Advanced architectures with AWS Transit Gateway

Tech Talk

Tom Adamski
Specialist Solutions Architect, Networking

Mar 2020

Agenda

- AWS Transit Gateway Recap
- Integrating Security Appliances
  - Egress Filtering
  - Ingress Filtering
  - VPC to VPC filtering
- Preserving IPv4 address space

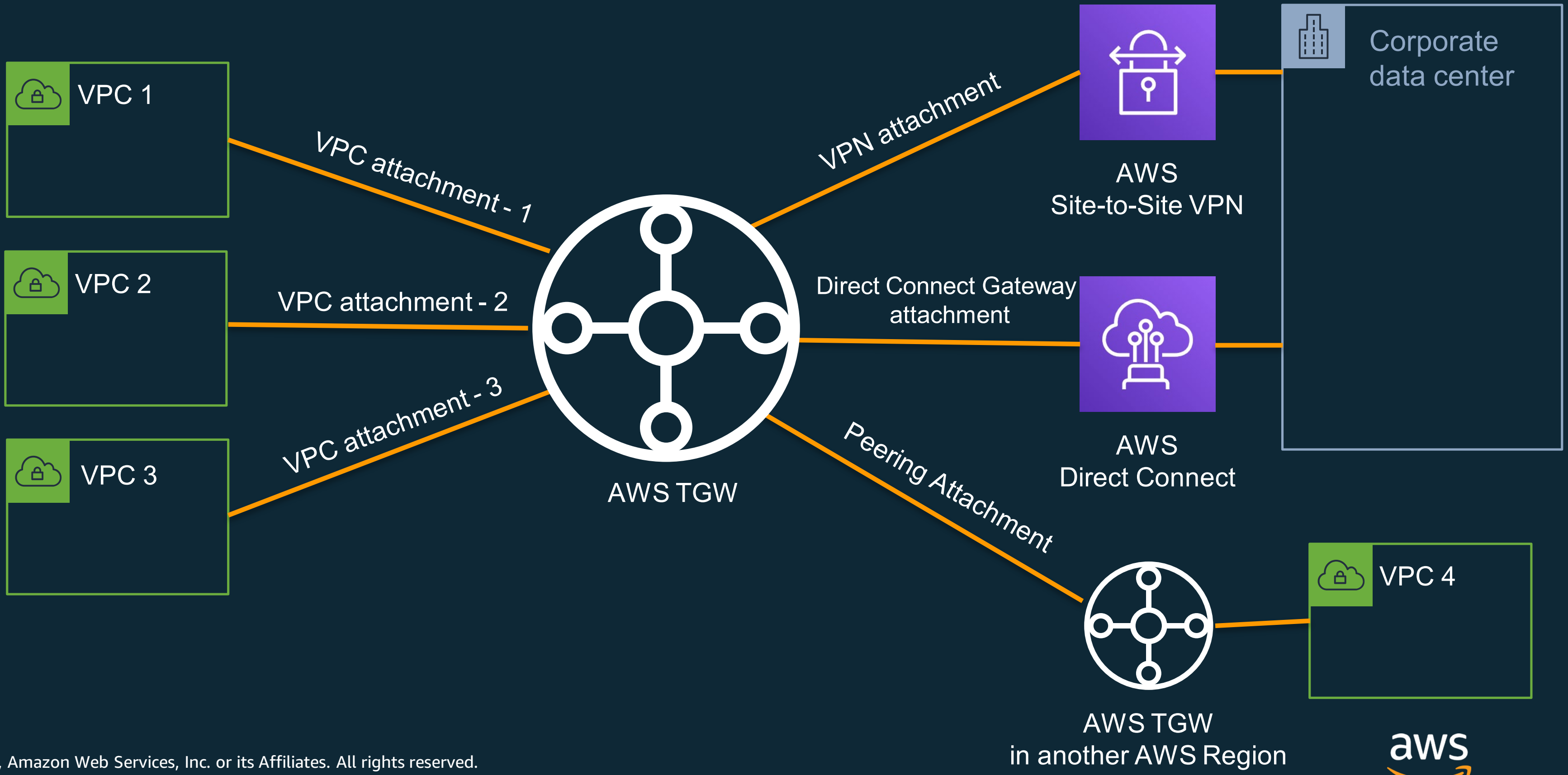
AWS Transit Gateway Recap

AWS Transit Gateway

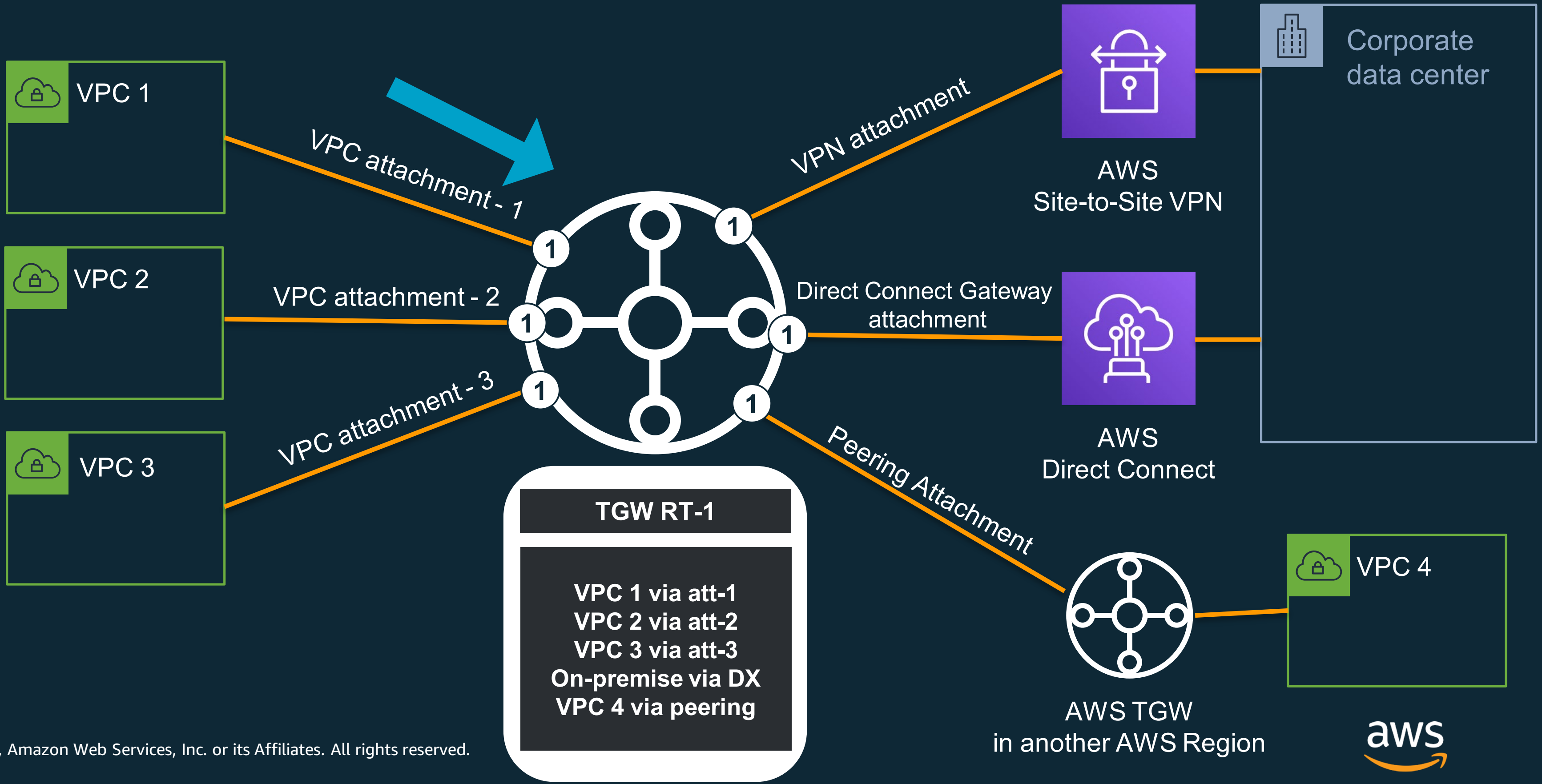
- Interconnecting VPCs at scale
- Consolidating edge connectivity
- Flexibility with routing domains

AWS Transit Gateway

AWS Transit Gateway Overview



AWS Transit Gateway Routing - Association



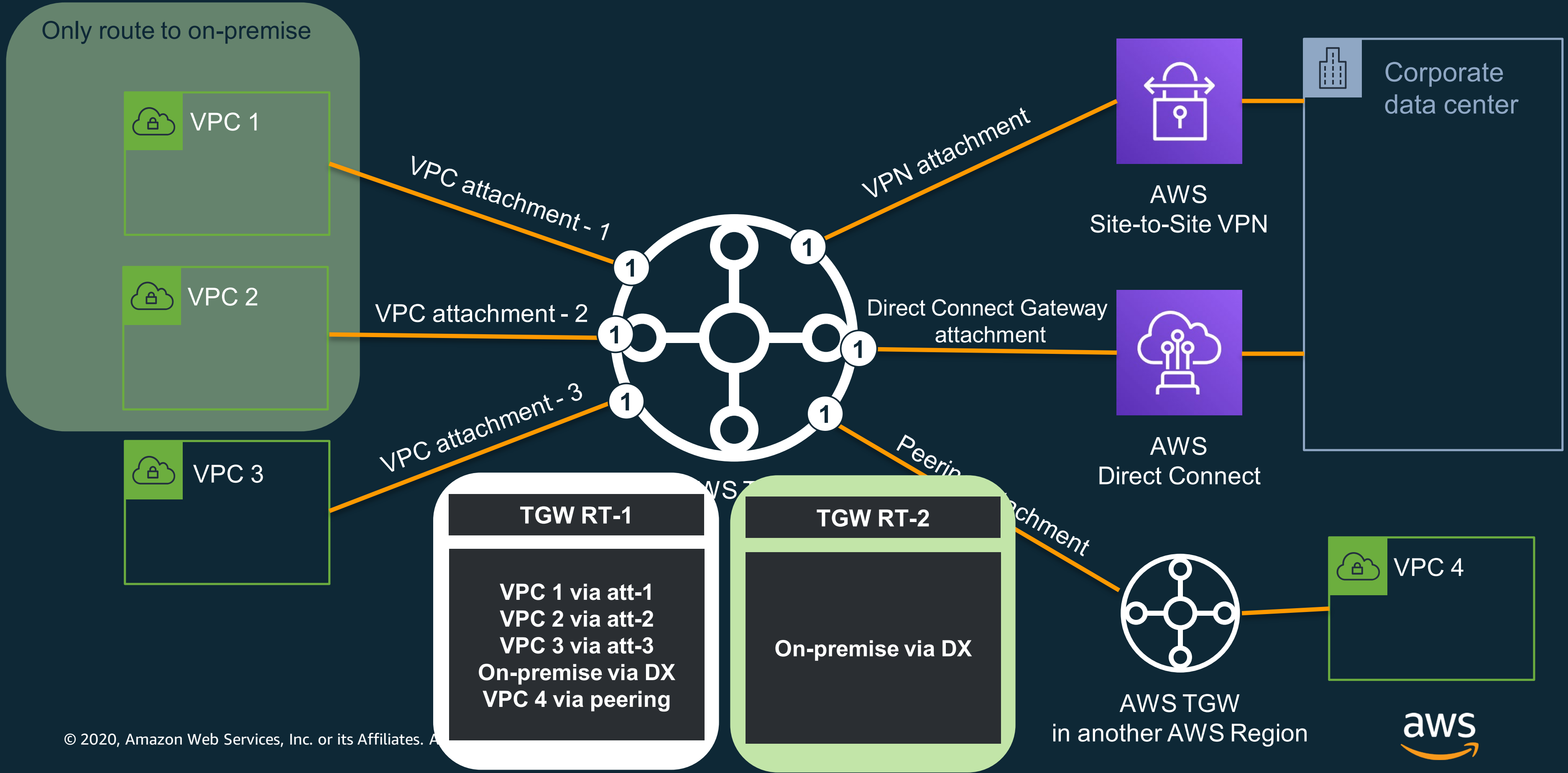
TGW RT-1

VPC 1 via att-1
VPC 2 via att-2
VPC 3 via att-3
On-premise via DX
VPC 4 via peering

Requirement:

- VPC 1 and VPC 2 can only reach on-premise networks
- VPC 1 and VPC 2 can’t reach each other or any other networks

AWS Transit Gateway Routing - Association



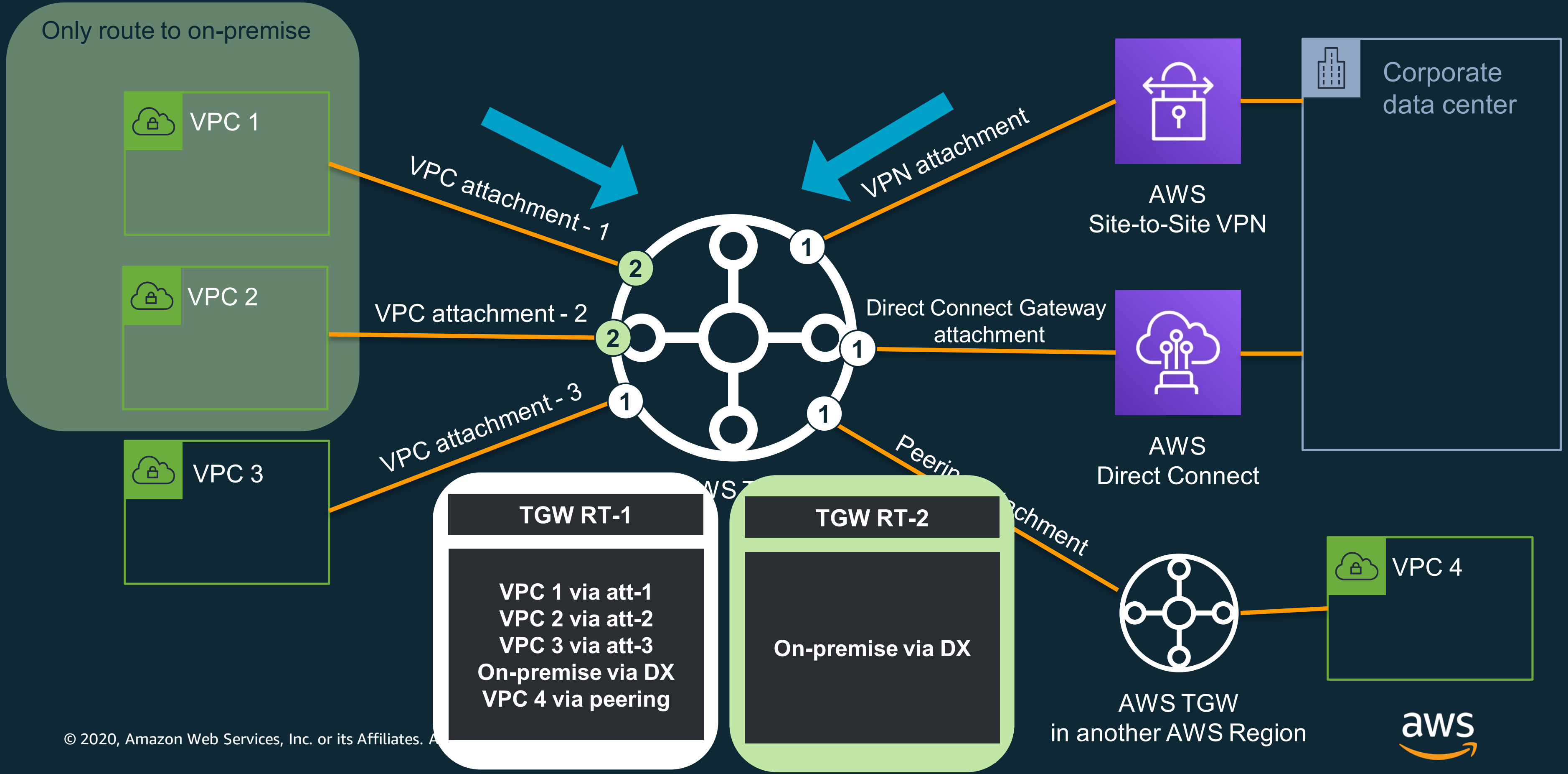
TGW RT-1

VPC 1 via att-1
VPC 2 via att-2
VPC 3 via att-3
On-premise via DX
VPC 4 via peering

