Target Attack => DDOS

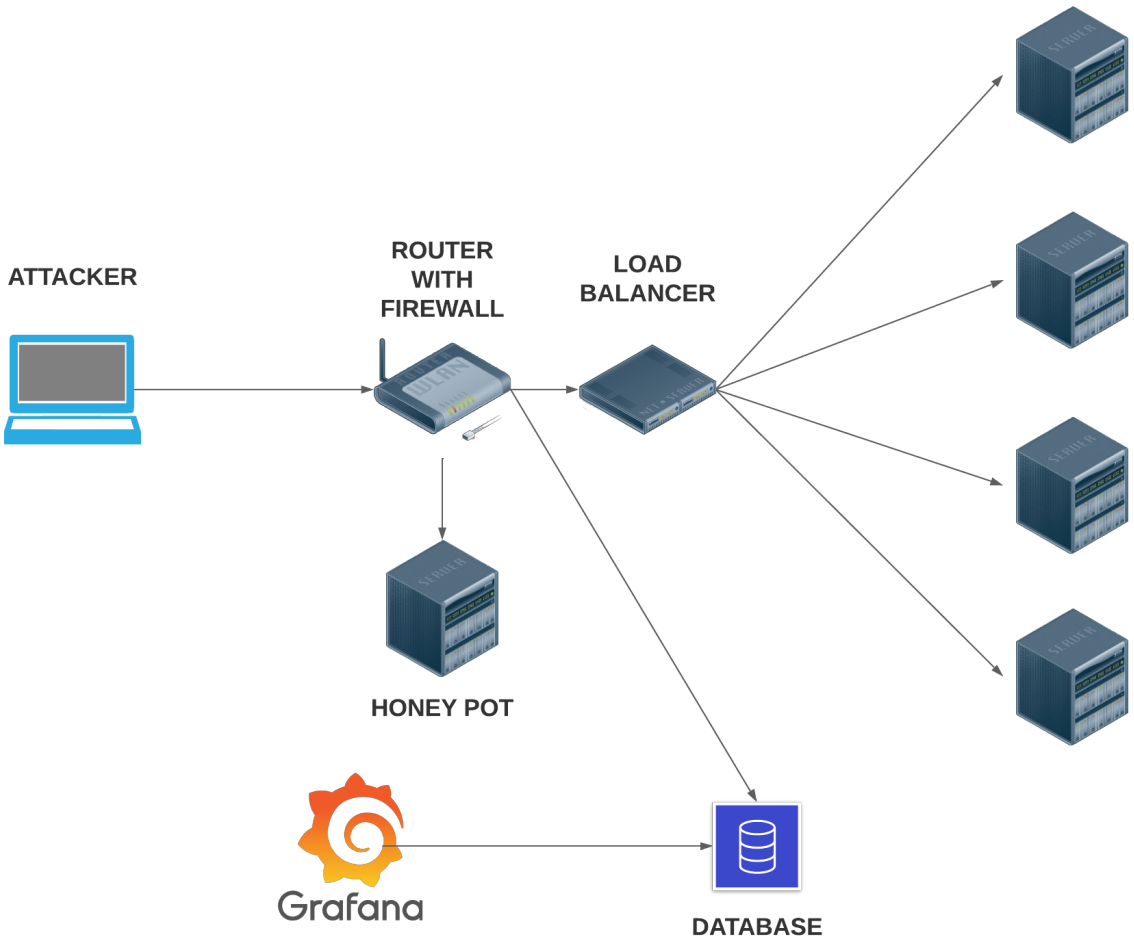
What we are going to do?

Generate a fake company network using mininet, then simulate a DDOS attack to the Network, the network will have a honeypot to detect attacks, also the network will mitigate this DDoS attacks using some firewall rules and a load balancer, finally the traffic will be shown on charts using grafana.

How we would implement this:

1. Setup a mininet network
2. Setup a network topology
3. Add the honeypot server
4. Configure the honeypot to monitor incoming traffic and detect DDoS attacks(maybe use Snort?)
5. Start a firewall, maybe setup some rules manually and then automatic rules generated by the honeypot.
6. Generate the load balancer to mitigate the error.
7. Simulate a DDOS attack (maybe use a python script)
8. The honeypot should detect the DDoS attack and alert the network administrator.
9. The firewall and load balancer should work together to mitigate the DDoS attack by filtering traffic and distributing it among the servers.
10. Finally we will use Grafana to display traffic on charts and graph.

Network topology
We will have the company service distributed as we want to avoid ddos attacks, the same service will be on different servers in case one fails the others still alive, maybe we would generate a network with 4 servers and a honeypot.



Grafana para los charts
InfluxDB para la DB
HoneyPot y firewall on RYU y Snort
Network topology con Mininet

Atac
Crear 100 @IP aleatòries i llançar peticions de connexió a servidor i anar escalant, ex: 10 per segon → 20 per segon …. etc (a veure quan ho podem detectar).

Pensar algun atac per agafar alguna ip i bloquejarla, i treure alguna alerta quan passi.

Monitoritzar les sessions del honeypot i quan arriba algun num, posar regles.