

Helping you create a
digitally secure future.

Public Cloud 201 AWS

Hiruy (Louie) Aberra & Mike Wooten
Public Cloud CSEs



Agenda



Introduction & Helpful Sites



AWS Networking 101 Refresher



Workshop Primer



Workshop Hands On



Close Out





Helpful Sites

What we used to get started in public cloud

- ✓ Self-paced training + hands-on [udemy.com](https://www.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 (AWS, FortiOS, FGT-ASG), Ansible Playbooks, etc fndn.fortinet.net
- ✓ SaaS + VM solutions, including free trials aws.amazon.com/mp
- ✓ Anything else...



Task1 Primer (VPC Peering)

Relevance & important questions to consider for this task

- ✓ Limited use case that can get complex & expensive fast, why?
- ✓ If you connected VPCs in full mesh, what is the max number of VPCs you could use?
- ✓ Where VPC peering connects affects how routing works!
- ✓ How would you insert FGT(s) to inspect ingress, egress, and/or east/west?
- ✓ What about FWBs for ingress HTTP(s)?
- ✓ What use case is this beneficial for?



Task2 Primer (Transit Gateway w/ VPCs)

Relevance & important questions to consider for this task

- ✓ Why do you think this would be a common & widely recommended design?
- ✓ Where do TGW attachments connect that allow transitive routing?
- ✓ How can multiple AWS accounts in the same region connect to one TGW?
- ✓ What happens to data processed costs with a centralized inspection design?



Task3 Primer (Transit Gateway w/ BGP)

Relevance & important questions to consider for this task

- ✓ What are the main benefits of attachments that provide overlay tunnelling & BGP?
- ✓ What is the limit of how many static routes in a TGW-RTB for a single attachment?
- ✓ What are the performance and scale limits of Connect vs VPN attachments?
- ✓ What path does Connect vs VPN attachments take?
- ✓ Does TGW or VPCs provide symmetrical routing?



Task4 Primer (Gateway Load Balancer)

Relevance & important questions to consider for this task

- ✓ Why do you think this would be a common & widely recommended design?
- ✓ How does GWLB track a flow and how does it know where to send return traffic?
- ✓ Can you configure flow TTLs in GWLB?
- ✓ Where does NAT, VPN, SDWAN, come into play with GWLB directly?



Task5 Primer (Cloud WAN)

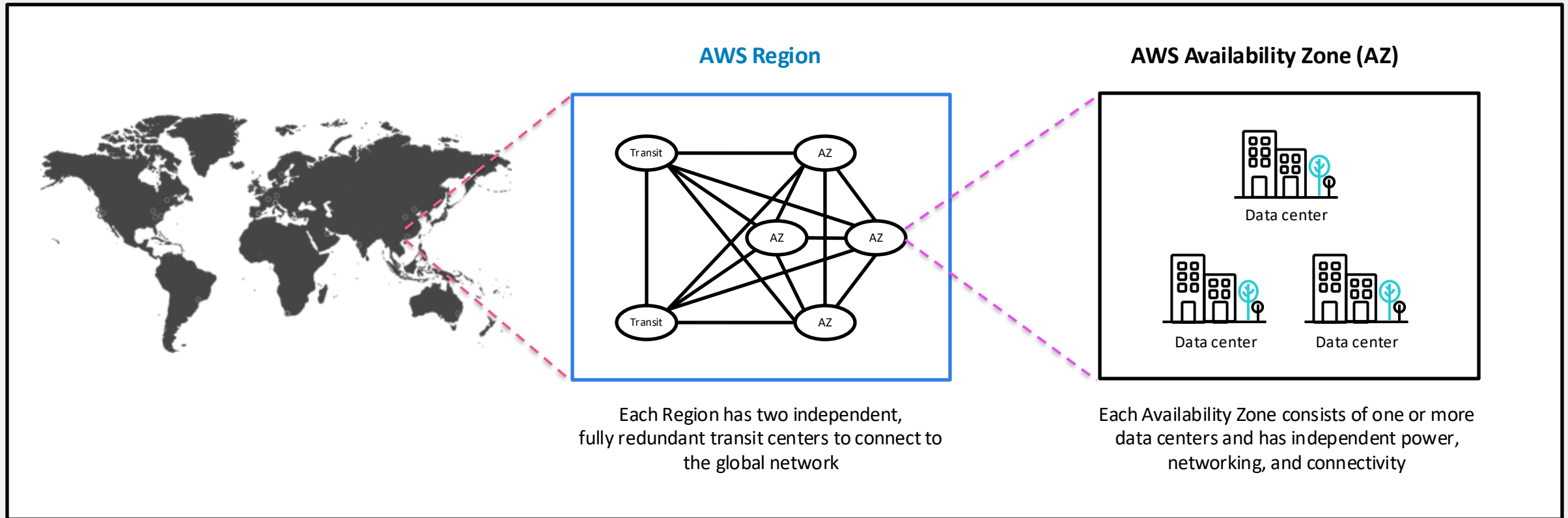
Relevance & important questions to consider for this task

- ✓ What are the main benefits CWAN provides over a TGW based design?
- ✓ What are the additional costs to consider with CWAN?
- ✓ What are the main benefits of Tunnel-less Connect attachments?



