

AWS
re:Invent



NET308

Introducing Gateway Load Balancer for deploying & running virtual appliances

Milind Kulkarni

Senior Product Manager, Networking
AWS

Agenda

1. Customer challenges
2. Solution
3. Use cases
4. Partner integrations
5. Next steps

Deployments today



Customers use third-party appliances

Appliance = Any virtual network function (VNF) running on EC2 instance

Example appliances

- NextGen firewalls (NGFW)
- Intrusion detection / intrusion prevention systems (IDS / IPS)
- DDoS prevention
- Visibility, performance, analytics tools
- ADC, SD-WAN, IoT, etc.

Why do customers use third-party appliances?

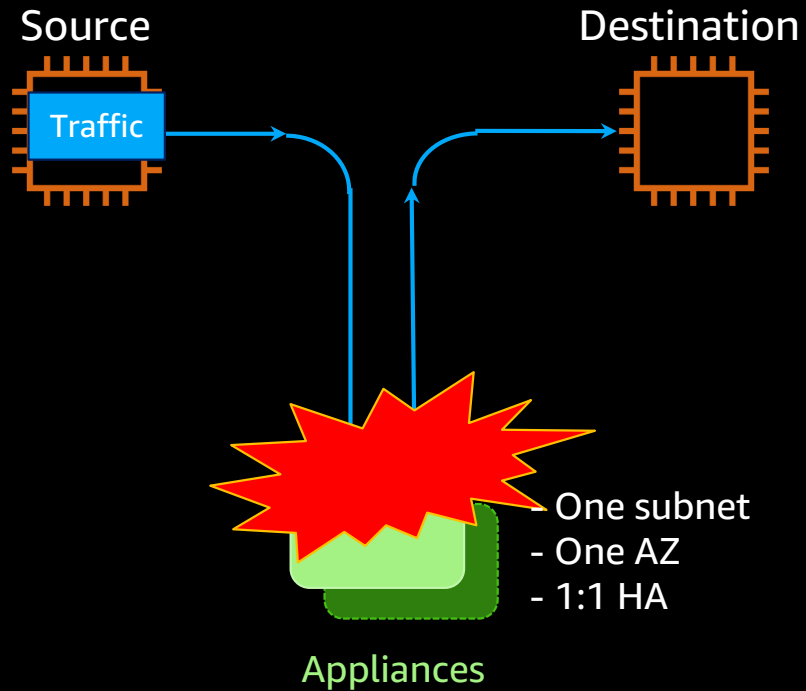
- Specialized functions
- Feature set
- Skill set
- Operating processes
- Existing investments

