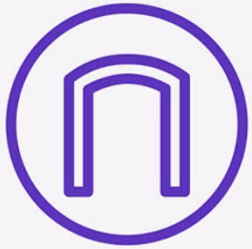
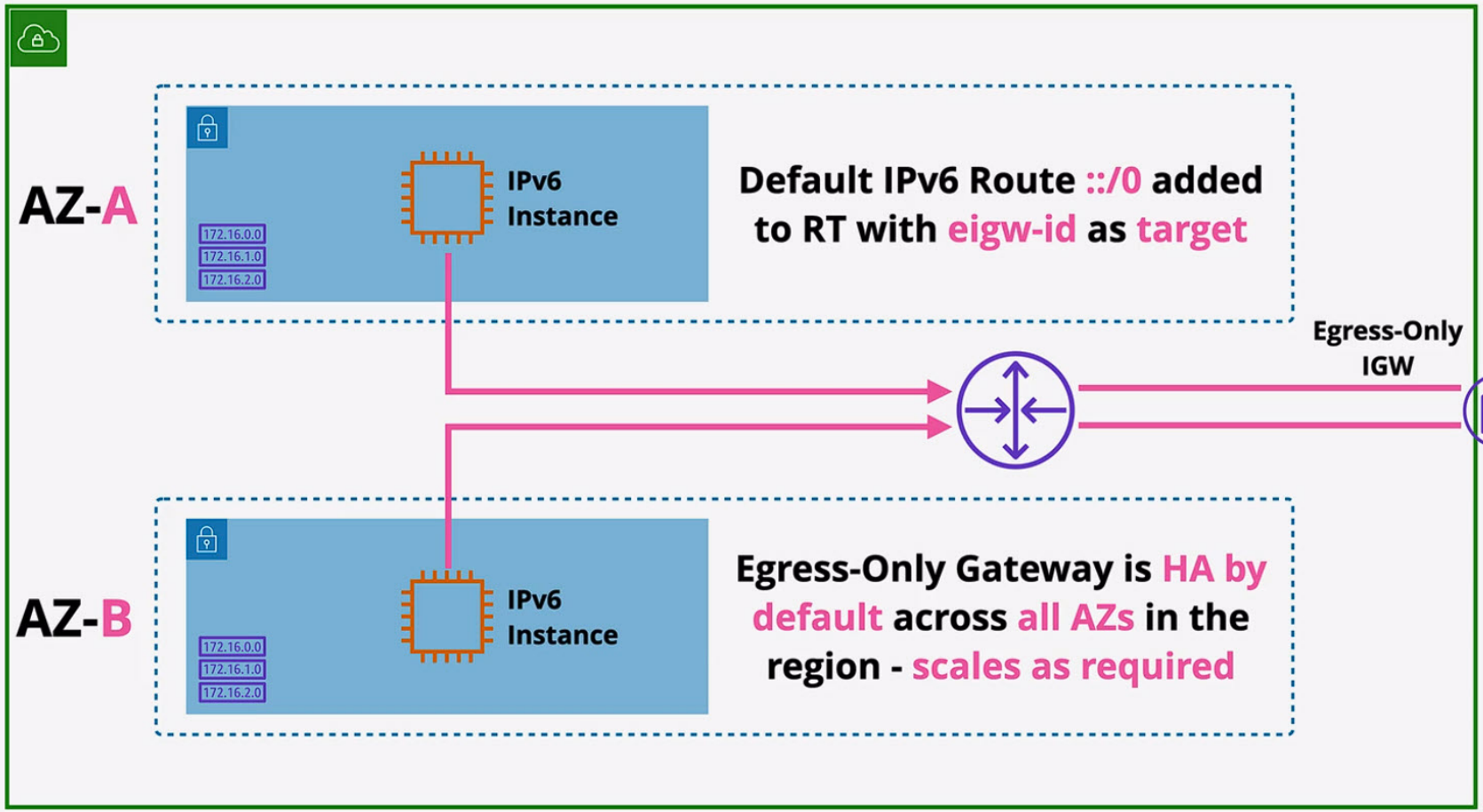
Egress-Only Internet Gateway



Egress-Only Internet Gateway

- With IPv4 addresses are **private** or **public**
- **NAT** allows **private IPs** to access **public networks**
- ... **without allowing** externally initiated connections (**IN**)
- With **IPv6** all IPs are **public**
- Internet Gateway (IPv6) allows all IPs **IN** and **OUT**
- Egress-Only is **outbound-only** for **IPv6**

