FORTINET | USA

XPERTS

SUMMIT 2024

Helping you create a digitally secure future.

Public Cloud - 201 Advanced FortiGate Deployments on AWS - TGW & GWLB

Louie Aberra & Jeremy Furtney
Cloud CSEs

Agenda

Introduction & Helpful Sites

AWS Networking 101 Refresher

Workshop Primer

Workshop Hands On

Section 5

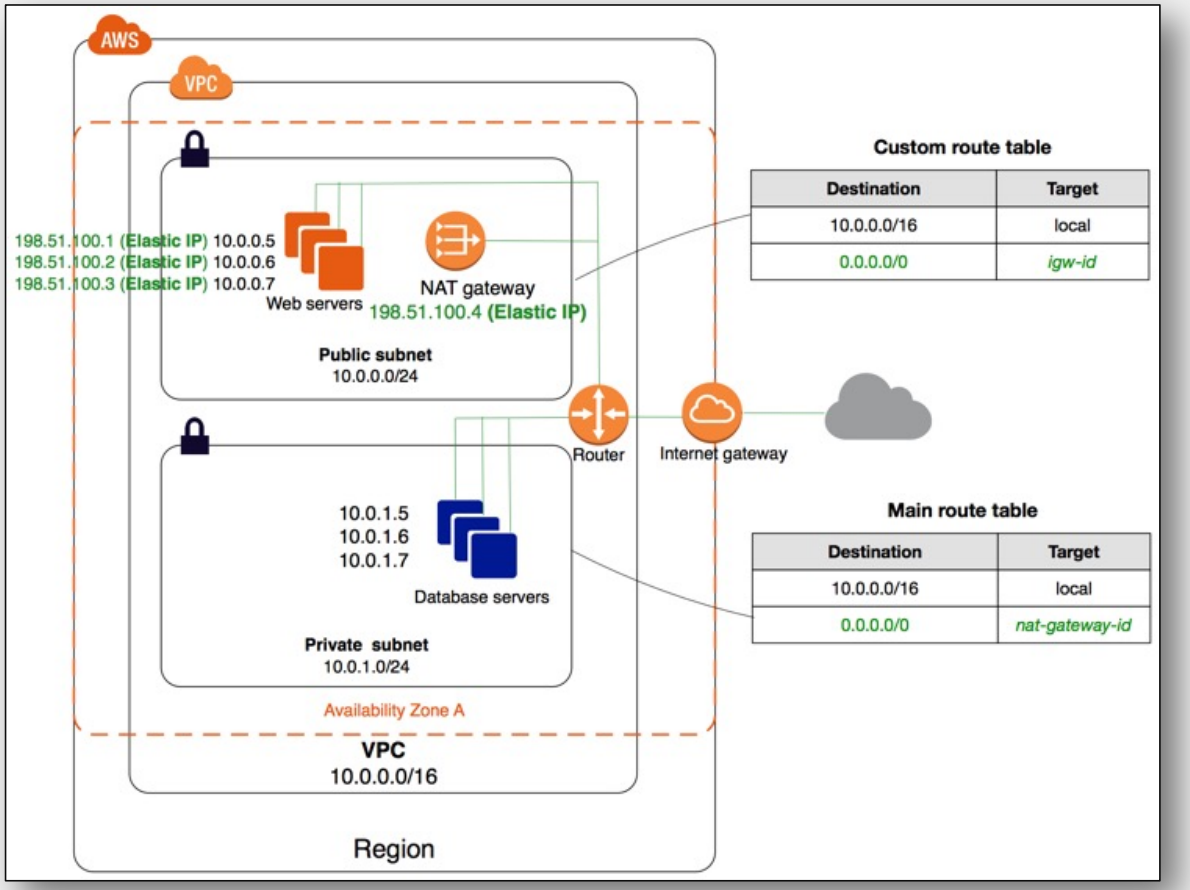
Helpful Sites

What we used to get started in public cloud

- Self-paced training + hands-on udemy.com & acloudguru.com
- Fortinet docs for public + private cloud docs.fortinet.com/cloud-solutions
- Infrastructure as Code + quick start guides + use cases github.com/FortinetCloudCSE
- API, Terraform Provider, Ansible Playbooks, etc fndn.fortinet.net
- SaaS + VM solutions, including free trials aws.amazon.com/mp
- Anything else…