Fault tolerance in our physical infrastructure

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





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

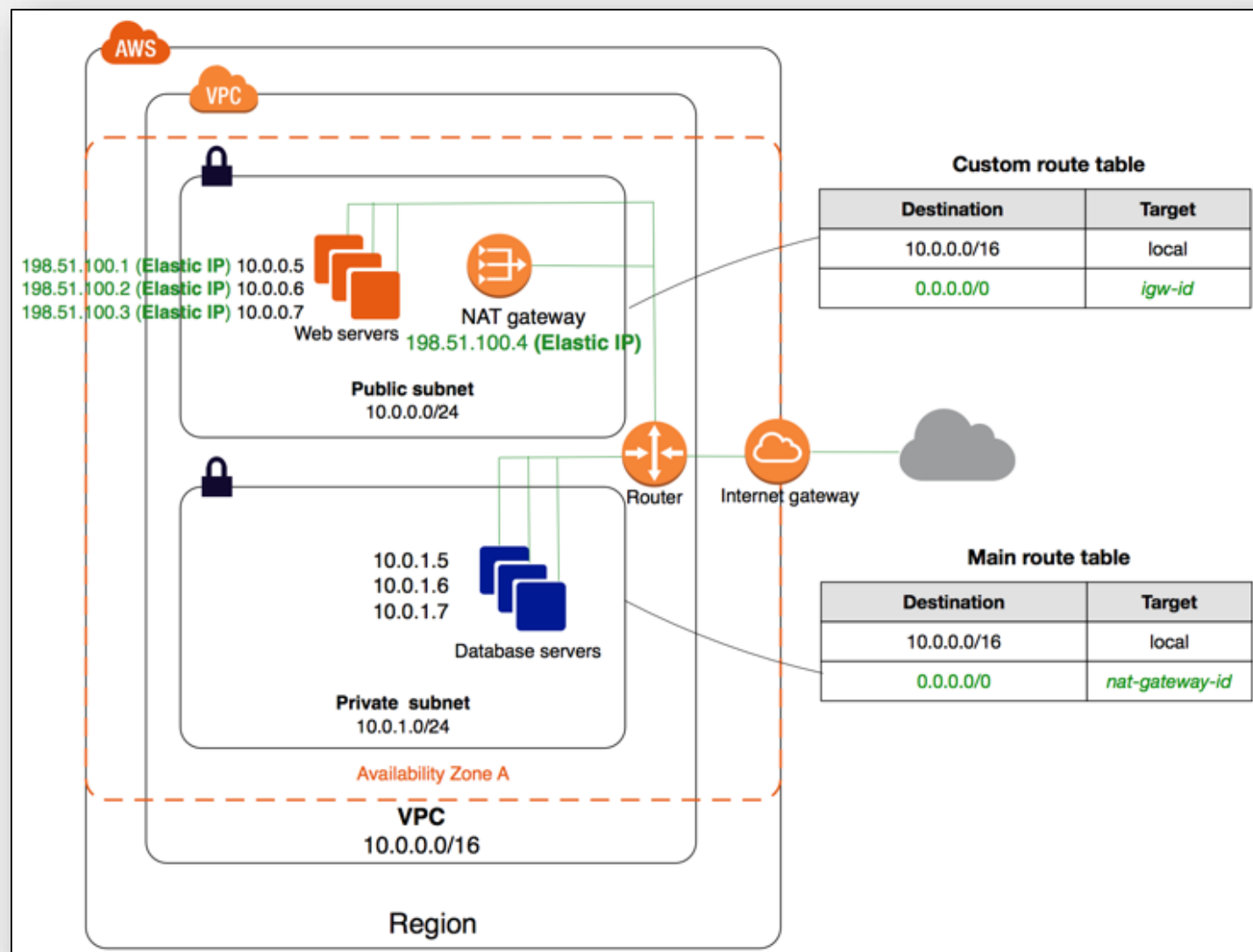


XPERTS 2025



AWS Intrinsic Router & Internet Gateway

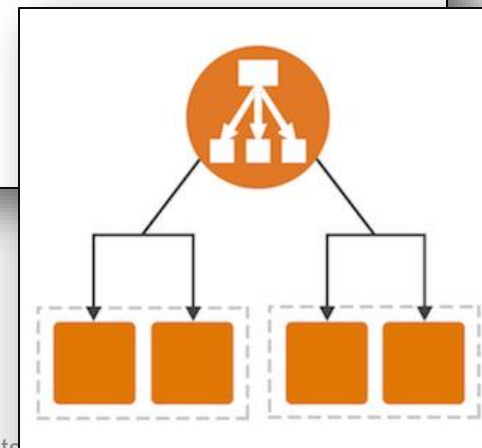
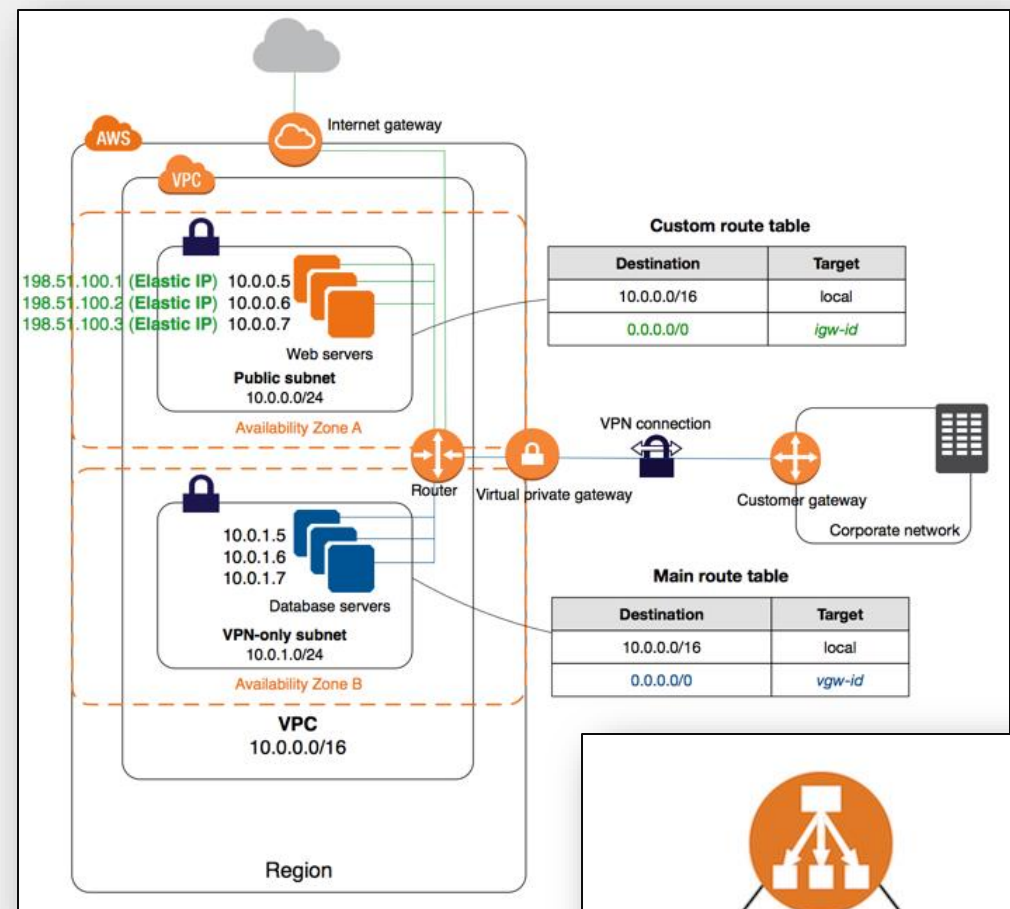
- Public: Subnet with a connected Internet Gateway.
- Private: Subnet without an Internet Gateway.
- All Subnets are connected to an Intrinsic Router that resides at VPC level (in all AZ).
- EC2 instances always use the VPC Router as default gateway and are redirected to each destination in the assigned 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