Egress-Only Internet Gateway

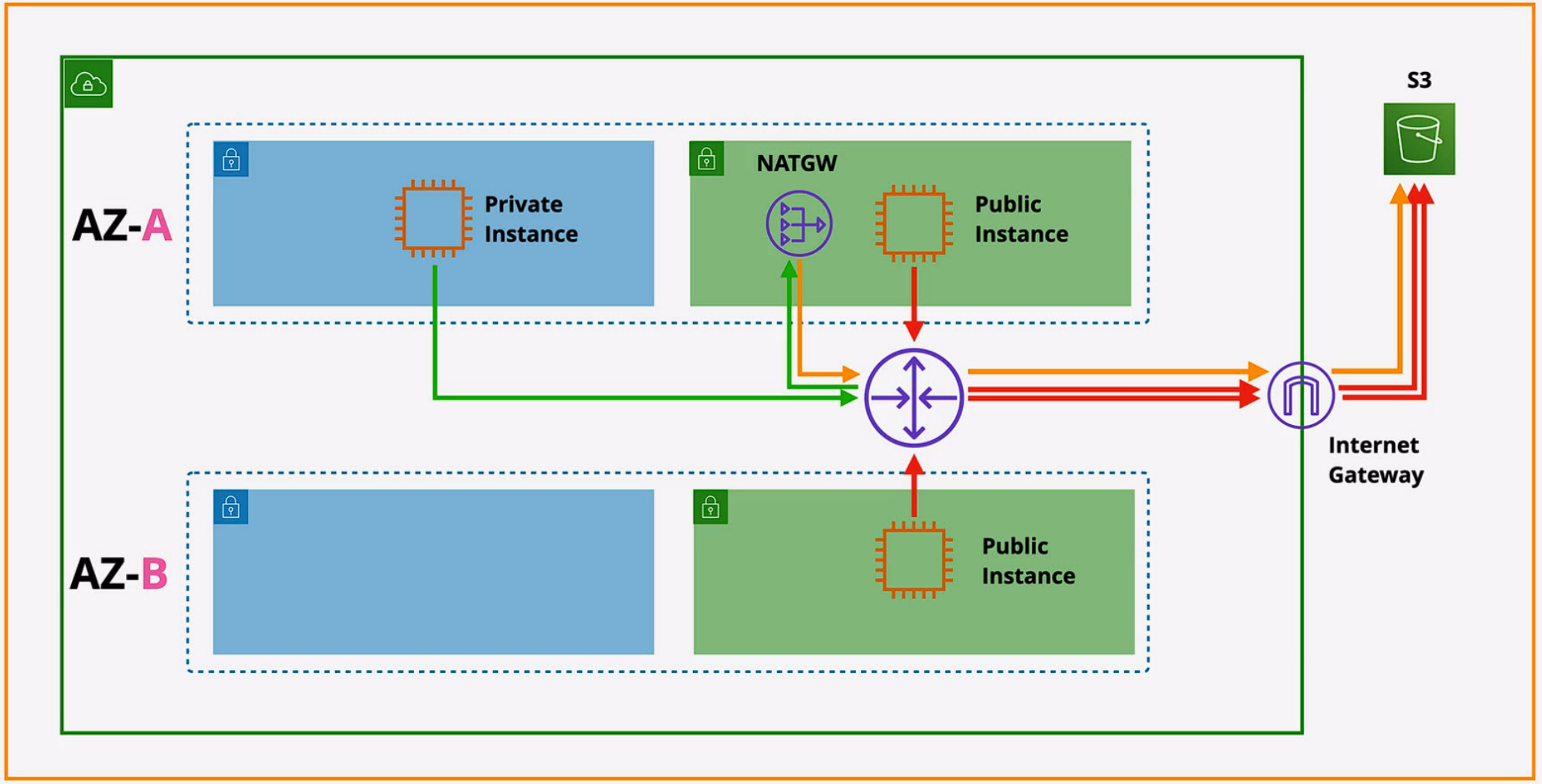


VPC Endpoints
(Gateway)

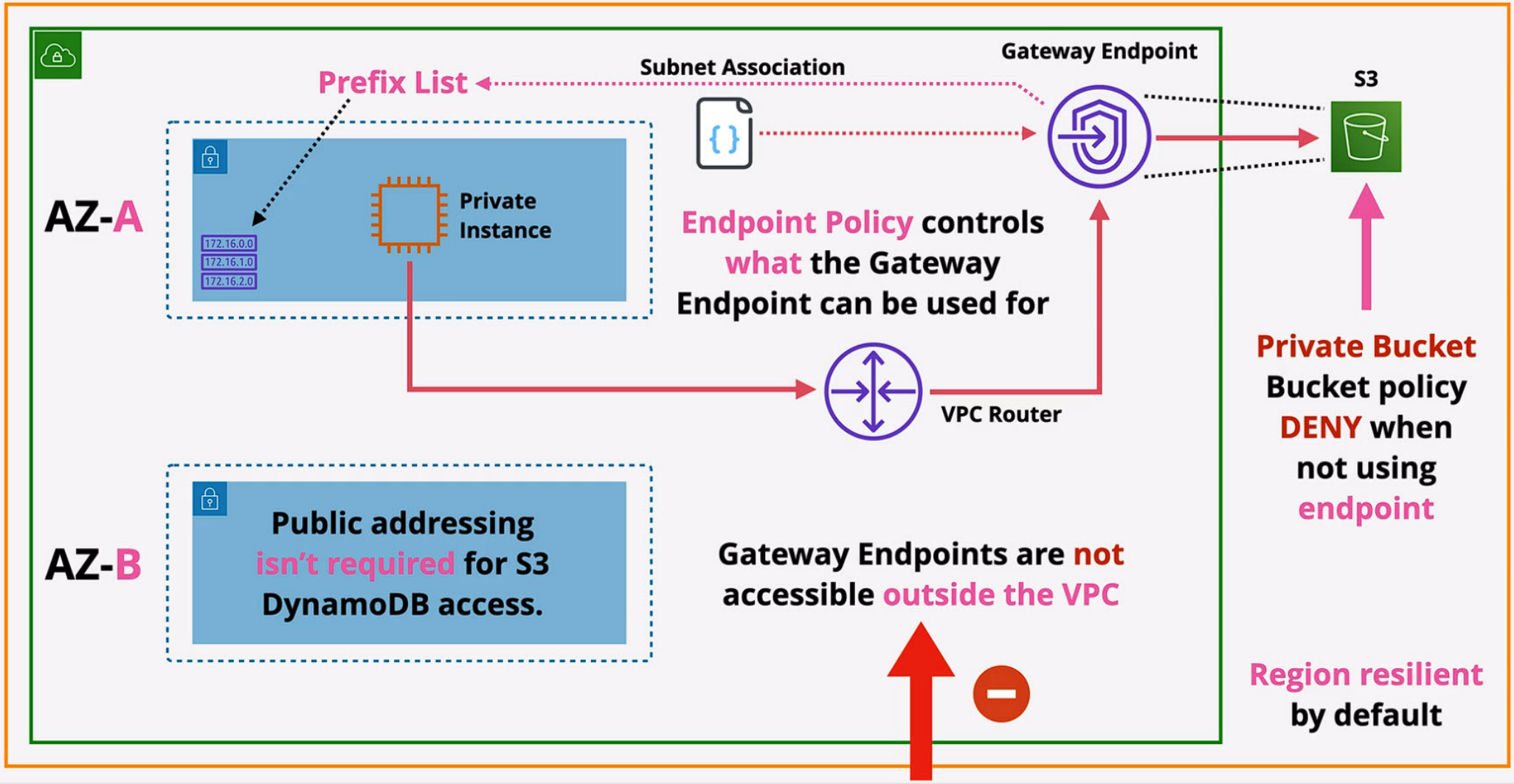
Gateway Endpoints

- Provide **private access** to **S3** and **DynamoDB**
- **Prefix List** added to **route table** => **Gateway Endpoint**
- Highly Available (**HA**) across all AZs in a region by default
- Endpoint policy is used to control what it can access
- Regional ... **can't access cross-region** services
- **Prevent Leaky Buckets** - S3 Buckets can be set to private only by allowing access ONLY from a gateway endpoint

w/o Gateway Endpoints



w/ Gateway Endpoints



VPC Endpoints
(Interface)

