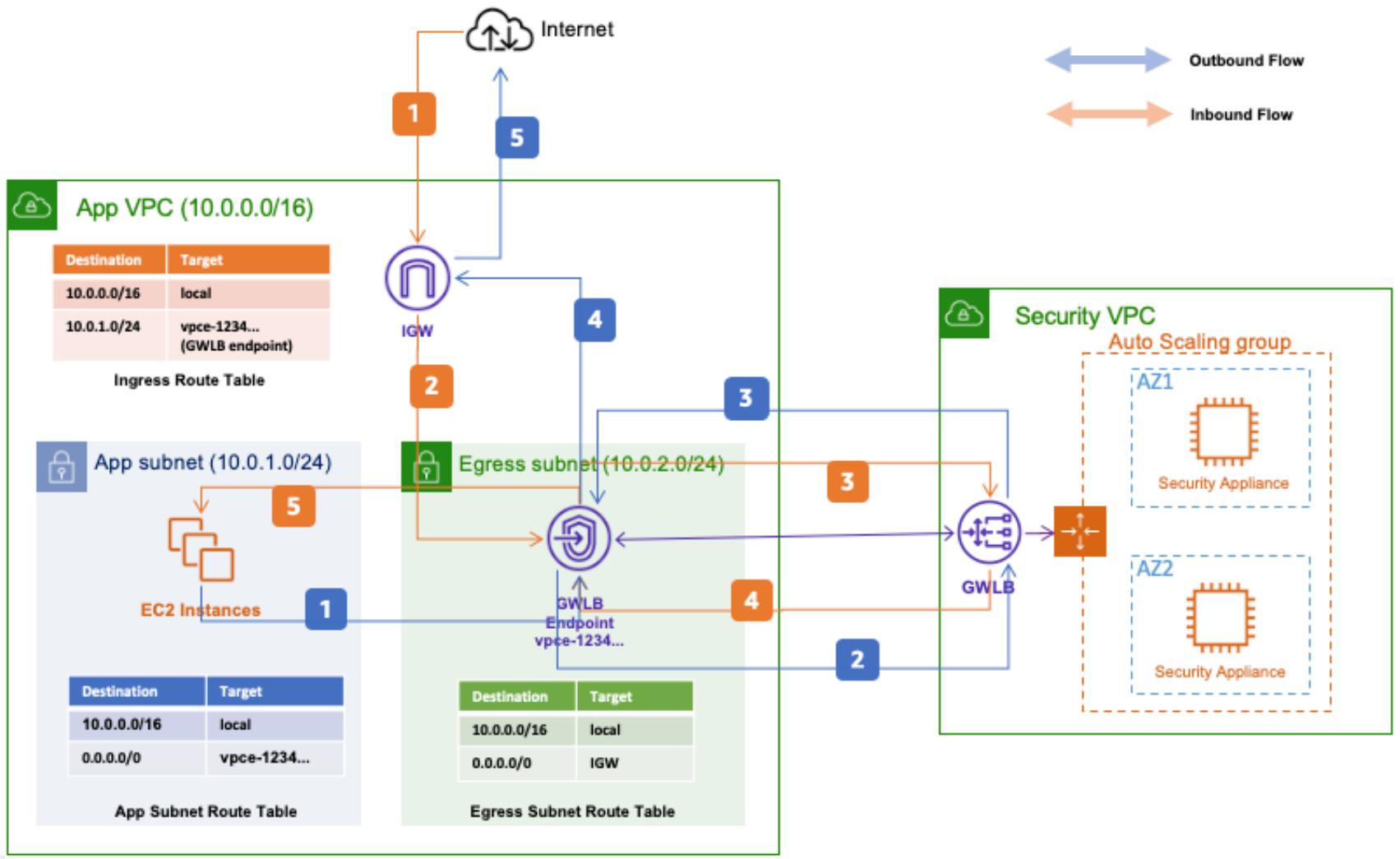
Architecture for Gateway Load Balancer – North/South Inspection

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



1. Traffic from resources in the APP subnet to the Internet is routed to the **Gateway Load Balancer** (GWLB) endpoint in the same virtual private cloud (VPC).
2. The **GWLB** endpoint is attached to the endpoint service for the **GWLB** in the Security VPC. Once **GWLB** receives the traffic, it forwards it encapsulated to the backend appliances.
3. Once the traffic is inspected by the appliances, the traffic returns to **GWLB** and then to the **GWLB** endpoint.
4. Once the traffic is back to the origin VPC, it follows the Egress Subnet Route Table and is sent to the internet gateway (IGW).
5. IGW sends the traffic to the internet.

1. Traffic coming from the Internet arrives at the IGW
2. Following the Ingress Route Table, traffic is routed to the **GWLB** endpoint.
3. **GWLB** endpoint is attached to the endpoint service for the **GWLB** in the Security VPC. Once **GWLB** receives the traffic, it forwards it encapsulated to the backend appliances.
4. Once the traffic is inspected by the appliances, it returns to **GWLB** and then to the **GWLB** endpoint.
5. Traffic arrives in the App VPC from the **GWLB** endpoint is locally routed to the resources in the App subnet.

AWS Reference Architecture

See also: Architecture for Gateway Load Balancer – East/West Inspection