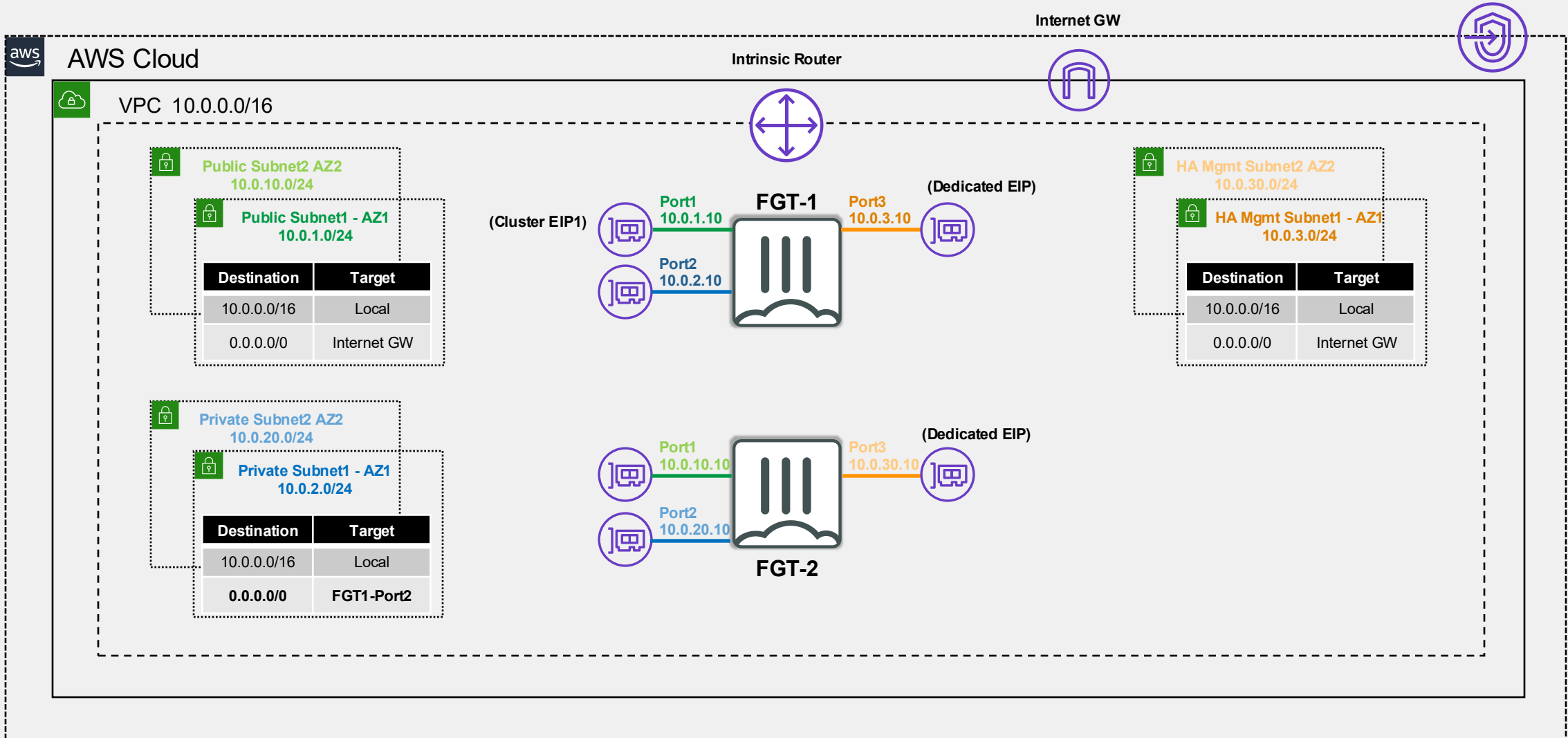
- Elastic Load Balancing (ALB, NLB, ELB\CLB)
 - Public and Private Server Load Balancing Services provided within the VPC.
 - Application LB: HTTP L7 based with content routing. Always SNATs with XFF in HTTP Header.
 - Network LB: TCP L4 based. Can preserve original source IP depending on listener type/settings.
 - 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.





FGCP Unicast A-P (Dual Zone)