TGW RT-2

On-premise via DX

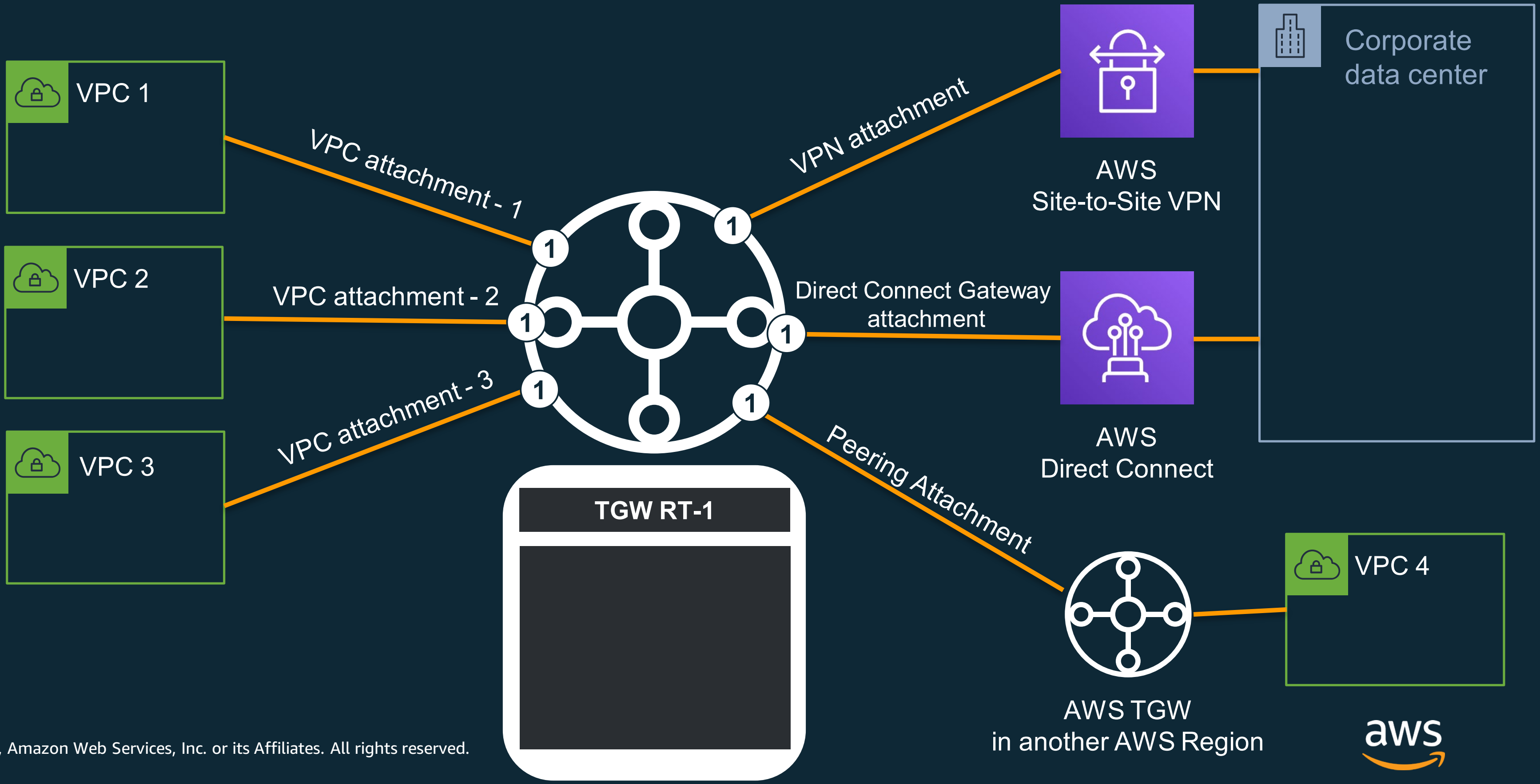
AWS Transit Gateway Routing - Association



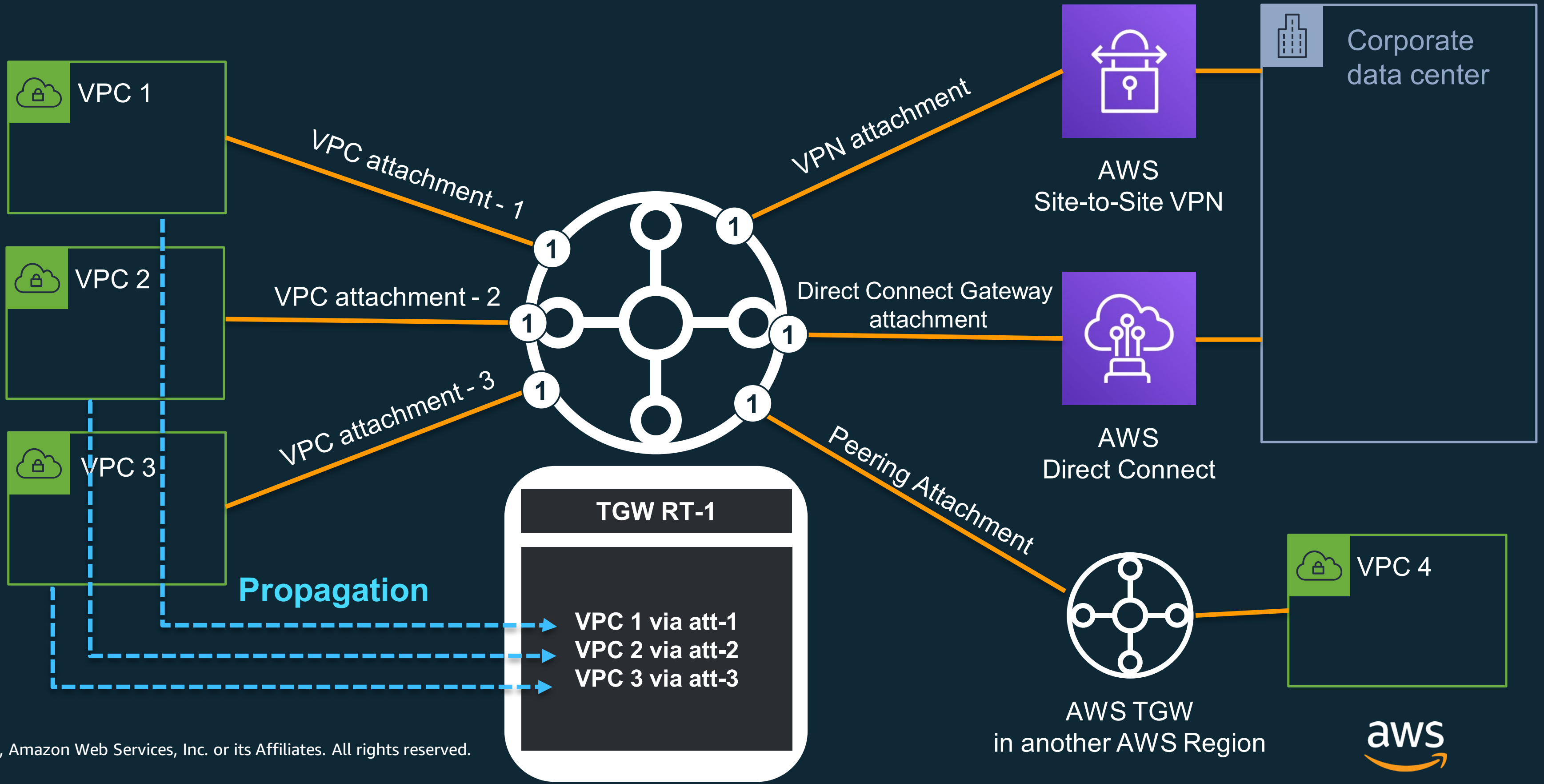
TGW RT-1
VPC 1 via att-1 VPC 2 via att-2 VPC 3 via att-3 On-premise via DX VPC 4 via peering

TGW RT-2
On-premise via DX

AWS Transit Gateway Routing - Propagation



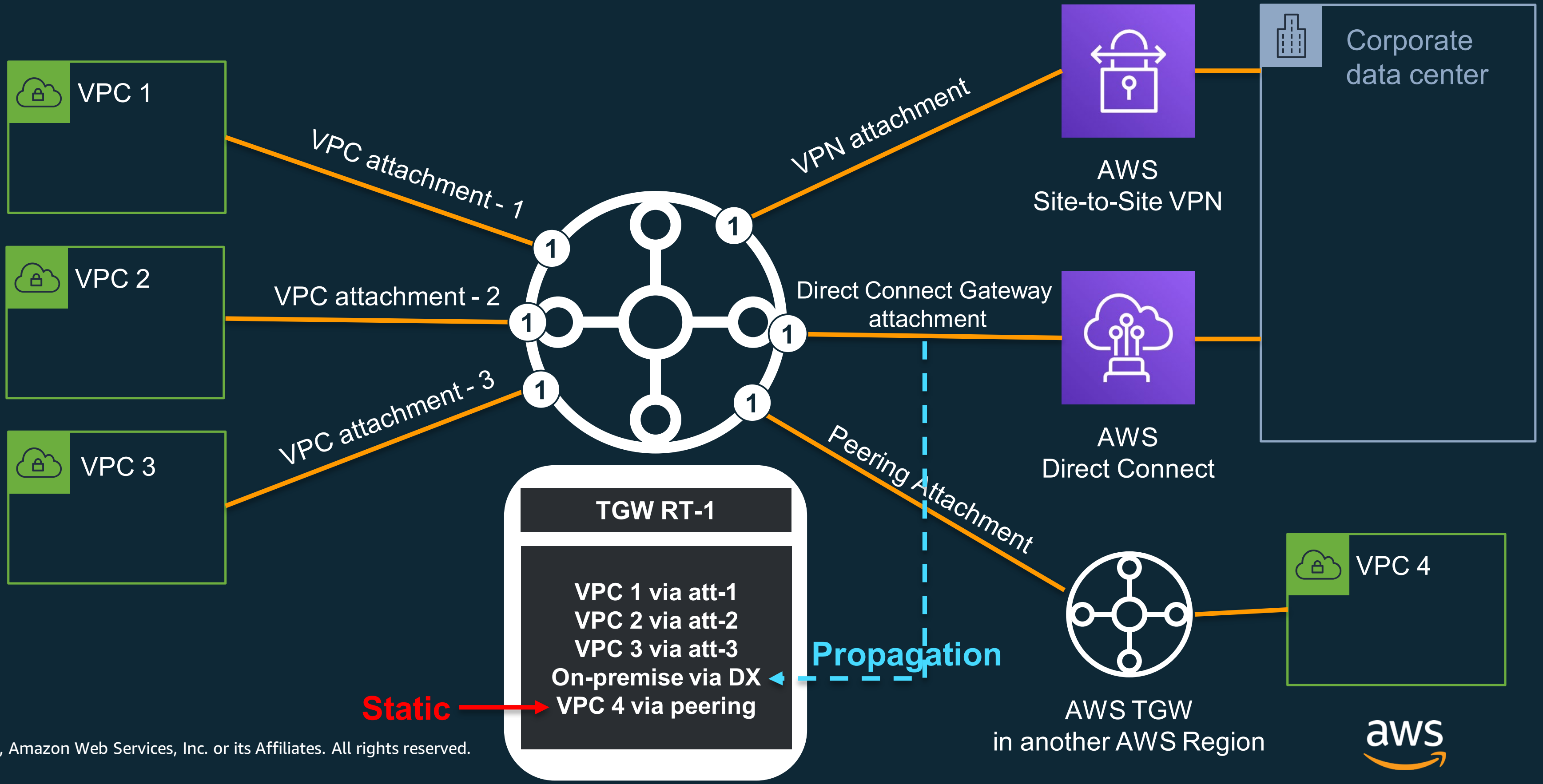
AWS Transit Gateway Routing - Propagation



