aws

Architecture Diagrams

Distributed Inspection Architectures with Gateway Load Balancer

Distributed Inspection Architectures with Gateway Load Balancer: Architecture Diagrams

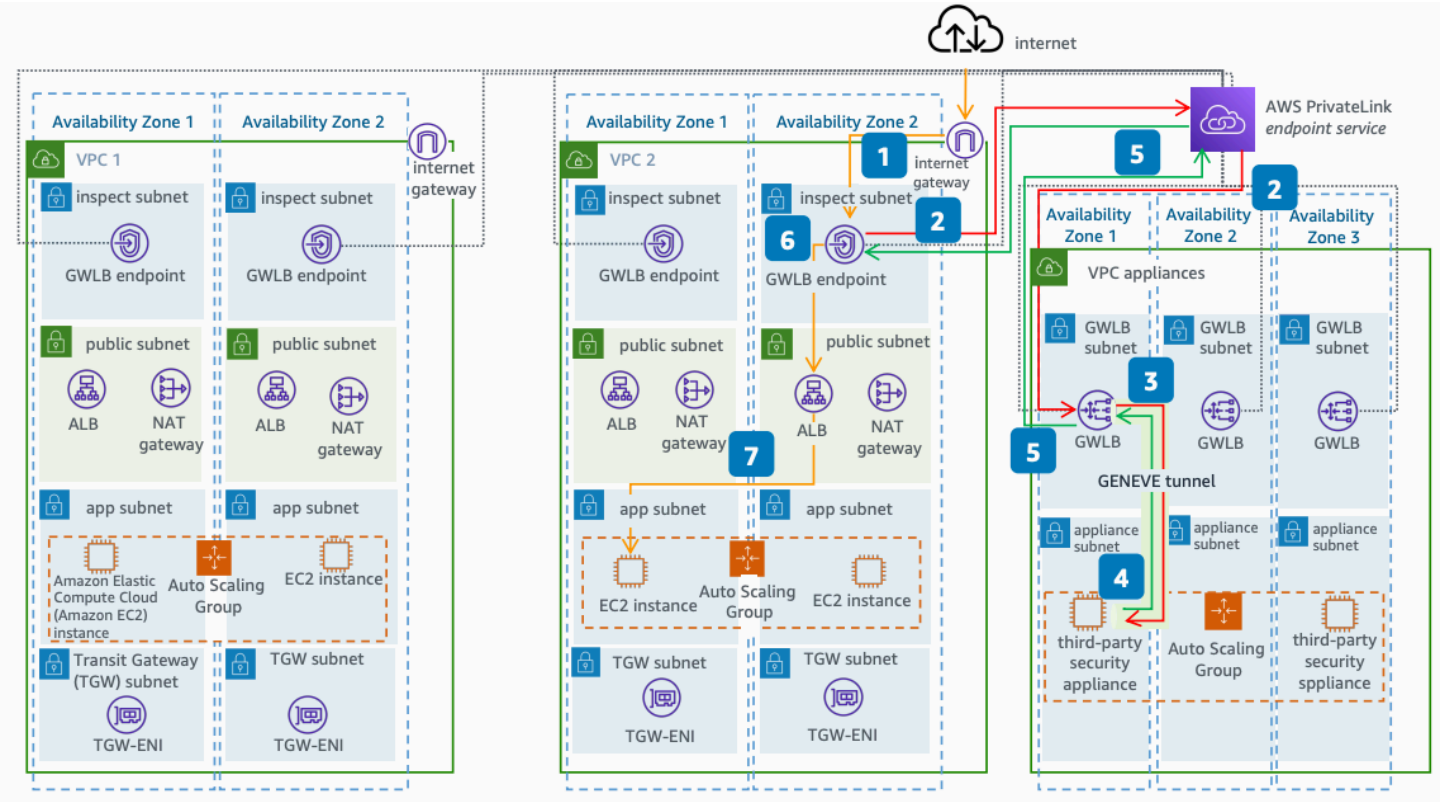
Table of Contents

North/South Inbound Distributed Inspection

Publication date: **July 21, 2022 (Diagram history)**

This architecture uses Gateway Load Balancer to inspect inbound traffic in a distributed fashion. Multiple VPCs share the same backend security appliances in a centralized appliances VPC connected through AWS PrivateLink.

