Steps to start the Routing and load balancing Application:

Start two Virtual Machines.

1. Start the Floodlight Controller on virtual Machine 1.
2. Start the Mininet1 on virtual Machine 1.
3. Start the Mininet 2 on virtual Machine 2.

Note: These two Mininets are controlled by single floodlight controller.

1. Use Custom.py file to create custom topology.
2. Try tunneling between the two switches which are in different Mininets. (follow the steps in document for gre tunneling).
3. Configure snort on one of the Virtual Machine. (follow the steps in the document for configuring the snort).
4. Start the routing and load balancing application using the python file LoadBalancer\_Floodlight.py.
5. Select the source and destination.(Source is in Mininet 1 and destination is in Mininet 2).
6. Start the traffic between source and destination using Iperf, or scapy tool. (use xterm to start the terminal of source and destination.)
7. Snort will detect all the packets passing through the interface on which it is listening.
8. Write the custom rules to detect the attacks.(use the rules file to create the custom rules in snort).
9. Logs.txt will collect all the logs from snort.
10. Start the FlowRule\_droppacket.py file analyzes Logs from Logs.txt file to detect the attack.
11. After detecting the attack it will the push rule through the rest api of floodlight controller to drop the packets to prevent the attack.
12. Hping3 can be used to create the dos attack. Also by using scapy we can create the custom packets.(Use scapy guide file to explore how to create the packes. )