TGW RT-1

VPC 1 via att-1
VPC 2 via att-2
VPC 3 via att-3

AWS Transit Gateway Routing - Propagation

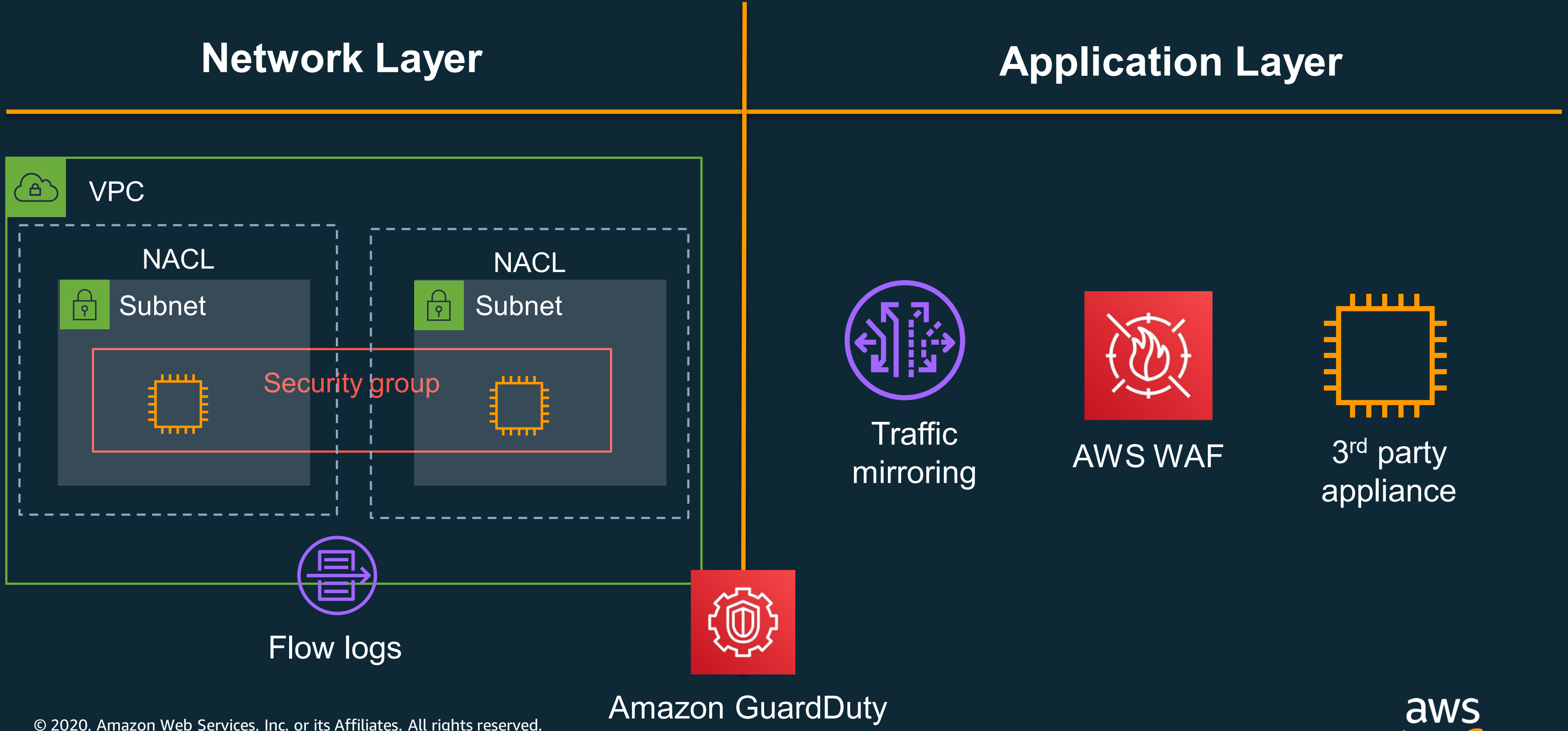


TGW RT-1

VPC 1 via att-1
VPC 2 via att-2
VPC 3 via att-3
On-premise via DX
VPC 4 via peering