Customer challenges



Customer deployment options until now

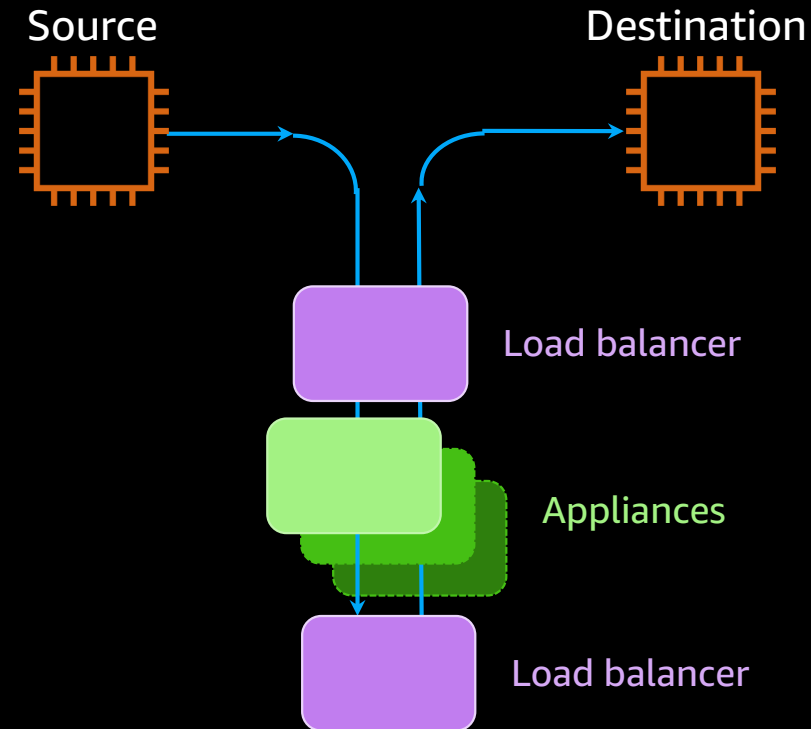
Appliance pairs



Challenges

1. Fixed throughput / scale
2. Single point of failure
3. Replicate everywhere
4. Difficult to manage

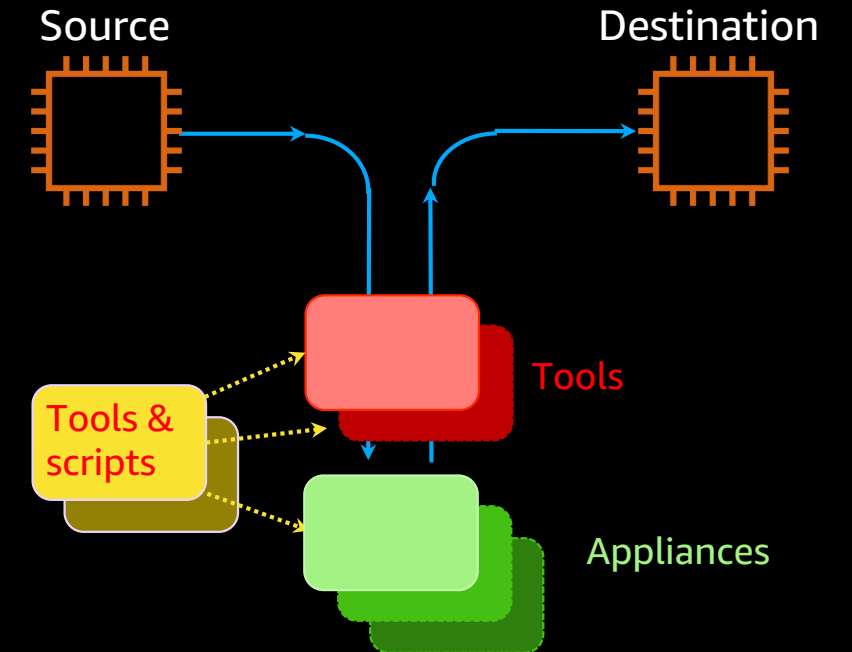
"Sandwich" deployment



Challenges

1. Complex
2. Misconfig prone
3. Single VPC / CIDR
4. Expensive

DIY tooling



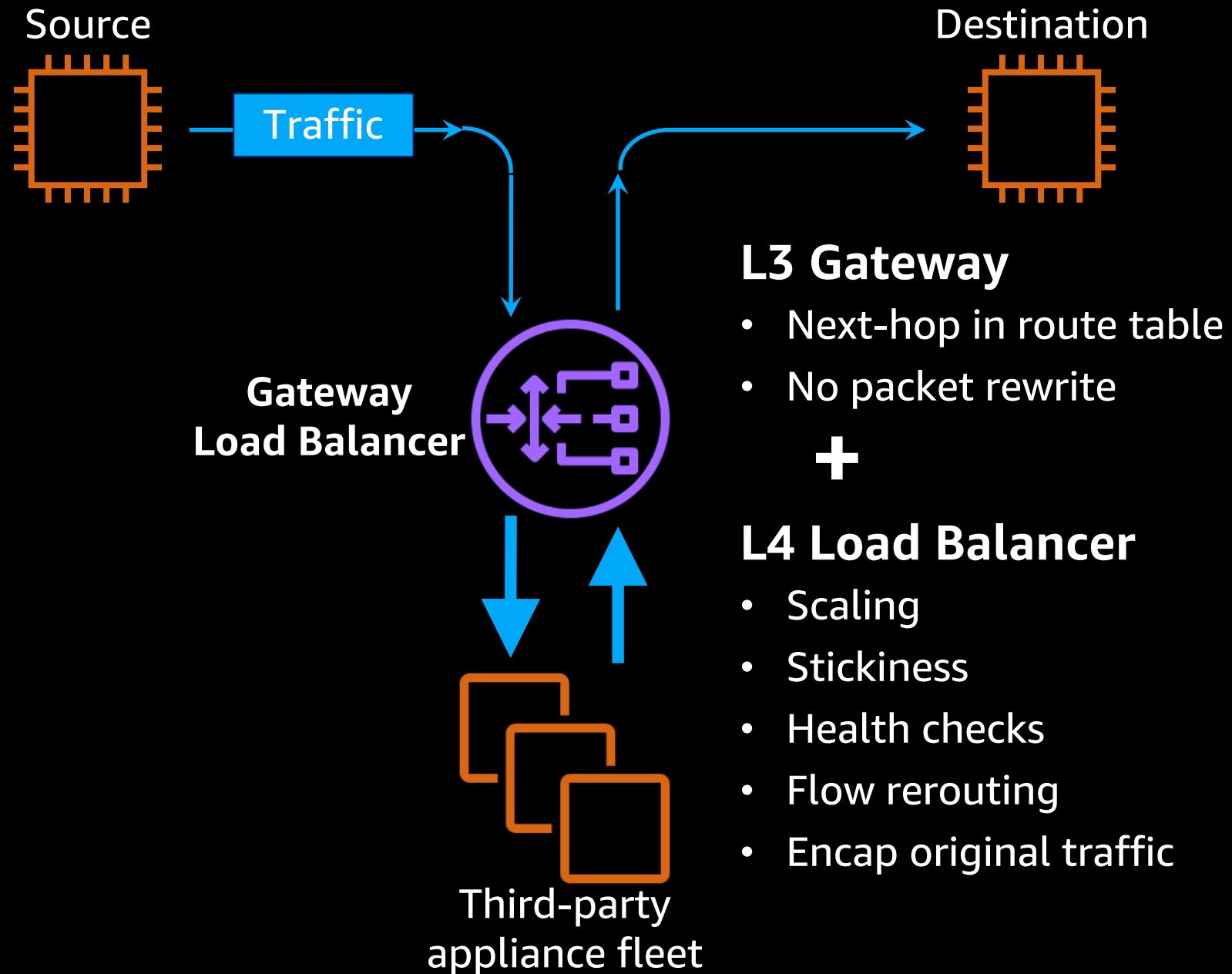
Challenges

1. Complex
2. Misconfig prone
3. Mixed admin domains
4. Expensive

Solution



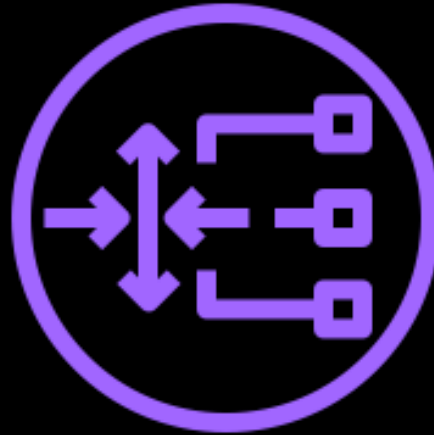
Now with Gateway Load Balancer



Architecture benefits

1. Scale
2. Reliability
3. Transparent insertion
4. As-a-Service
5. AWS native

Gateway Load Balancer (GWLB): TL;DR



- Using GWLB, customers can deploy and manage fleets of virtual appliances in elastic, fault-tolerant, and transparent manner
- GWLB service is available to customers and technology partners

Benefits for customers

1. Use existing third-party appliance skills
2. Leverage existing tools and practices
3. Simplify appliance deployments
4. Deploy appliances at elastic scale
5. Improve availability of appliances
6. Share appliances across VPCs and across accounts

