attachments
Transit Gateway Route Tables

Create Transit Gateway attachment | Actions

Filter by tags and attributes or search by keyword

Transit Gateway attachment ID	Transit Gateway ID	Resource type	Resource ID	State	Associated route table ID	Association state
tgw-attach-0454fb69bb42c5258	tgw-0174e65e24e6ed02e	VPC	vpc-020b5386c993c588b	available	tgw-rtb-05c844b0ae308a214	associated
tgw-attach-0521c77259deb33d9	tgw-0174e65e24e6ed02e	VPC	vpc-0142574d0fb51ec5d	available	tgw-rtb-05c844b0ae308a214	associated
tgw-attach-0d1c68aa210848d48	tgw-0174e65e24e6ed02e	VPC	vpc-0cb9f3ed83dab7f7b	available	tgw-rtb-05c844b0ae308a214	associated
tgw-attach-0fc05db8116babc40	tgw-0174e65e24e6ed02e	VPC	vpc-0ef32707c3e17e465	available	tgw-rtb-05c844b0ae308a214	associated

Transit Gateway attachment: tgw-attach-0454fb69bb42c5258

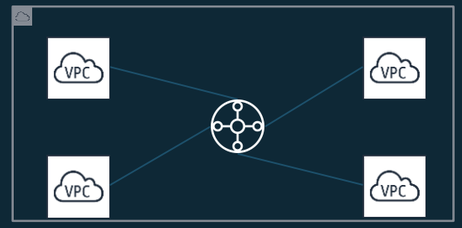
Details | Tags

Transit Gateway attachment ID tgw-attach-0454fb69bb42c5258
Transit Gateway owner ID [redacted]
Resource type VPC
State available
Association state associated

Transit Gateway ID tgw-0174e65e24e6ed02e
Resource owner account ID [redacted]
Resource ID vpc-020b5386c993c588b
Associated route table tgw-rtb-05c844b0ae308a214
Subnet IDs subnet-05095040d10f960de
subnet-0473018a7208323e8

aws

Transit Gateway Route Table



aws Services Resource Groups

- Elastic IPs
- Endpoints
- Endpoint Services
- NAT Gateways
- Peering Connections

Security

- Network ACLs
- Security Groups

VPN Connections

- Customer Gateways
- Virtual Private Gateways
- VPN Connections

Transit Gateways

- Transit Gateways
- Transit Gateway Attachments
- Transit Gateway Route Tables

Create Transit Gateway route table | Actions

Filter by tags and attributes or search by keyword

Name	Transit Gateway route table ID	Transit Gateway ID	State
	tgw-rtb-05c844b0ae308a214	tgw-0174e65e24e6ed02e	available

Transit gateway route table: tgw-rtb-05c844b0ae308a214

Details | Associations | Propagations | **Routes** | Tags

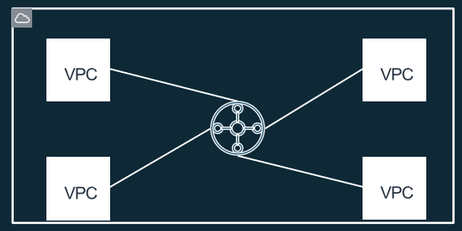
Create route | Delete route

Filter by attributes or search by keyword

CIDR	Attachment ID	Resource type	Resource ID	Route type	Route state
10.1.0.0/16	tgw-attach-0521c77259deb33d9	VPC	vpc-0142574d0fb51ec5d	propagated	active
10.2.0.0/16	tgw-attach-0454fb69bb42c5258	VPC	vpc-020b5386c993c588b	propagated	active
10.3.0.0/16	tgw-attach-0d1c68aa210848d48	VPC	vpc-0cb9f3ed83dab7f7b	propagated	active
10.4.0.0/16	tgw-attach-0fc05db8116babc40	VPC	vpc-0ef32707c3e17e465	propagated	active

aws

Update VPC Route Tables



aws Services Resource Groups

VPC Dashboard

Filter by VPC:

vpc-01425...

vpc-0142574d0fb51ec5

VPC-1

Virtual Private Cloud

- Your VPCs
- Subnets
- Route Tables
- Internet Gateways
- Egress Only Internet Gateways
- DHCP Options Sets
- Elastic IPs
- Endpoints
- Endpoint Services

Create Route Table | Delete Route Table | Set As Main Table

Search Route Tables and thei

Name	Route Table ID	Explicitly Associat	Main	VPC
VPC-1-RT-Private	rtb-0f127cab1e2dc1...	2 Subnets	No	vpc-0142574d0fb51ec5d | VPC-1
	rtb-0b108ccbcad3b...	0 Subnets	Yes	vpc-0142574d0fb51ec5d | VPC-1
VPC-1-RT-Public	rtb-0f5816b6a840a...	2 Subnets	No	vpc-0142574d0fb51ec5d | VPC-1

rtb-0f127cab1e2dc1196 | VPC-1-RT-Private

Summary | Routes | Subnet Associations | Route Propagation | Tags

Cancel | Save

View: All rules

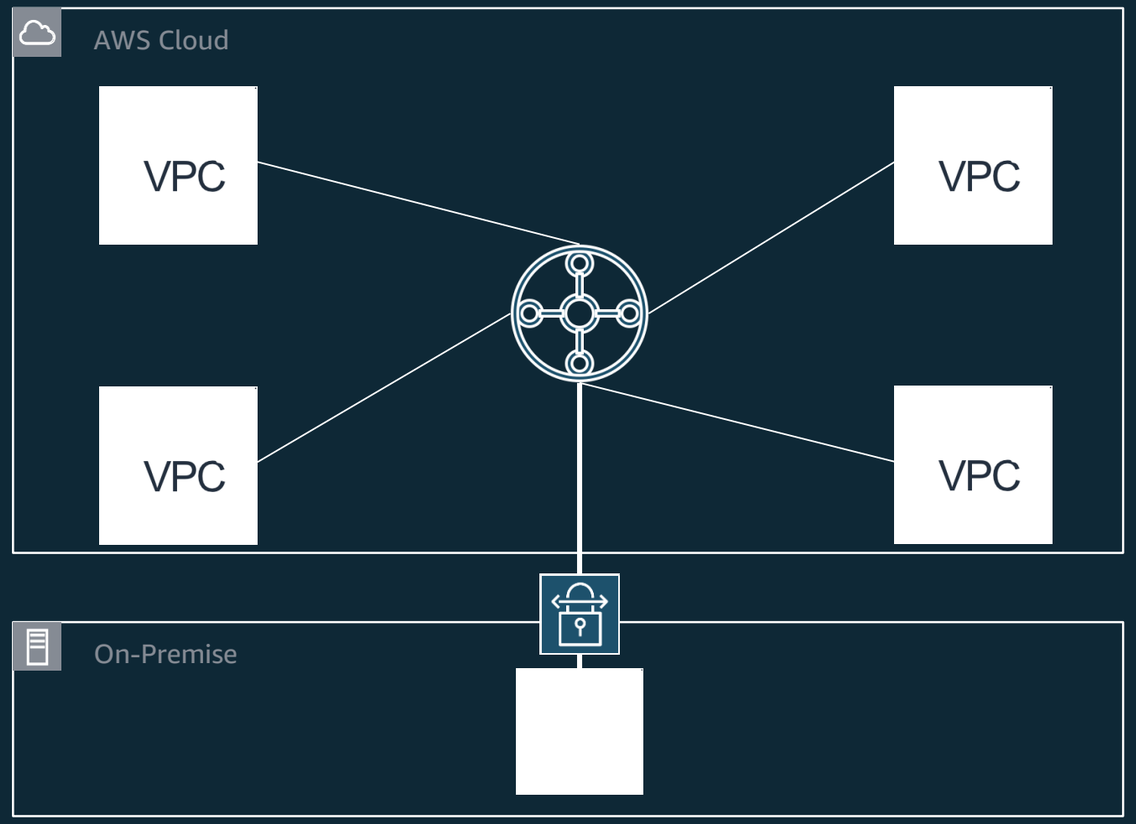
Destination	Target	Status	Propagated	Remove
10.1.0.0/16	local	Active	No	
10.0.0.0/8	tgw-0174e65e24e6ed02		No	

