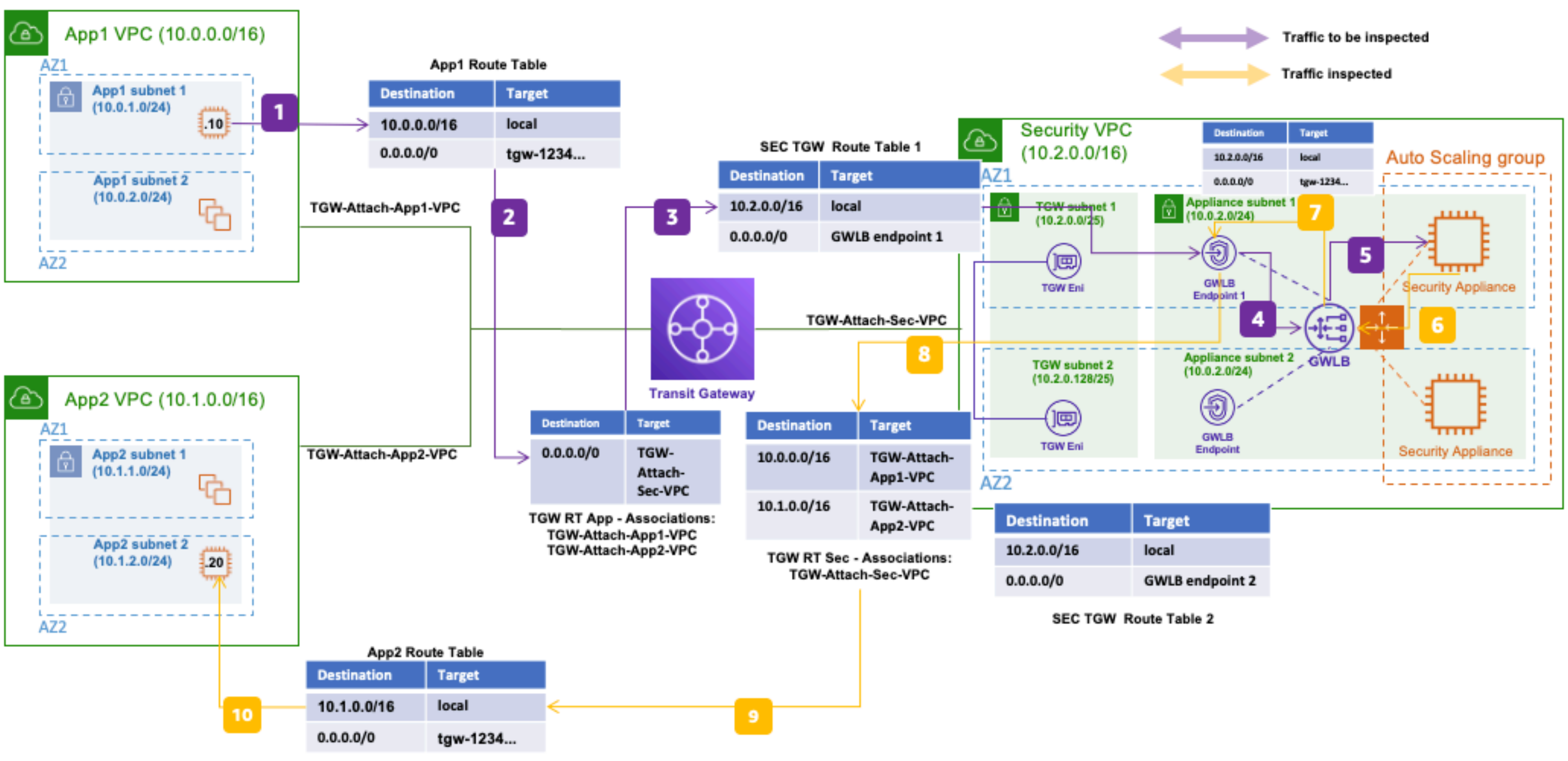
Architecture for Gateway Load Balancer – East/West Inspection

Use Gateway Load Balancer and Transit Gateway to create a highly available and scalable bump-in-the-wire solution for East/West inspection.



App1 Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	tgw-1234...

SEC TGW Route Table 1

Destination	Target
10.2.0.0/16	local
0.0.0.0/0	GWLB endpoint 1

Destination	Target
10.2.0.0/16	local
0.0.0.0/0	tgw-1234...

Destination	Target
0.0.0.0/0	TGW-Attach-Sec-VPC

TGW RT App - Associations:
TGW-Attach-App1-VPC
TGW-Attach-App2-VPC

Destination	Target
10.0.0.0/16	TGW-Attach-App1-VPC
10.1.0.0/16	TGW-Attach-App2-VPC

TGW RT Sec - Associations:
TGW-Attach-Sec-VPC

Destination	Target
10.2.0.0/16	local
0.0.0.0/0	GWLB endpoint 2

SEC TGW Route Table 2

App2 Route Table

Destination	Target
10.1.0.0/16	local
0.0.0.0/0	tgw-1234...

1 Traffic from IP 10.0.1.10 wants to reach IP 10.1.2.20 in the App2 virtual private cloud (VPC). The subnet's route table routes it to the TGW via the default route (0.0.0.0/0).

2 App1 VPC is associated with the "TGW RT APP" route table in the AWS Transit Gateway (TGW), which forwards all traffic (0.0.0.0/0) via the Security VPC (Virtual Private Cloud) attachment.

3 The TGW ENI in the Security VPC uses its subnet's route table to forward all traffic to the **Gateway Load Balancer** (**GWLB**) endpoint 1.

4 **GWLB** endpoint forwards the traffic to **GWLB**.

5 Traffic is send for inspection to one of the security appliance instances behind the **GWLB**.

6 Once the traffic is inspected, it is sent back to **GWLB**.

7 **GWLB** forwards the traffic to the **GWLB** endpoint.

8 The **GLWB** endpoint uses its subnet route table to forward all non-local traffic to the TGW via the TGW ENI using the TGW attachment.

9 Once the traffic reaches TGW, it uses the "TGW RT Sec" route table that it is associated with Security VPC to find the destination via the App2 VPC attachment.

10 Once it reaches the App2 Route table, the destination of the packet (10.1.2.20) is a local address, and it is forwarded to the destination instance.

See also: Architecture for Gateway Load Balancer – North/South Inspection

AWS Reference Architecture