
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

NET320

Building your own cloud services using ELB Gateway Load Balancer

Milind Kulkarni (he/him)

Sr. Product Manager, EC2 Load Balancing
AWS

Andrew Gray (he/him)

Principal Solutions Architect, Network Specialist
AWS

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

About this session

- This is an interactive chalk-talk, not a presentation
- Please ask questions

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

GWLB & GWLBE: Quick primer

What is GWLB/GWLBE?

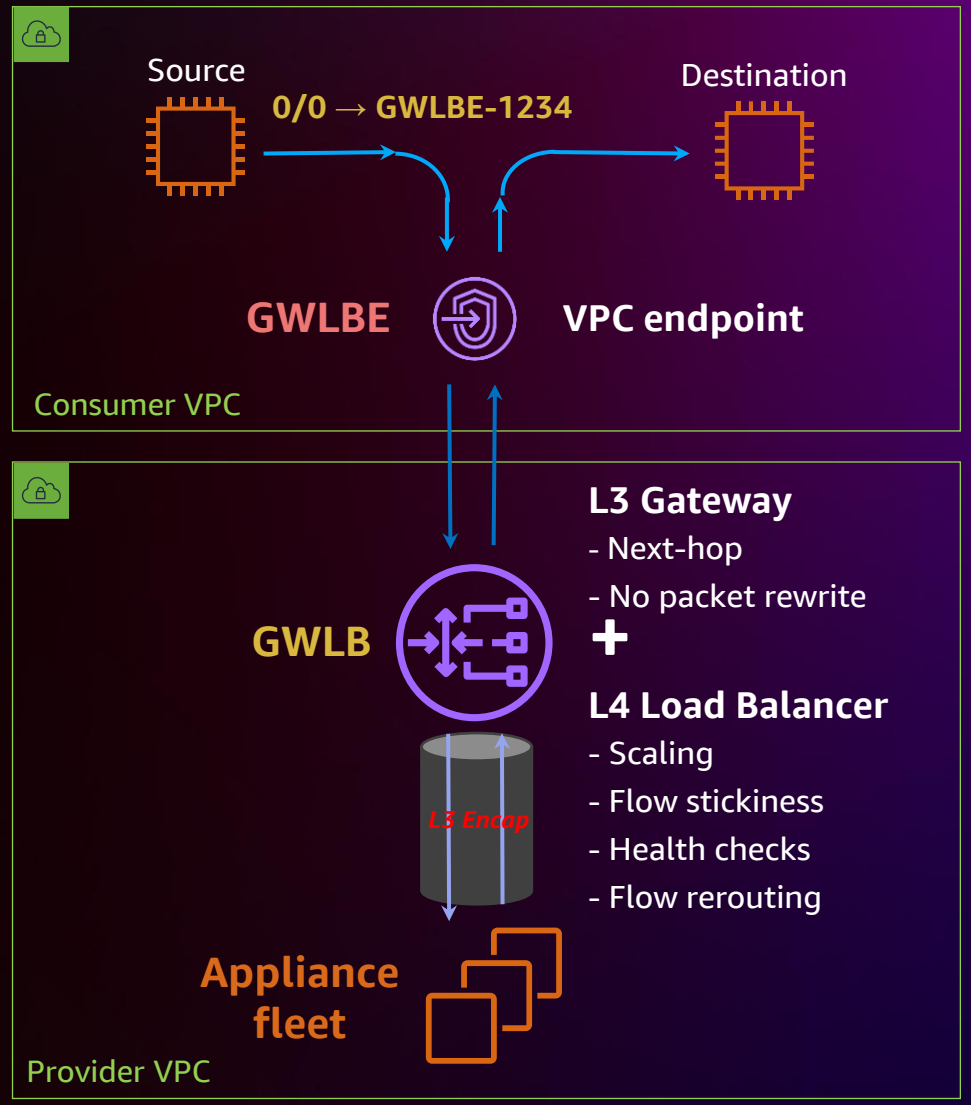
1. **GWLB** – LB that has L3 Gateway and L4 Load Balancer capabilities
2. **GWLBE** – VPC endpoint that can be a next-hop in route table
3. Insert transparently by adding GWLBE in route table

What are the benefits of GWLB?