Add another route

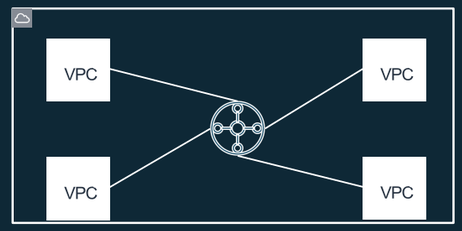
aws

Scenario

- Connecting Multiple VPC’s
- Any to any communication
- Sharing a single VPN Connection



Test Connectivity

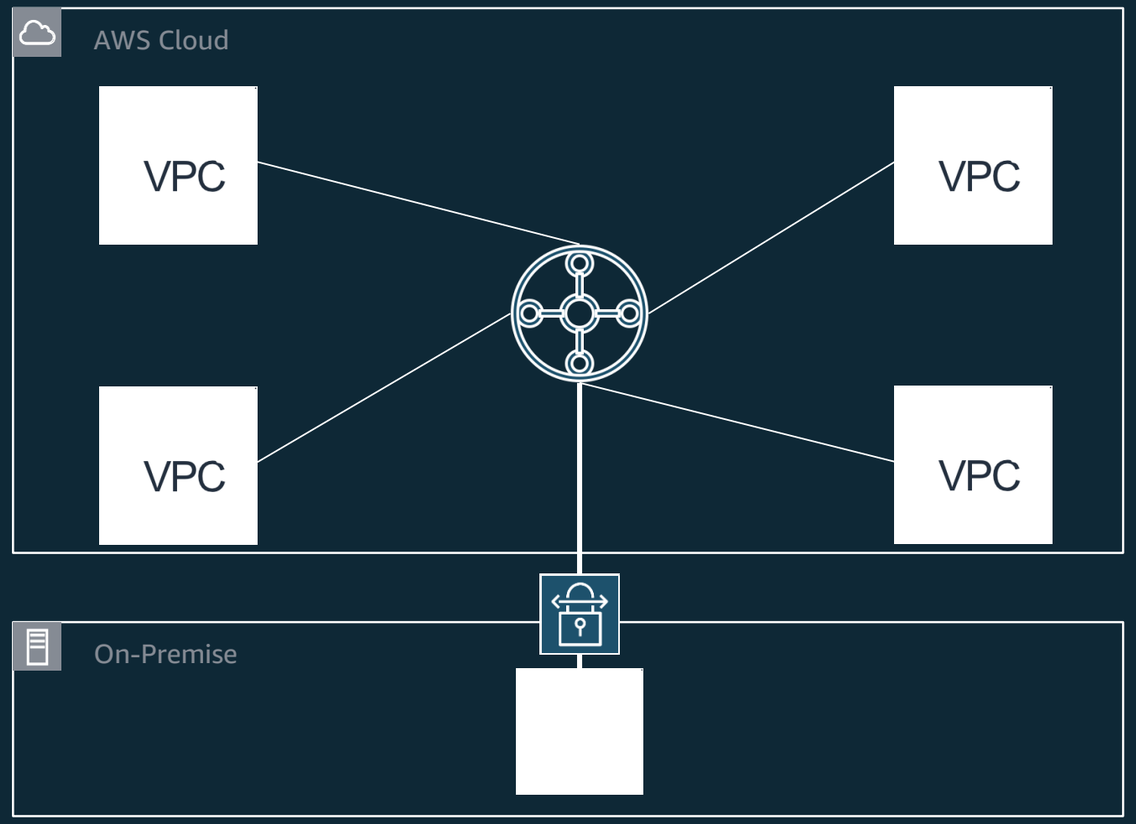


Name	Instance ID	Instance Type	Instance State	VPC ID	Private IP Addr
Instance-1-A	i-08fdbef264243bf76	t2.micro	running	vpc-0142574d0fb51ec5d	10.1.0.50
Instance-2-A	i-061b03d453f547ed8	t2.micro	running	vpc-020b5386c993c588b	10.2.0.50
Instance-3-A	i-06cfb15e33d42a58b	t2.micro	running	vpc-0cb9f3ed83dab7f7b	10.3.0.50
Instance-4-A	i-02d9df47ba3146f79	t2.micro	running	vpc-0ef32707c3e17e465	10.4.0.50

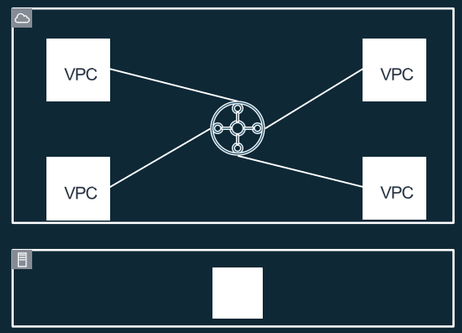
```
       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
[ec2-user@ip-10-1-0-50 ~]$
[ec2-user@ip-10-1-0-50 ~]$ for((i=2;i<5;i++)); do ping -c 1 -w 1 10.$i.0.50 &>/dev/null && echo 10.$i.0.50 is alive; done
10.2.0.50 is alive
10.3.0.50 is alive
10.4.0.50 is alive
[ec2-user@ip-10-1-0-50 ~]$
```

Scenario

- Connecting Multiple VPC’s
- Any to any communication
- Sharing a single VPN Connection



Create a VPN Attachment



aws Services Resource Groups

Transit Gateway attachments > Create Transit Gateway attachment

Create Transit Gateway attachment

Create a VPC or VPN attachment to a Transit Gateway.

Transit Gateway ID* tgw-0174e65e24e6ed02e

Attachment Type
- ○ VPC
- ◉ VPN

VPN Attachment

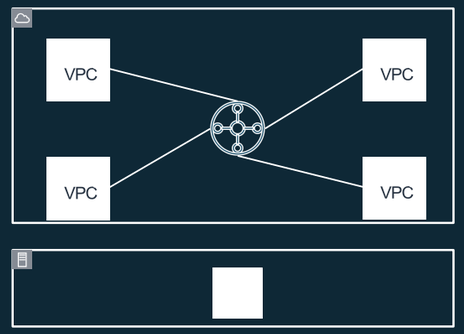
Create a new customer gateway or select an existing customer gateway that you would like to connect to the Transit Gateway via a VPN connection.