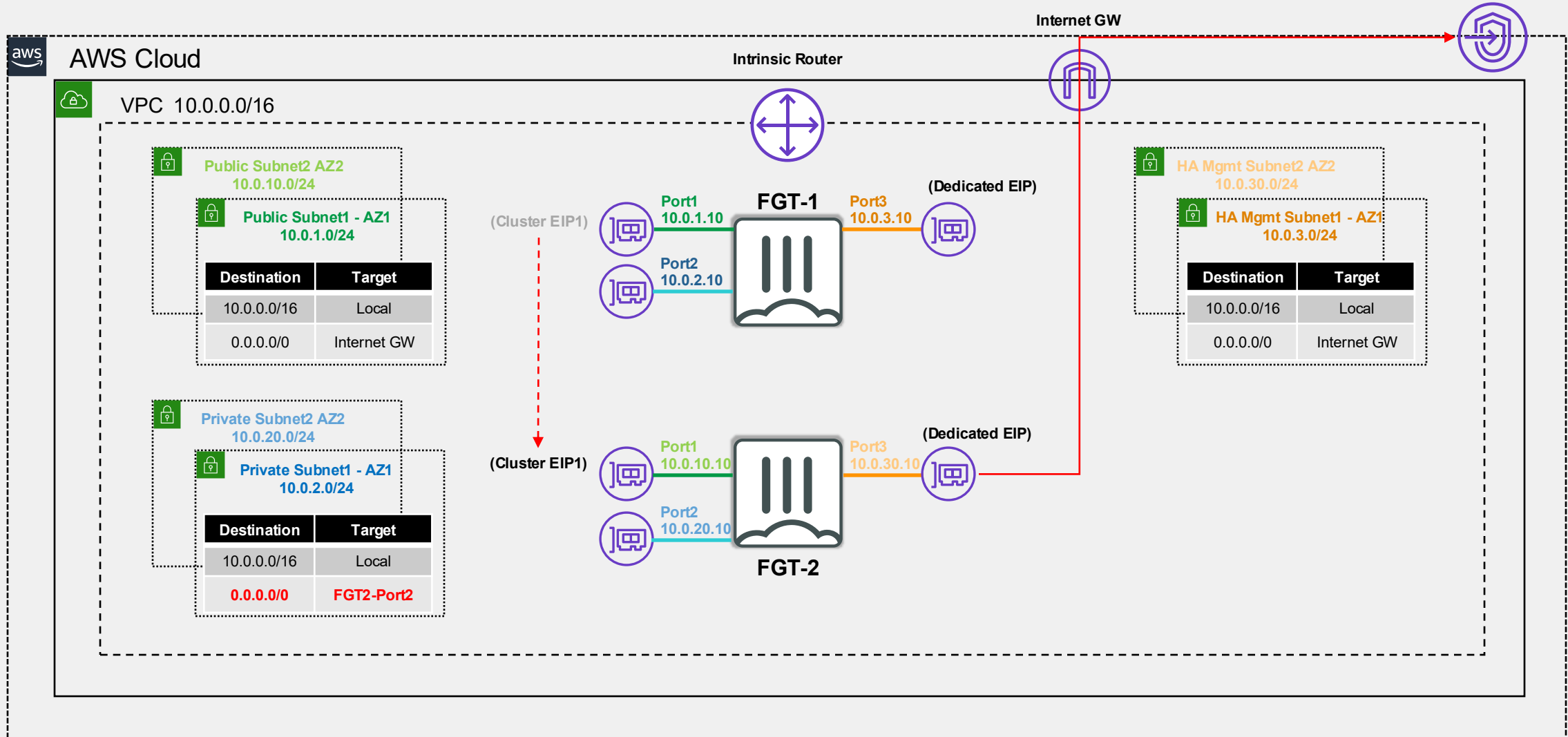
<https://ec2.region-code.amazonaws.com>





FGCP Unicast A-P Failover (Dual Zone)