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

How to use GWLB?

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



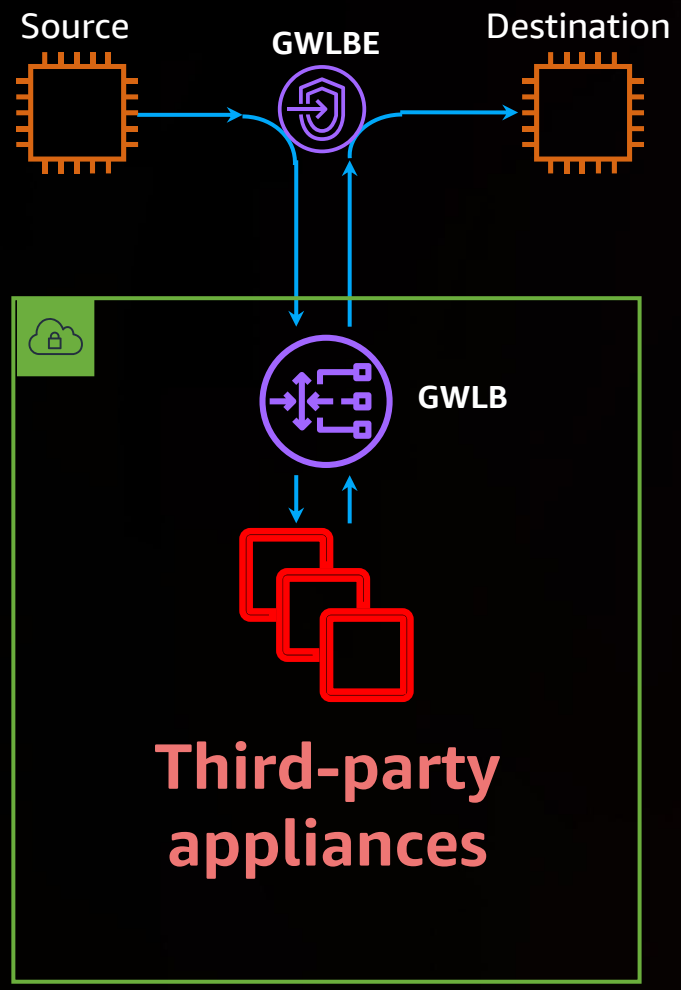
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