Customer Gateway
- ◉ Existing
- ○ New

Customer Gateway ID cgw-09e3cae25754cbfbf

aws

Download the Configuration



aws Services Resource Groups

NAT Gateways
Peering Connections

Security
Network ACLs
Security Groups

VPN Connections
Customer Gateways
Virtual Private Gateways
VPN Connections

Transit Gateways
Transit Gateways
Transit Gateway Attachments
Transit Gateway Route Tables

Create VPN Connection | Download Configuration | Actions

Filter by tags and attributes or search by

Name	VPN ID
	vpn-0f0d1d9575a22bd78

VPN Connection: vpn-0f0d1d9575a22bd78

Details | Tunnel Details | Tags

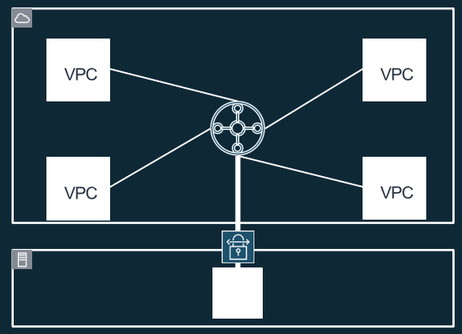
Outside IP Address	Inside IP CIDR
18.188.221.47	169.254.56.20/30
52.14.244.145	169.254.57.184/30

vpn-0f0d1d9575a22bd78.txt

```
azon Web Services
ual Private Cloud

! AWS utilizes unique identifiers to manipulate the configuration of
! a VPN Connection. Each VPN Connection is assigned an identifier and is
! associated with two other identifiers, namely the
! Customer Gateway Identifier and Virtual Private Gateway Identifier.
!
! Your VPN Connection ID                 : vpn-0f0d1d9575a22bd78
! Your Virtual Private Gateway ID        :
! Your Customer Gateway ID               : cgw-09e3cae25754cbfbf
!
!
! This configuration consists of two tunnels. Both tunnels must be
! configured on your Customer Gateway.
!
! ------------------------------------------------------------------------
! IPSec Tunnel #1
! ------------------------------------------------------------------------
! #1: Internet Key Exchange (IKE) Configuration
!
! A policy is established for the supported ISAKMP encryption,
! authentication, Diffie-Hellman, lifetime, and key parameters.
! Please note, these sample configurations are for the minimum requirement of AES128,
SHA1, and DH Group 2.
! Category "VPN" connections in the GovCloud region have a minimum requirement of AES128,
SHA2, and DH Group 14.
! You will need to modify these sample configuration files to take advantage of AES256,
SHA256, or other DH groups like 2, 14-18, 22, 23, and 24.
! Higher parameters are only available for VPNs of category "VPN," and not for "VPN-
```


aws

Complete – VPN UP



VPN Connection: vpn-0f0d1d9575a22bd78

Details | **Tunnel Details** | Tags

Outside IP Address	Inside IP CIDR	Status
18.188.221.47	169.254.56.20/30	UP
52.14.244.145	169.254.57.184/30	UP

Transit Gateway Route Table: tgw-rtb-05c844b0ae308a214

Details | Associations | Propagations | **Routes** | Tags

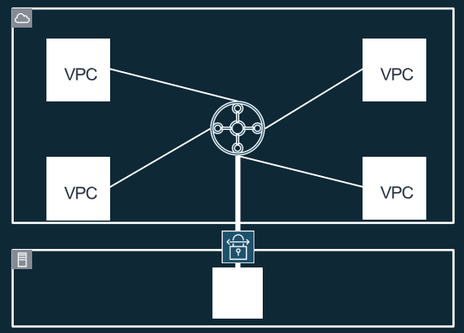
The table below will return a maximum of 1000 routes.

Create route | Delete route | Replace route

Filter by attributes or search by keyword — 1 to 6 of 6

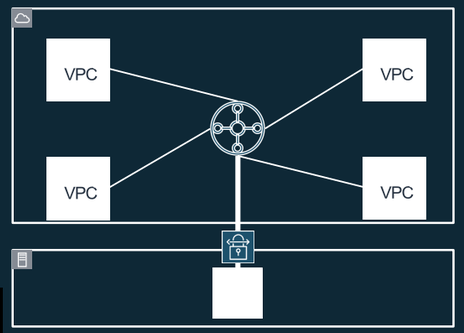
CIDR	Attachment ID	Resource type	Resource ID	Route type	Route state
0.0.0.0/0	tgw-attach-0521c77259deb33d9	VPC	vpc-0142574d0fb51ec5d	static	active
10.1.0.0/16	tgw-attach-0521c77259deb33d9	VPC	vpc-0142574d0fb51ec5d	propagated	active
10.2.0.0/16	tgw-attach-0454fb69bb42c5258	VPC	vpc-020b5386c993c588b	propagated	active
10.3.0.0/16	tgw-attach-0d1c68aa210848d48	VPC	vpc-0cb9f3ed83dab7f7b	propagated	active
10.4.0.0/16	tgw-attach-0fc05db8116babc40	VPC	vpc-0ef32707c3e17e465	propagated	active
10.99.99.0/24	tgw-attach-0216039bf48212a27	VPN	vpn-0f0d1d9575a22bd78	propagated	active

Complete – VPC to the CGW via VPN




```
       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/
[ec2-user@ip-10-1-0-50 ~]$ ping -c 5 10.99.99.50
PING 10.99.99.50 (10.99.99.50) 56(84) bytes of data.
64 bytes from 10.99.99.50: icmp_seq=1 ttl=253 time=115 ms
64 bytes from 10.99.99.50: icmp_seq=2 ttl=253 time=110 ms
64 bytes from 10.99.99.50: icmp_seq=3 ttl=253 time=108 ms
64 bytes from 10.99.99.50: icmp_seq=4 ttl=253 time=108 ms
64 bytes from 10.99.99.50: icmp_seq=5 ttl=253 time=119 ms

--- 10.99.99.50 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 108.045/112.625/119.811/4.541 ms
[ec2-user@ip-10-1-0-50 ~]$
```

Complete – view from the CGW




```
CGW-1#show ip bgp
BGP table version is 7, local router ID is 10.99.99.50
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  10.1.0.0/16      169.254.57.185         100             0 64512 e
*>                  169.254.56.21          100             0 64512 e
*  10.2.0.0/16      169.254.57.185         100             0 64512 e
*>                  169.254.56.21          100             0 64512 e
*  10.3.0.0/16      169.254.57.185         100             0 64512 e
*>                  169.254.56.21          100             0 64512 e
*  10.4.0.0/16      169.254.57.185         100             0 64512 e
*>                  169.254.56.21          100             0 64512 e
*> 10.99.99.0/24    0.0.0.0                  0         32768 i
CGW-1#
```

Transit Gateway Basics

Attachment

The connection from a Amazon VPC and VPN to a TGW

Association

The route table used to route packets coming from an attachment (from an Amazon VPC and VPN)