Use cases



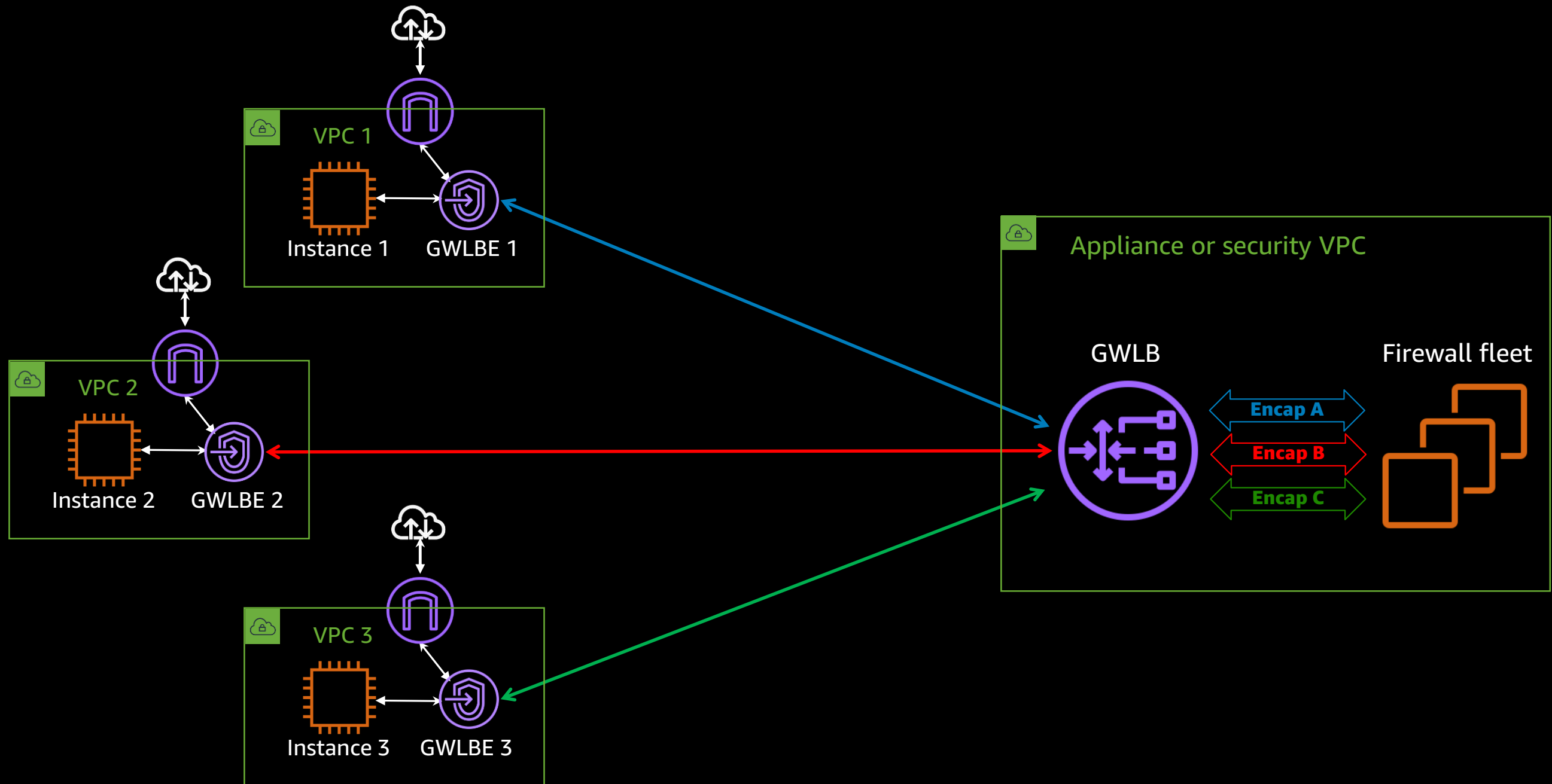
Customers' security use cases

1. N-S inspection (VPC to / from internet) using IGW
2. N-S inspection (VPC to / from internet) using TGW
3. Inter-VPC traffic inspection using TGW

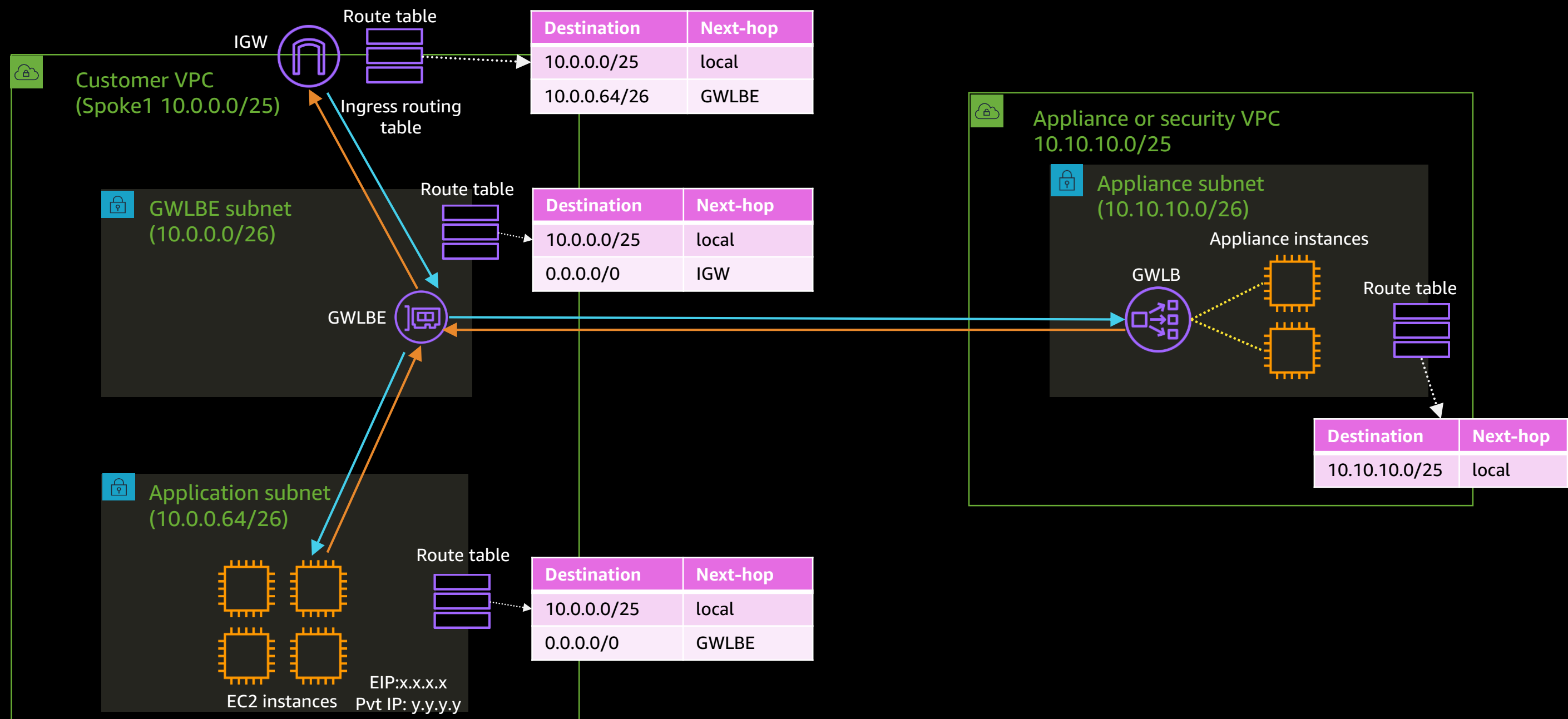
Customers' security use cases

1. N-S inspection (VPC to / from internet) using IGW
2. N-S inspection (VPC to / from internet) using TGW
3. Inter-VPC traffic inspection using TGW