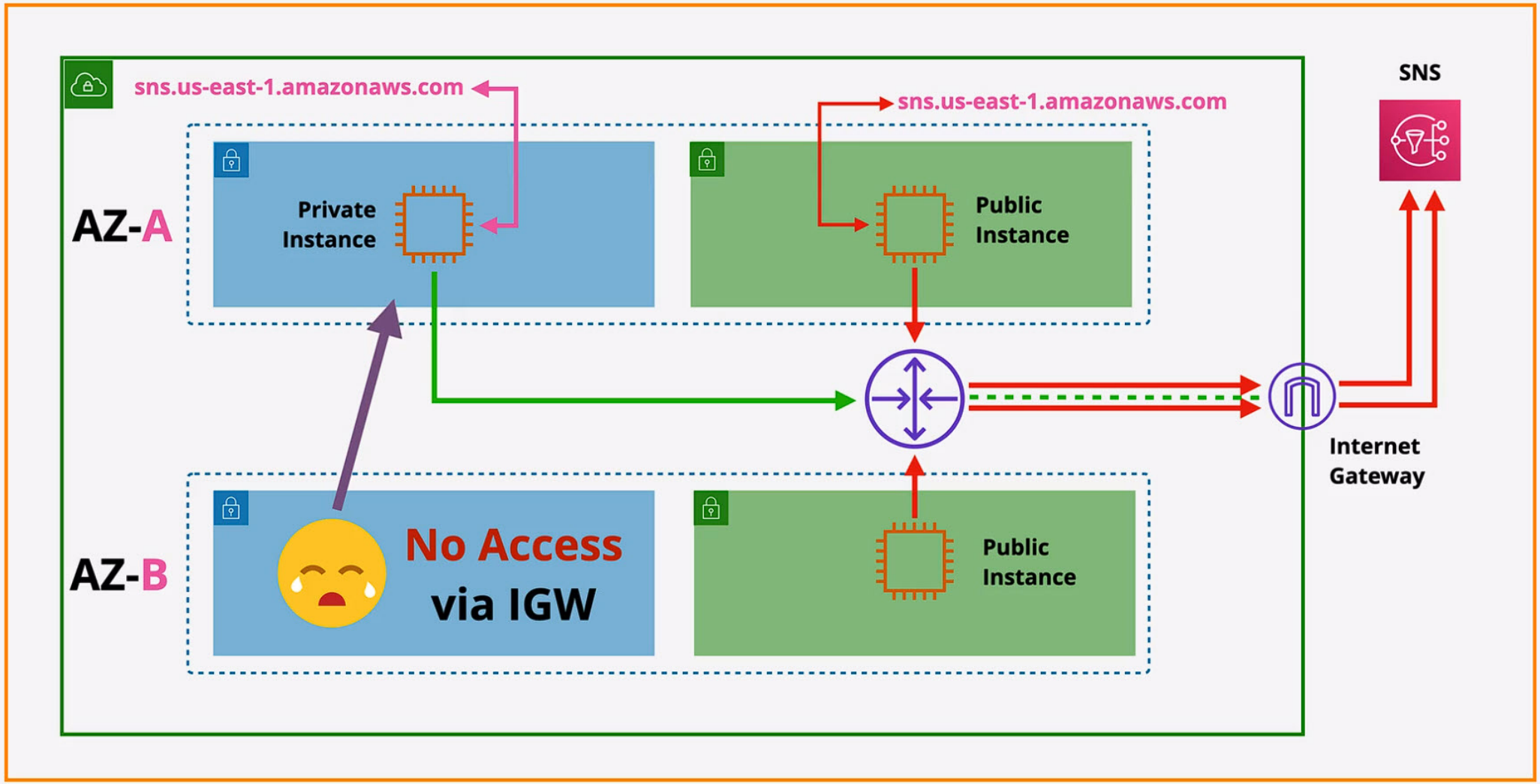
Interface Endpoints

- Provide **private access** to AWS Public Services
- historically.... anything **NOT S3** and **DDB** **.. but S3 is now supported** 🎉 🤗 🧁
- Added to **specific subnets** - an **ENI** - **not HA**
- For HA .. add **one endpoint**, to **one subnet**, **per AZ** used in the VPC
- Network access controlled via **Security Groups**
- **Endpoint Policies** - restrict what can be done with the endpoint
- **TCP** and **IPv4** ONLY
- Uses **PrivateLink**

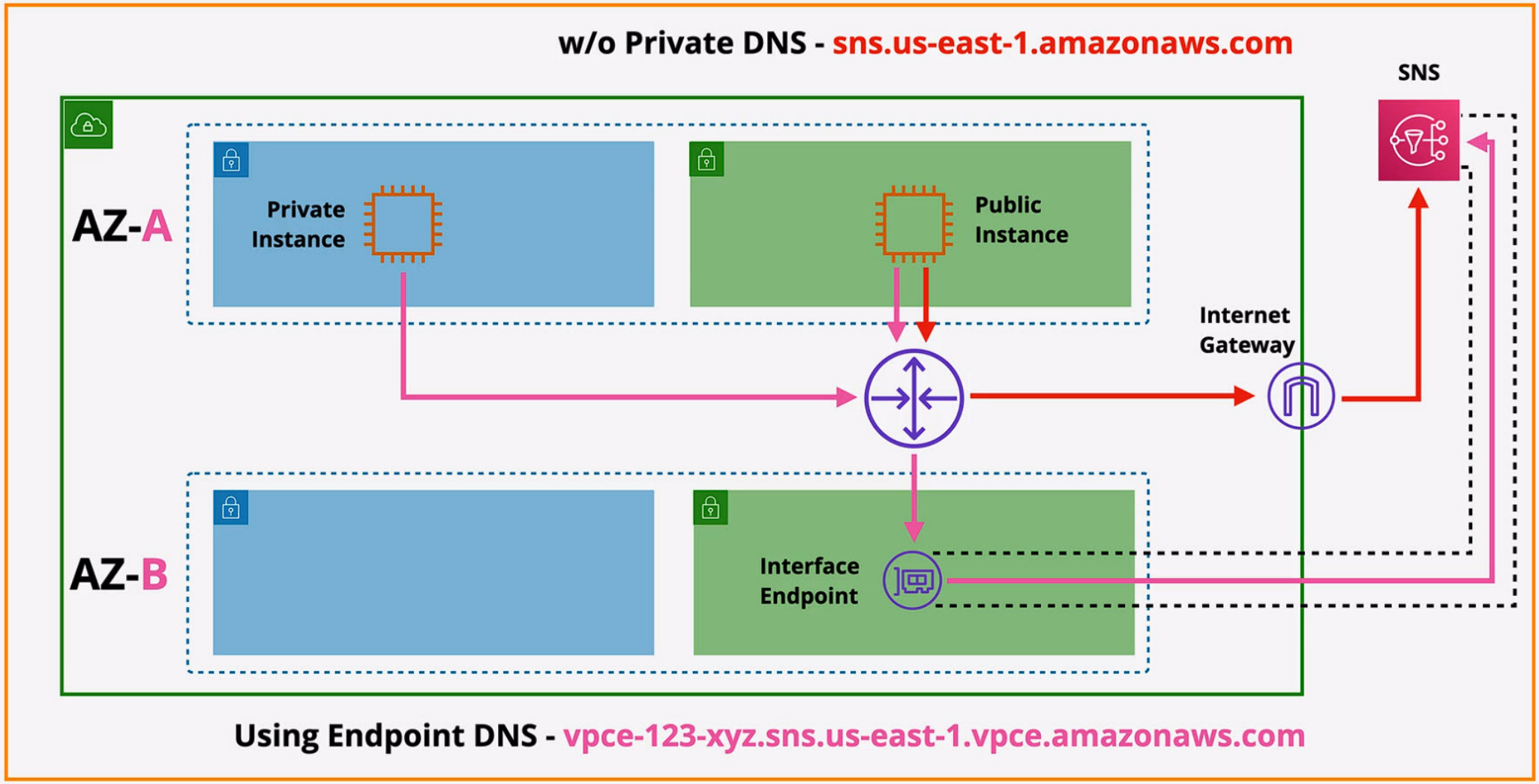
Interface Endpoints

- Endpoint provides a NEW service endpoint DNS
- e.g. **vpce-123-xyz.sns.us-east-1.vpce.amazonaws.com**
- Endpoint **Regional DNS**
- Endpoint **Zonal DNS**
- Applications can optionally use these, or ...
- **PrivateDNS overrides** the **default DNS** for services