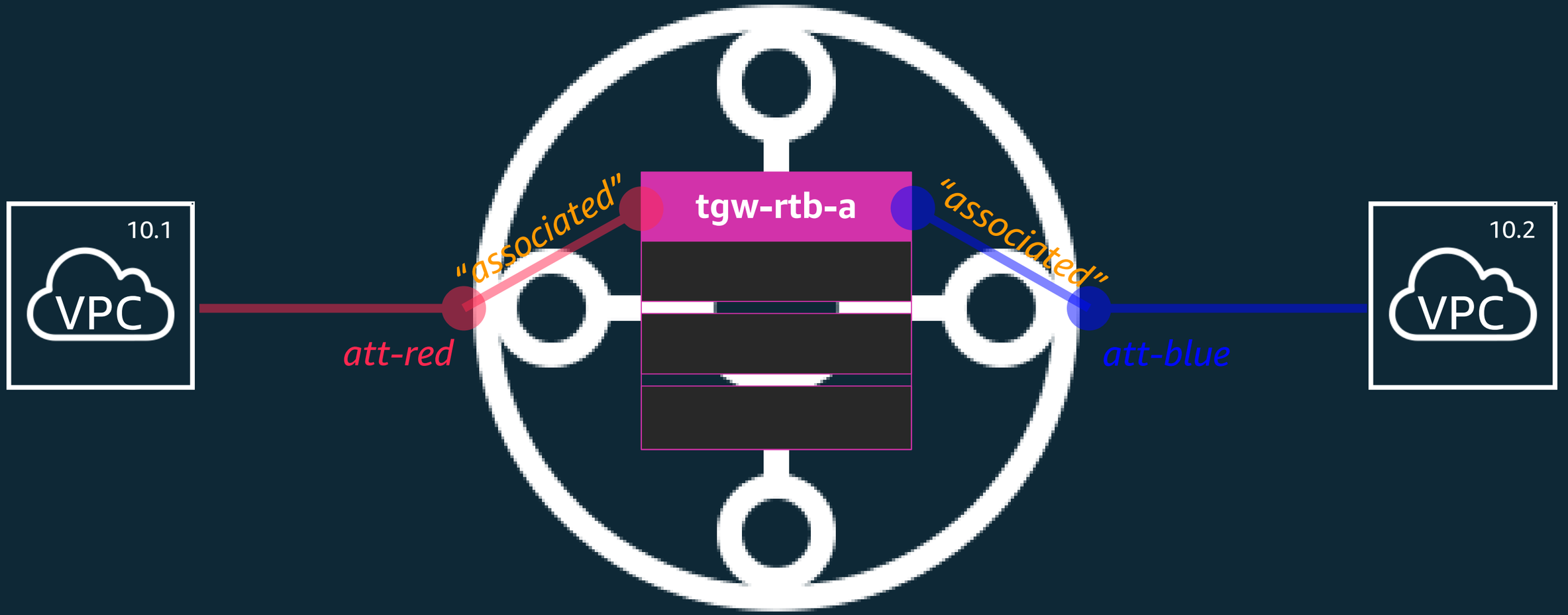
Propagation

The route table where the attachment's routes are installed

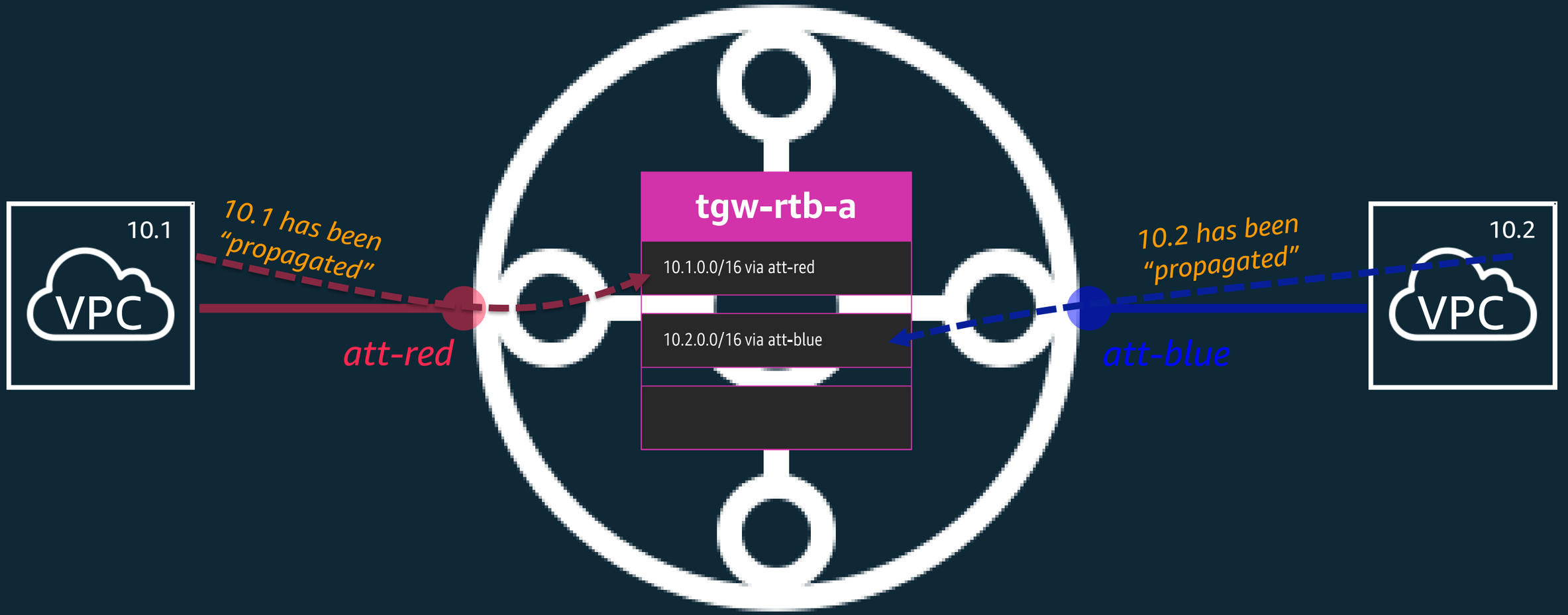
Attachments – VPC’s

Attachments – VPC’s

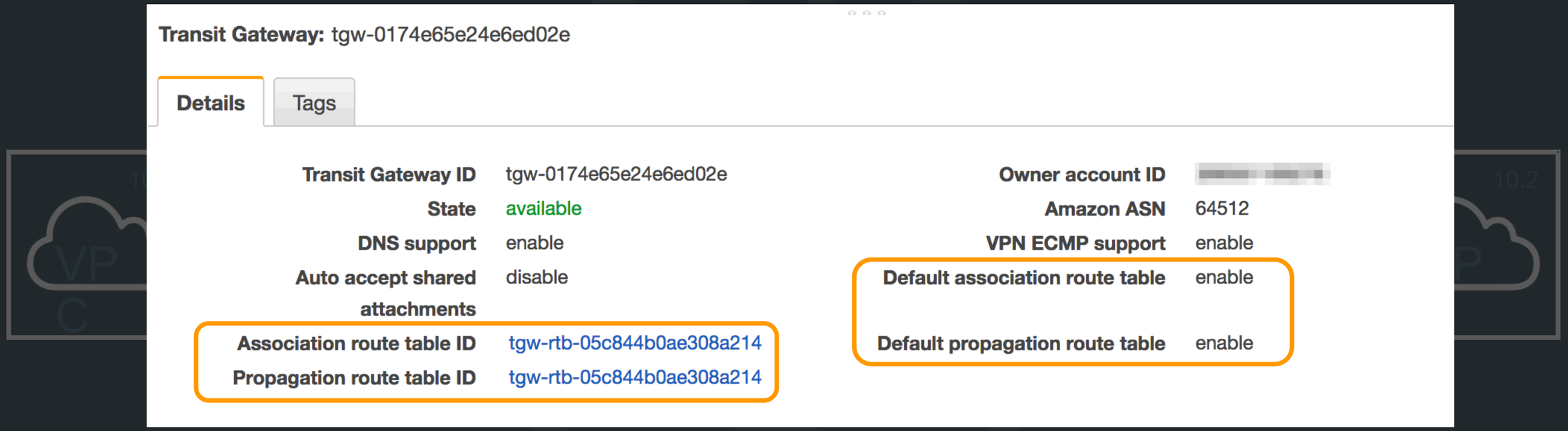