Topology 1: N-S inspection with IGW



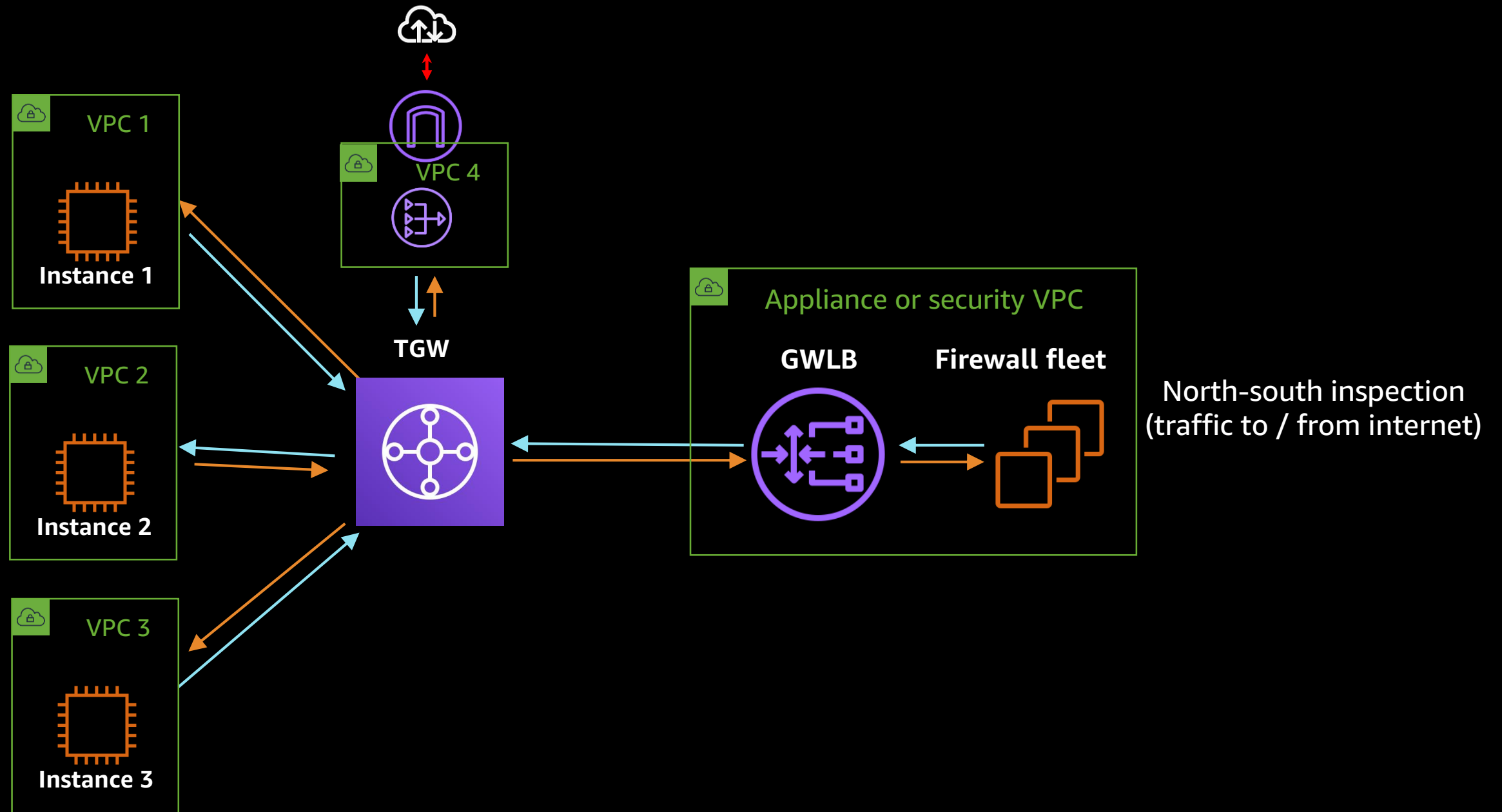
Details of topology 1: N-S inspection with IGW



Customers' security use cases

1. N-S inspection (VPC to / from internet) using IGW
2. N-S inspection (VPC to / from internet) using TGW
3. Inter-VPC traffic inspection using TGW

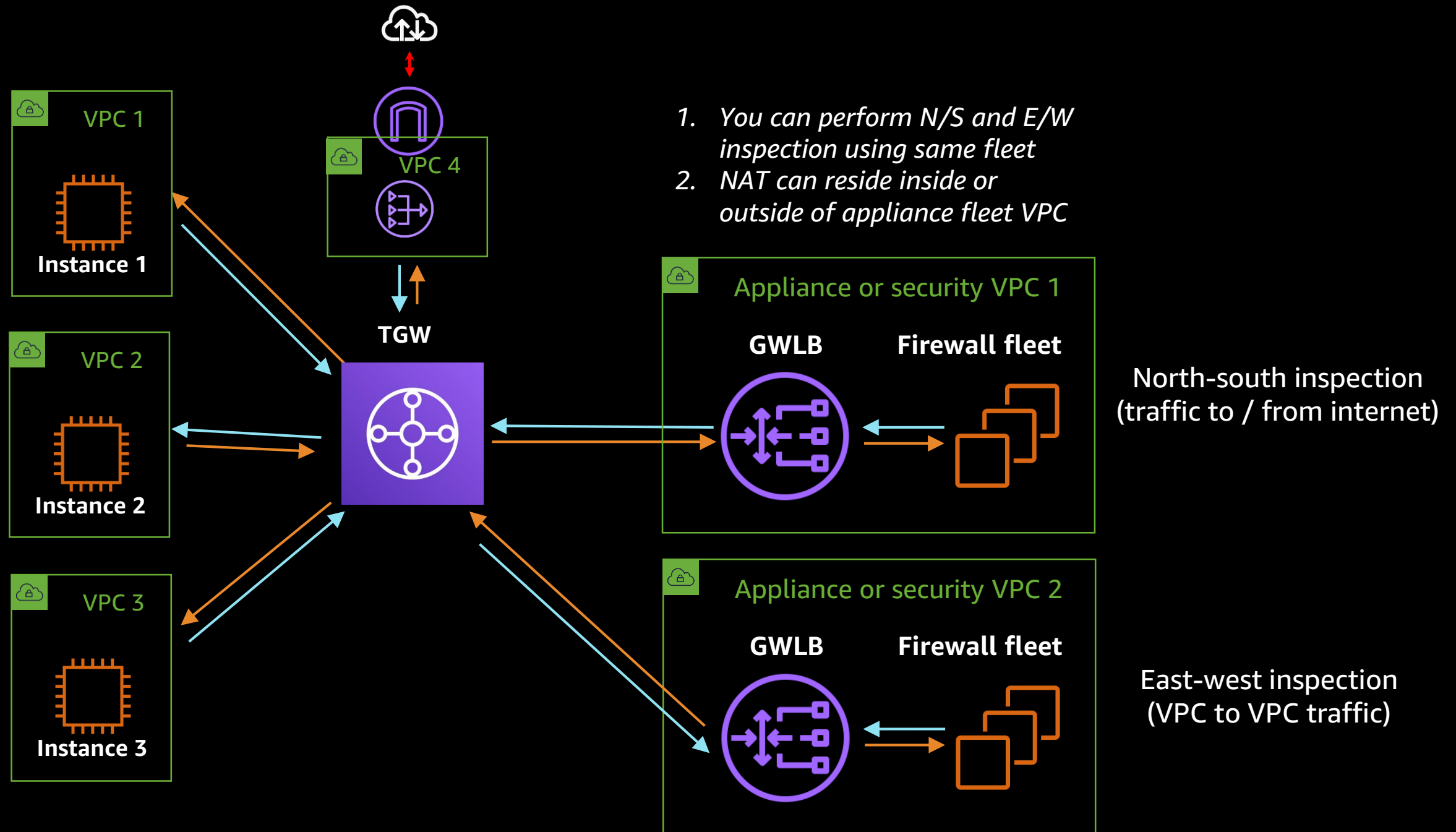
Topology 2: Security inspection with TGW