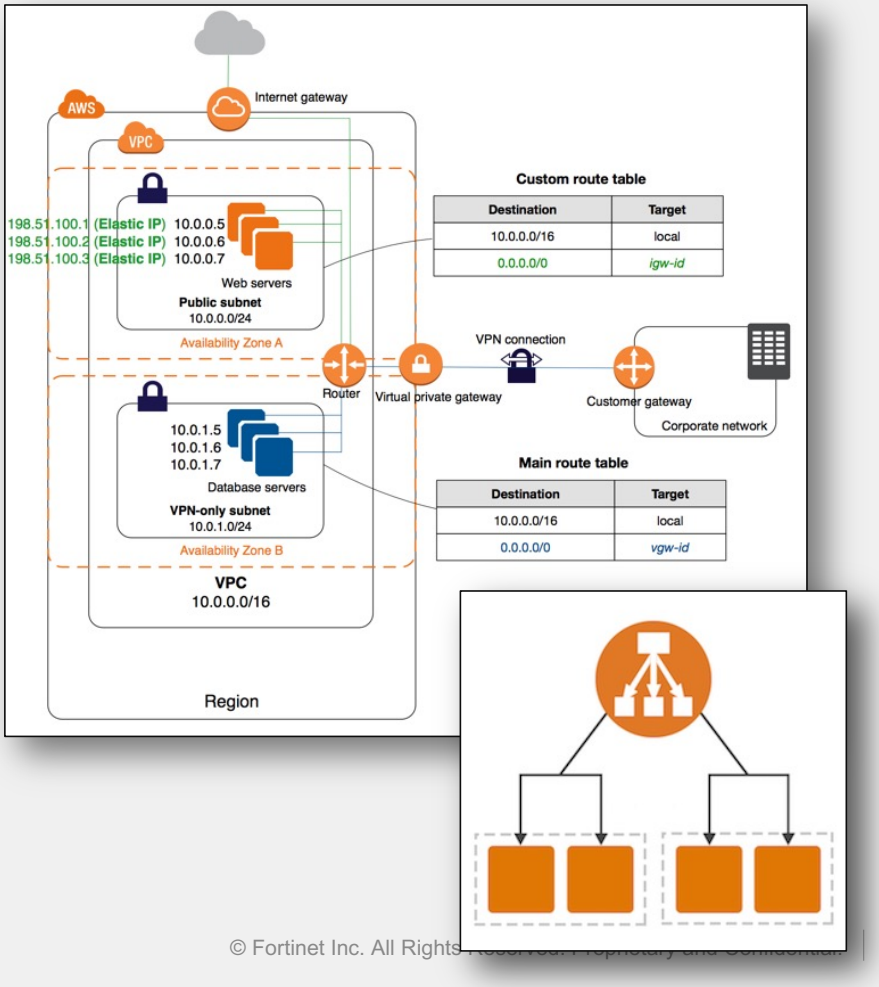
AWS Intrinsic Router & Internet Gateway

- Public: Subnet with a connected Internet Gateway.
- Private: Subnet without an Internet Gateway.
- All Subnets are connected to an Intrinsic Router that resides at VPC level (in all AZ).
- EC2 instances always use the VPC Router as default gateway and are redirected to each destination in the assigned route table.
- A main routing table is associated to subnets by default. Can create more and associate them to a subnet.
- Gateway is not defined by IP, instead uses the Elastic Network Interface.