w/o Interface Endpoints

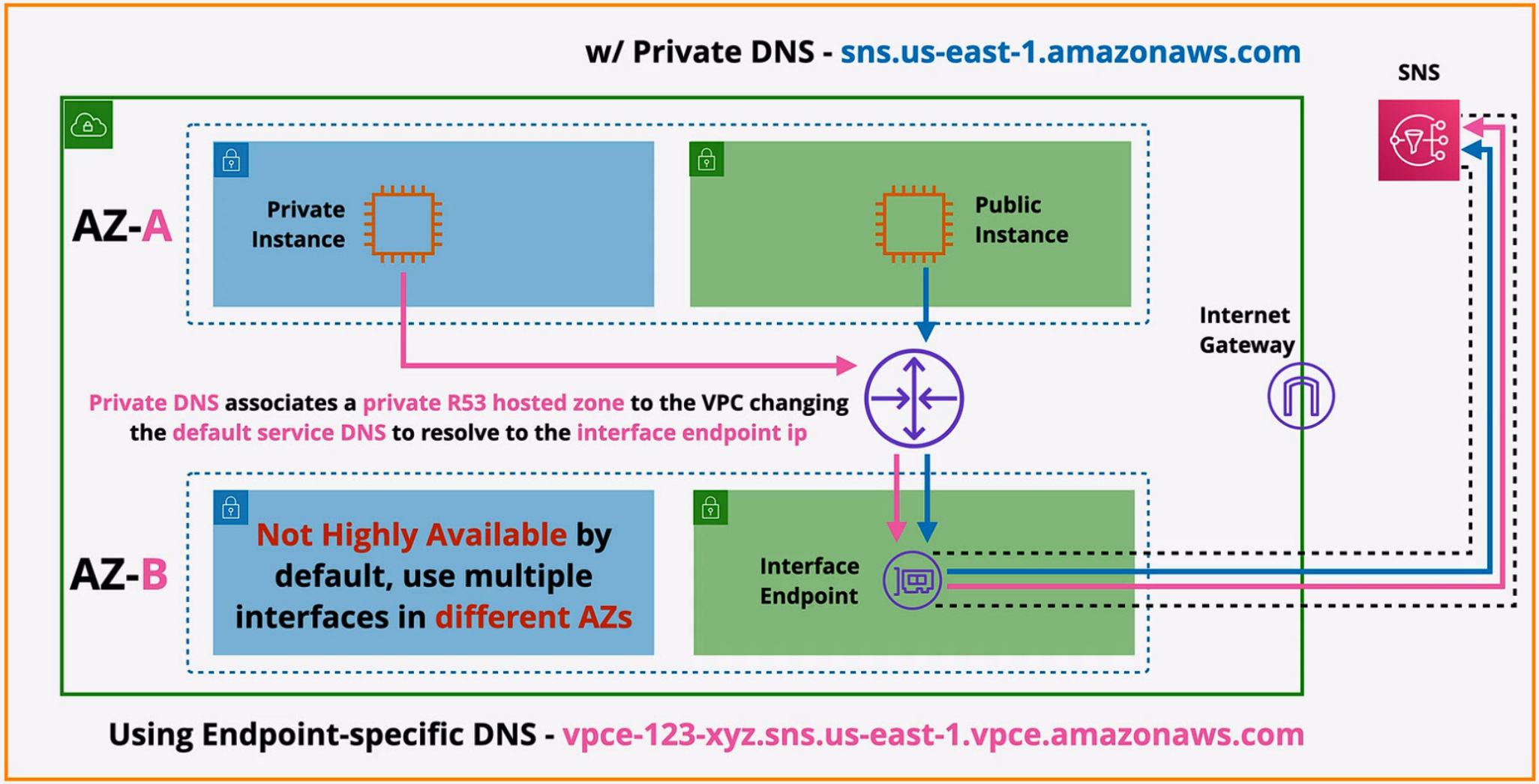


w/ Interface Endpoints



w/ Interface Endpoint & PrivateDNS

https://learn.cantrill.io adriancantrill

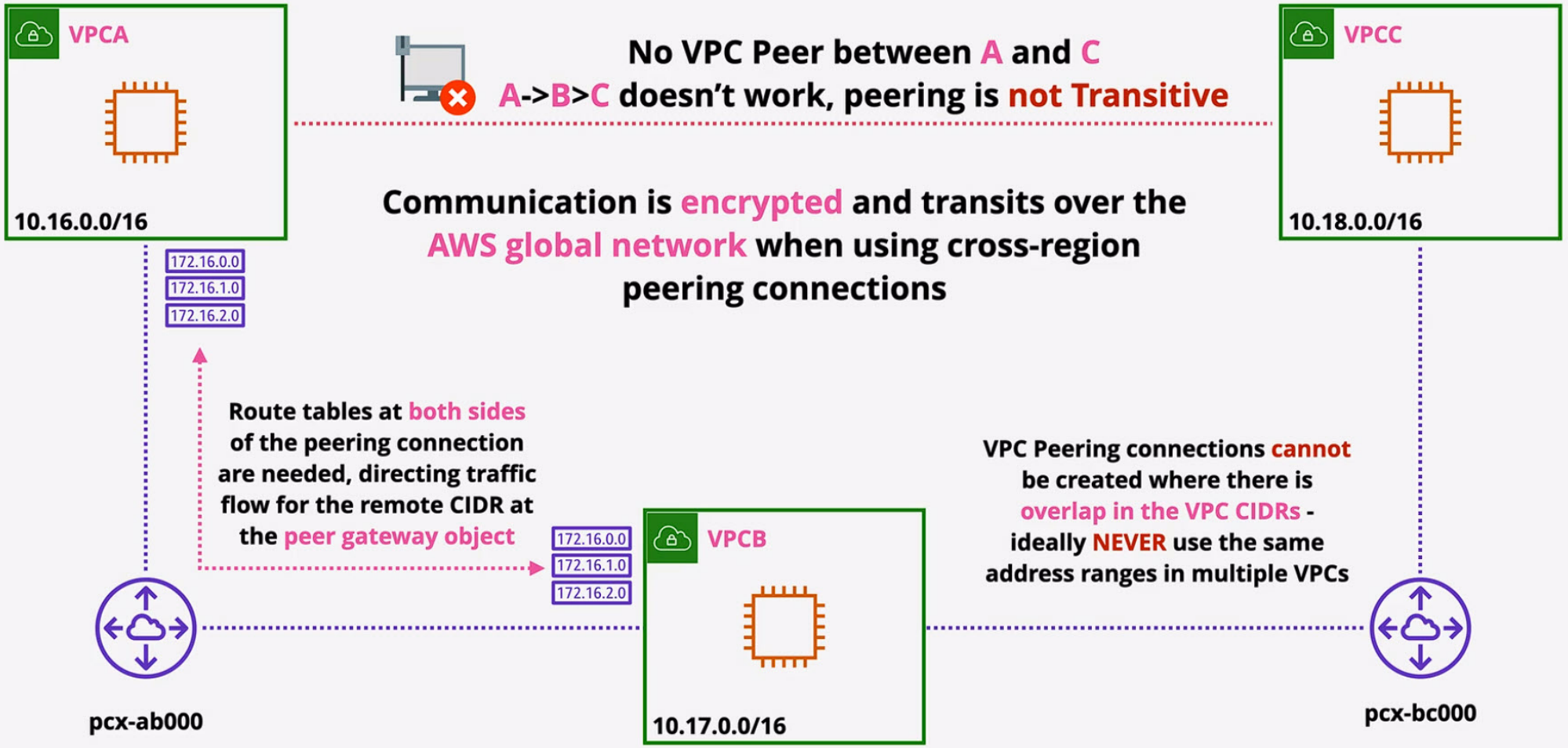


VPC Peering

VPC Peering

- Direct encrypted network link between **two VPCs**
- Works **same**/**cross-region** and **same**/**cross-account**
- (***optional***) **Public Hostnames** resolve to **private IPs**
- **Same region SG's** can reference **peer SGs**
- VPC Peering does **NOT** support **transitive peering**
- **Routing** Configuration is needed, **SGs** & **NACLs** can filter