Customers' security use cases

1. N-S inspection (VPC to / from internet) using IGW
2. N-S inspection (VPC to / from internet) using TGW
3. Inter-VPC traffic inspection using TGW

Topology 3: Inter-VPC inspection with TGW



Partners integrated with GWLB



GWLB launch partners and providers

Advanced Security Partners:

Provide advanced security capabilities using GWLB



Analytics Partners and Providers:

Provide analytics capabilities using GWLB



Orchestration Partners:

Orchestrate networks that use GWLB



System Integration Partners:

Can implement architectures using GWLB

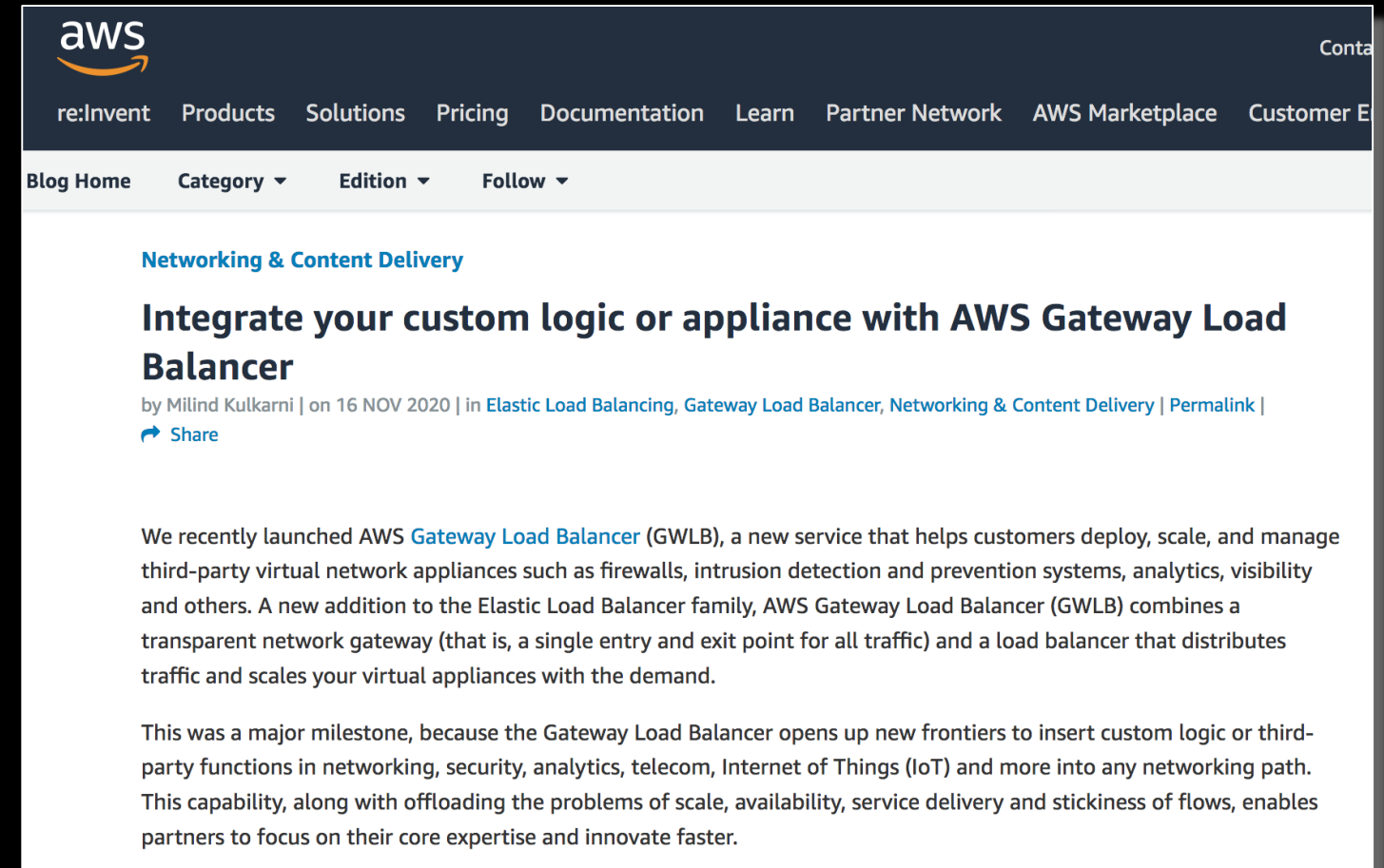


Benefits for AWS Partners

1. Get cloud-native elastic scale and availability
2. Simplify appliance deployments
3. Innovate faster by focusing on core expertise
4. Offer appliance as a managed service

What does GWLB integration require?