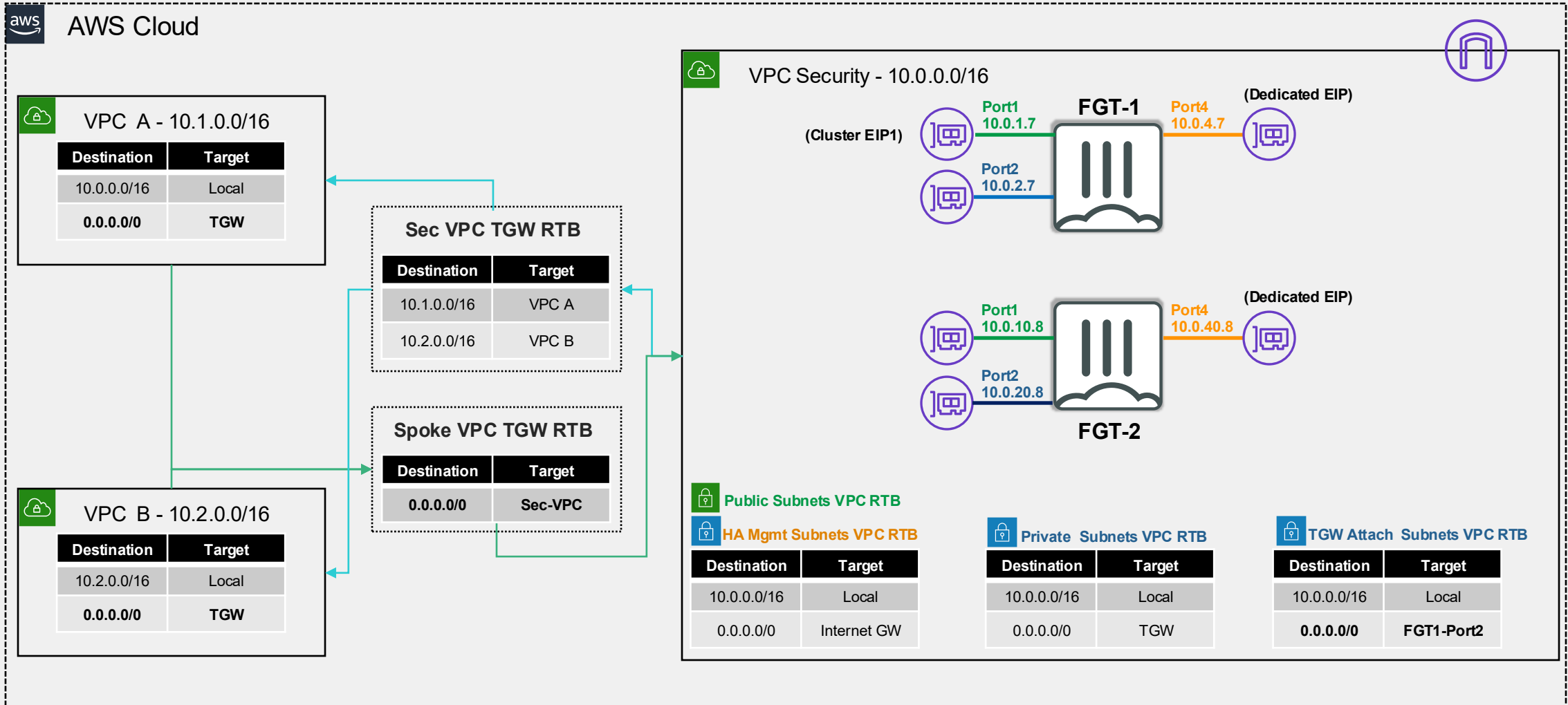
<https://ec2.region-code.amazonaws.com>





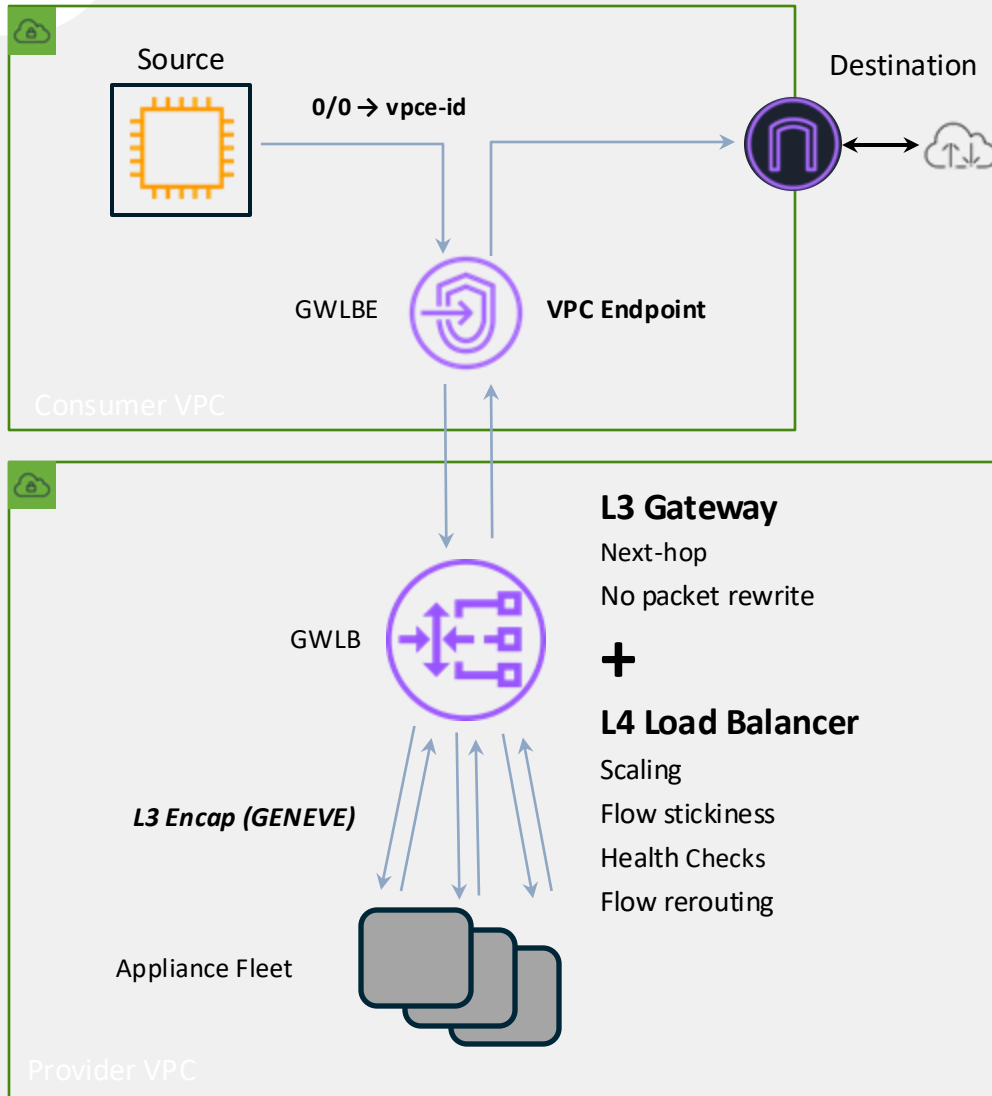
TGW & FGCP Unicast A-P (Dual Zone)

<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 (GWLBE) - A new type of load balancer that includes L3 Gateway + L4 Load Balancer capabilities
- Both components powered by AWS Hyperplane