Integrating Security Appliances

VPC Security Capabilities



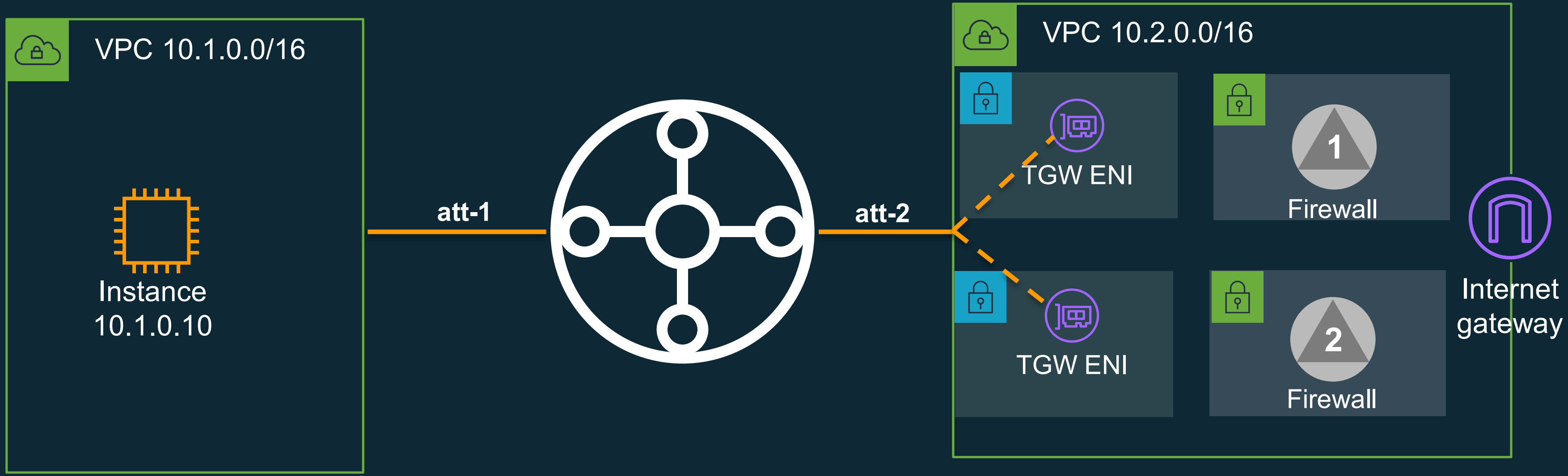
Egress Filtering with Transit Gateway

VPC Attachment Model

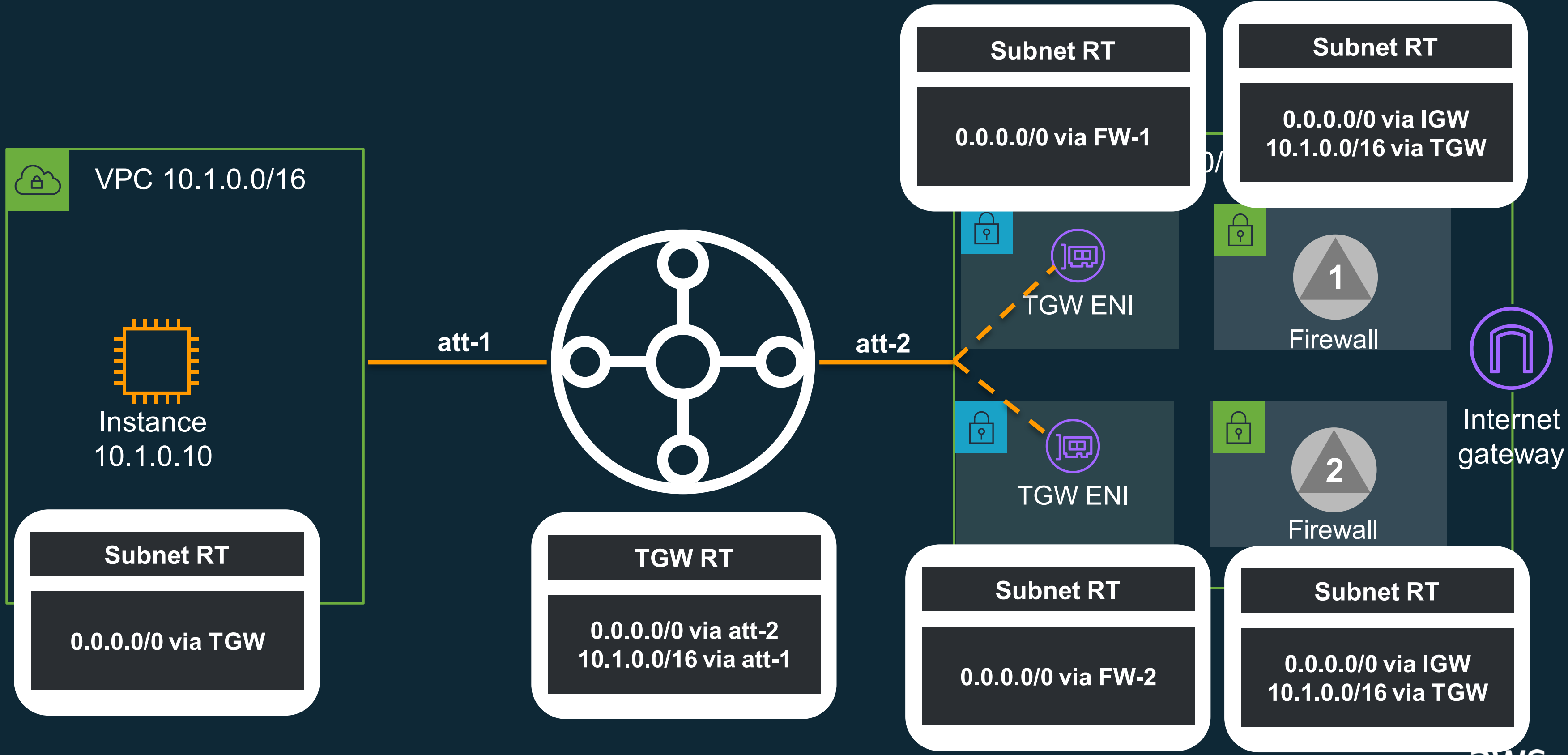
VPN Attachment Model

Explicit Proxy Model

VPC Attachment Model



VPC Attachment – Routing



Subnet RT

0.0.0.0/0 via TGW

TGW RT

0.0.0.0/0 via att-2
10.1.0.0/16 via att-1

Subnet RT

0.0.0.0/0 via FW-1

Subnet RT

0.0.0.0/0 via IGW
10.1.0.0/16 via TGW

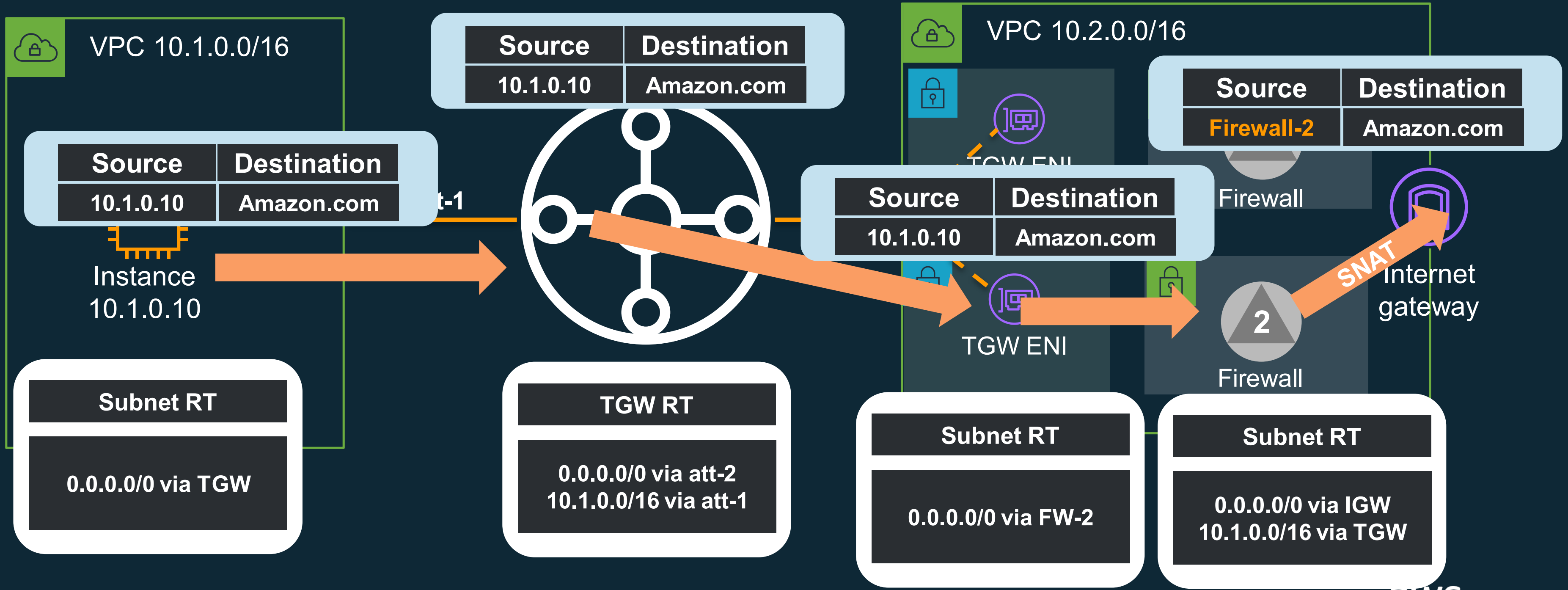
Subnet RT

0.0.0.0/0 via FW-2

Subnet RT

0.0.0.0/0 via IGW
10.1.0.0/16 via TGW

VPC Attachment – Traffic Flow



Source	Destination
10.1.0.10	Amazon.com

Source	Destination
10.1.0.10	Amazon.com

Source	Destination
10.1.0.10	Amazon.com

Source	Destination
Firewall-2	Amazon.com

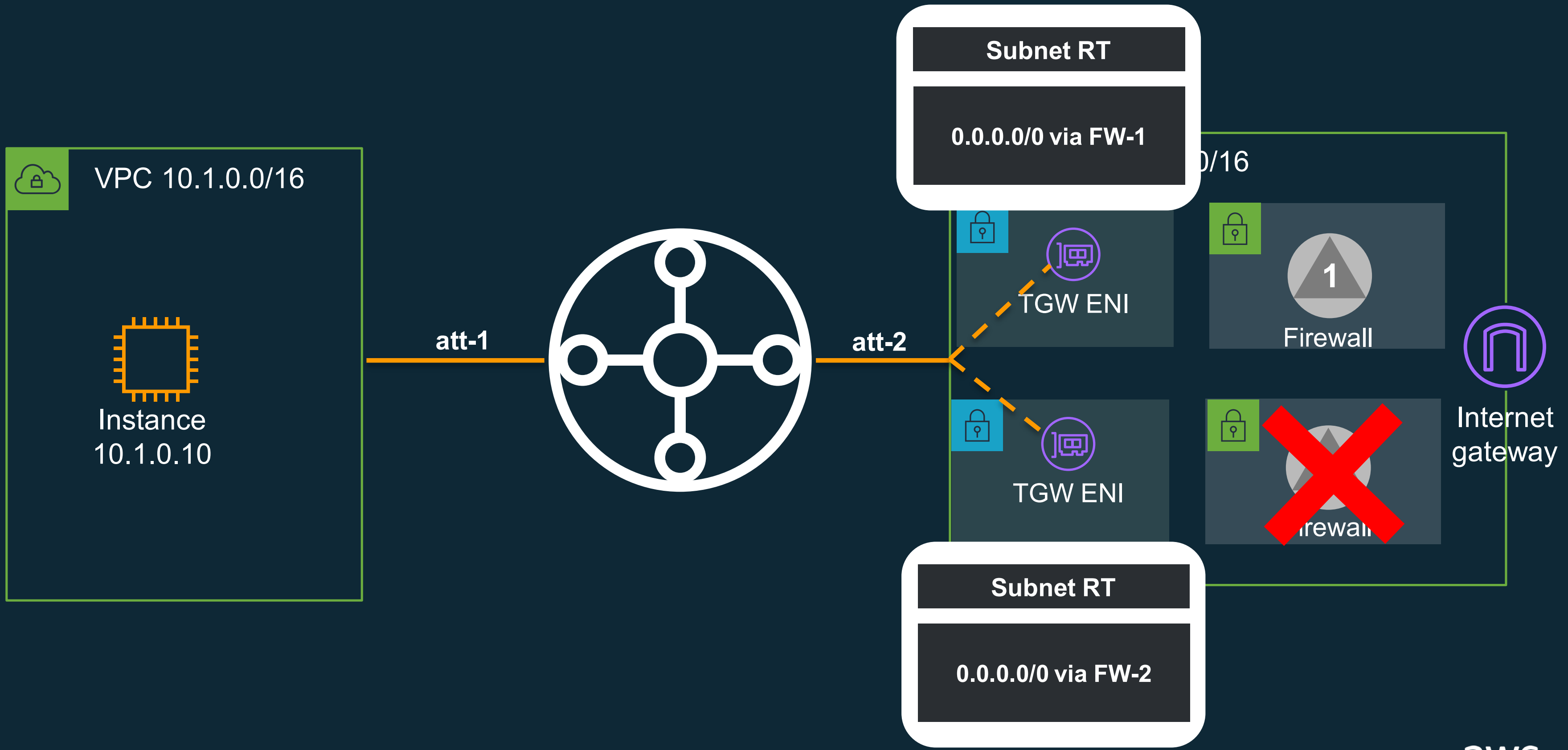
Subnet RT
0.0.0.0/0 via TGW

TGW RT
0.0.0.0/0 via att-2 10.1.0.0/16 via att-1

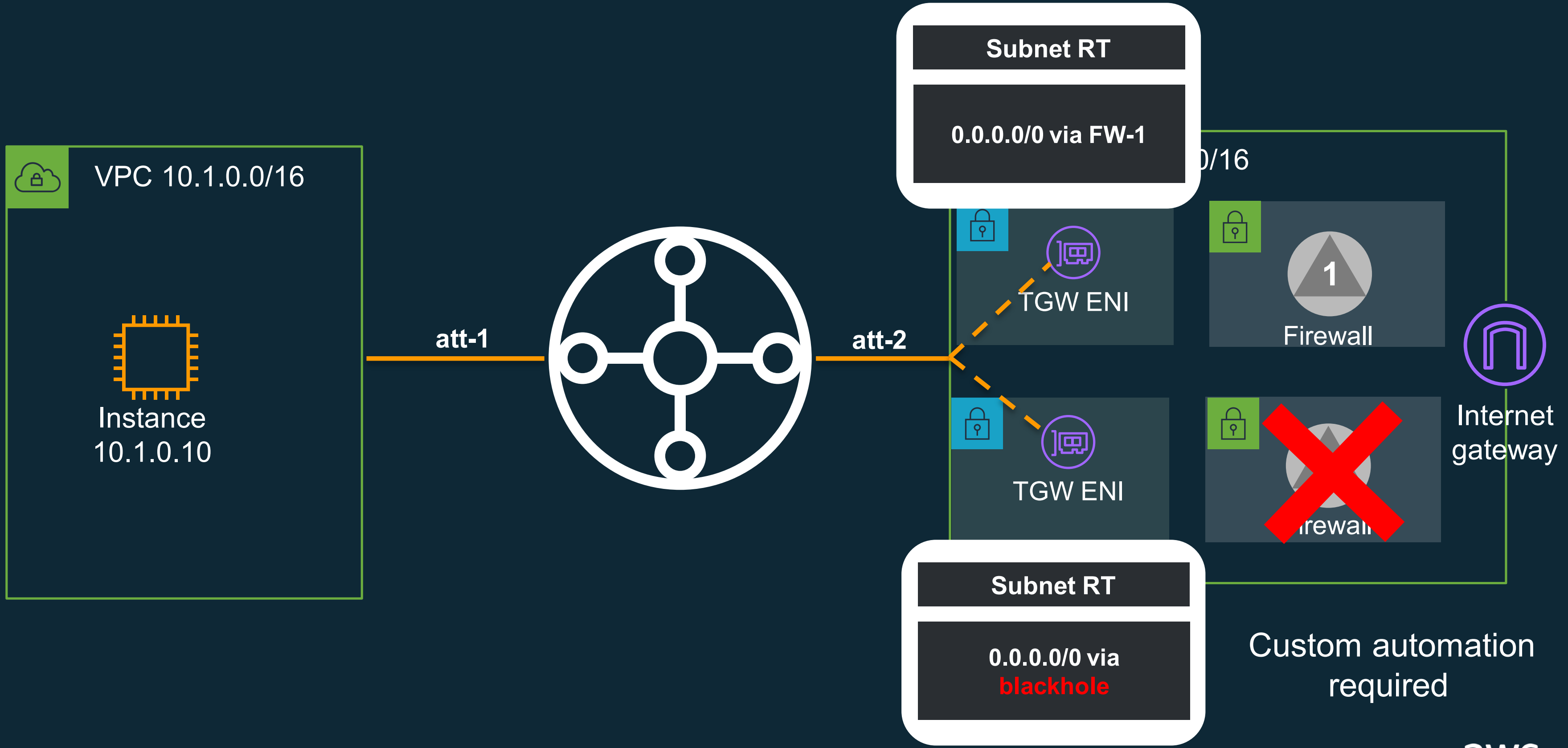
Subnet RT
0.0.0.0/0 via FW-2

Subnet RT
0.0.0.0/0 via IGW 10.1.0.0/16 via TGW

VPC Attachment – High Availability

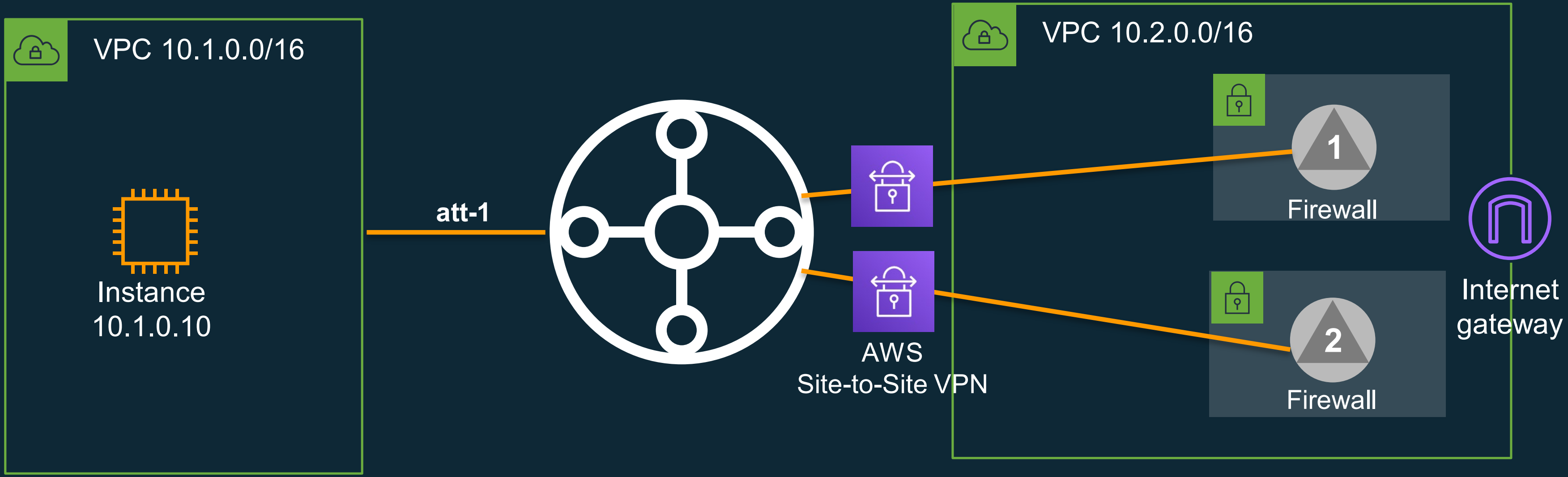


VPC Attachment – High Availability