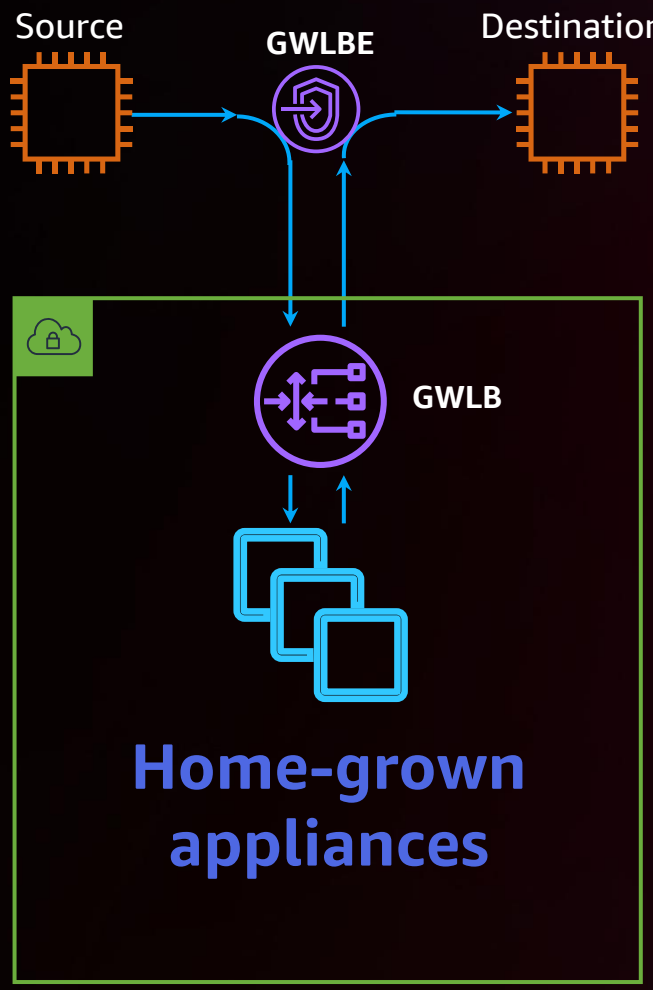
Typical GWLB use cases

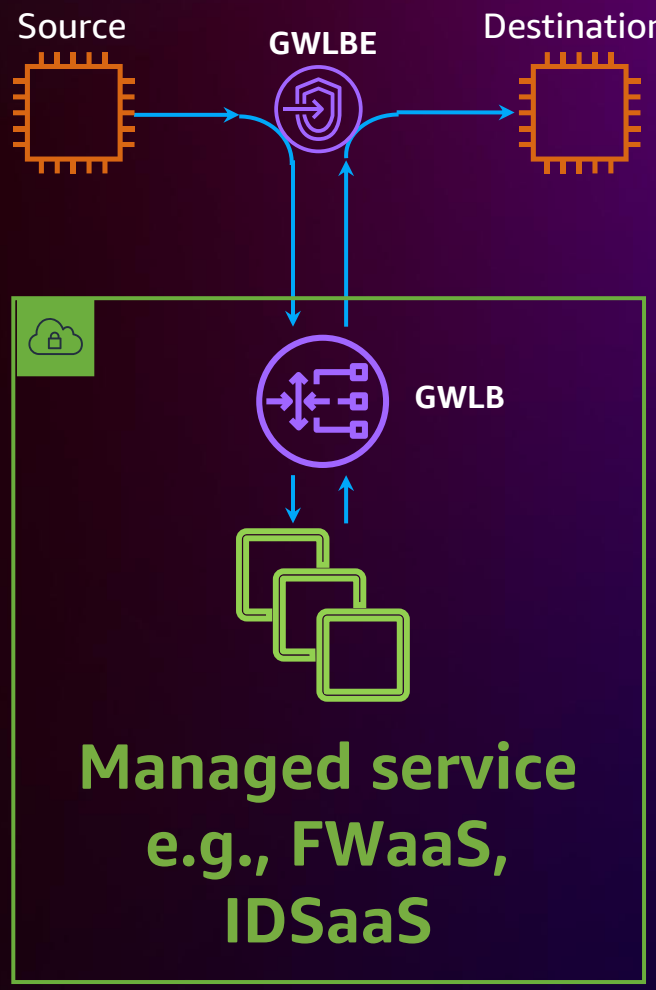
- Security inspection and blocking of undesired traffic (IDS/IPS/Firewall)
- Detailed traffic capture and monitoring
- Network impairment testing