Attachments – ”associated” route table



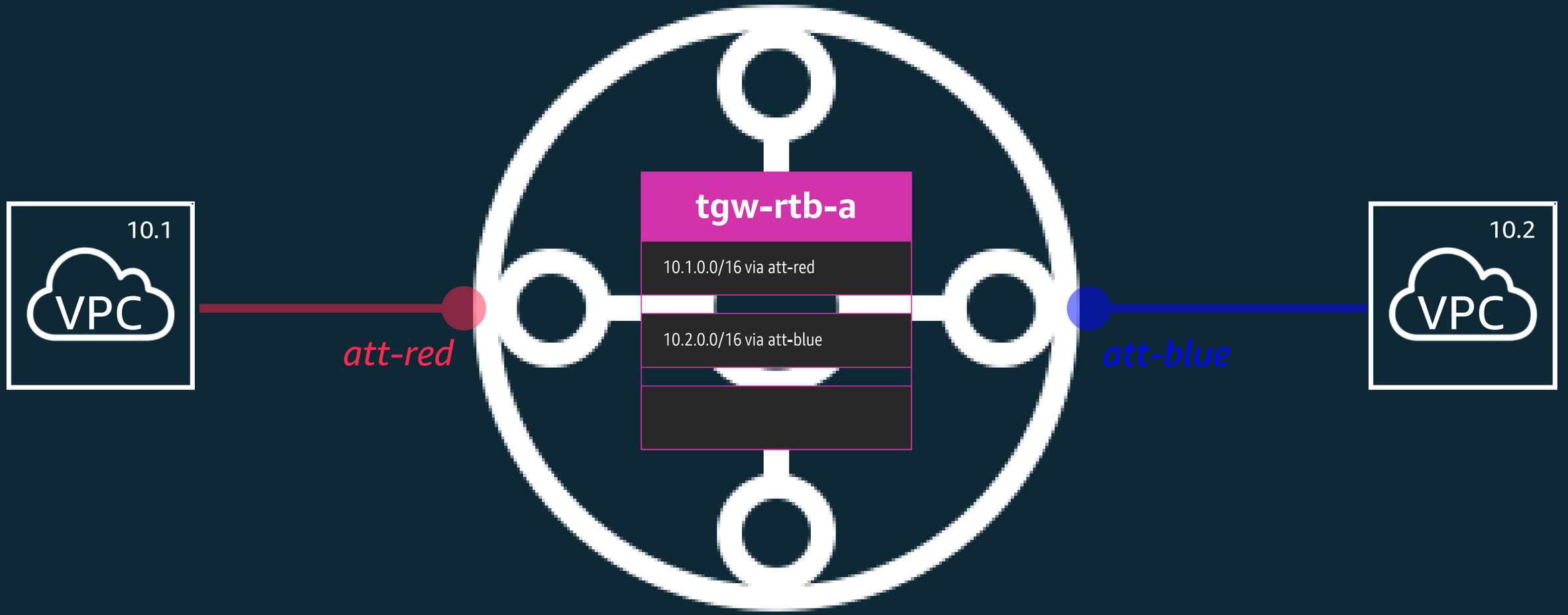
Attachments – “propagation” of routes



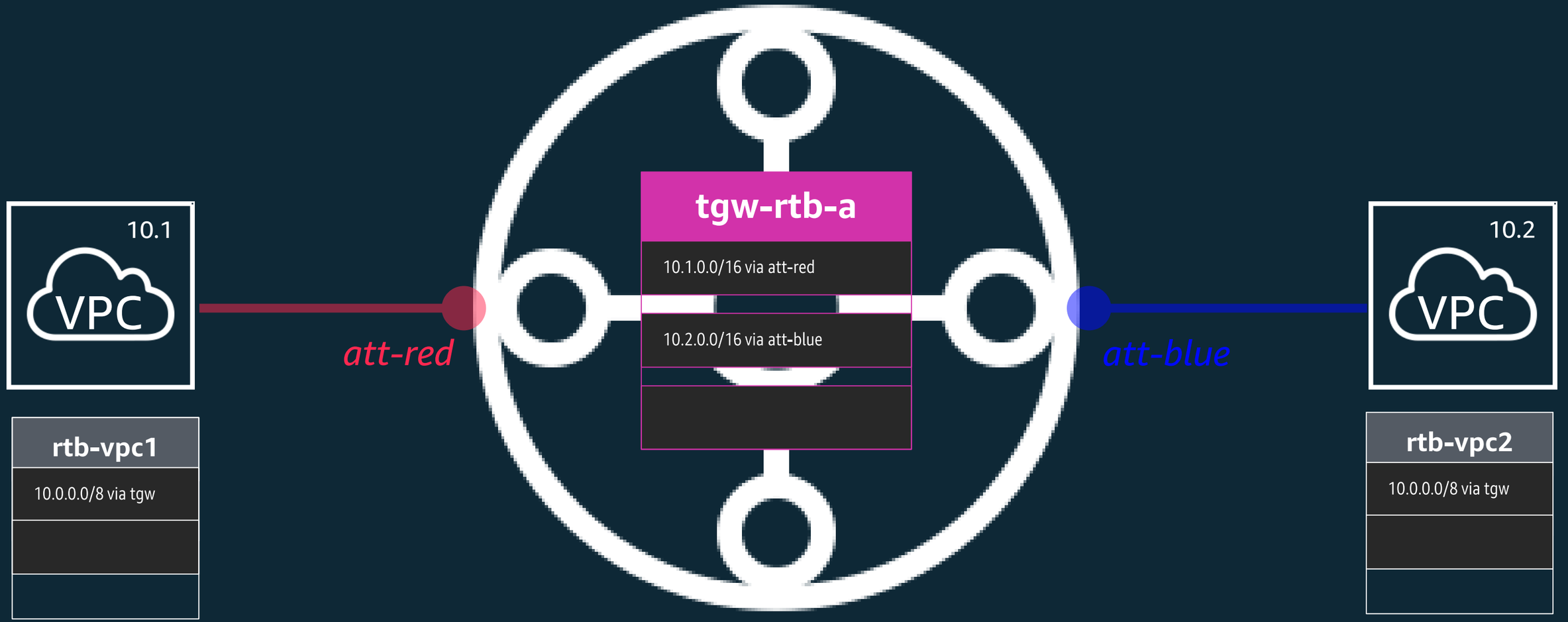
Attachments – ‘associated & propagated route table’