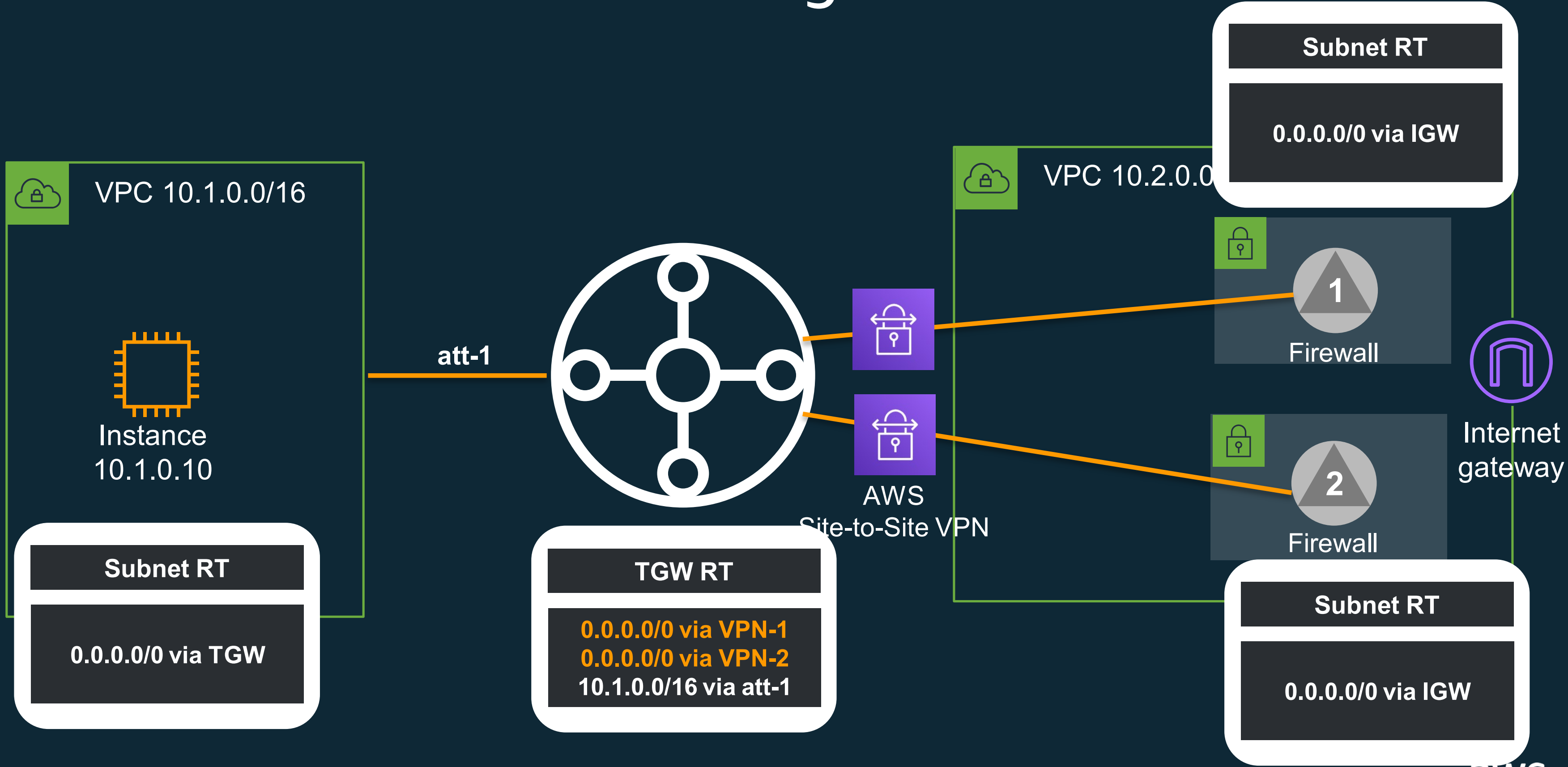


Custom automation required

VPN Attachment Model



VPN Attachment – Routing



VPC 10.1.0.0/16

Instance
10.1.0.10

att-1

AWS
Site-to-Site VPN

VPC 10.2.0.0

1
Firewall

2
Firewall

Internet
gateway

Subnet RT

0.0.0.0/0 via TGW

TGW RT

0.0.0.0/0 via VPN-1
0.0.0.0/0 via VPN-2
10.1.0.0/16 via att-1

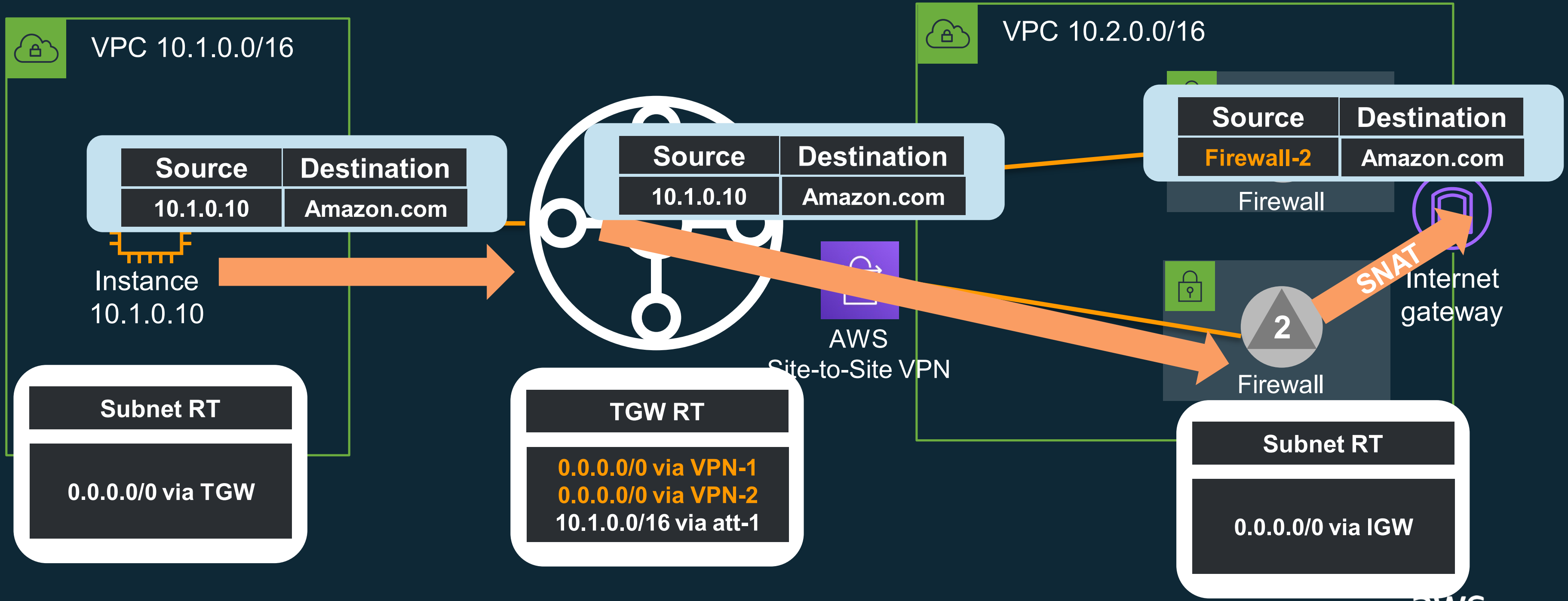
Subnet RT

0.0.0.0/0 via IGW

Subnet RT

0.0.0.0/0 via IGW

VPN Attachment – Traffic Flow



Source	Destination
10.1.0.10	Amazon.com

Source	Destination
10.1.0.10	Amazon.com

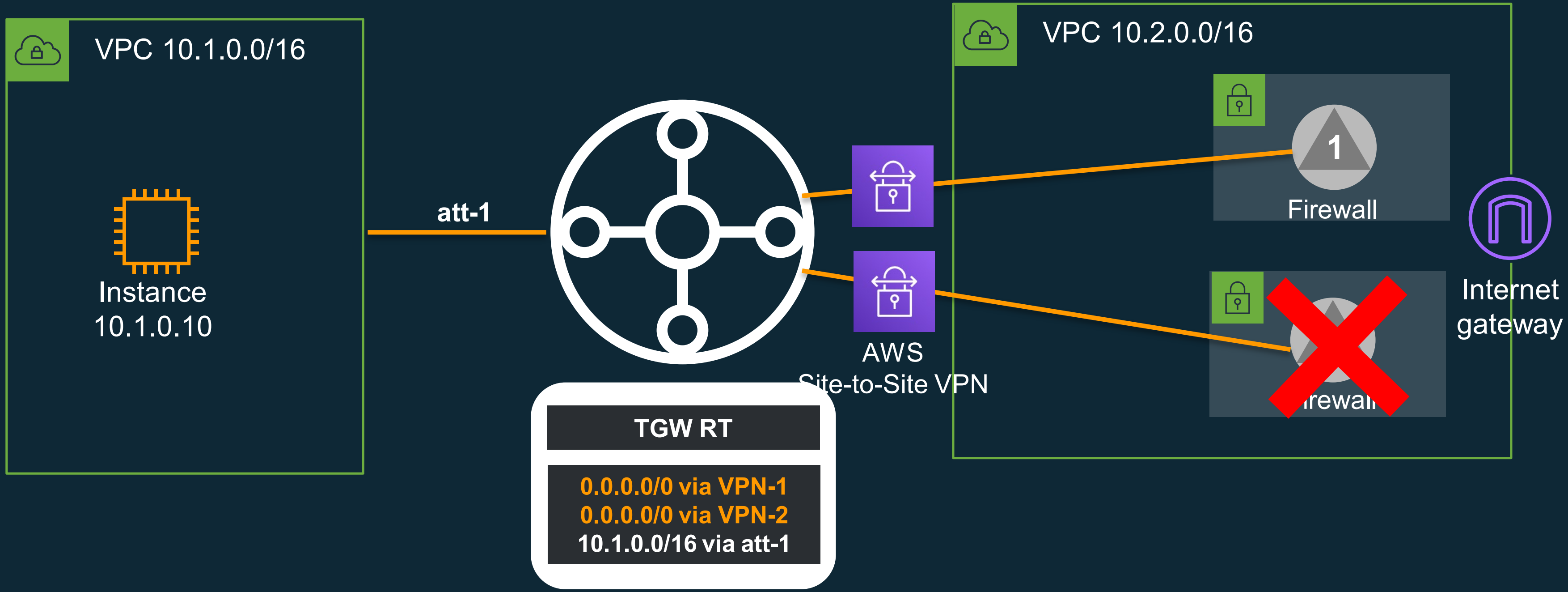
Source	Destination
Firewall-2	Amazon.com

Subnet RT
0.0.0.0/0 via TGW

TGW RT
0.0.0.0/0 via VPN-1 0.0.0.0/0 via VPN-2 10.1.0.0/16 via att-1

Subnet RT
0.0.0.0/0 via IGW

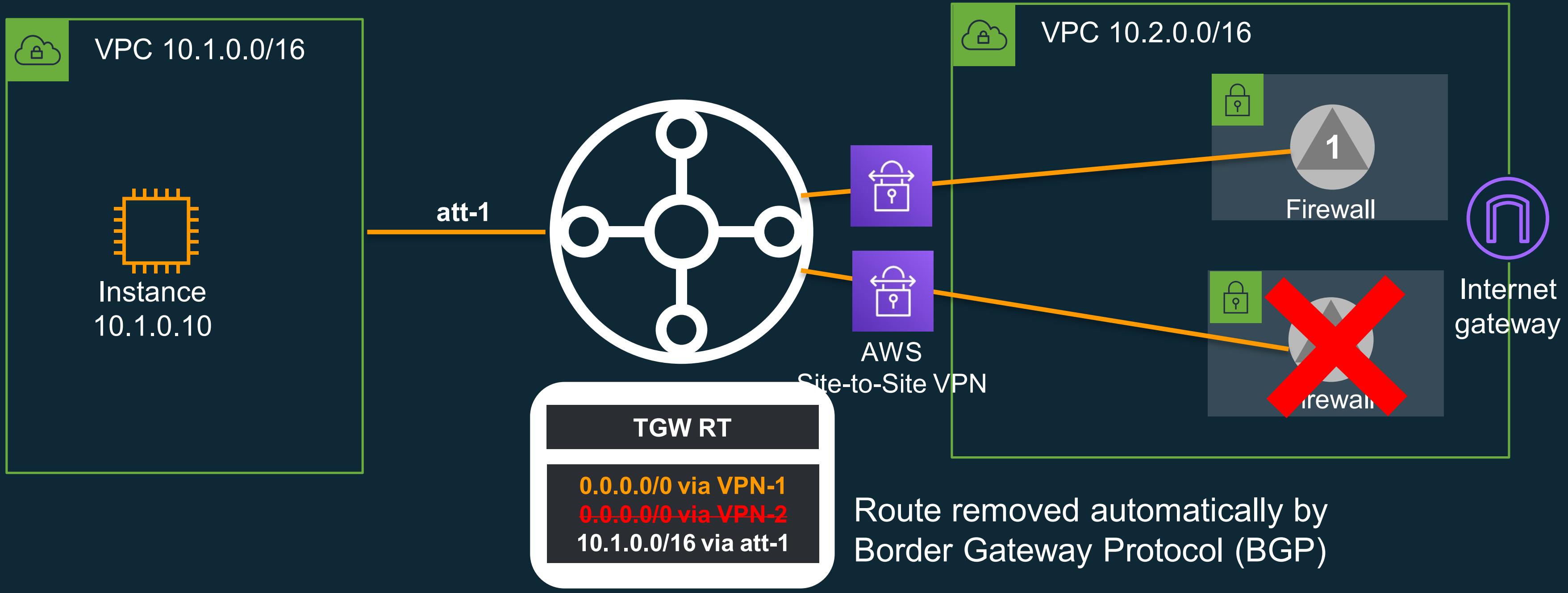
VPN Attachment – High Availability



TGW RT

0.0.0.0/0 via VPN-1
0.0.0.0/0 via VPN-2
10.1.0.0/16 via att-1

VPN Attachment – High Availability

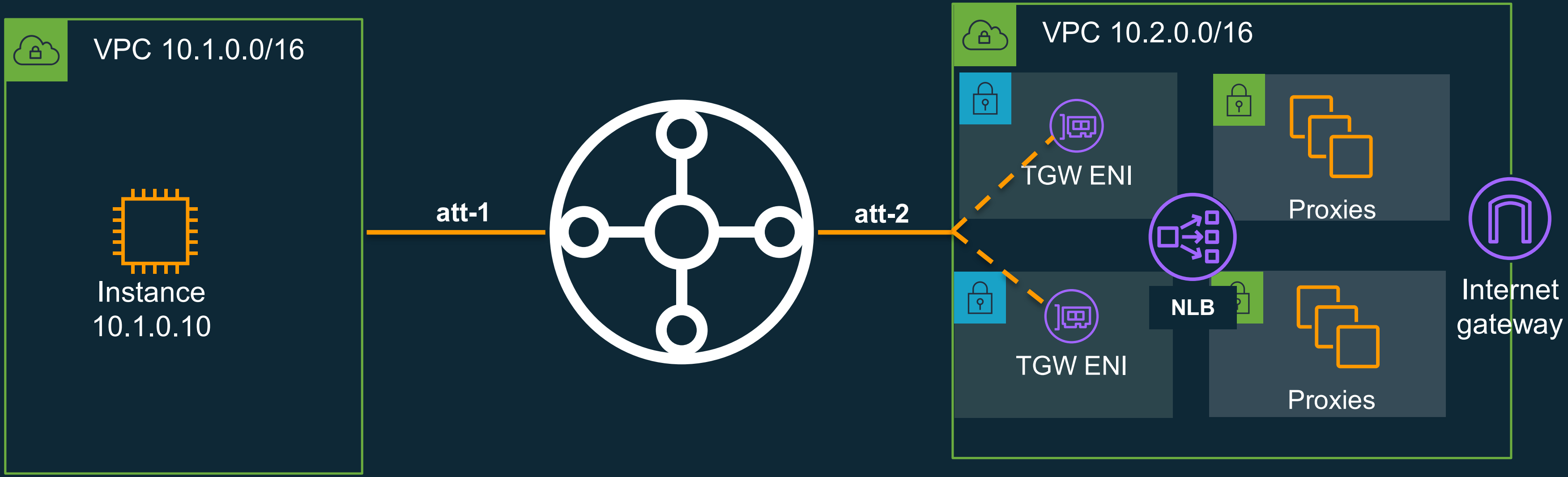


TGW RT

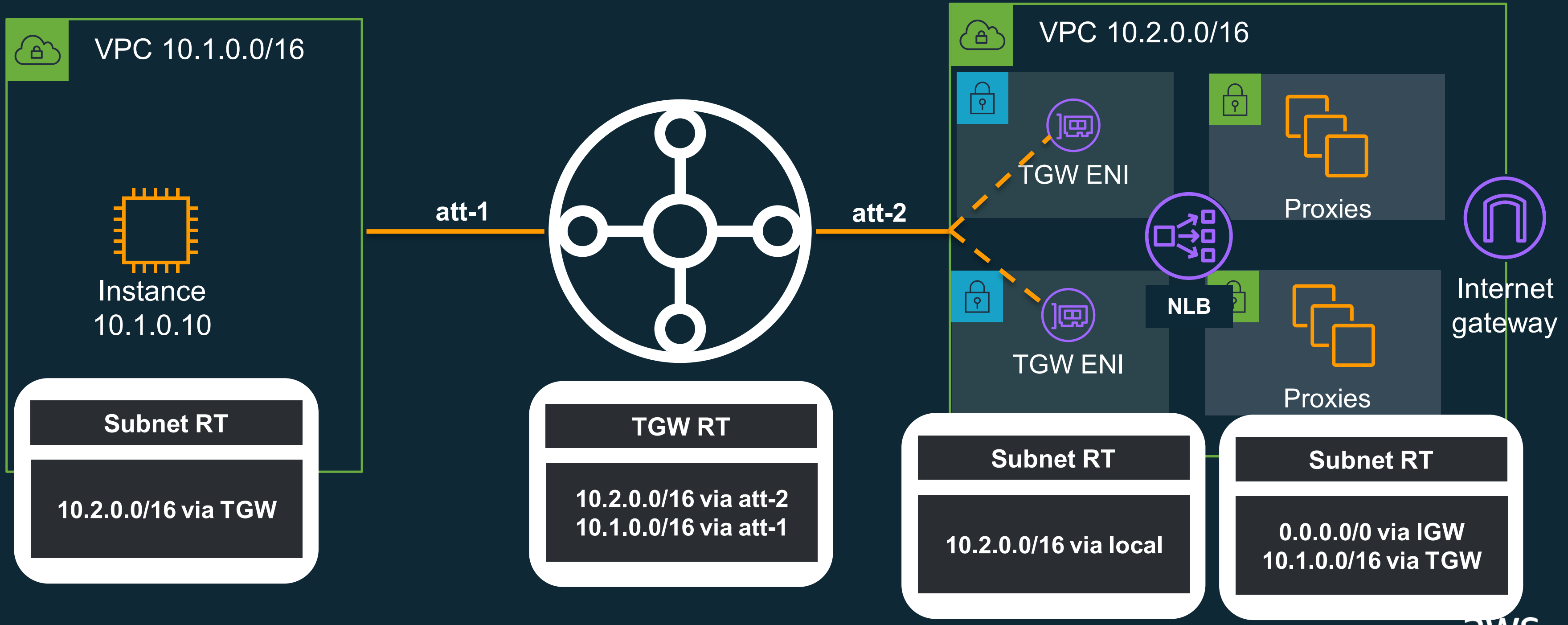
0.0.0.0/0 via VPN-1
~~0.0.0.0/0 via VPN-2~~
10.1.0.0/16 via att-1

Route removed automatically by Border Gateway Protocol (BGP)