VPC Peering


VPCA
10.16.0.0/16
VPCC
10.18.0.0/16
No VPC Peer between A and C
A->B>C doesn't work, peering is not Transitive
Communication is encrypted and transits over the AWS global network when using cross-region peering connections
172.16.0.0
172.16.1.0
172.16.2.0
Route tables at both sides of the peering connection are needed, directing traffic flow for the remote CIDR at the peer gateway object
172.16.0.0
172.16.1.0
172.16.2.0
VPCB
10.17.0.0/16
VPC Peering connections cannot be created where there is overlap in the VPC CIDRs - ideally NEVER use the same address ranges in multiple VPCs
pcx-ab000
pcx-bc000

Border Gateway Protocol (BGP) 101

Border Gateway Protocol (BGP)

- Autonomous System (**AS**) - Routers controlled by one entity … a network in BGP
- **ASN** are unique and allocated by IANA (**0-65535**), **64512** - **65534** are private
- BGP Operates over **tcp/179** - it's **reliable**
- **Not automatic** - peering is **manually configured**
- BGP is a **path-vector** protocol it exchanges the **best path** to a **destination** between **peers** … the path is called the **ASPATH**
- **iBGP** = Internal BGP - Routing **within** an AS
- **eBGP** = External BGP - Routing **between** AS's

Border Gateway Protocol (BGP)

https://learn.cantrill.io adriancantrill

1 Gbps Fibre

5Mbps Satellite

i is the origin - the network was learned from a locally connected network

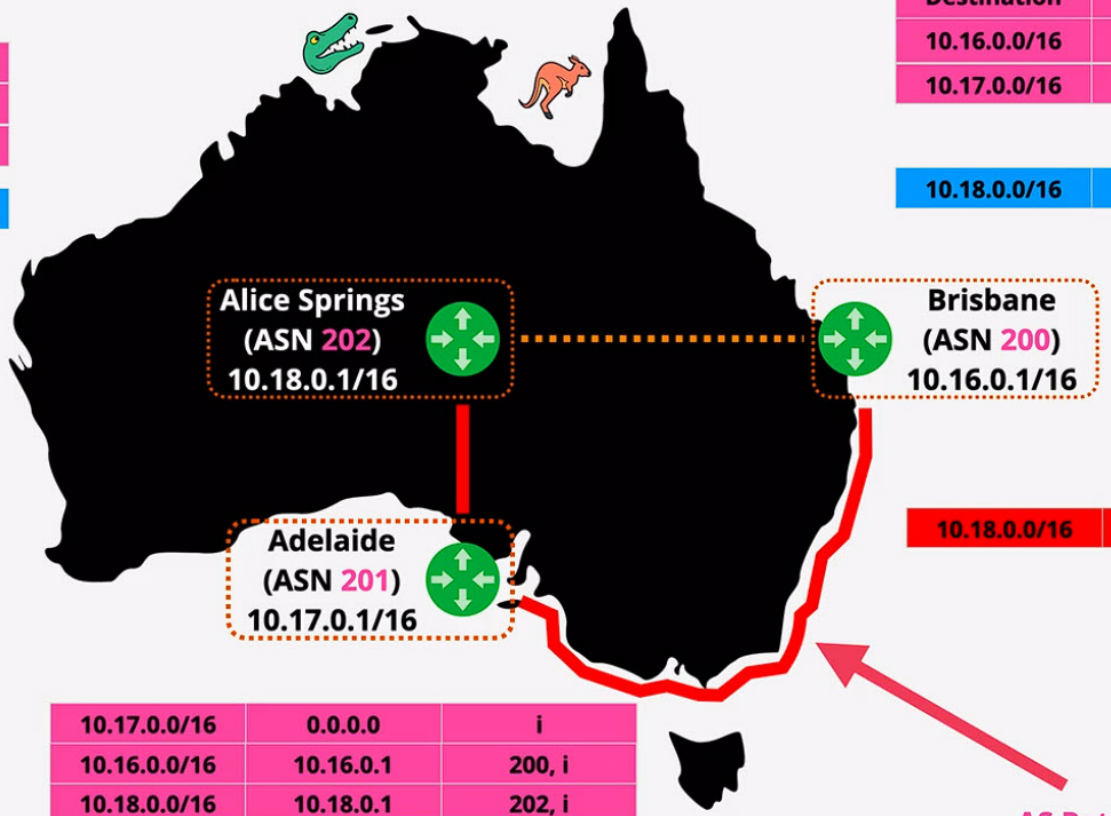
Destination	Next Hop	ASPATH
10.16.0.0/16	0.0.0.0	i
10.17.0.0/16	10.17.0.1	201,i
10.18.0.0/16	10.17.0.1	201, 202,i

10.18.0.0/16	10.18.0.1	202,202,202,i

10.18.0.0/16	10.17.0.1	201,200, i

10.17.0.0/16	0.0.0.0	i
10.16.0.0/16	10.16.0.1	200, i
10.18.0.0/16	10.18.0.1	202, i

10.18.0.0/16	10.16.0.1	200, 202,i



Shorter

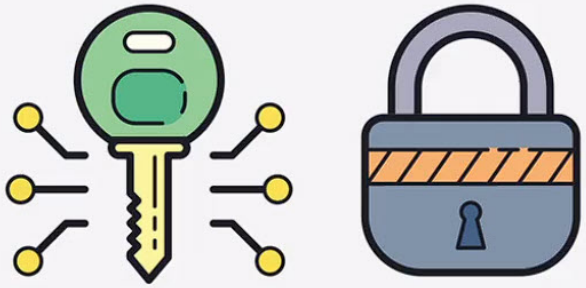
An AS will advertise all the shortest paths it knows to all its peers, the AS prepends its own AS number onto the path - this creates a source to destination path which BGP routers can learn & propagate.

BGP exchanges the shortest ASPATH between peers. Brisbane -> Alice Springs would default to the satellite link .. even though the longer fibre would provide better performance.

AS Path Prepending can be used to artificially make the satellite path look longer making the fibre path preferred.