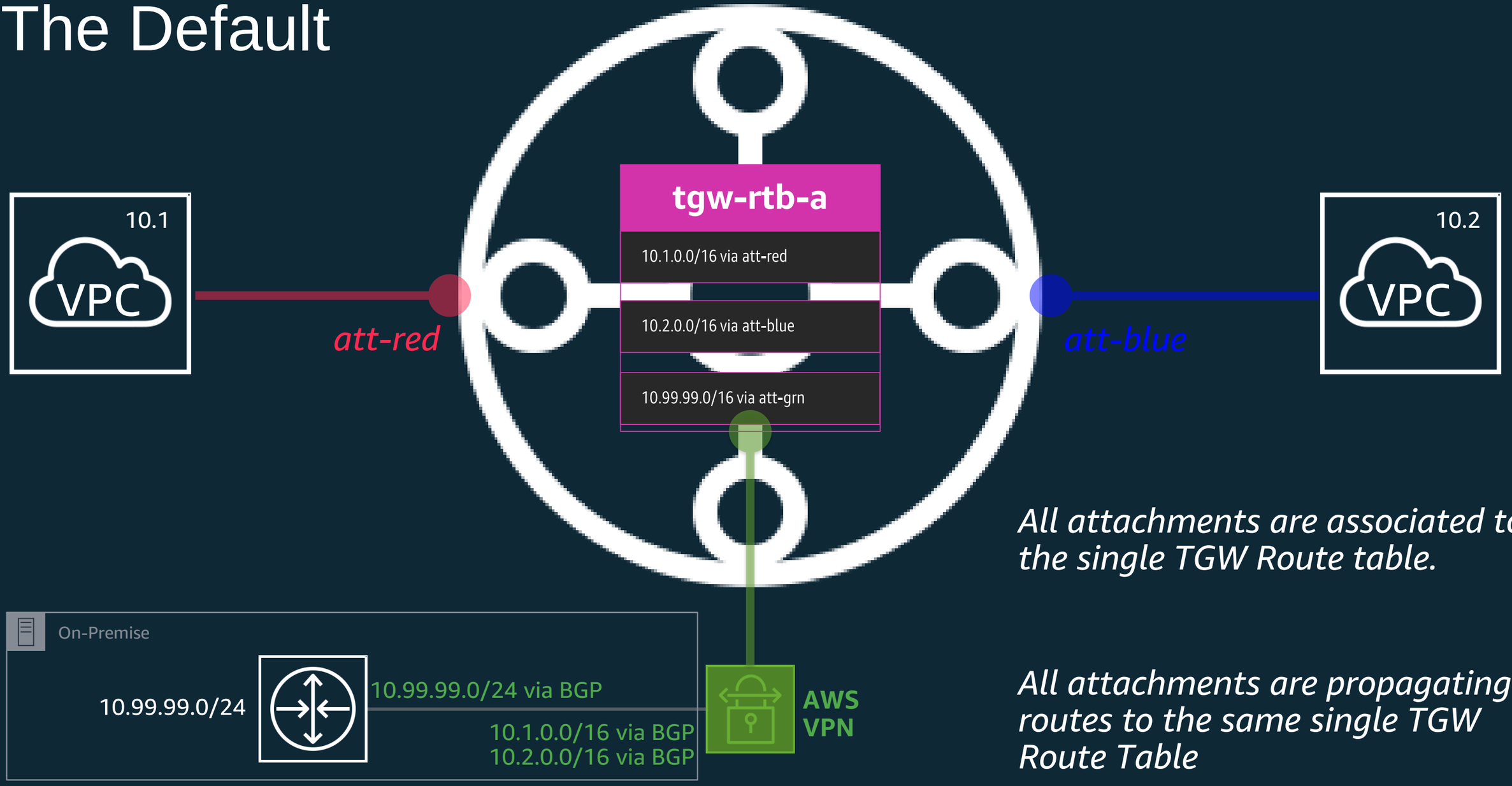
Attachments – TGW Route Table is complete



Attachments – VPC's Route Tables



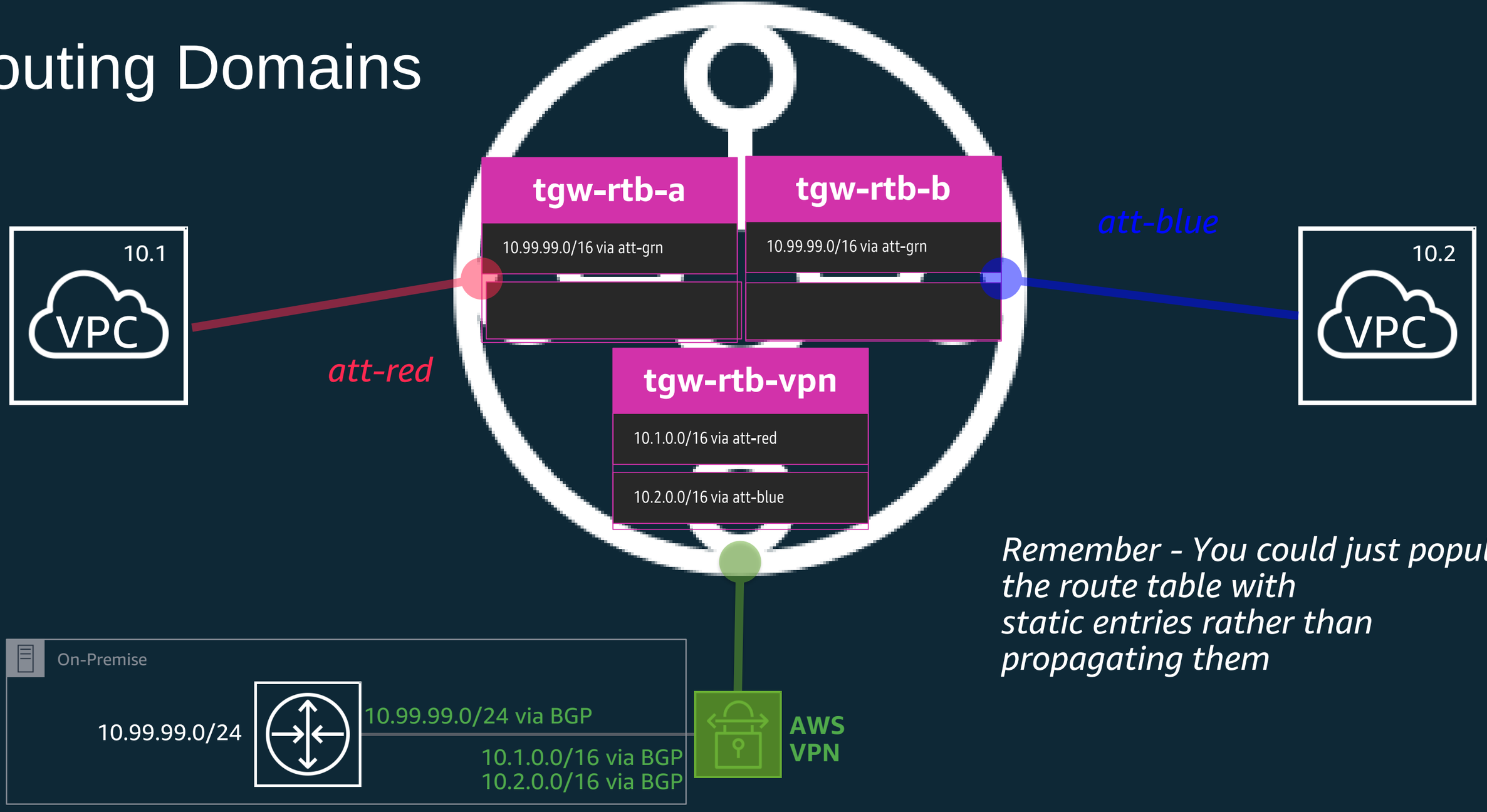
The Default



All attachments are associated to the single TGW Route table.