Explicit Proxy Model



Explicit Proxy - Routing



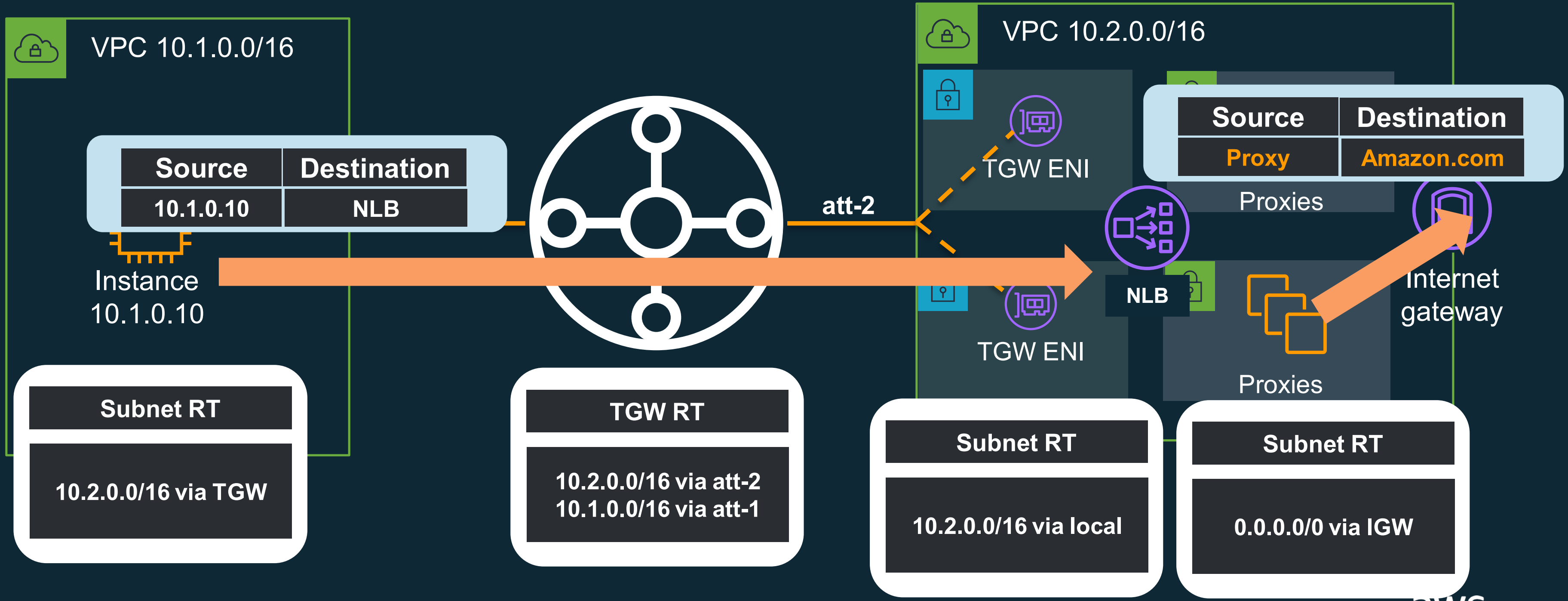
Subnet RT
10.2.0.0/16 via TGW

TGW RT
10.2.0.0/16 via att-2 10.1.0.0/16 via att-1

Subnet RT
10.2.0.0/16 via local

Subnet RT
0.0.0.0/0 via IGW 10.1.0.0/16 via TGW

Explicit Proxy – Traffic Flow



Source	Destination
10.1.0.10	NLB

Source	Destination
Proxy	Amazon.com

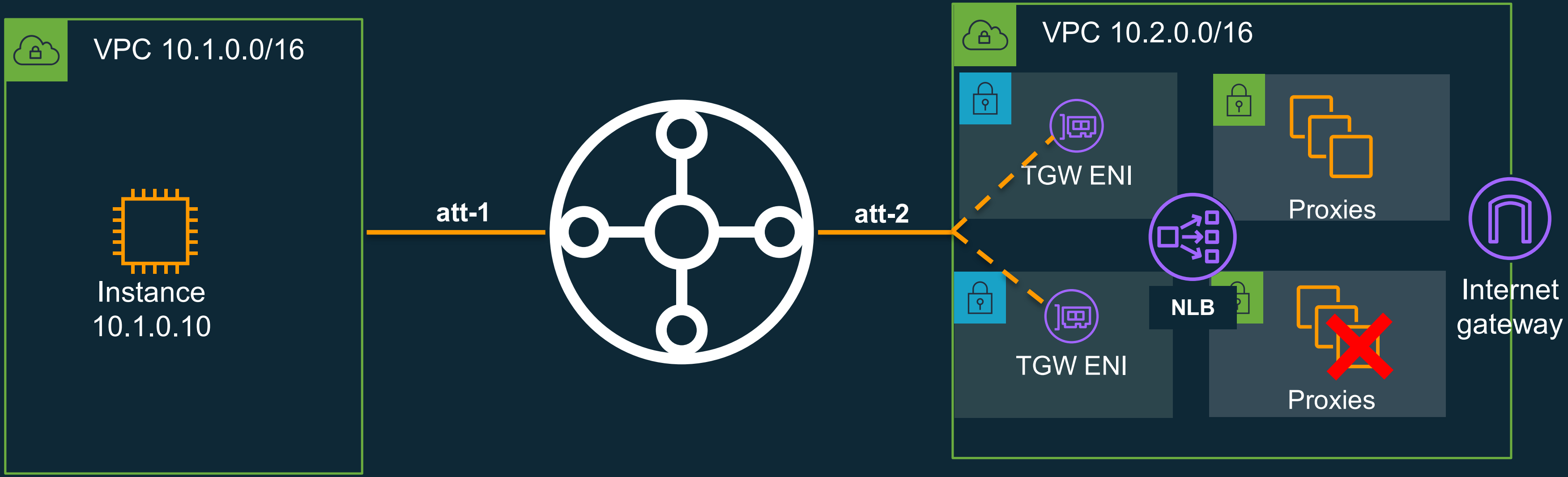
Subnet RT
10.2.0.0/16 via TGW

TGW RT
10.2.0.0/16 via att-2 10.1.0.0/16 via att-1

Subnet RT
10.2.0.0/16 via local

Subnet RT
0.0.0.0/0 via IGW

Explicit Proxy – High Availability



Proxy health-checks provided by Network Load Balancer (NLB)

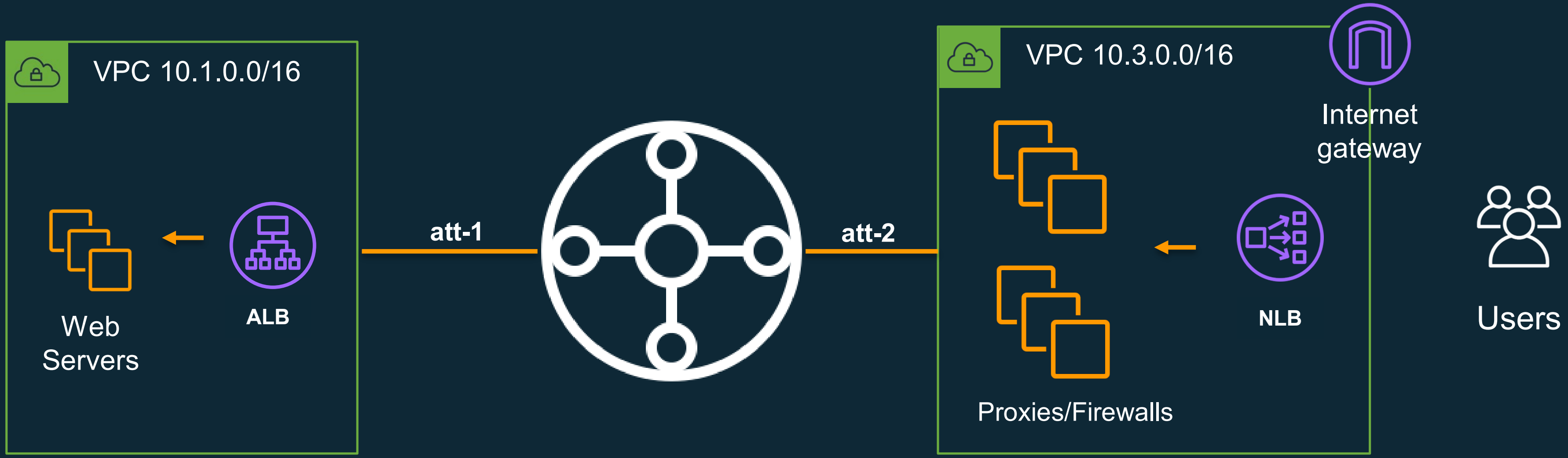
Egress Filtering Summary

	High Availability	No Encryption Overhead	Transparent to clients
VPC Attachment Model	✗ **Custom Automation**	✓	✓
VPN Attachment Model	✓ **BGP**	✗	✓
Explicit Proxy Model	✓ **NLB Health-Check**	✓	✗

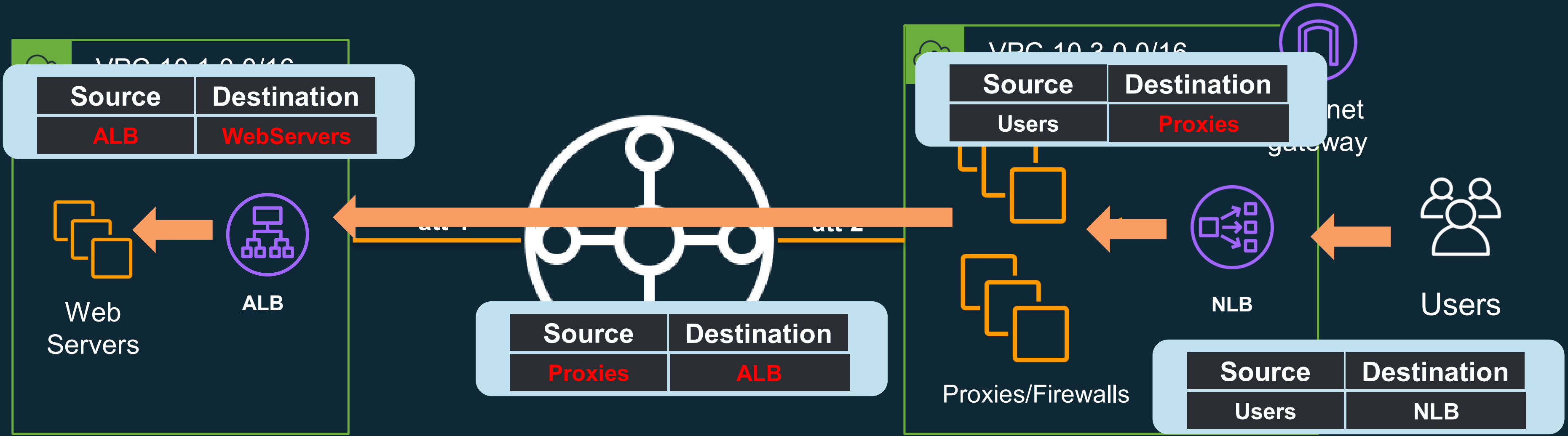
Ingres Filtering with Transit Gateway

Reverse Proxy
Model

Reverse Proxy Model



Reverse Proxy Model



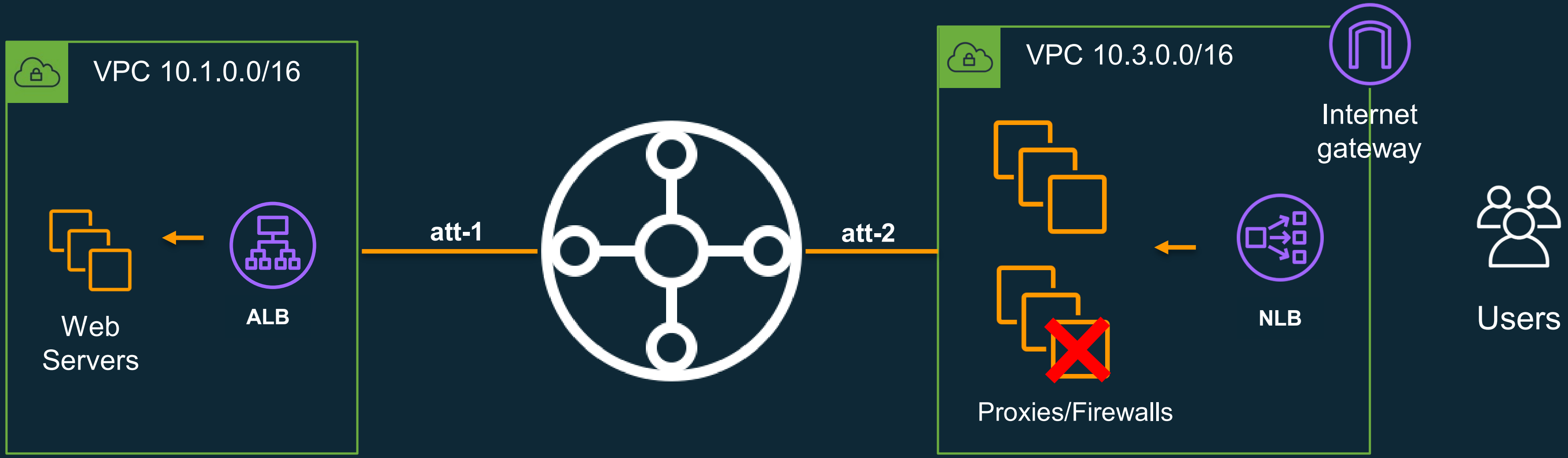
Source	Destination
ALB	WebServers

Source	Destination
Proxies	ALB

Source	Destination
Users	Proxies

Source	Destination
Users	NLB

Reverse Proxy Model – High Availability



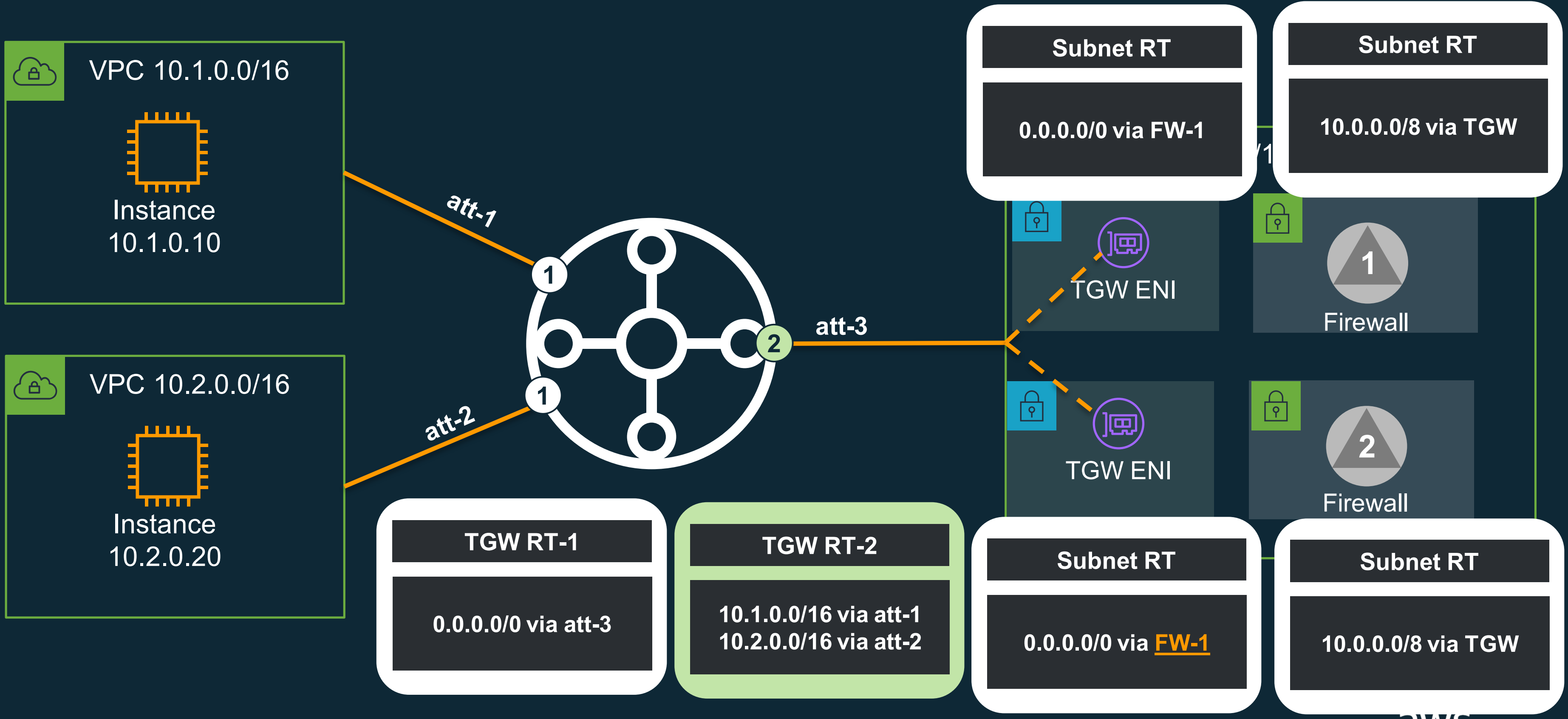
Proxy health-checks provided by Network Load Balancer (NLB)