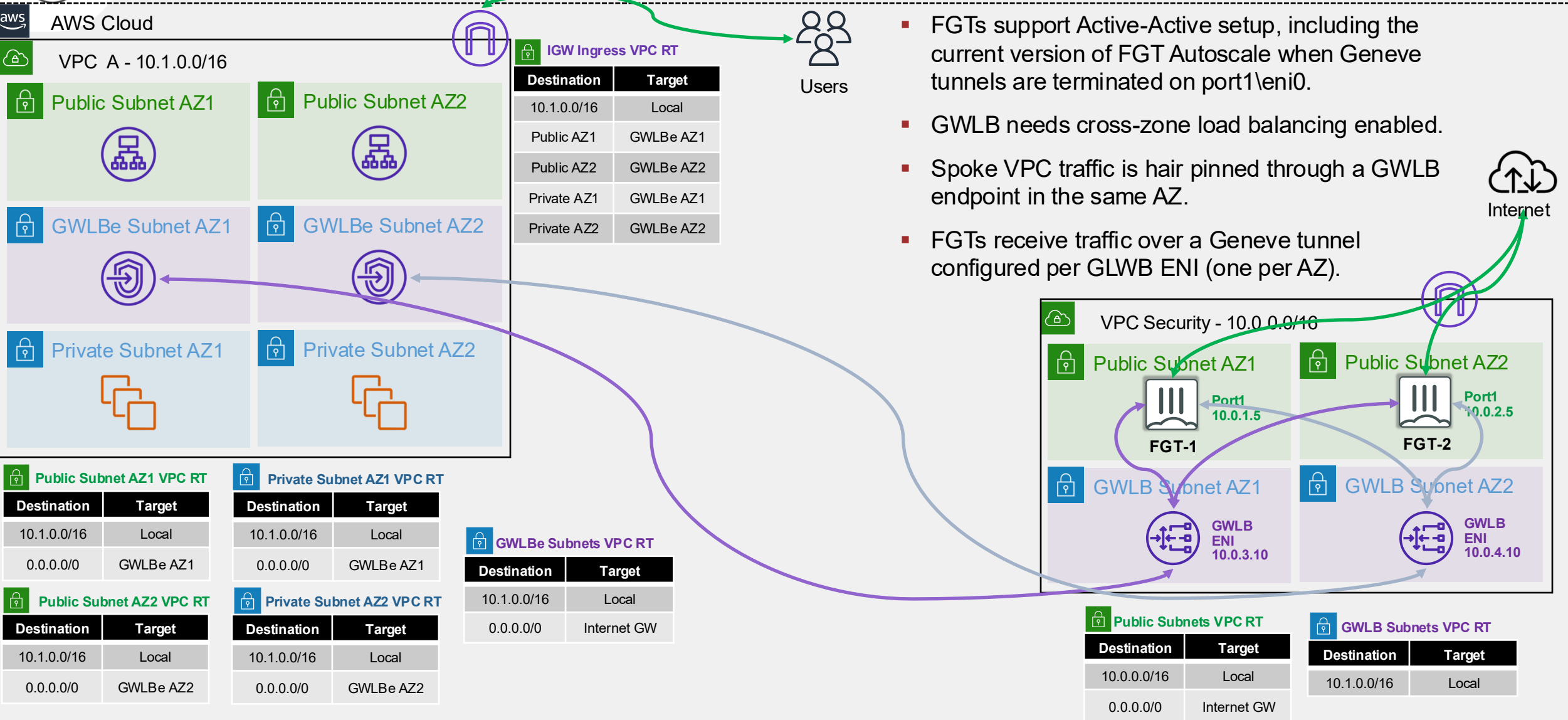
Benefits

- 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

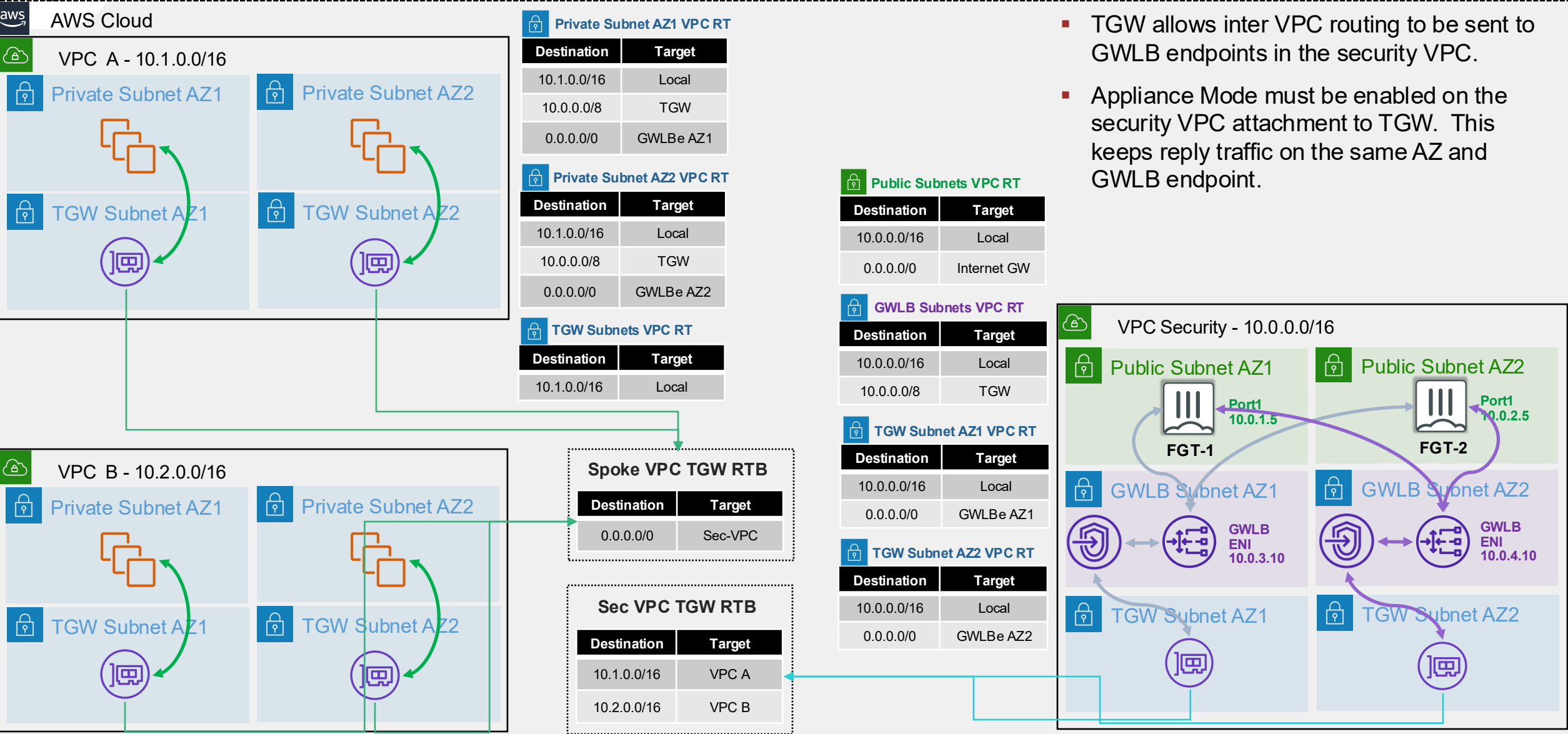
- Create GWLB and appliance fleet using steps similar to NLB
- Send traffic to GWLBE by updating VPC route tables