North/South inbound distributed inspection architecture



The following steps describe the data flow in this architecture:

1. Traffic from the internet destined for the Application Load Balancer arrives at the internet gateway. The **ingress route table** forwards it to a Gateway Load Balancer endpoint.
2. The Gateway Load Balancer endpoint forwards the traffic to Gateway Load Balancer in the **appliances VPC** using AWS PrivateLink.
3. Gateway Load Balancer encapsulates the traffic in Generic Network Virtualization Encapsulation (GENEVE) and sends it to a security appliance for inspection.
4. The security appliance inspects the traffic and returns it to Gateway Load Balancer.

5. The traffic returns to the Gateway Load Balancer endpoint in the **inspect subnet**.
6. The Gateway Load Balancer endpoint uses the **inspect subnet route table** to forward the traffic to the Application Load Balancer in the **public subnet**.
7. The Application Load Balancer forwards the traffic to one of its healthy Amazon EC2 instances.

For best practices when deploying Gateway Load Balancer, see Best practices for deploying Gateway Load Balancer.

For more information about implementing a distributed inspection architecture, see Scaling network traffic inspection using AWS Gateway Load Balancer.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	July 21, 2022
Initial publication	Reference architecture diagram first published.	July 21, 2022
Initial publication	Reference architecture diagram first published.	July 21, 2022
Initial publication	Reference architecture diagram first published.	July 21, 2022

Note

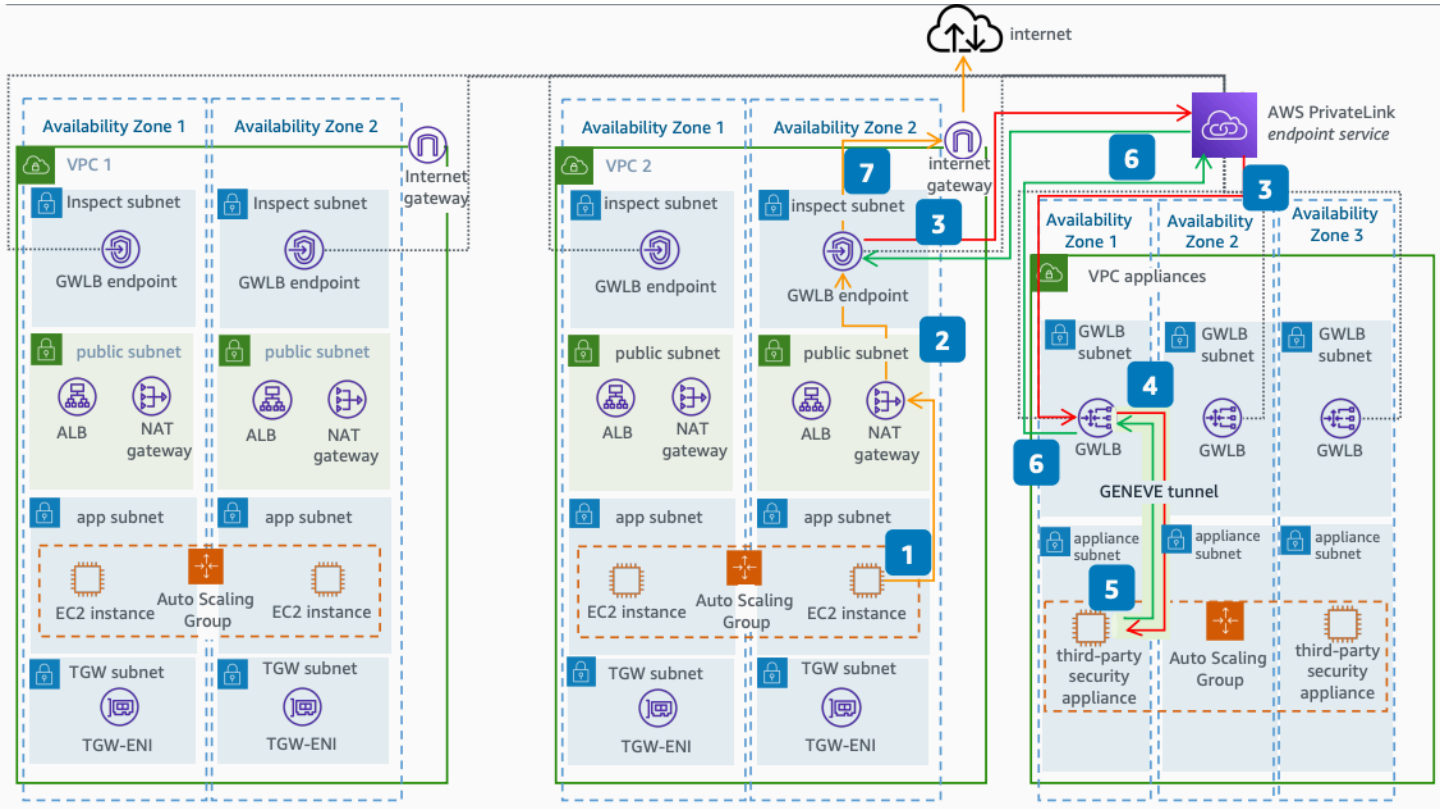
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