VPC to VPC Filtering

VPC Attachment Model

VPN Attachment Model

VPC Attachment Model



Subnet RT
0.0.0.0/0 via FW-1

Subnet RT
10.0.0.0/8 via TGW

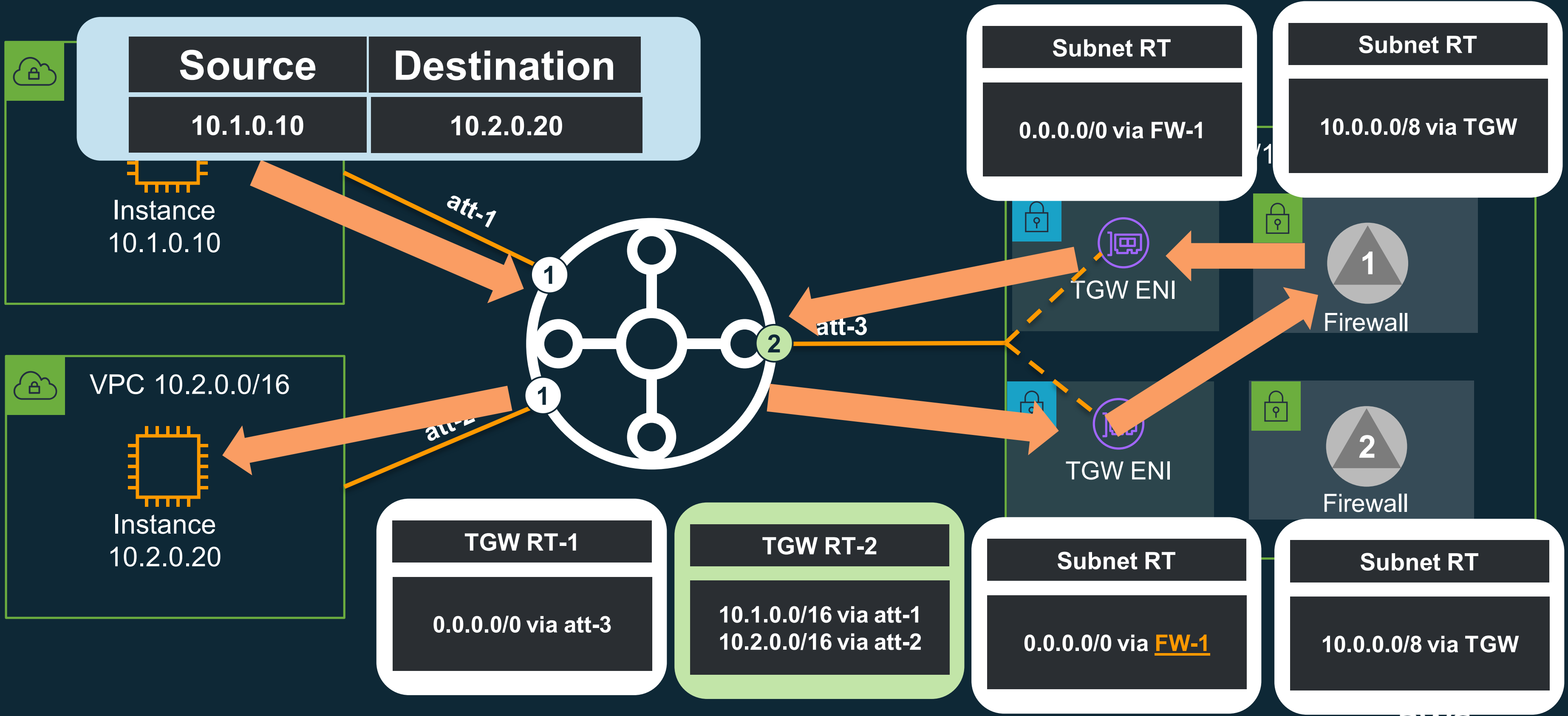
TGW RT-1
0.0.0.0/0 via att-3

TGW RT-2
10.1.0.0/16 via att-1 10.2.0.0/16 via att-2

Subnet RT
0.0.0.0/0 via FW-1

Subnet RT
10.0.0.0/8 via TGW

VPC Attachment Model – Request Flow



Source	Destination
10.1.0.10	10.2.0.20

TGW RT-1

0.0.0.0/0 via att-3

TGW RT-2

10.1.0.0/16 via att-1
10.2.0.0/16 via att-2

Subnet RT

0.0.0.0/0 via FW-1

Subnet RT

10.0.0.0/8 via TGW

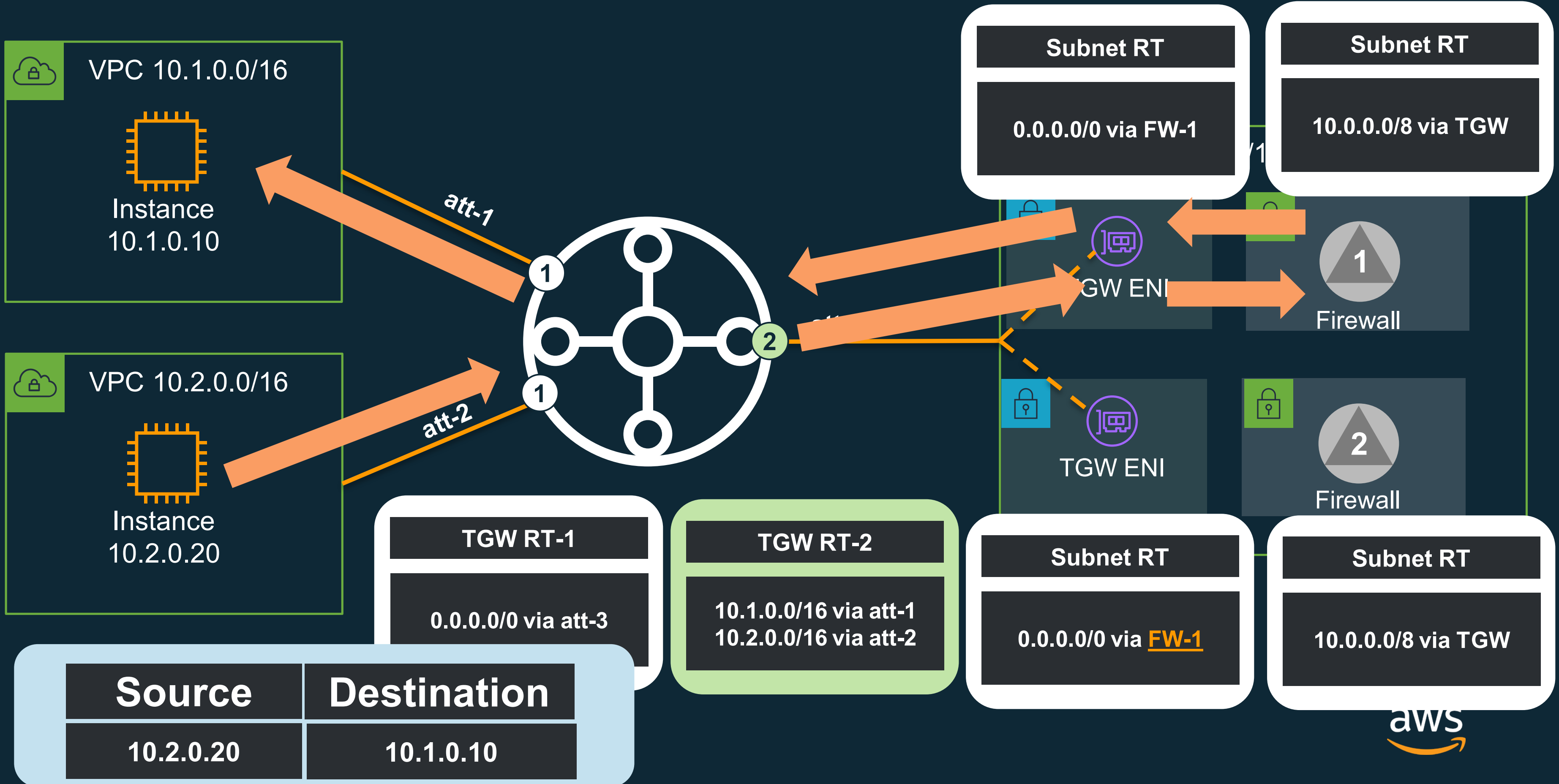
Subnet RT

0.0.0.0/0 via FW-1

Subnet RT

10.0.0.0/8 via TGW

VPC Attachment Model – Reply Flow



Subnet RT
0.0.0.0/0 via FW-1

Subnet RT
10.0.0.0/8 via TGW

TGW RT-1
0.0.0.0/0 via att-3

TGW RT-2
10.1.0.0/16 via att-1 10.2.0.0/16 via att-2

Subnet RT
0.0.0.0/0 via FW-1

Subnet RT
10.0.0.0/8 via TGW

Source	Destination
10.2.0.20	10.1.0.10

Summary

Egress Filtering

- Active/Active
- HA depends on the model
- Lowest operational overhead

Ingress Filtering

- Active/Active
- HA through ELB
- Changes on appliances required for every new service

VPC to VPC Filtering

- Active/Passive (no-NAT)
- HA depends on the model
- Medium operational overhead

Architecting for IPv4 Preservation

Available IPv4 Private IPs

RFC 1918:

• 10.0.0.0/8	16 Million IPs (65k x /24s)
• 172.16.0.0/12	1 Million IPs (4k x /24s)
• 192.168.0.0/16	65 Thousand IPs (256 x /24s)

RFC 6598:

• 100.64.0.0/10	4 Million IPs (16k x /24s)

Address Planning Benefits

Simpler routing configuration

Cleaner security polices

Better visibility

IPv4 Preservation Options

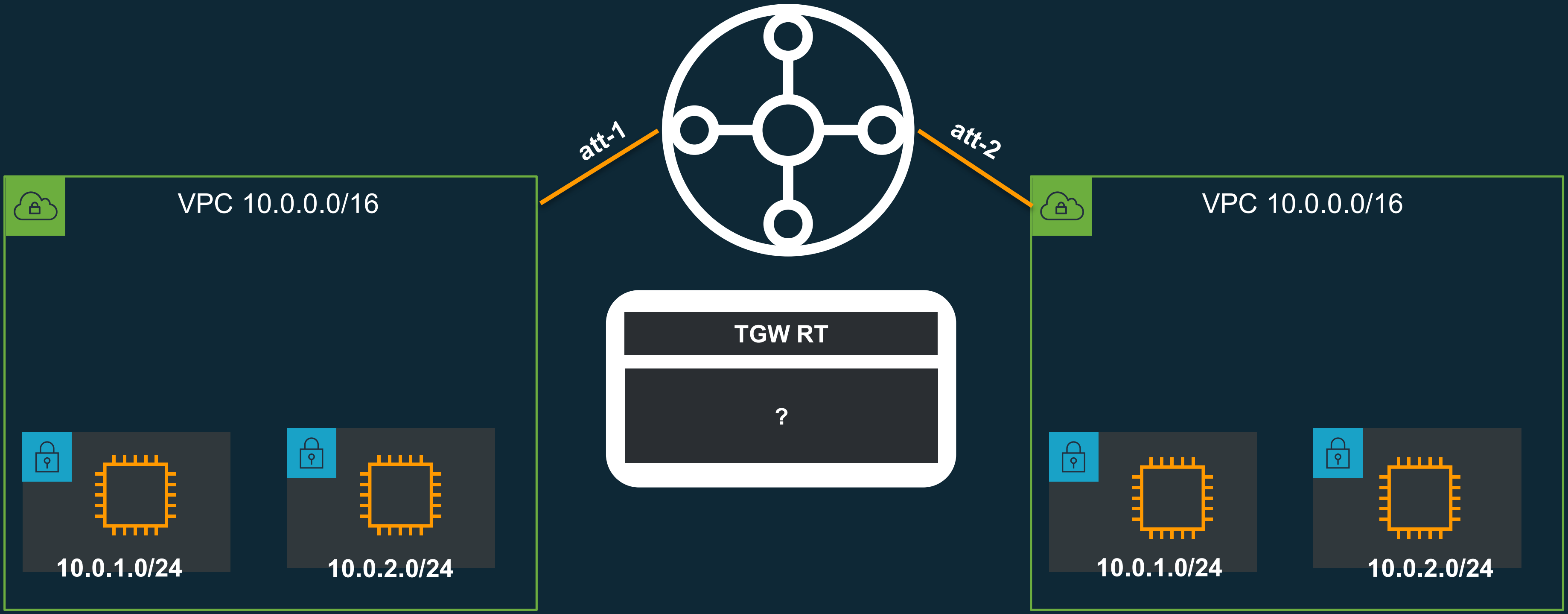
NAT

IPv6

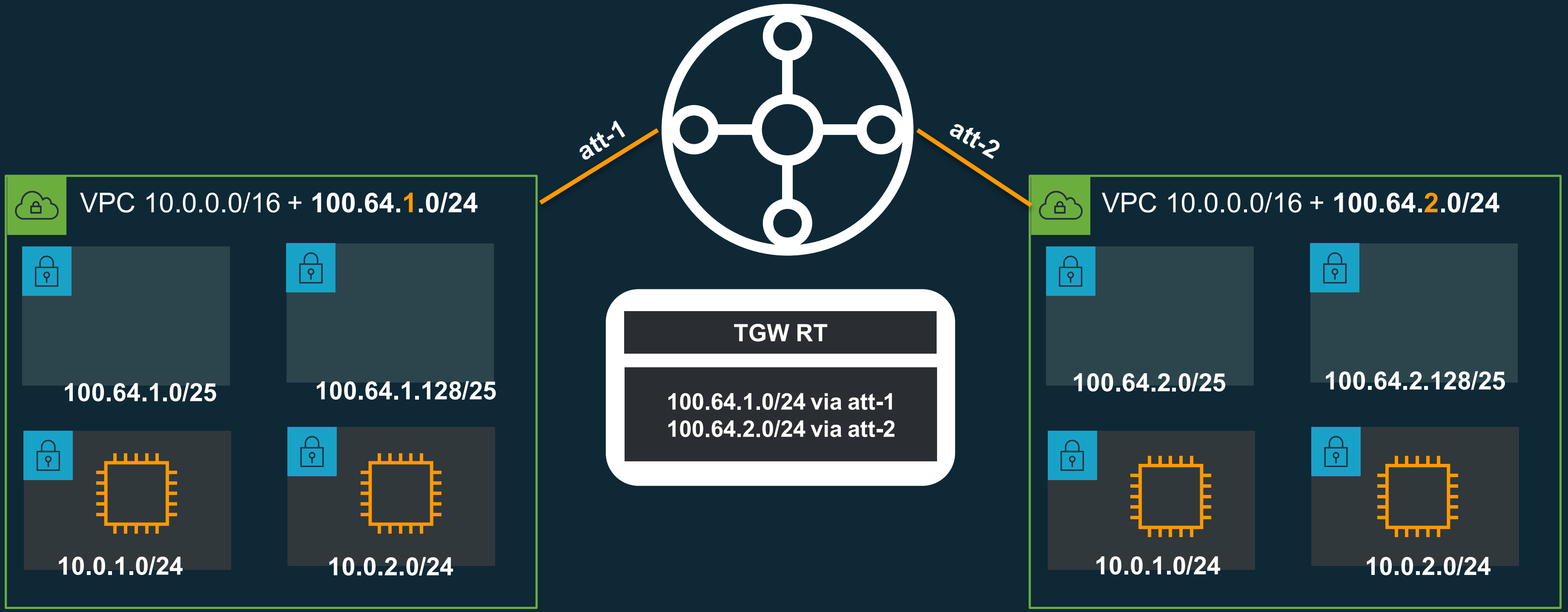
AWS PrivateLink

Network Address Translation (NAT)