All attachments are propagating routes to the same single TGW Route Table

Routing Domains



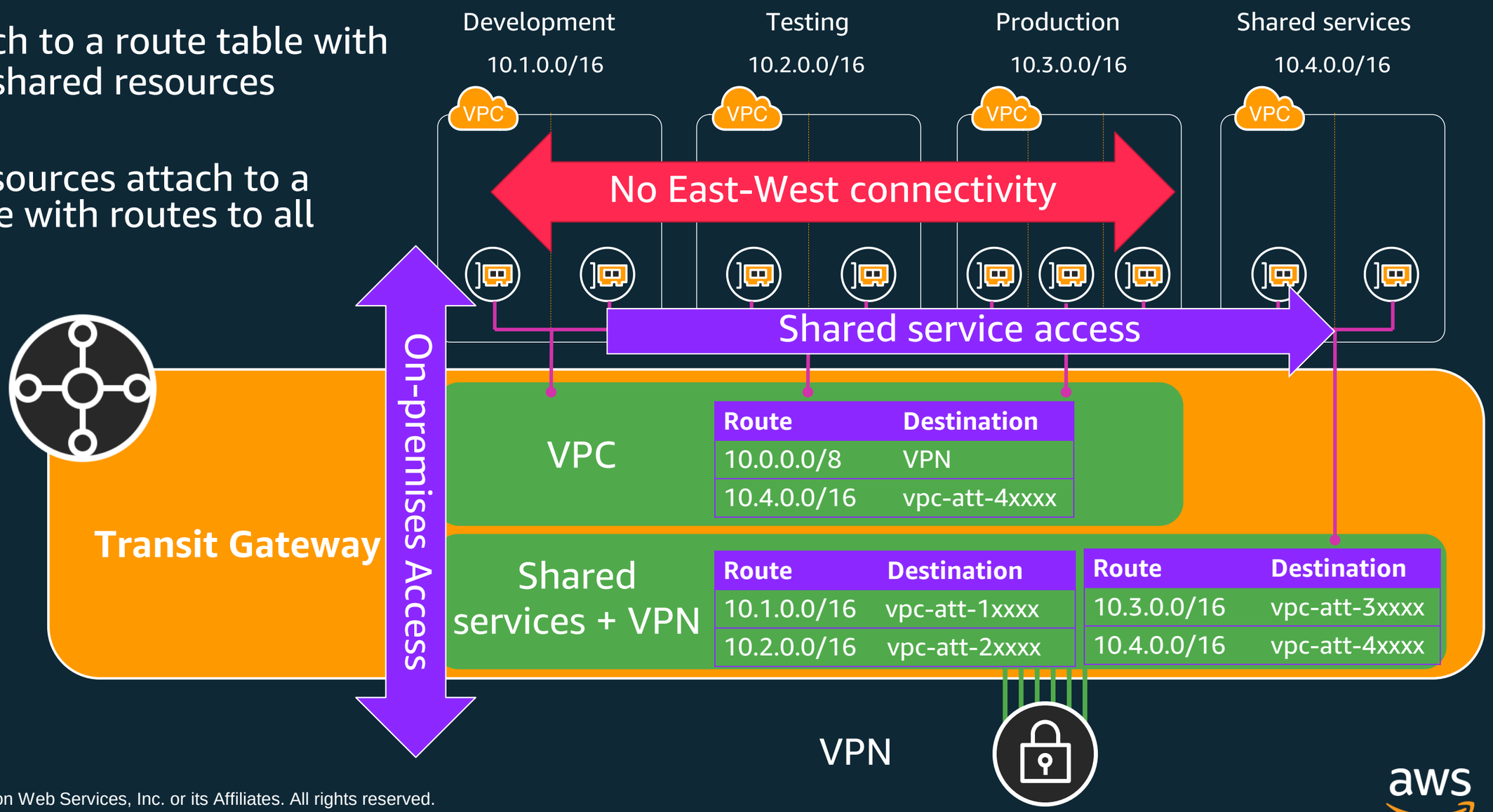
Remember - You could just populate the route table with static entries rather than propagating them

Transit Gateway Use Cases

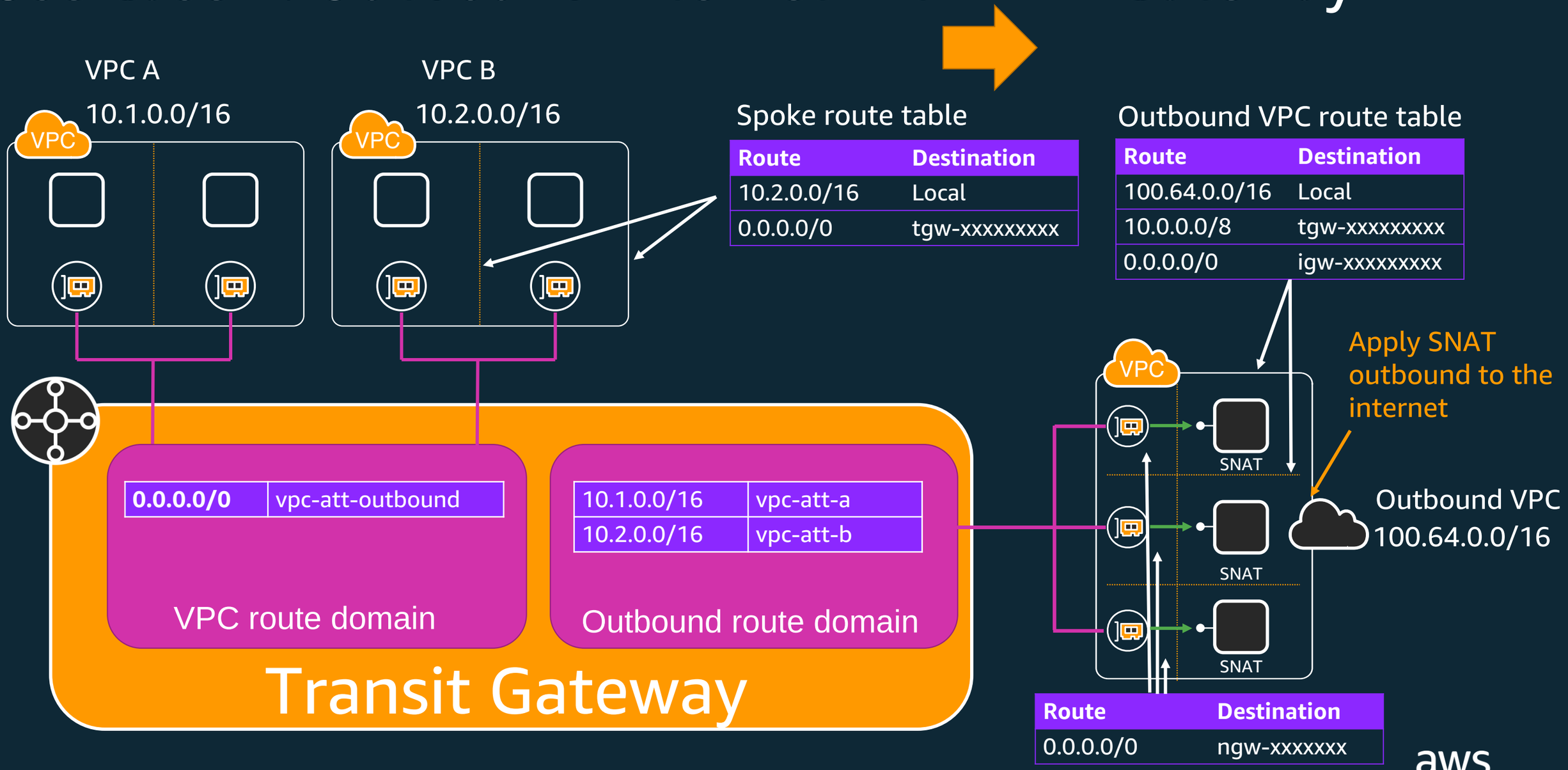
Use Case 1: Shared Services with Transit Gateway