North/South Outbound Distributed Inspection

Publication date: **July 21, 2022 (Diagram history)**

This architecture uses Gateway Load Balancer to inspect outbound traffic in a distributed fashion. Multiple VPCs share the same backend security appliances through AWS PrivateLink for traffic destined to the internet.

North/South outbound distributed inspection architecture



The following steps describe the data flow in this architecture:

1. Traffic from an Amazon EC2 instance destined for the internet arrives at NAT Gateway, which translates the source IP of the packets.
2. NAT Gateway forwards the translated packets to a Gateway Load Balancer endpoint using the **public subnet route table**.
3. The Gateway Load Balancer endpoint forwards the traffic to Gateway Load Balancer in the **appliances VPC** using AWS PrivateLink.

4. Gateway Load Balancer encapsulates the traffic in GENEVE and sends it to a security appliance for inspection.
5. The security appliance inspects the traffic and returns it to Gateway Load Balancer.
6. The traffic returns to the Gateway Load Balancer endpoint in the **inspect subnet**.
7. The Gateway Load Balancer endpoint uses the **inspect subnet route table** to forward the traffic to the internet gateway.

For best practices when deploying Gateway Load Balancer, see Best practices for deploying Gateway Load Balancer.

For more information about implementing a distributed inspection architecture, see Scaling network traffic inspection using AWS Gateway Load Balancer.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	July 21, 2022
Initial publication	Reference architecture diagram first published.	July 21, 2022
Initial publication	Reference architecture diagram first published.	July 21, 2022

Initial publication	Reference architecture diagram first published.	July 21, 2022

Note

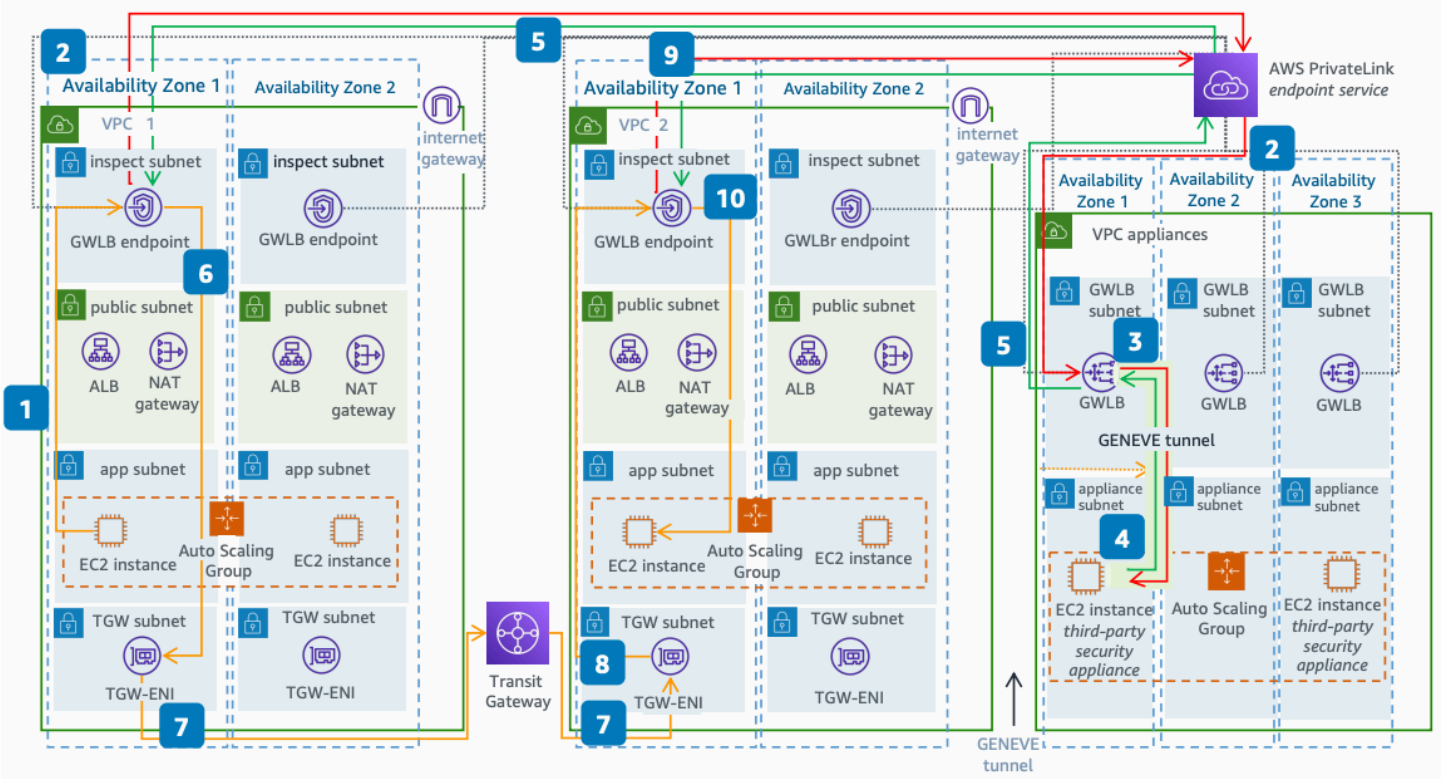
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