Transit Gateway + NAT



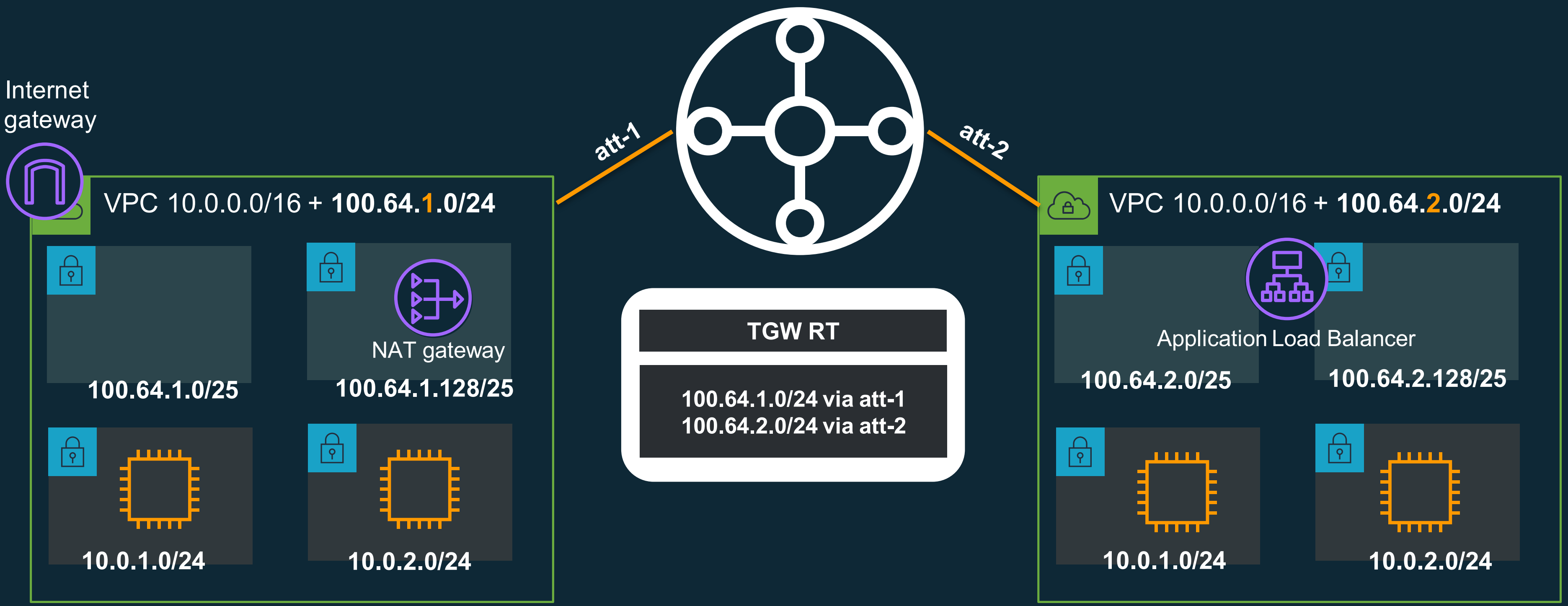
Transit Gateway + NAT



TGW RT

100.64.1.0/24 via att-1
100.64.2.0/24 via att-2

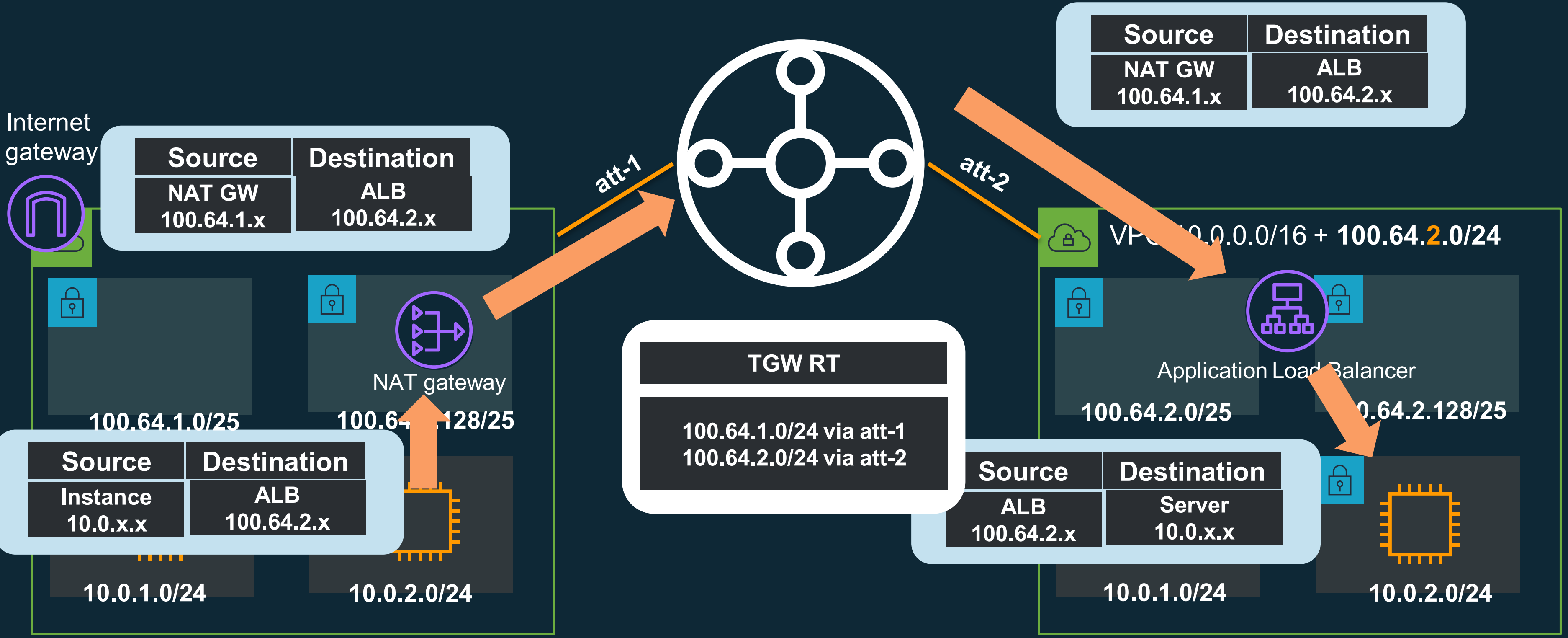
Transit Gateway + NAT



TGW RT

100.64.1.0/24 via att-1
100.64.2.0/24 via att-2

Transit Gateway + NAT



Source	Destination
NAT GW 100.64.1.x	ALB 100.64.2.x

Source	Destination
Instance 10.0.x.x	ALB 100.64.2.x

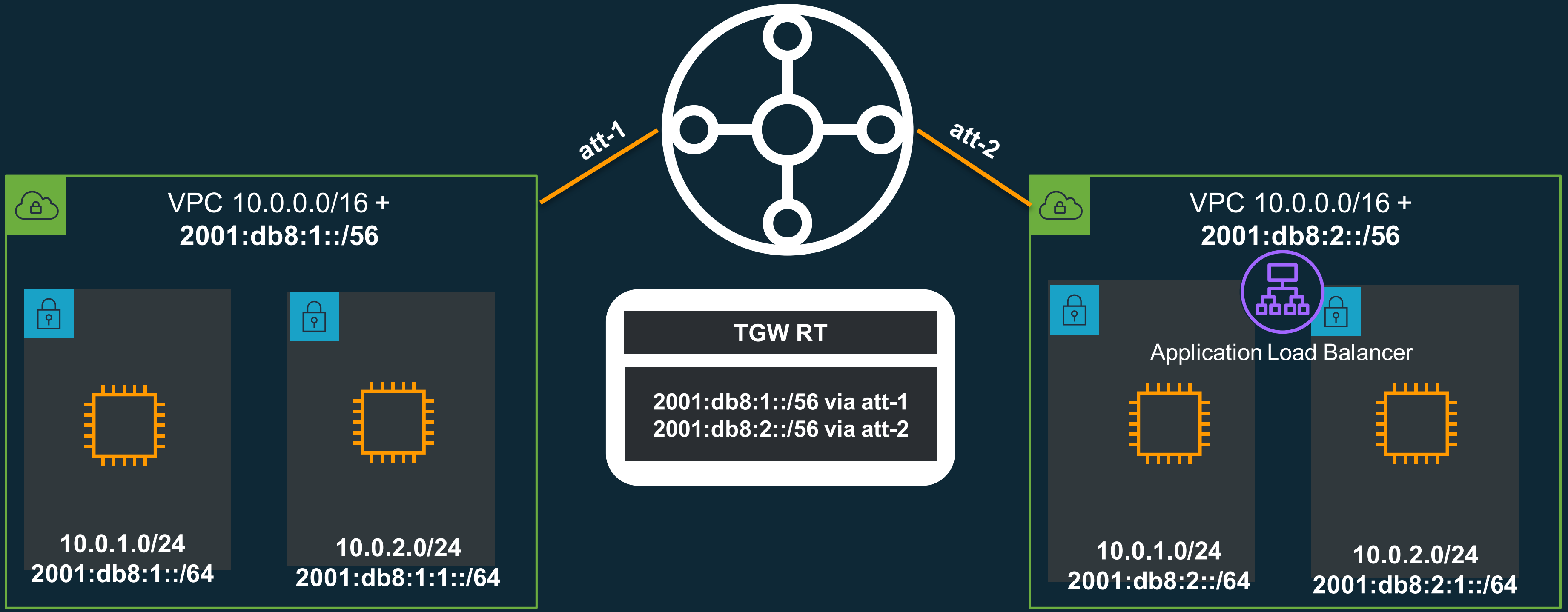
TGW RT
100.64.1.0/24 via att-1 100.64.2.0/24 via att-2

Source	Destination
NAT GW 100.64.1.x	ALB 100.64.2.x

Source	Destination
ALB 100.64.2.x	Server 10.0.x.x

IPv6

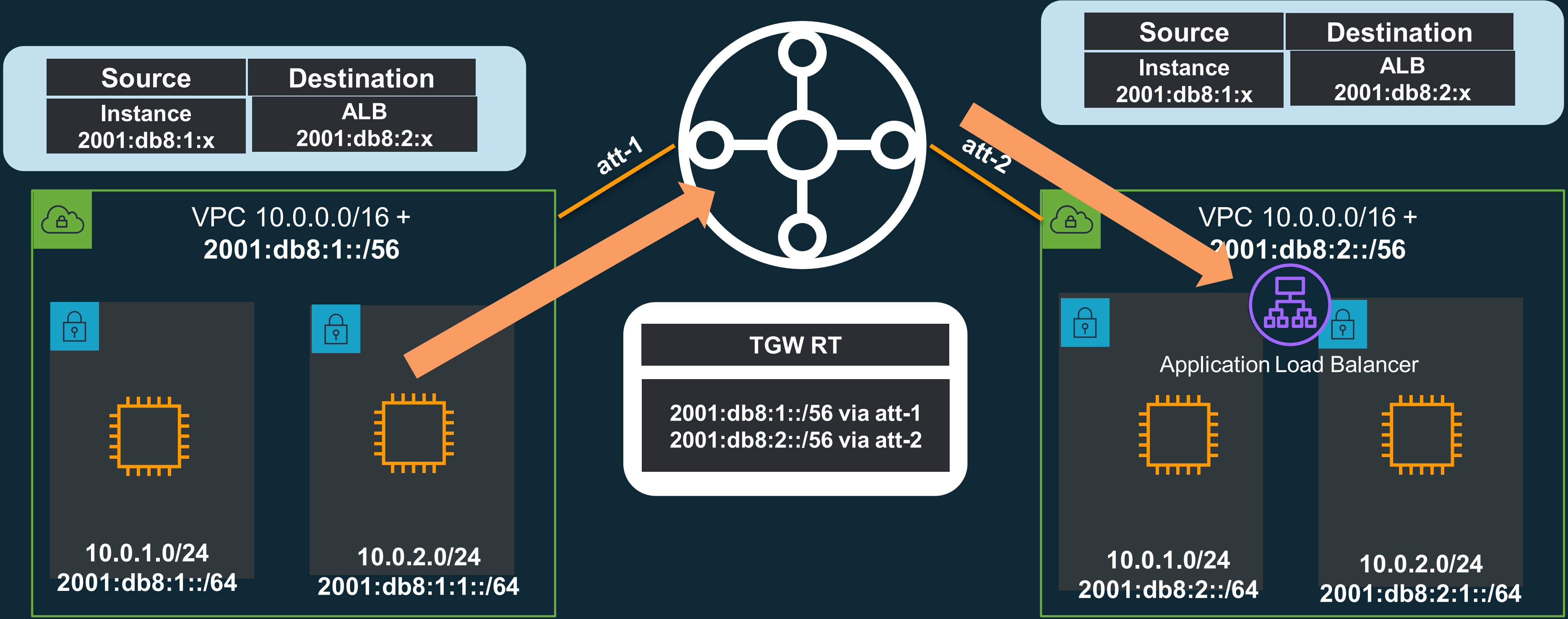
Transit Gateway + IPv6



TGW RT

2001:db8:1::/56 via att-1
2001:db8:2::/56 via att-2

Transit Gateway + IPv6



Source	Destination
Instance 2001:db8:1:x	ALB 2001:db8:2:x

Source	Destination
Instance 2001:db8:1:x	ALB 2001:db8:2:x

att-1

att-2

VPC 10.0.0.0/16 +
2001:db8:1::/56

10.0.1.0/24
2001:db8:1::/64

10.0.2.0/24
2001:db8:1:1::/64

TGW RT
2001:db8:1::/56 via att-1 2001:db8:2::/56 via att-2

VPC 10.0.0.0/16 +
2001:db8:2::/56

Application Load Balancer

10.0.1.0/24
2001:db8:2::/64

10.0.2.0/24
2001:db8:2:1::/64

Thank You!

Tom Adamski
Specialist Solutions Architect, Networking