VPCs attach to a route table with routes to shared resources

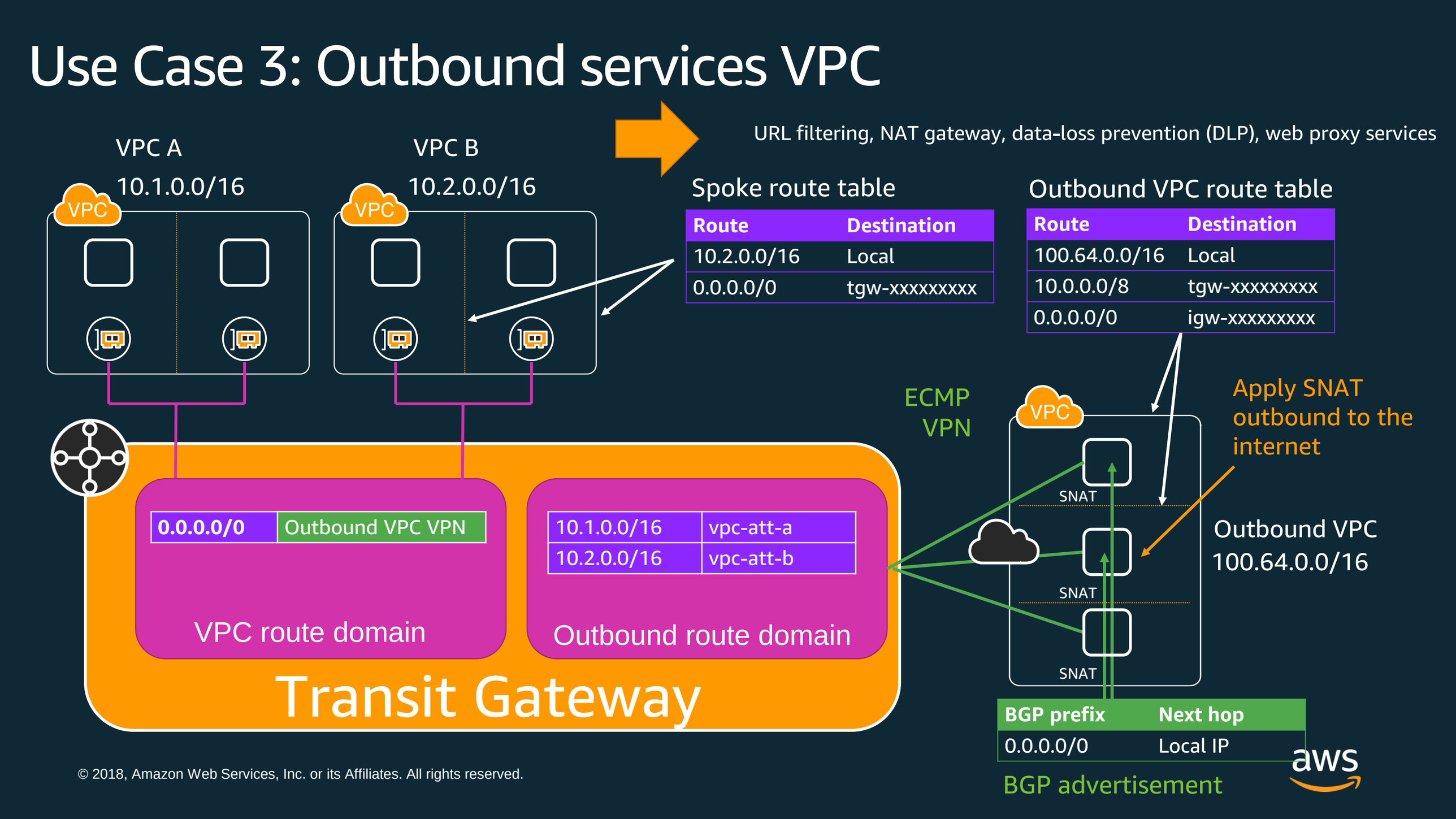
Shared resources attach to a route table with routes to all resources



Use Case 2: Outbound Internet with NAT Gateway

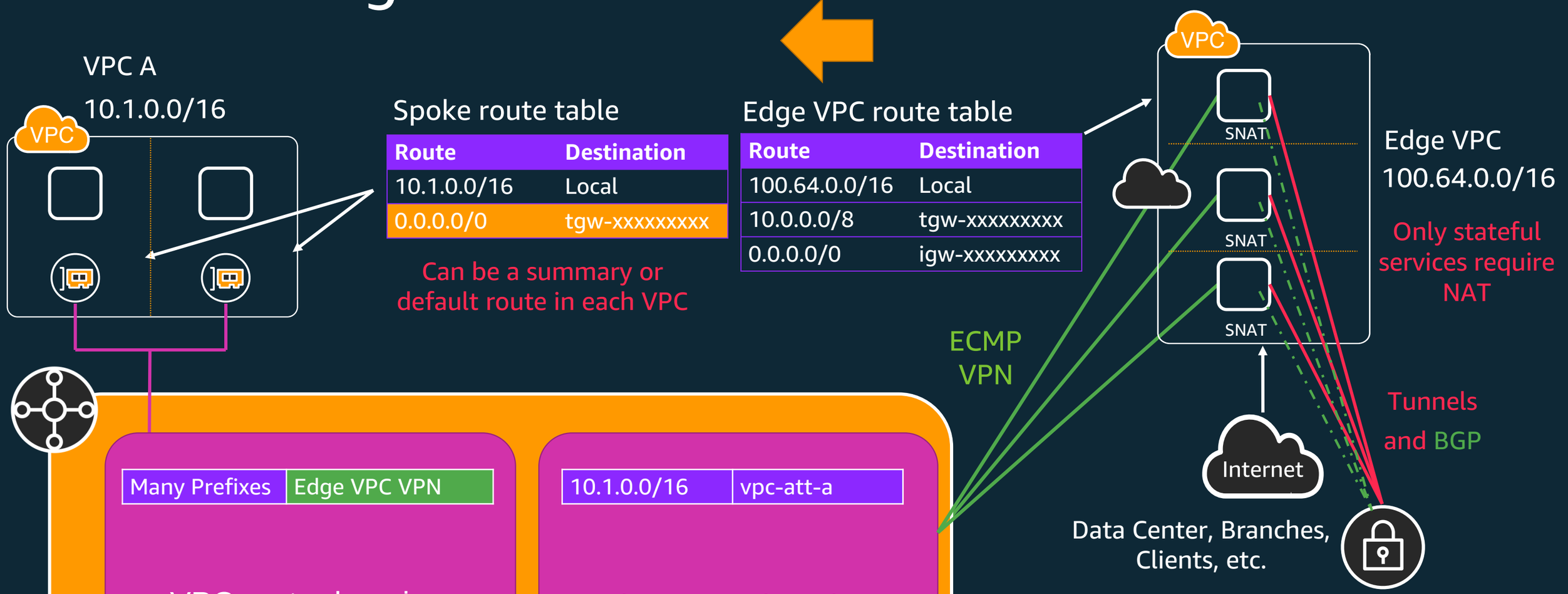


Use Case 3: Outbound services VPC



Use case 4: Edge services VPC: SD-WAN

BGP prefix	Next hop
Many prefixes	Local IP



Use cases:

SD-WAN, Routing, Third-party client VPN, AWS Direct Connect over a Private VIF

Future plans and Conclusion

Future Plans

- Direct Connect Gateway Attachments
- Transit Gateway Inter-Region Peering
- Additional advanced routing features

AWS Transit Gateway

- Easier connectivity
- Better visibility and control
- On-demand bandwidth
- Routing
- Edge connectivity
- Feature interoperability
- Monitoring
- Security

FAQ

- What is the bandwidth Limit for a VPC attachment?
- How does high availability of Transit Gateway work?
- Does it work with PrivateLink and Network Load Balancers?
- What if I am using SD-WAN, how do I connect Transit Gateway?
- Should I use multiple Transit Gateways or routing domains?
- How does Transit Gateway handle encryption?

Related Material

- Product Page

  https://aws.amazon.com/transit-gateway/
- Documentation

  https://docs.aws.amazon.com/vpc/latest/tgw/
- NET331 : Introducing AWS Transit Gateway (300 Level Deep Dive)

  https://youtu.be/yQGxPEGt_-w
- NET402 : Transit Gateway : Reference Architectures for Many VPC’s

  https://youtu.be/ar6sLmJ45xs

Thank you, questions?

tgw-feedback@amazon.com