East/West Distributed Inspection

Publication date: **July 21, 2022 (Diagram history)**

This architecture uses Gateway Load Balancer for distributed East/West inspection between VPCs. Traffic between VPCs routes through Gateway Load Balancer endpoints for inspection in both the source and destination VPCs.

East/West distributed inspection architecture



The following steps describe the data flow in this architecture:

1. Traffic from an Amazon EC2 instance in **VPC 1** destined for an instance in **VPC 2** forwards to a Gateway Load Balancer endpoint.
2. The Gateway Load Balancer endpoint forwards the traffic to Gateway Load Balancer in the **appliances VPC** using AWS PrivateLink.
3. Gateway Load Balancer encapsulates the traffic in GENEVE and sends it to a security appliance for inspection.
4. The security appliance inspects the traffic and returns it to Gateway Load Balancer.

5. The traffic returns to the Gateway Load Balancer endpoint in the **inspect subnet**.
6. The Gateway Load Balancer endpoint uses the **inspect subnet route table** to forward the traffic to the Transit Gateway endpoint in the **TGW subnet**.
7. The traffic forwards according to the Transit Gateway route table and arrives in **VPC 2**.
8. In **VPC 2**, traffic forwards to the Gateway Load Balancer endpoint for re-inspection.
9. The traffic is re-inspected following the same flow through Gateway Load Balancer and the security appliance.
10. The Gateway Load Balancer endpoint forwards the traffic to the destination instance in the app subnet.

Use Transit Gateway appliance mode in the **Inspection VPC** Transit Gateway attachment to maintain flow symmetry.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	July 21, 2022
Initial publication	Reference architecture diagram first published.	July 21, 2022
Initial publication	Reference architecture diagram first published.	July 21, 2022

Initial publication	Reference architecture diagram first published.	July 21, 2022