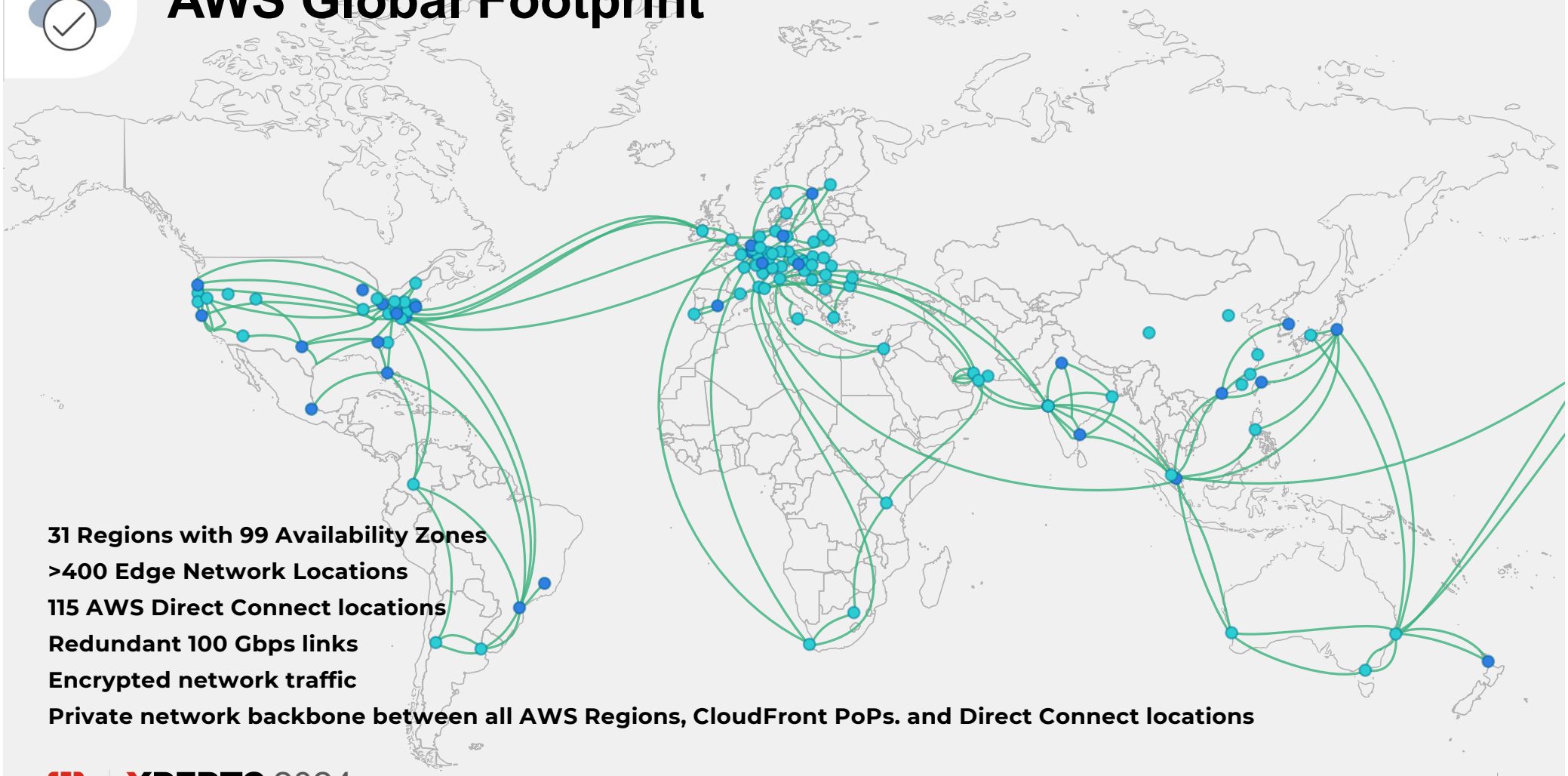


AWS Common Networking Services

- Elastic Load Balancing (ALB, NLB, ELB\CLB)
  - Public and Private Server Load Balancing Services provided within the VPC.
  - Application LB: HTTP L7 based with content routing. Always SNATs with XFF in HTTP Header.
  - Network LB: TCP L4 based. Can preserve original source IP depending on listener type/settings.
  - Elastic\Classic LB: Legacy L4-7 based with no content routing. Always SNATs with XFF in HTTP Header
- Route53
  - Public and Private AWS DNS service.
  - Provides health checks with load sharing and failover.
- Site to VPC Access
  - Software VPN: C2S SSL\IPsec VPN to a FGT.
  - Hardware VPN: S2S IPsec to AWS VPN GW or TGW.
  - Direct Connect: Dedicated private circuit to AWS.