IPSEC VPN

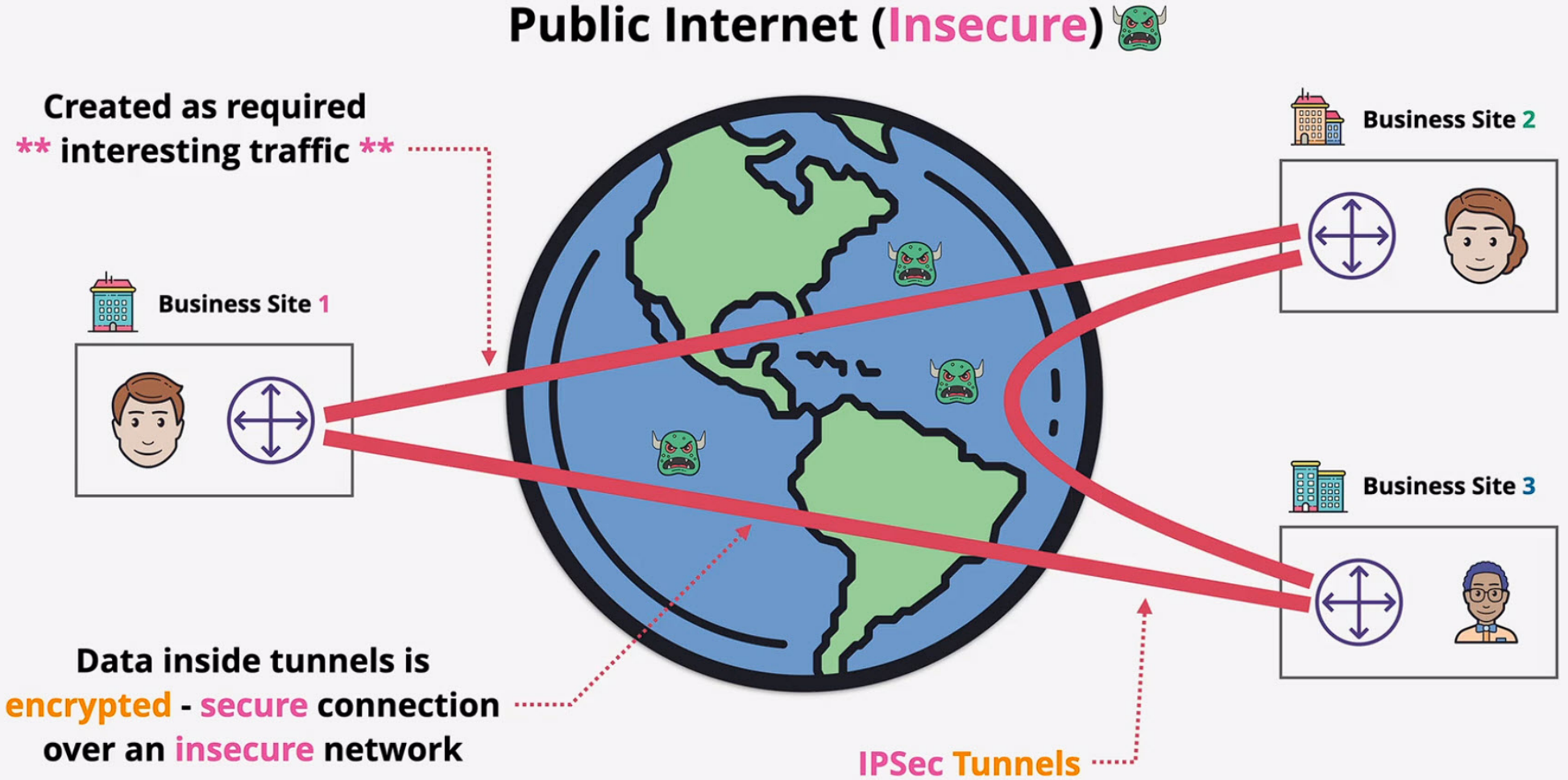
Fundamentals



- IPSEC is a group of protocols ...
- It sets up **secure tunnels** across **insecure networks**
- .. between **two peers** (**local** and **remote**)
- Provides **Authentication** ...
- .. and **encryption**

IPSEC VPN Fundamentals

https://learn.cantrill.io adriancantrill



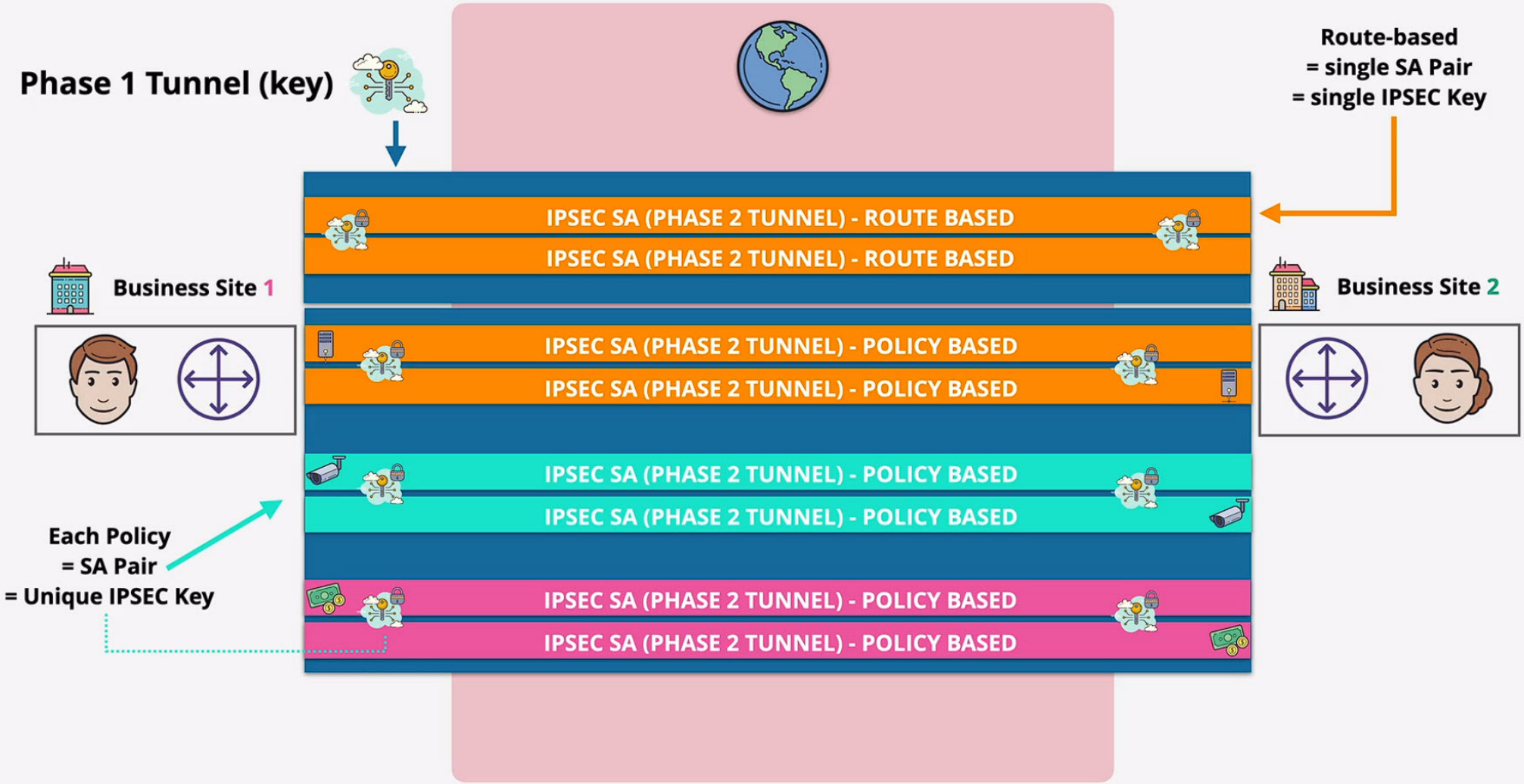
- Remember - **Symmetric Encryption** is fast ... 
- ... but it's a challenge to exchange keys securely
- **Asymmetric Encryption** is slow ... 
- ... but you can easily exchange public keys