1. Support GENEVE protocol on the appliance
2. Encode/decode GENEVE options (aka TLVs)
3. Respond to health checks from GWLB

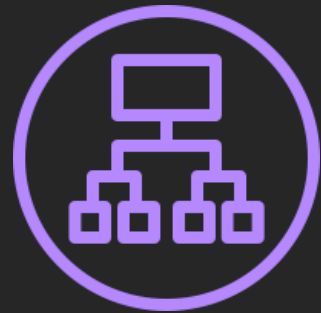


SCAN ME

Summary



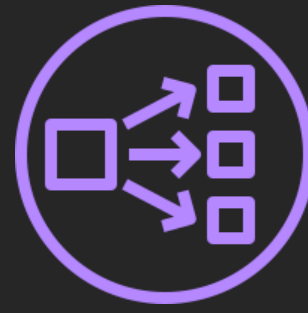
ELB portfolio



ALB

L7 Load Balancer

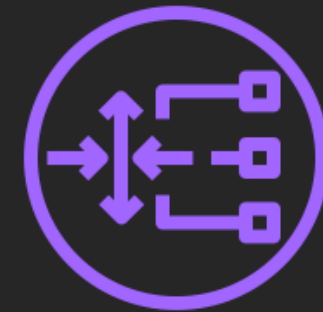
for HTTP, HTTPS traffic



NLB

L4 Load Balancer

for TCP, UDP, TLS traffic

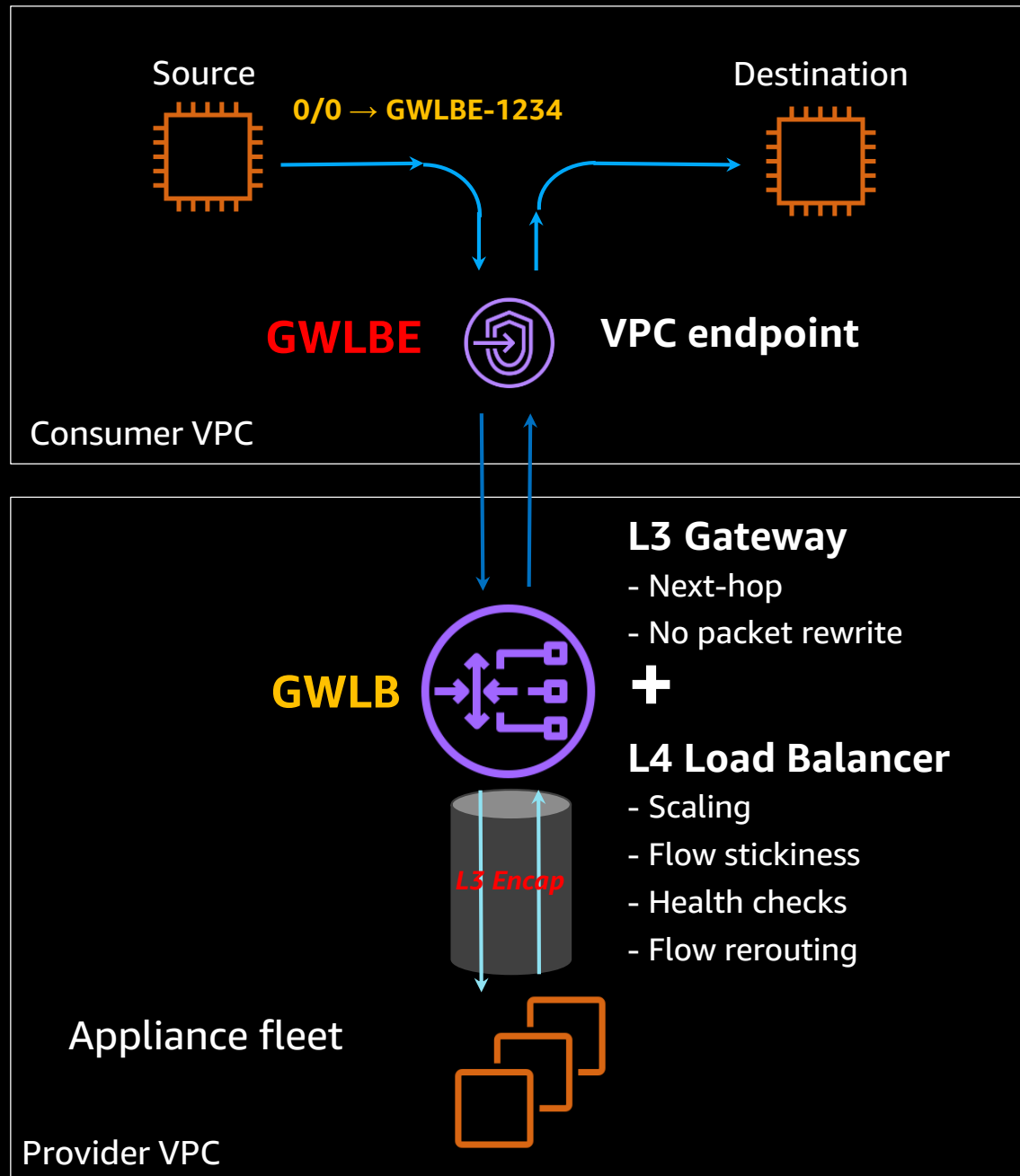


GWLB

L3 Load Balancer

for IP traffic and third-party appliances

GWLB / GWLBE at a glance



What is GWLB/GWLBE?

1. **GWLB** – Includes L3 Gateway + L4 Load Balancer capabilities
2. **GWLBE** – VPC endpoint that can be a next-hop in route table
3. Based on route table

Why use GWLB?

1. Provide horizontal scale to appliances
2. Provide fault tolerance to appliances
3. Insert services transparently
4. Share across different VPCs and accounts
5. Provide appliance-as-a-service