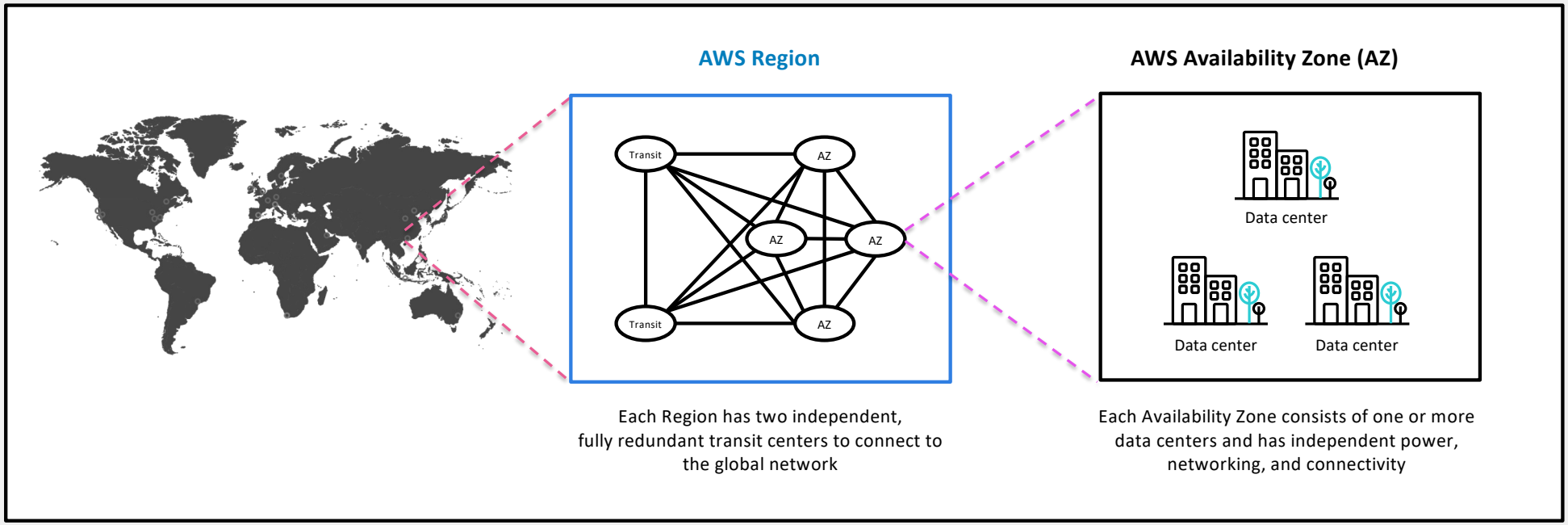
AWS Global Footprint



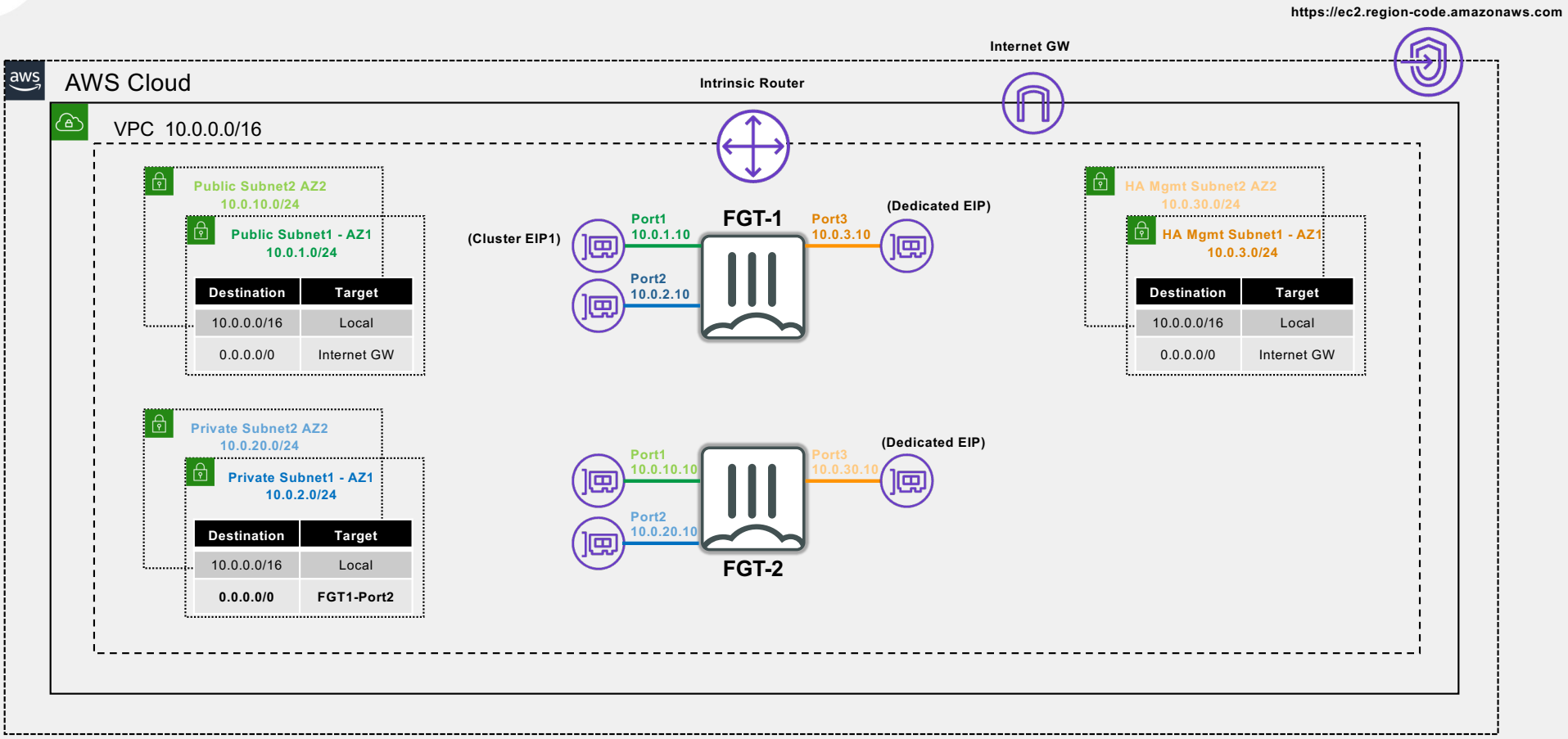
31 Regions with 99 Availability Zones
>400 Edge Network Locations
115 AWS Direct Connect locations
Redundant 100 Gbps links
Encrypted network traffic
Private network backbone between all AWS Regions, CloudFront PoPs. and Direct Connect locations