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Common deployment scenarios

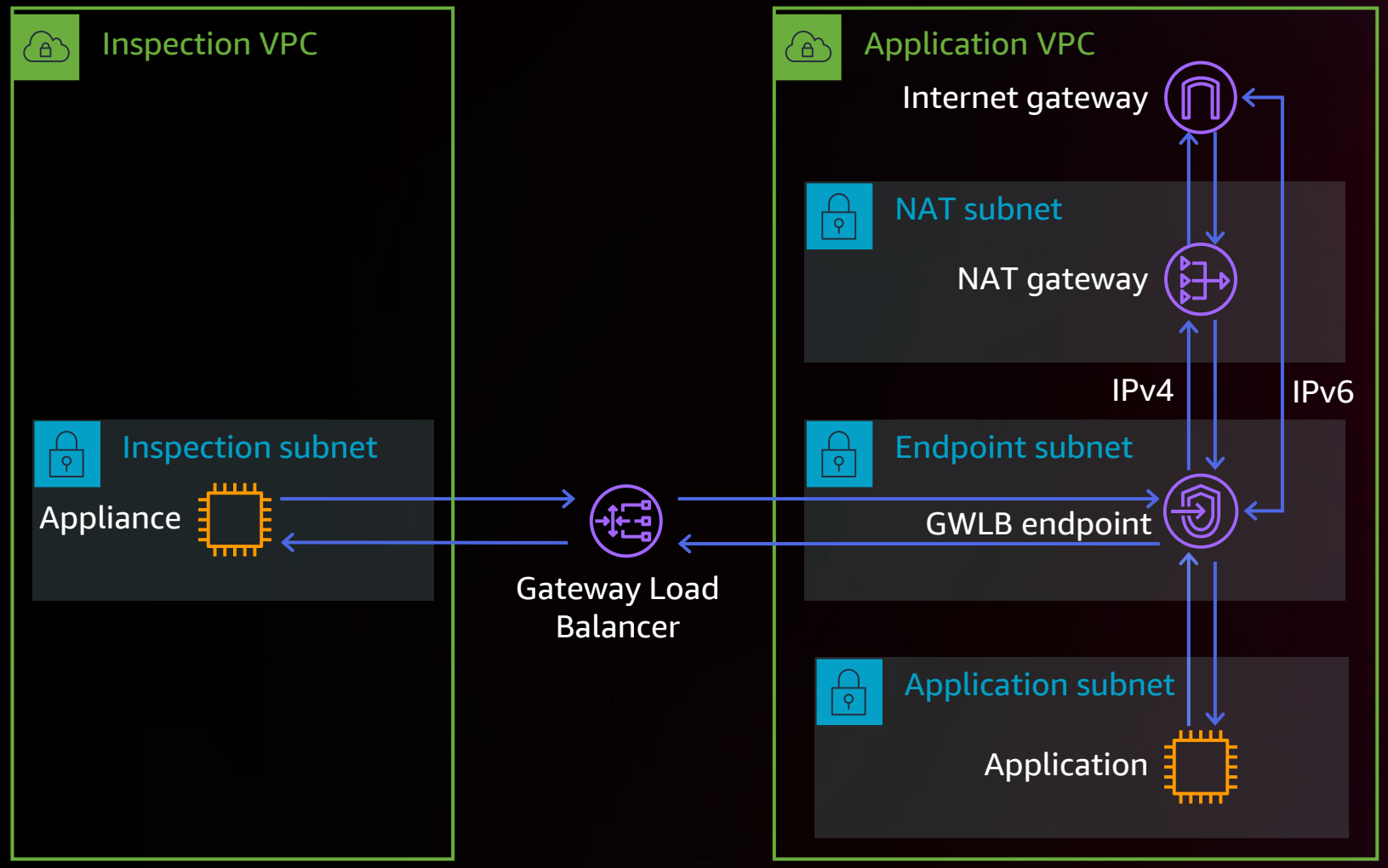






aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example topology: GWLB in one-arm mode