IPSEC VPN Fundamentals

- IPSEC has **two** main phases
- **IKE Phase 1** (Slow & heavy)
  - Authenticate - Pre-shared key (password) / Certificate
  - Using Asymmetric encryption to agree on, and create a shared Symmetric key ...
  - IKE SA Created (phase 1 tunnel)
- **IKE Phase 2** (Fast & Agile)
  - Uses the keys agreed in phase 1
  - Agree encryption method, and keys used for bulk data transfer
  - Create IPSEC SA ... phase 2 tunnel (architecturally running over phase 1)

IPSEC VPN - Route vs Policy Based

https://learn.cantrill.io adriancantrill



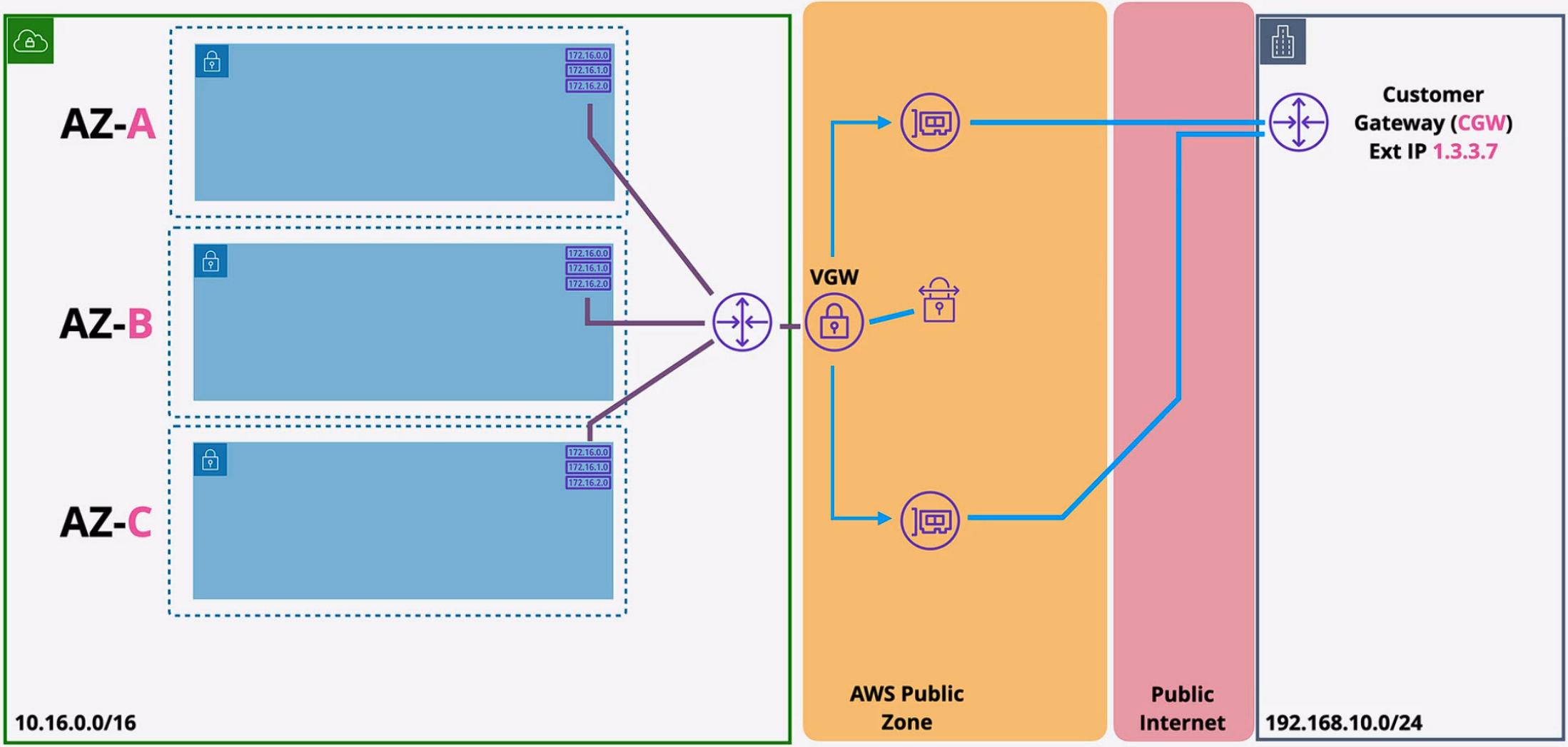
AWS Site-to-Site VPN

AWS Site-to-Site VPN

- A logical connection between a VPC and on-premises network encrypted using IPSec, running over the **public internet***
- Full HA - if you design and implement it correctly 
- Quick to provision ... **less than an hour** 
- Virtual Private Gateway (**VGW**)
- Customer Gateway (**CGW**)
- VPN Connection between the **VGW** and **CGW**

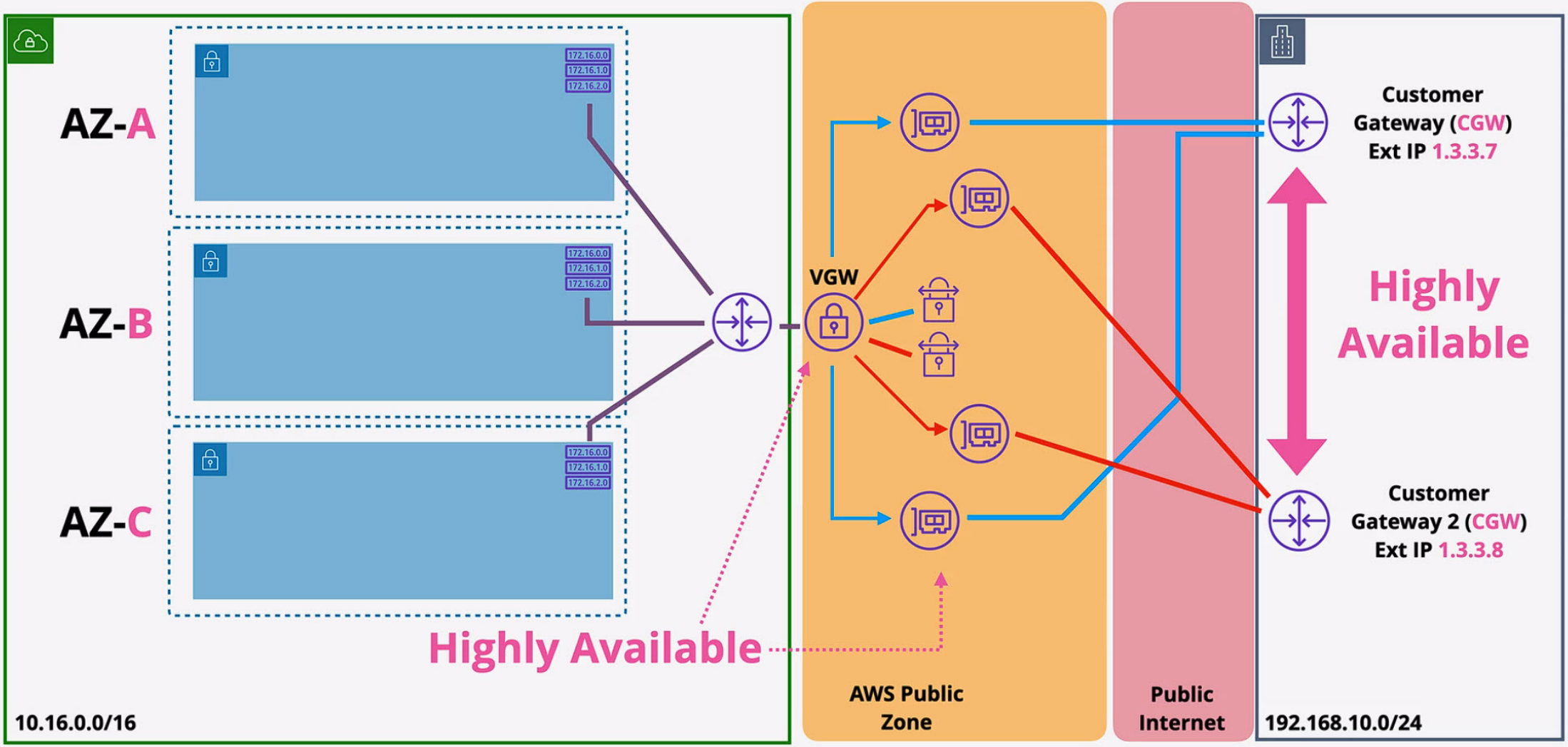
AWS Site-to-Site VPN (HA)

