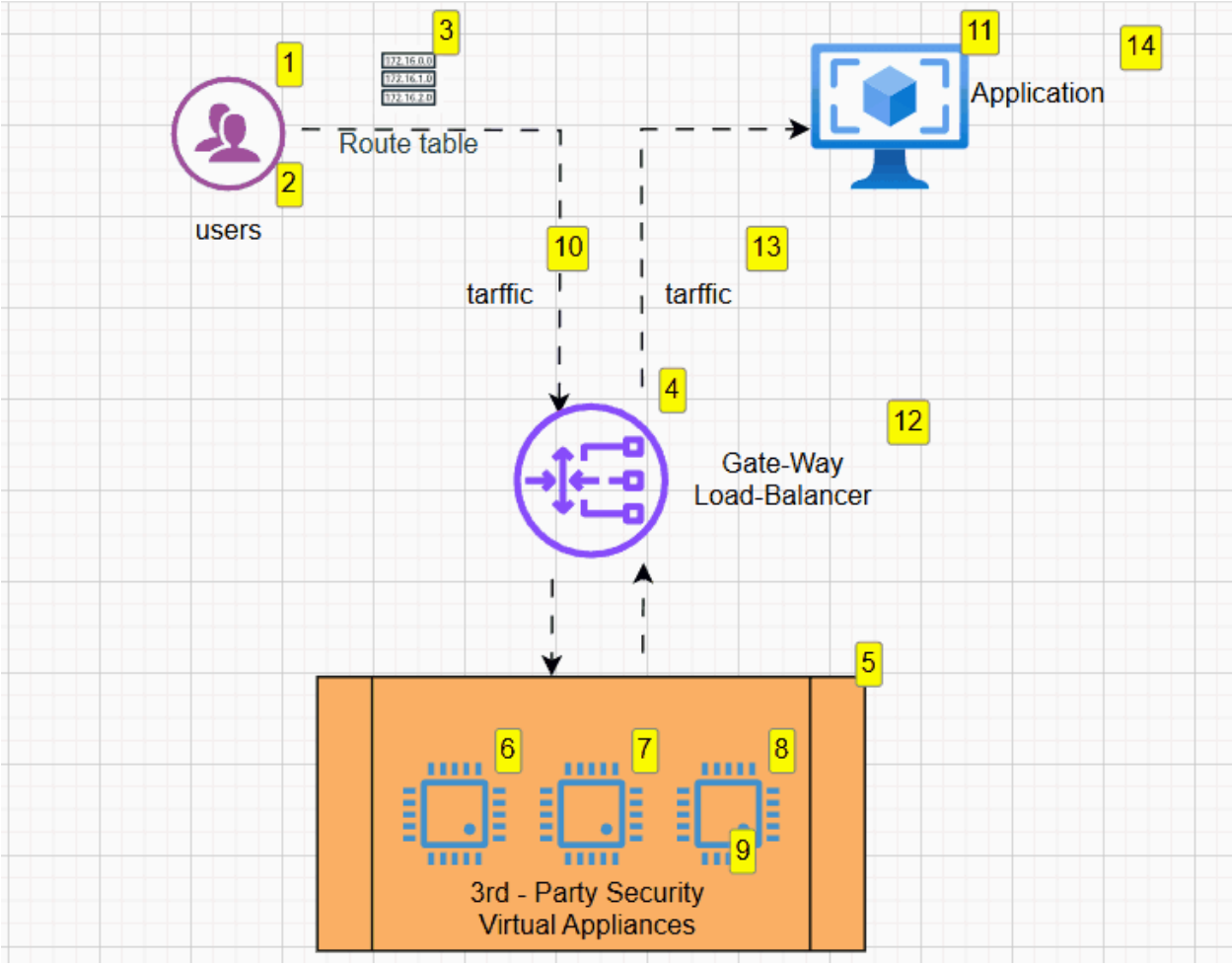
🛡️ AWS Gateway Load Balancer (GWLB) – Explained

The **AWS Gateway Load Balancer (GWLB)** is a **Layer 3 (Network Layer)** load balancer designed **specifically to deploy, scale, and manage third-party virtual appliances** such as firewalls, intrusion detection and prevention systems (IDS/IPS), deep packet inspection systems (DPI), and traffic monitoring tools.

It combines **transparent traffic forwarding** with **load balancing**, enabling security appliances to scale elastically and integrate seamlessly into your AWS network.



🔧 Key Components of AWS Gateway Load Balancer

Component	Description
Gateway Load Balancer (GWLB)	Distributes traffic across virtual appliances using **GENEVE encapsulation**
Gateway Load Balancer Endpoint (GWLBe)	A VPC endpoint for privately forwarding traffic to the GWLB
Target Group	Group of virtual appliances (e.g., firewalls) the GWLB balances traffic to
GENEVE Protocol	Used for encapsulating traffic transparently; allows metadata tagging
Elastic Network Interface (ENI)	Interface used by virtual appliances to receive traffic from GWLB

📦 How AWS Gateway Load Balancer Works

1. **Traffic Flow Initiation**
    - A client request or packet destined for a resource passes through a **Gateway Load Balancer Endpoint (GWLBe)**.
2. **Encapsulation**
    - The traffic is encapsulated using the **GENEVE protocol** by the GWLBe and forwarded to the GWLB.
3. **Load Balancing**
    - GWLB distributes the traffic to one of the healthy **virtual appliances** in its **target group**.
4. **Appliance Processing**
    - The virtual appliance (e.g., a firewall) inspects, modifies, or logs the traffic.

5. **Return Path**
    - The appliance sends the processed packet back to the GWLB, which **decapsulates** and forwards it to its destination.

🧠 Use Cases

- Deploying third-party **next-gen firewalls** (e.g., Palo Alto, Fortinet, Check Point)
- Centralizing **network security inspection**
- **Intrusion detection/prevention**
- **Traffic mirroring and analysis**
- Enabling **service chaining** of security tools

🧱 Architecture Overview (Simplified)

Internet / VPC Traffic
|
GWLBe (Gateway Load Balancer Endpoint)
|
GWLB (Encapsulates, Balances)
|
Target Group (Security Appliances)
|
Appliance processes and returns traffic

✅ Benefits of GWLB

- **Transparent Deployment**: No need to change routing or application code.
- **Elastic Scaling**: Automatically scales security appliances.
- **High Availability**: Built-in failover and multi-AZ support.
- **Centralized Security**: Single point of traffic inspection.

📌 **Comparison with Other Load Balancers**

Feature	ALB	NLB	GWLB
OSI Layer	Layer 7 (App)	Layer 4 (Transport)	**Layer 3 (Network)**
Protocols Supported	HTTP, HTTPS	TCP, UDP, TLS	**All IP traffic (L3)**
Target Types	Web servers	EC2, IPs	**Virtual appliances**
Traffic Inspection	No	No	**Yes (via appliances)**
Use Case	Web apps	Low-latency apps	**Security/middleware**