Prefix	Destination
Application subnet's IPv6	GWLB endpoint

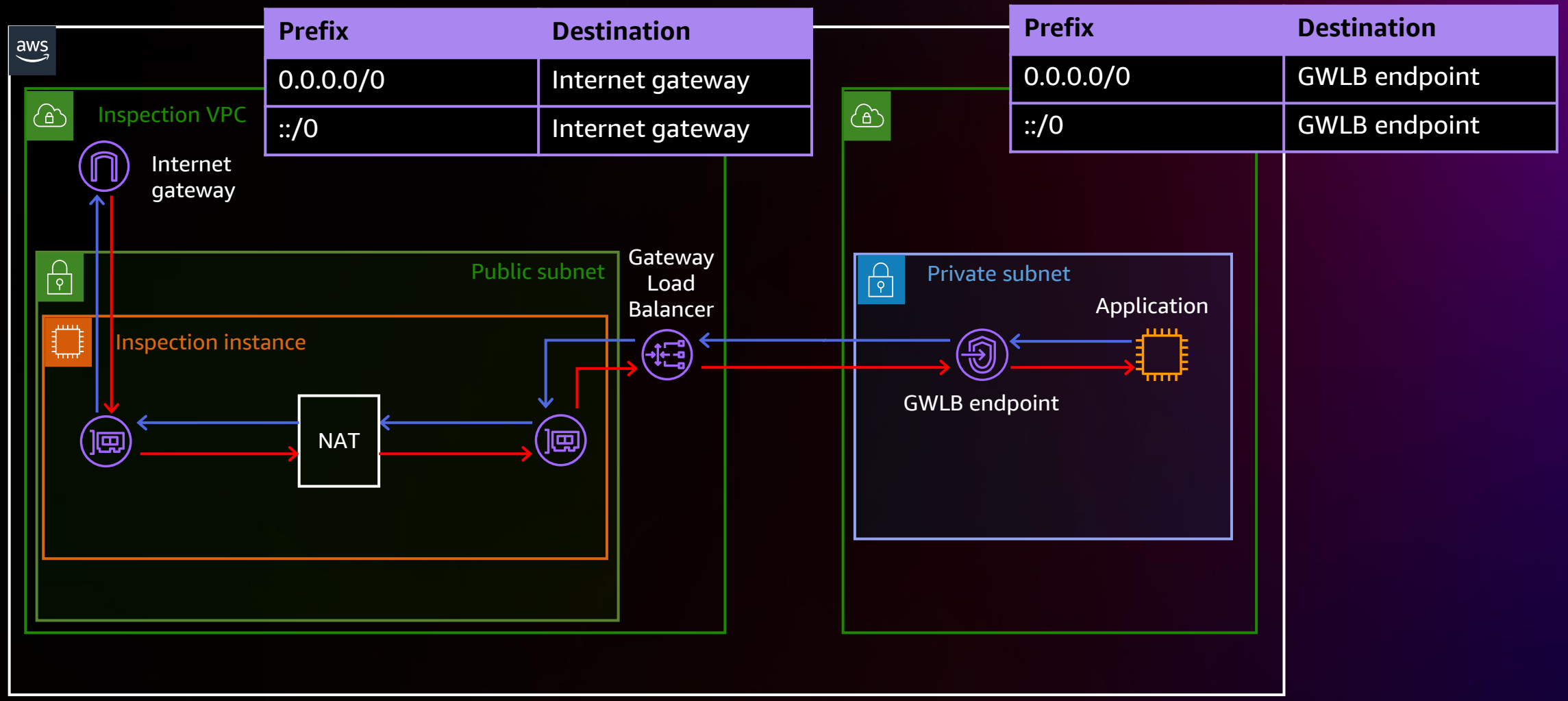
Prefix	Destination
0.0.0.0/0	Internet gateway
Application subnet	GWLB endpoint