https://learn.cantrill.io adriancantrill



AWS Site-to-Site VPN (HA)

https://learn.cantrill.io adriancantrill



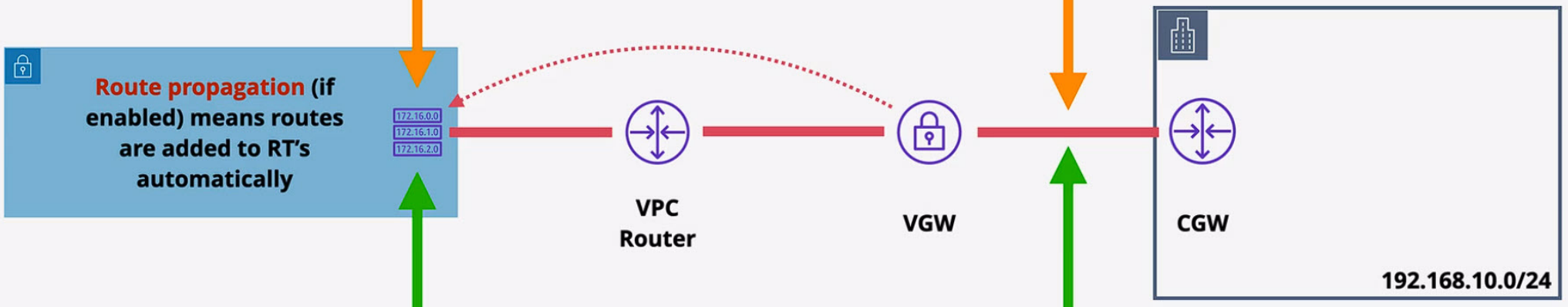
Static vs Dynamic VPN (BGP)

Static

Routes for remote side added to route tables as static routes

Networks for remote side statically configured on the VPN connection

No load balancing and multi connection failover



Dynamic

Routes for remote side added to route tables as static routes

Border Gateway Protocol (BGP) is configured on both the customer and AWS side using (ASN). Networks are exchanged via BGP

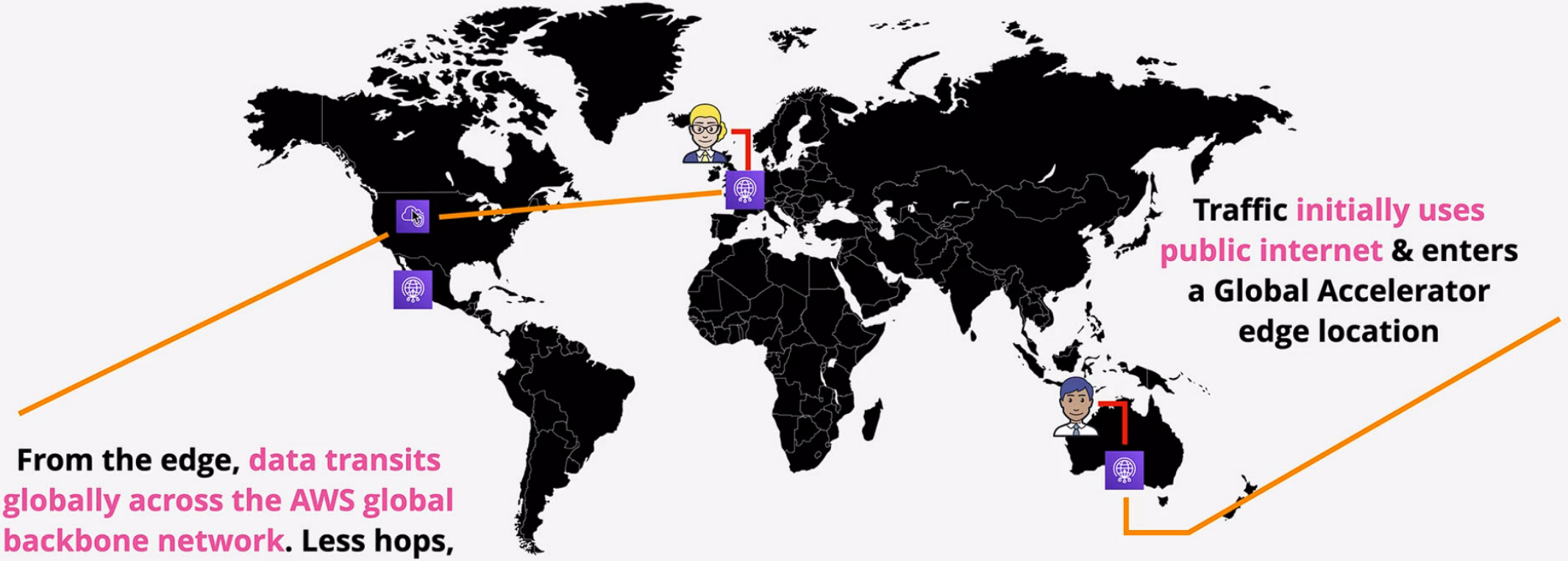
Multiple VPN Connections provide HA and traffic distribution

VPN Considerations

- Speed Limitations ~ **1.25Gbps**
- Latency Considerations - **inconsistent**, **public internet**
- Cost - AWS hourly cost, GB out cost, data cap (on premises)
- Speed of setup - **hours** .. all **software** configuration
- Can be used as a backup for Direct Connect (**DX**)
- Can be used with Direct Connect (**DX**)

AWS Global Accelerator

Global Accelerator



Traffic initially uses public internet & enters a Global Accelerator edge location

From the edge, data transits globally across the AWS global backbone network. Less hops, directly under AWS control, significantly better performance.

2 x anycast IP Addresses
1.2.3.4 & 4.3.2.1

Anycast IP's allow a single IP to be in multiple locations. Routing moves traffic to closest location

Key Concepts

- Moves the **AWS network closer** to customers
- Connections **enter at edge** .. using anycast IPs
- **Transit over AWS backbone** to **1+** locations
- Can be used for **NON HTTP/S** (**TCP**/**UDP**) - **Difference from CloudFront**