Firewall 1:

1. H1 (100.0.0.10) and H2 (100.0.0.11) can ping LB1 (100.0.0.25) and vice versa. This includes request and response
2. H1 (100.0.0.10) and H2 (100.0.0.11) can ping LB2 (100.0.0.45) and vice versa. This includes request and response
3. UDP service is accessible from “DNS service” on port 53.

* LB1 can establish UDP connection to public zone (srcip: 100.0.0.25, srcprt:53 ::: dstip: 100.0.0.10, 100.0.0.11, dstprt: any)

1. TCP service is accessible from “HTTP service” on port 80.

* LB2 can establish TCP connection to public zone (srcip: 100.0.0.45, srcprt:80 ::: dstip: 100.0.0.10, 100.0.0.11, dstprt: any)

**Imp: Rest other traffic is blocked!**

1. H1 (100.0.0.10) and H2 (100.0.0.11) can ping Private Zone (100.0.0.1). Note: exclusive rule to block the icmp request from public zone towards private zone is installed in Firewall2!

Firewall 2:

Note: Here srcip is the ip given by napt after translation, i.e., 100.0.0.1. This will be my srcip for private zone. Let’s consider this as PH (private host)

1. PH (100.0.0.1) can initiate ping to H1 (100.0.0.10), H2 (100.0.0.11), LB1 (100.0.0.25), LB2 (100.0.0.45)
2. PH (100.0.0.1) can establish UDP connection to LB1 (100.0.0.25)
3. PH (100.0.0.1) can establish TCP connection to LB2 (100.0.0.45)
4. No TCP/UDP connection should be established from LB2/LB1 respectively towards PH
5. Firewall blocks all ping initiation from H1, H2, LB1, LB2 towards PH