How to use GWLB

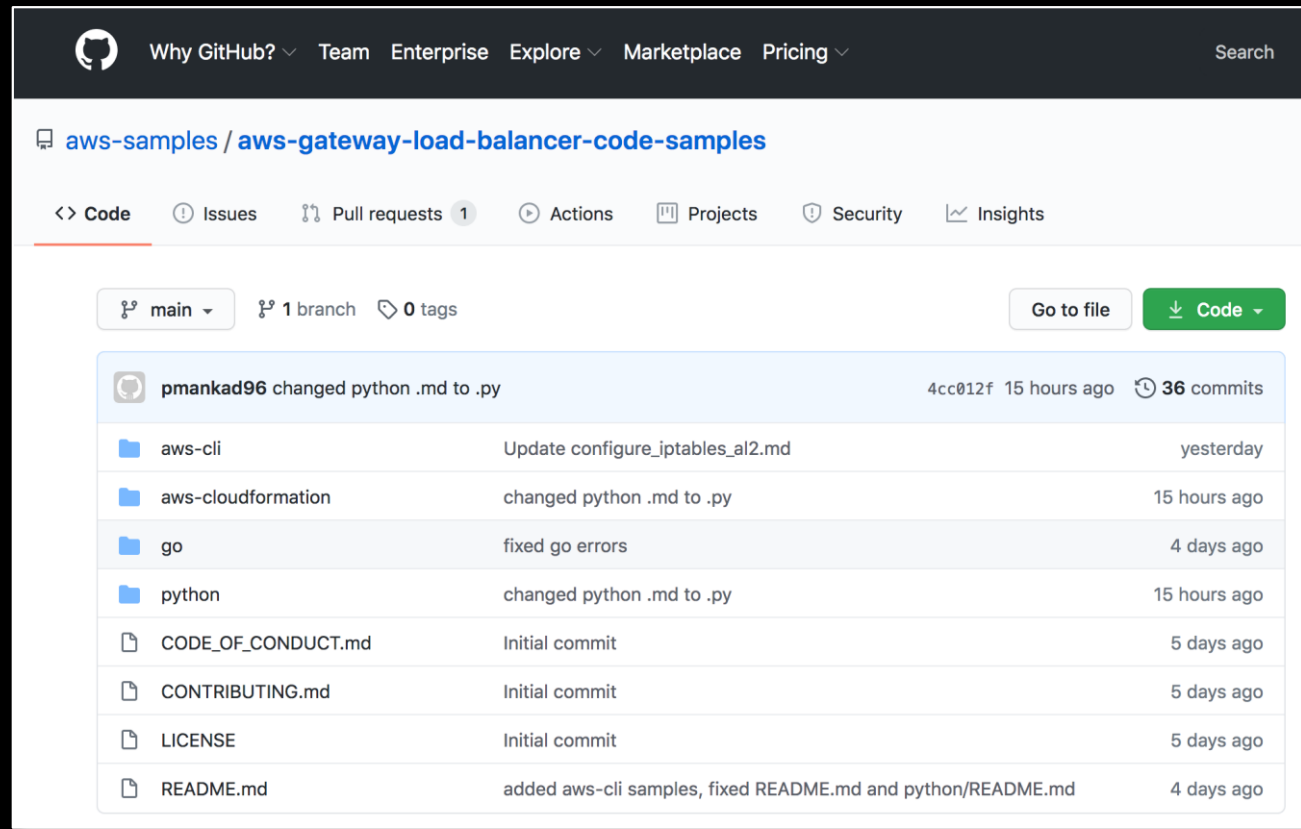
1. Create GWLB and appliance fleet using steps similar to ELB
2. Send traffic to GWLB/GWLBE by updating route table

Call to action



Code examples: Python, Go, CLI, AWS CloudFormation

Terraform

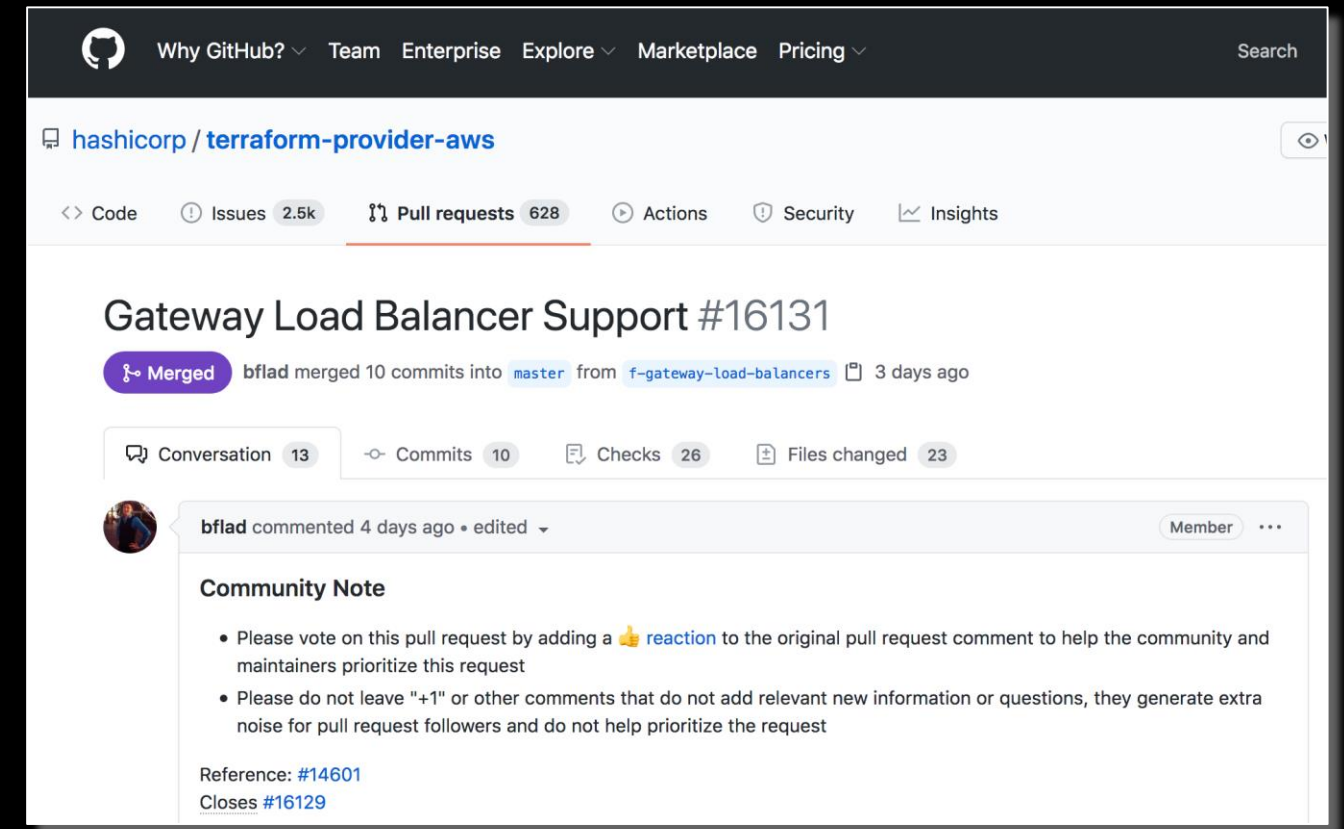


The screenshot shows the GitHub repository page for `aws-samples / aws-gateway-load-balancer-code-samples`. The repository is in the `main` branch and has 1 branch and 0 tags. The commit history shows a recent commit by `pmankad96` titled "changed python .md to .py" 15 hours ago. The repository contains several folders and files:

File/Folder	Commit Message	Time Ago
aws-cli	Update configure_iptables_al2.md	yesterday
aws-cloudformation	changed python .md to .py	15 hours ago
go	fixed go errors	4 days ago
python	changed python .md to .py	15 hours ago
CODE_OF_CONDUCT.md	Initial commit	5 days ago
CONTRIBUTING.md	Initial commit	5 days ago
LICENSE	Initial commit	5 days ago
README.md	added aws-cli samples, fixed README.md and python/README.md	4 days ago