Fault tolerance in our physical infrastructure

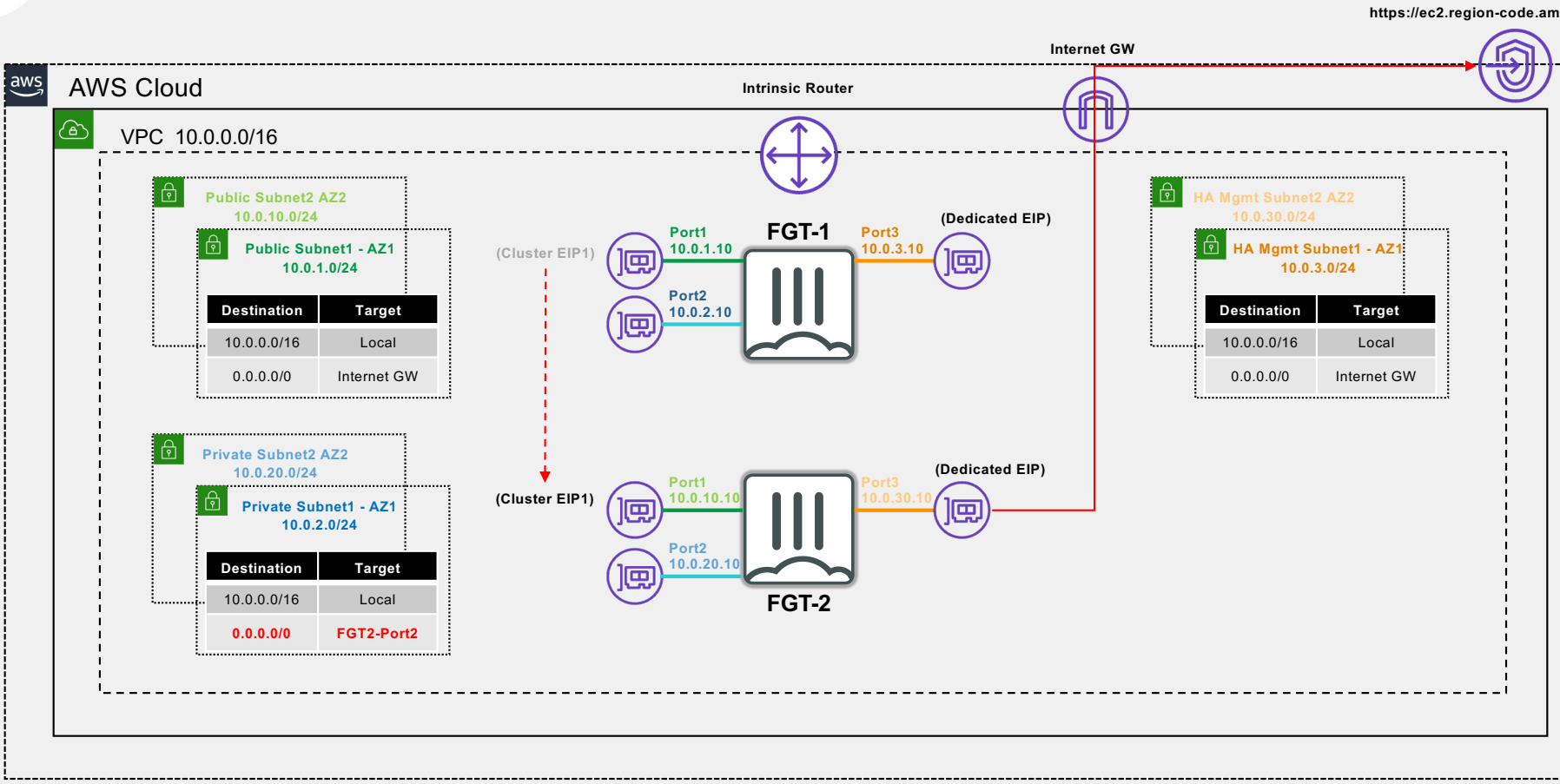
AWS Regions are comprised of multiple AZs for high availability and scalability



FGCP Unicast A-P (Dual Zone)