Note

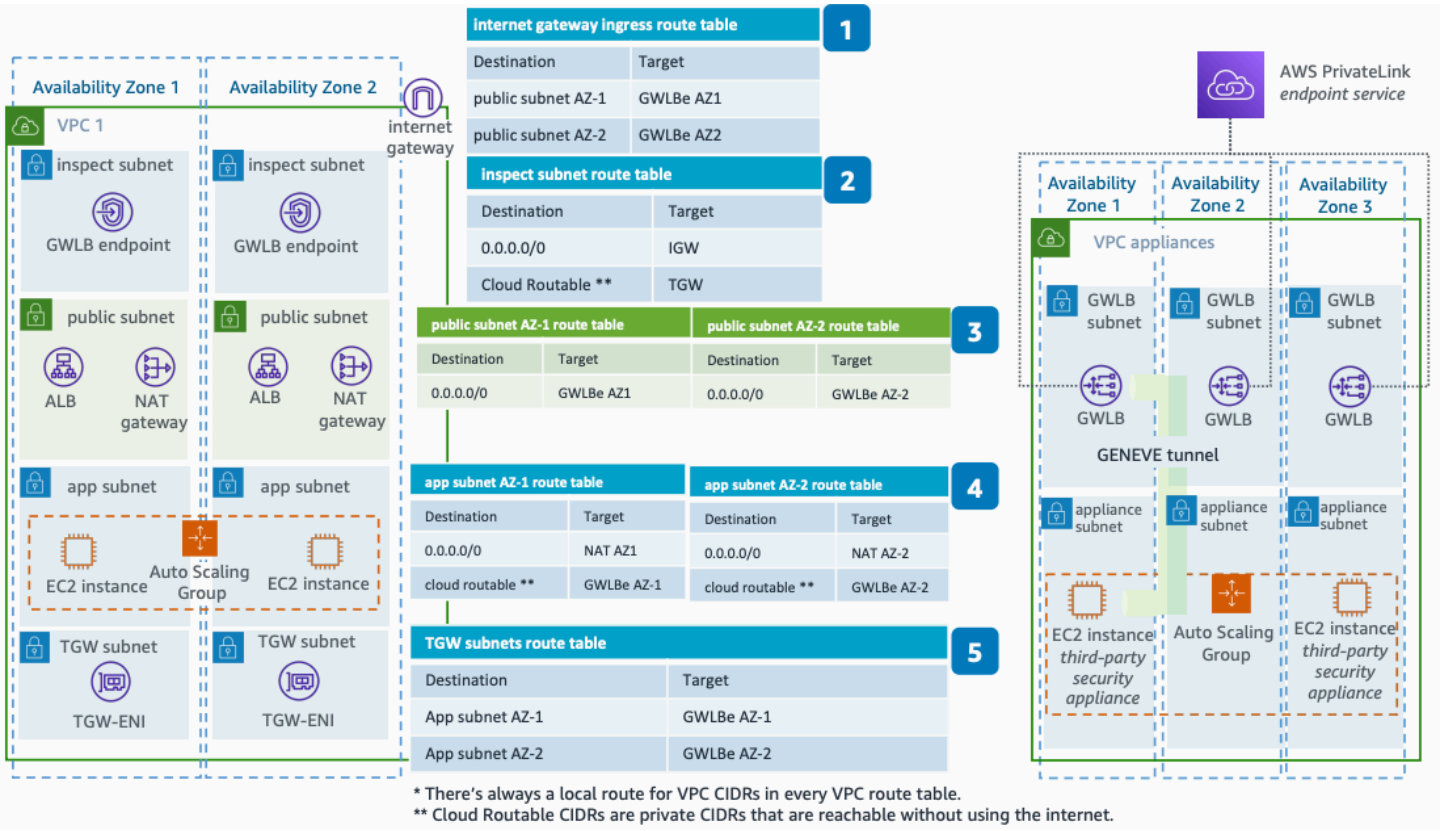
To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.

Distributed Inspection Route Tables

Publication date: **July 21, 2022 (Diagram history)**

This diagram shows the route table configuration for distributed inspection architectures using Gateway Load Balancer in multiple Availability Zones. Proper route table configuration maintains flow symmetry across all traffic patterns.

Distributed inspection route tables architecture



The following route tables control traffic flow in this architecture:

1. The **internet gateway ingress route table** applies to traffic from the internet to public subnets. It forwards traffic to the Gateway Load Balancer endpoint in the destination Availability Zone to maintain flow symmetry.
2. The **inspect subnet route table** applies to already-inspected traffic. This table defines which traffic routes to the internet and which routes to AWS Transit Gateway.
3. The **public subnet route tables** forward all traffic to the Gateway Load Balancer endpoints in the source Availability Zone.

4. The **application subnet route tables** forward traffic differently based on whether the destination IP is public or private. All traffic forwards to Gateway Load Balancer endpoints in the same Availability Zone to maintain symmetry.
5. The **Transit Gateway subnet route table** applies to traffic from AWS Transit Gateway. It sends traffic to the Gateway Load Balancer endpoint in the destination Availability Zone to maintain symmetry.

For more information about implementing a distributed inspection architecture, see Scaling network traffic inspection using AWS Gateway Load Balancer.

Further reading

For additional information, see the following resources:

- AWS Architecture Icons
- AWS Architecture Center
- AWS Well-Architected

Diagram history

To be notified about updates to this reference architecture diagram, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Reference architecture diagram first published.	July 21, 2022
Initial publication	Reference architecture diagram first published.	July 21, 2022
Initial publication	Reference architecture diagram first published.	July 21, 2022
Initial publication	Reference architecture diagram first published.	July 21, 2022

Note

To subscribe to RSS updates, you must have an RSS plugin enabled for the browser you are using.