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).

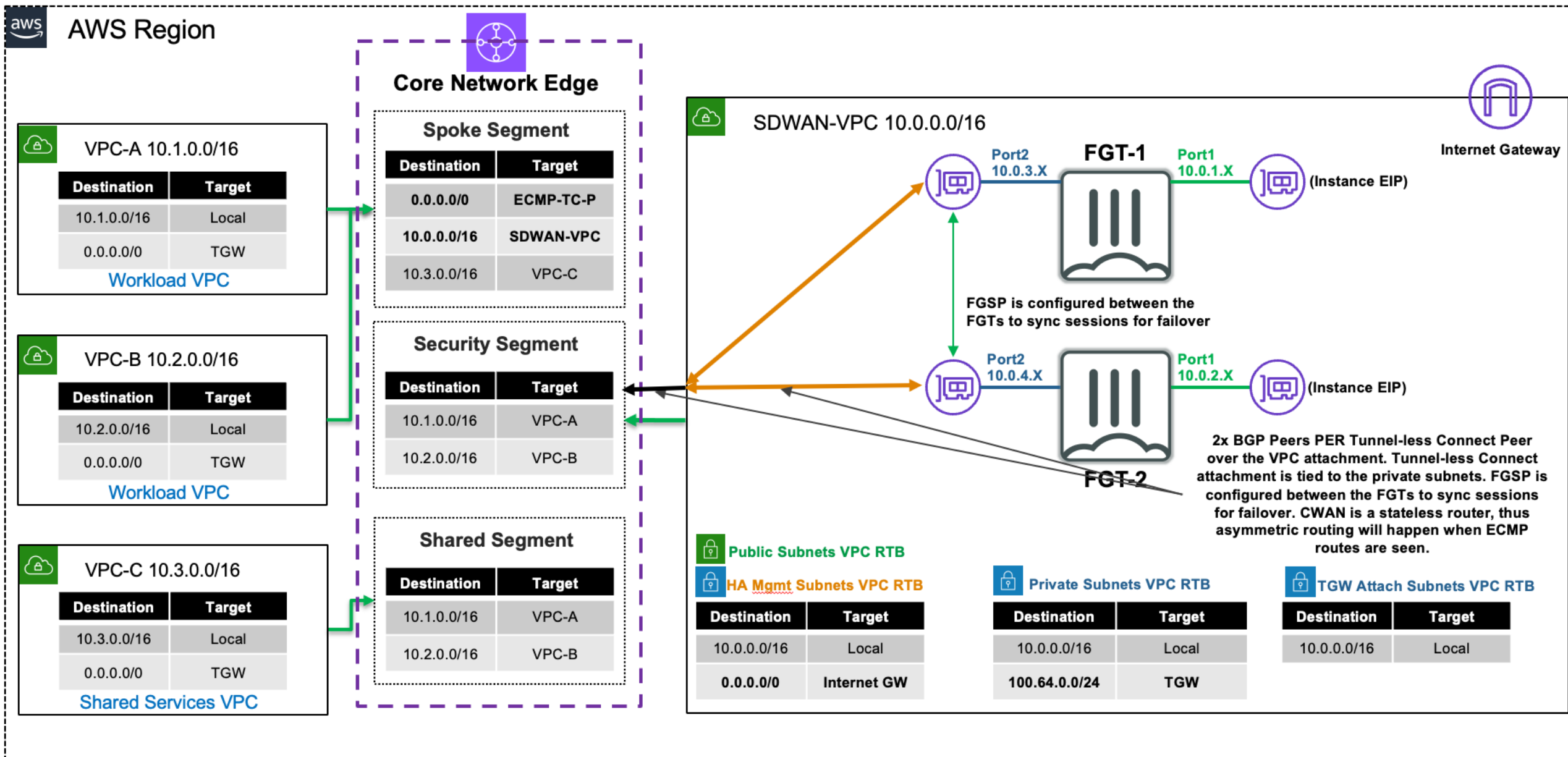
Gateway Load Balancer (East-West)



- 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.



Cloud WAN Tunnel-less Connect



<https://fortinetcloudcse.github.io/AWS-FGT-201>

FORTINET®