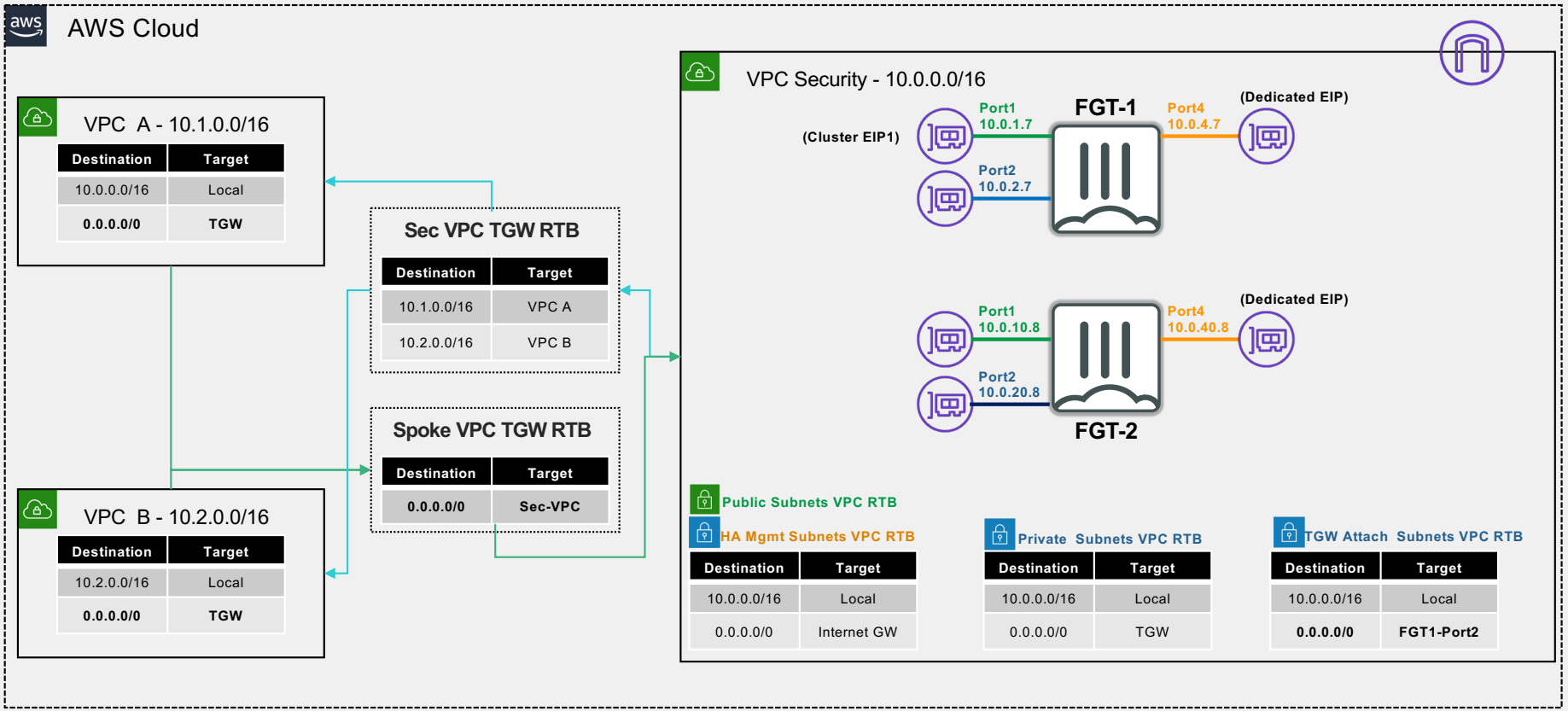


FGCP Unicast A-P Failover (Dual Zone)

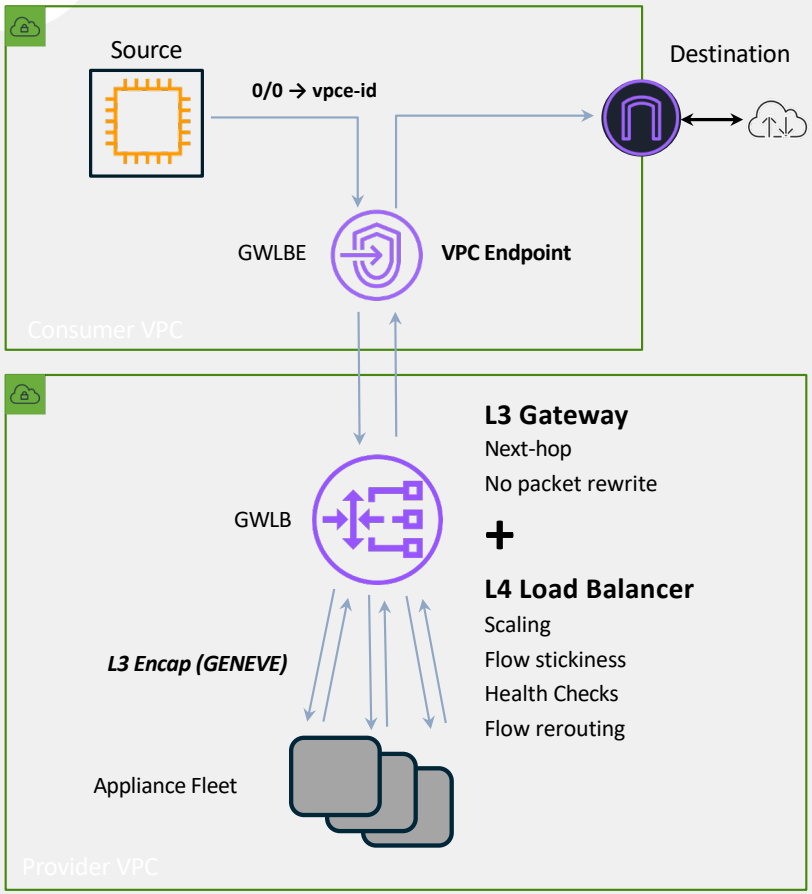


TGW & FGCP Unicast A-P (Dual Zone)

https://ec2.region-code.amazonaws.com



Gateway Load Balancer: At-a-Glance



Components

- Gateway Load Balancer Endpoint (GWLBE) - A new type of VPC endpoint that can be a next-hop in a VPC route table
- Gateway Load Balancer (GWLB) - A new type of load balancer that includes L3 Gateway + L4 Load Balancer capabilities
- Both components powered by AWS Hyperplane