Prefix	Destination
0.0.0.0/0	NAT gateway
::/0	Internet gateway
Local	Local

Prefix	Destination
0.0.0.0/0	GWLB endpoint
::/0	GWLB endpoint

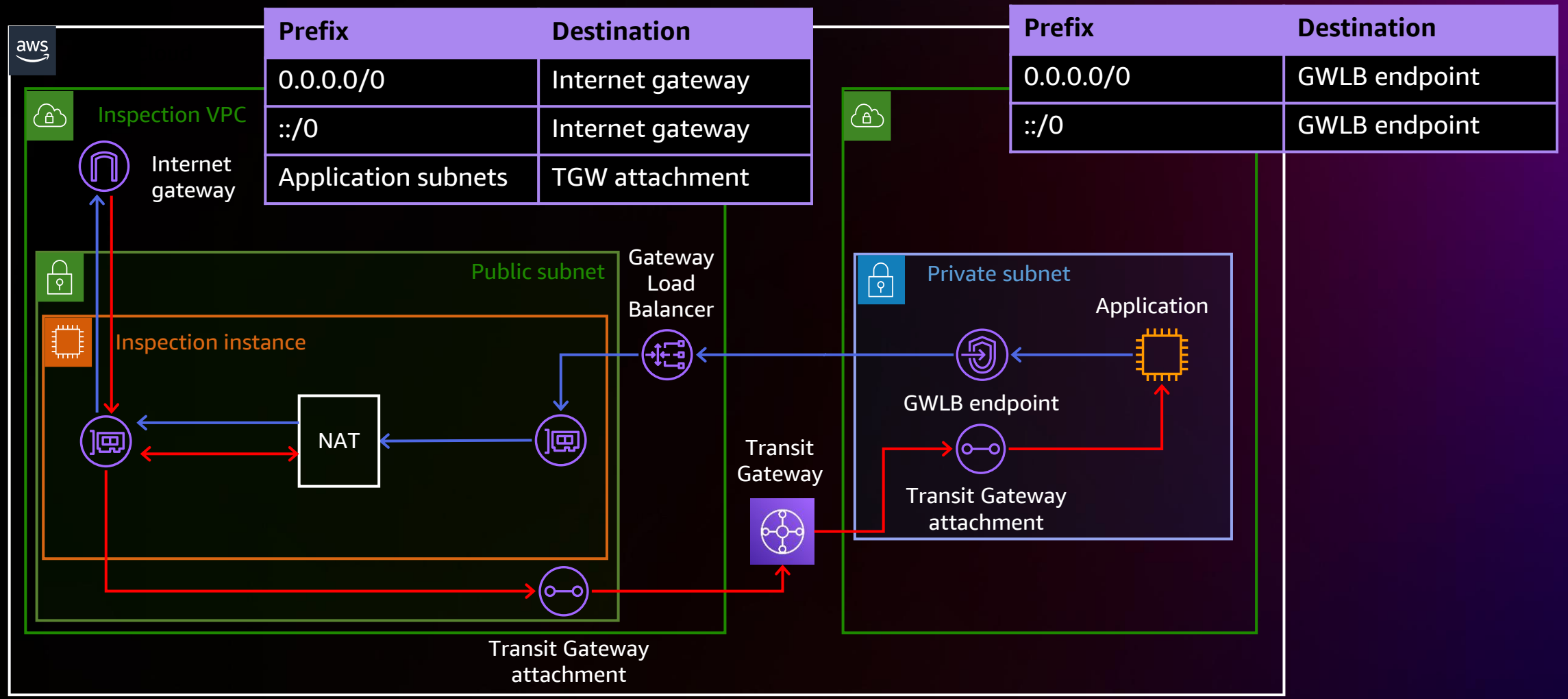