SCAN ME

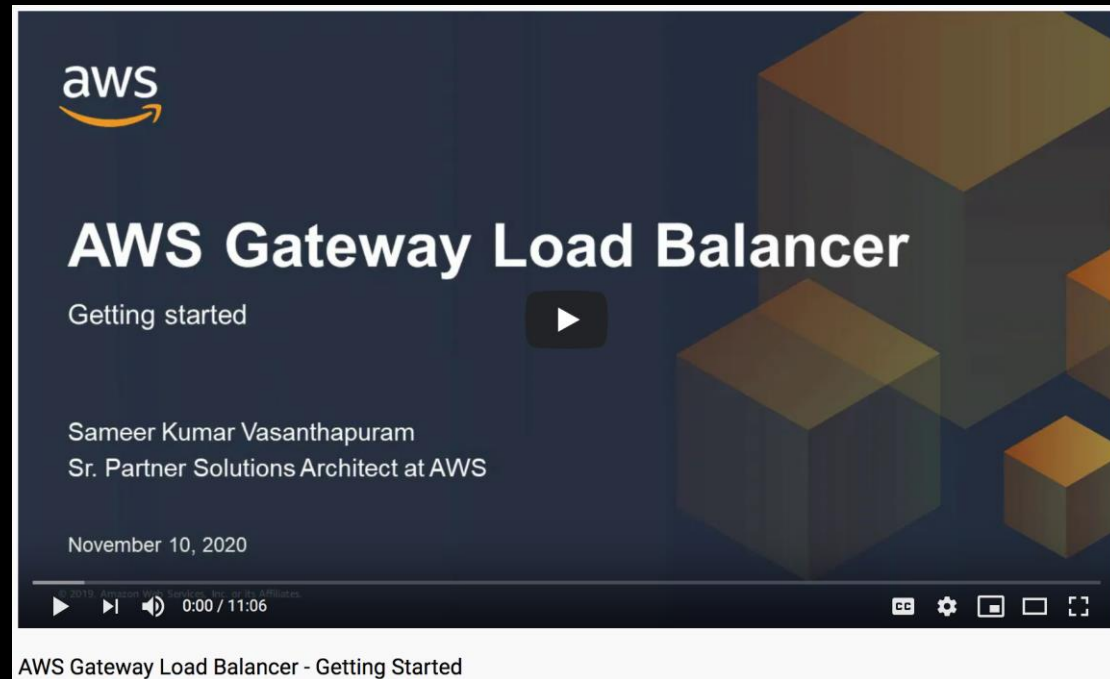


The screenshot shows the GitHub pull request page for `hashicorp / terraform-provider-aws`. The pull request is titled "Gateway Load Balancer Support #16131" and is in the `Merged` state. It was merged by `bflad` 3 days ago. The pull request has 13 conversations, 10 commits, 26 checks, and 23 files changed. A community note is displayed, asking users to vote on the pull request by adding a thumbs up reaction to the original pull request comment to help the community and maintainers prioritize this request. The note also mentions that users should not leave "+1" or other comments that do not add relevant new information or questions, as they generate extra noise for pull request followers and do not help prioritize the request. The note includes a reference to pull request #14601 and states that it closes pull request #16129.



SCAN ME

Start using GWLB in minutes



1. Locate partner's virtual appliance in AWS Marketplace
2. Launch appliance instances in your VPC
3. Create GWLB and target group with appliance instances
4. Create GWLBe where the traffic needs to be inspected
5. Update route table to send traffic to GWLBe



▶ SCAN ME

All AWS blogs related to GWLB



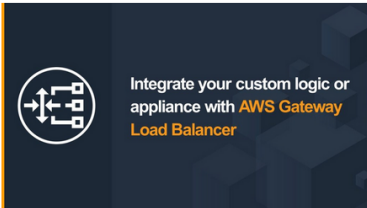
[Contact Sales](#) [Support](#) [My Account](#) [Create an AWS Account](#)

[re:Invent](#) [Products](#) [Solutions](#) [Pricing](#) [Documentation](#) [Learn](#) [Partner Network](#) [AWS Marketplace](#) [Customer Enablement](#) [Explore More](#) [Search](#)

[Blog Home](#) [Category](#) [Edition](#) [Follow](#)

[Networking & Content Delivery](#)

Category: Gateway Load Balancer



Integrate your custom logic or appliance with **AWS Gateway Load Balancer**

Integrate your custom logic or appliance with AWS Gateway Load Balancer

by Milind Kulkarni | on 16 NOV 2020 | in [Elastic Load Balancing](#), [Gateway Load Balancer](#), [Networking & Content Delivery](#) | [Permalink](#) | [Share](#)

We recently launched AWS Gateway Load Balancer (GWLB), a new service that helps customers deploy, scale, and manage third-party virtual network appliances such as firewalls, intrusion detection and prevention systems, analytics, visibility and others. A new addition to the Elastic Load Balancer family, AWS Gateway Load Balancer (GWLB) combines a transparent network gateway (that is, [...])

[Read More](#)



Scaling network traffic inspection using **AWS Gateway Load Balancer**

Scaling network traffic inspection using AWS Gateway Load Balancer

by Pratik R. Mankad and Sameer Kumar Vasanthapuram | on 11 NOV 2020 | in [AWS Marketplace](#), [Elastic Load Balancing](#), [Gateway Load Balancer](#), [Networking & Content Delivery](#), [Technical How-to](#) | [Permalink](#) | [Share](#)

Organizations use next-generation firewalls (NGFW) and intrusion prevention systems (IPS) as part of their defense in depth strategy. In an on-premises network, these often take the form of dedicated hardware or software or virtual “appliances.” As companies move to the cloud, they want to add virtual appliances to their AWS environments. While spinning up these [...]

[Read More](#)



Introduction to **AWS Gateway Load Balancer**: architectural patterns and

Introducing AWS Gateway Load Balancer: Supported architecture patterns

by Justin Davies | on 11 NOV 2020 | in [Announcements](#), [AWS Marketplace](#), [Elastic Load Balancing](#), [Gateway Load Balancer](#), [Networking & Content Delivery](#) | [Permalink](#) | [Share](#)

Customers often have to choose between different architectures to connect their on-premises applications to the cloud. The traditional approach is to use a VPN or a dedicated network connection. However, this approach has several limitations. For example, it is not scalable and it is not secure. AWS Gateway Load Balancer (GWLB) is a new service that helps customers deploy, scale, and manage third-party virtual network appliances such as firewalls, intrusion detection and prevention systems, analytics, visibility and others. A new addition to the Elastic Load Balancer family, AWS Gateway Load Balancer (GWLB) combines a transparent network gateway (that is, [...])



 SCAN ME

Gateway Load Balancer resources



[Product overview](#)



[Technical docs](#)



[Getting started video](#)



[GitHub code samples](#)



[All blogs on GWLB](#)

Watch these sessions

NET306: Which inspection architecture is right for you?

NET309: Advanced VPC design and new capabilities for Amazon VPC

Thank you!





Please complete
the session survey