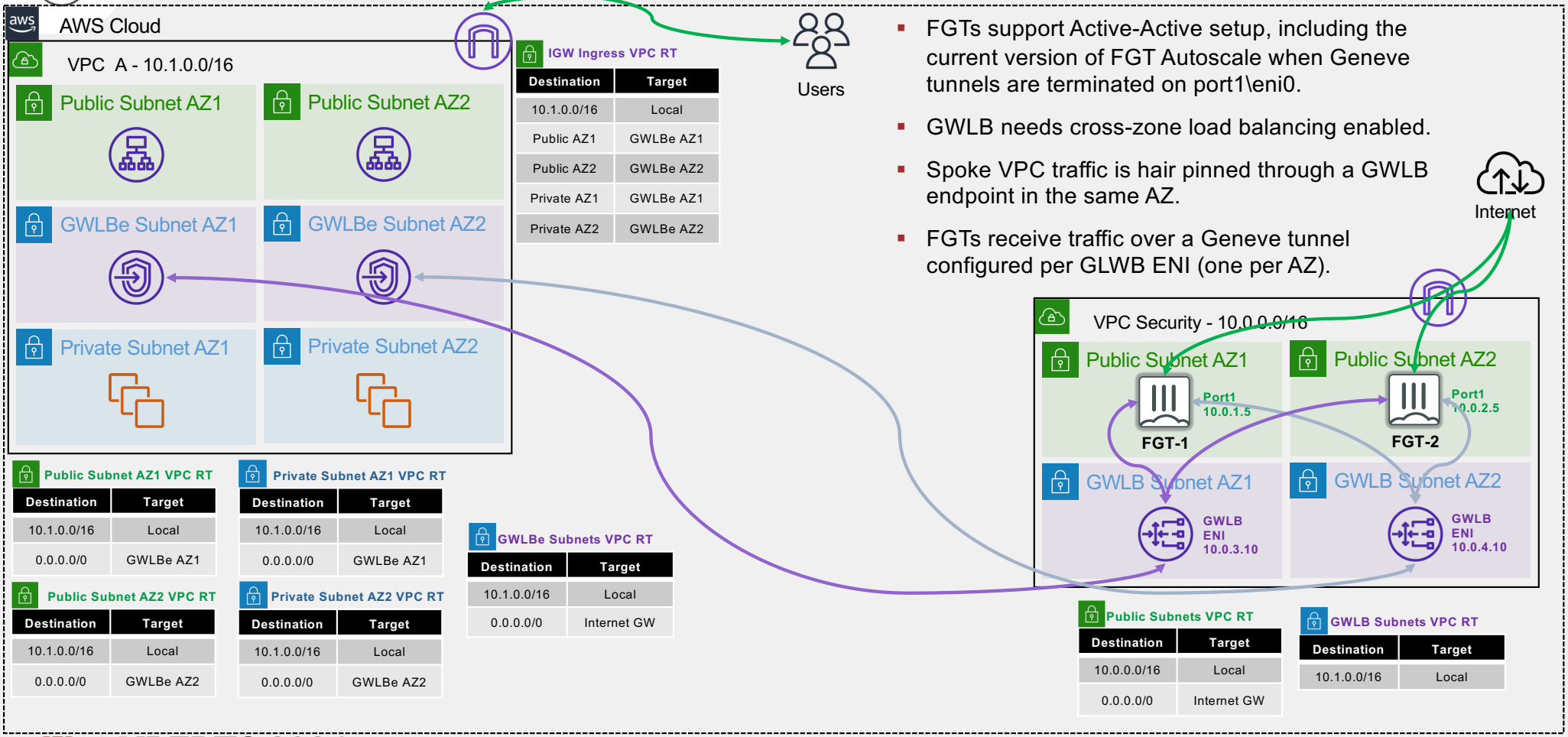
Benefits

- Horizontal auto-scaling
- Fault tolerant (active/active)
- Transparent network insertion
- Separate security and user admin domains, share across different VPCs and AWS accounts
- Provide Appliance-as-a-Service, (e.g. Firewall-as-a-Service)

Deployment

- Create GWLB and appliance fleet using steps similar to NLB
- Send traffic to GWLBE by updating VPC route tables

Gateway Load Balancer (North-South)



- FGTs support Active-Active setup, including the current version of FGT Autoscale when Geneve tunnels are terminated on port1\eni0.
- GWLB needs cross-zone load balancing enabled.
- Spoke VPC traffic is hair pinned through a GWLB endpoint in the same AZ.
- FGTs receive traffic over a Geneve tunnel configured per GLWB ENI (one per AZ).