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example topology: GWLB in two-arm mode



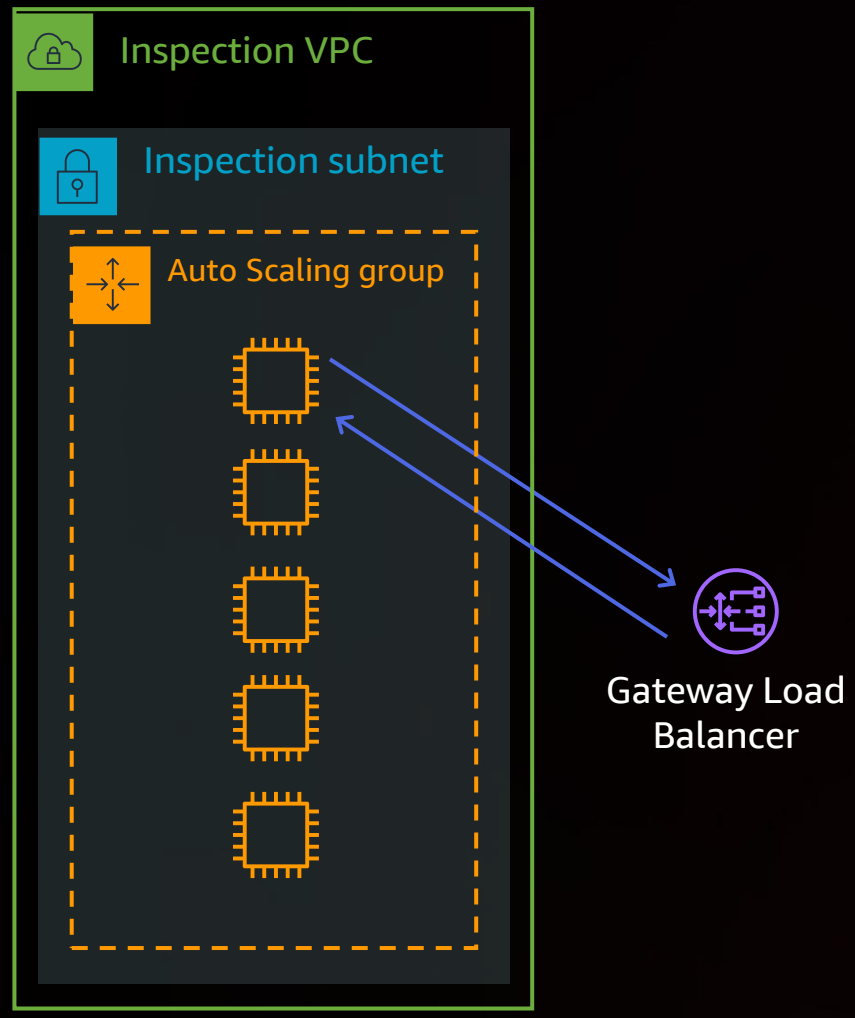
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example topology: GWLB in two-arm with TGW



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Reference: Auto-Scaling Groups with GWLB



When the target group attributes target_failover.on_deregistration and target_failover.on_unhealthy are

`no_rebalance`	The Gateway Load Balancer continues to send existing flows to failed or drained targets, however new flows are sent to healthy targets – this is the default behavior
`rebalance`	The Gateway Load Balancer rehashes existing flows and sends them to healthy targets after the deregistration delay timeout

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Reference: GENEVE encapsulation diagram

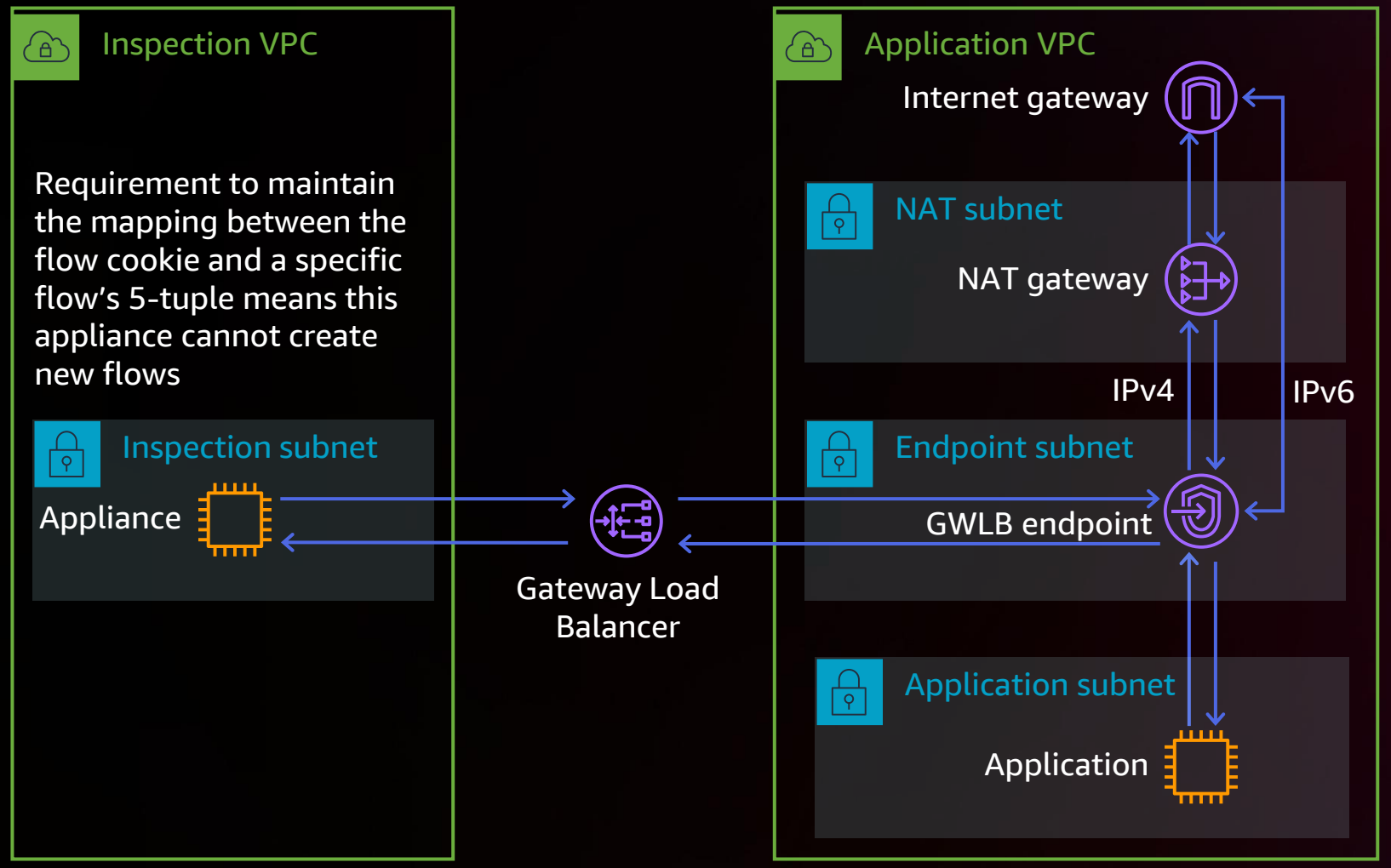
Outer IPv4 header (applied by GWLB to send the traffic to our appliance)	Standard IPv4 header bytes (version, length, and so on)
	Source IP address (the GWLB itself)
	Destination IP address (our instance)
Outer UDP header (applied by GWLB to send the traffic to our appliance)	Source port (randomly assigned by GWLB)
	Destination port (always 6081 for GENEVE)
	UDP length and checksum
GENEVE header (applied by GWLB to send the traffic to our appliance)	GENEVE header bytes (version, type, and so forth)
	VNI ID
	GENEVE options
Original IPv4 or IPv6 encapsulated packet	Original IP header
	Original ICMP header
	Original payload

```
Options: (32 bytes)
    Unknown, Class: Amazon.com, Inc. (0x0108) Type: 0x01
        Class: Amazon.com, Inc. (0x0108)
        Type: 0x01 (GWLBe ENI ID)
        Length: 12 bytes
        Option Data: 754a0cd0ba2fe61b
    Unknown, Class: Amazon.com, Inc. (0x0108) Type: 0x02
        Class: Amazon.com, Inc. (0x0108)
        Type: 0x02 (Attachment ID)
        Length: 12 bytes
        Option Data: 0000000000000000
    Unknown, Class: Amazon.com, Inc. (0x0108) Type: 0x03
        Class: Amazon.com, Inc. (0x0108)
        Type: 0x03 (Flow Cookie)
        Length: 8 bytes
        Option Data: f23f2356
```

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Reference: Implications of GWLB Flow Cookie



Prefix	Destination
Application subnet's IPv6	GWLB endpoint

Prefix	Destination
0.0.0.0/0	Internet gateway
Application subnet	GWLB endpoint

Prefix	Destination
0.0.0.0/0	NAT gateway
::/0	Internet gateway
Local	Local

Prefix	Destination
0.0.0.0/0	GWLB endpoint
::/0	GWLB endpoint

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Milind Kulkarni
milindku@amazon.com
linkedin.com/in/milindmkulkarni

Andrew Gray
grayaw@amazon.com
linkedin.com/in/grayaw

https://aws.amazon.com/elasticloadbalancing/gateway-load-balancer/



Please complete the session survey in the **mobile app**

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.