IGW Ingress VPC RT

Destination	Target
10.1.0.0/16	Local
Public AZ1	GWLBe AZ1
Public AZ2	GWLBe AZ2
Private AZ1	GWLBe AZ1
Private AZ2	GWLBe AZ2

Public Subnet AZ1 VPC RT

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	GWLBe AZ1

Private Subnet AZ1 VPC RT

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	GWLBe AZ1

Public Subnet AZ2 VPC RT

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	GWLBe AZ2

Private Subnet AZ2 VPC RT

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	GWLBe AZ2

GWLBe Subnets VPC RT

Destination	Target
10.1.0.0/16	Local
0.0.0.0/0	Internet GW

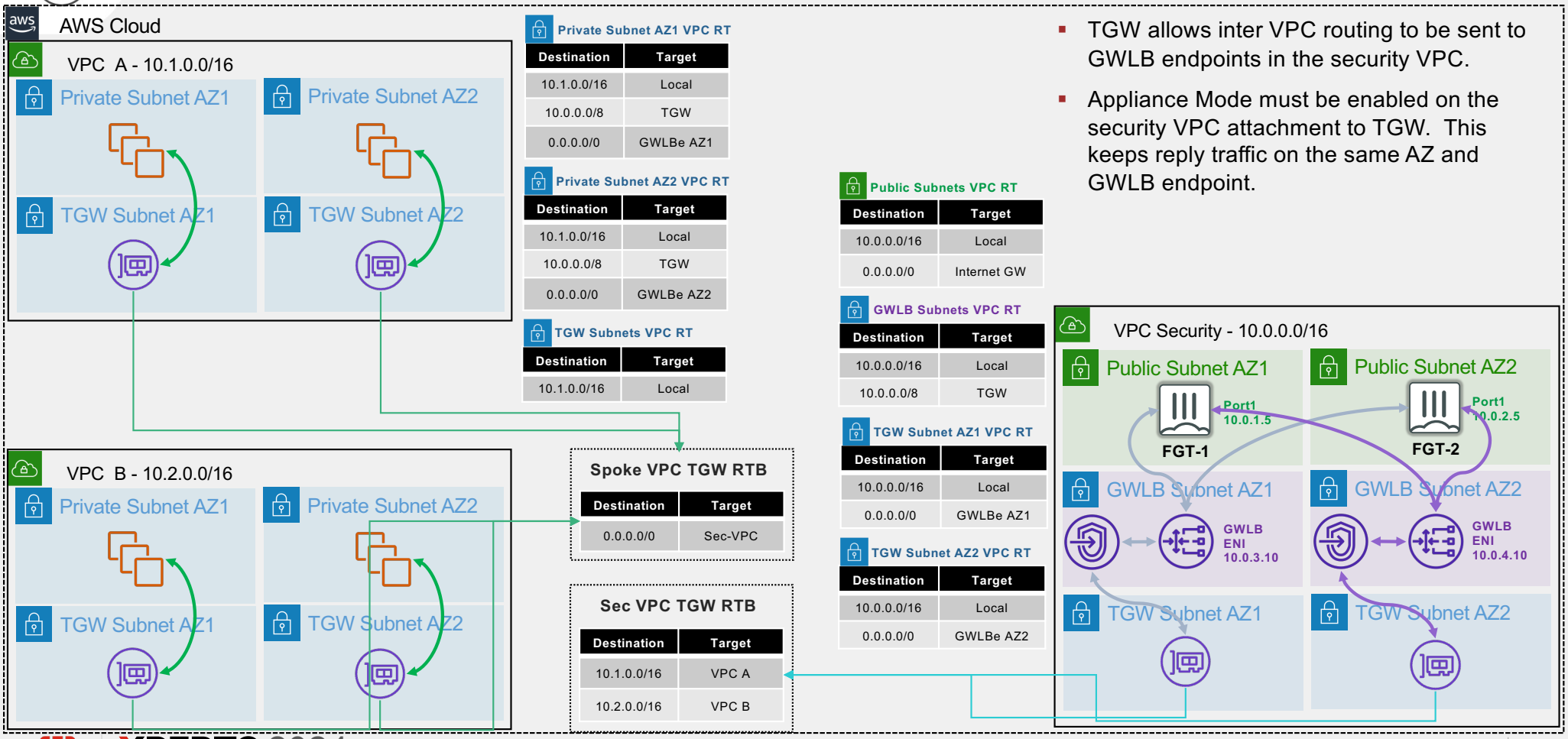
Public Subnets VPC RT

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet GW

GWLB Subnets VPC RT

Destination	Target
10.1.0.0/16	Local

Gateway Load Balancer (East-West)



- TGW allows inter VPC routing to be sent to GWLB endpoints in the security VPC.
- Appliance Mode must be enabled on the security VPC attachment to TGW. This keeps reply traffic on the same AZ and GWLB endpoint.


FORTINET