# Praarthana Ramakrishnan

C82908385

# ADVANCED NETWORK SECURITY

## PROJECT 3 - FLOODLIGHT FIREWALL APP

1. STEPS INVOLVED IN CREATING THE FLOODLIGHT FIREWALL APP

* After downloading the Floodlight VM, it is started in the VirtualBox by adding the .vmdk hard disk file.
* Once the VM gets started, the terminal is opened inside the Floodlight VM.
* The following commands are typed as shown below in Figure 1.

1. The floodlight is updated to add new features and fix bugs.

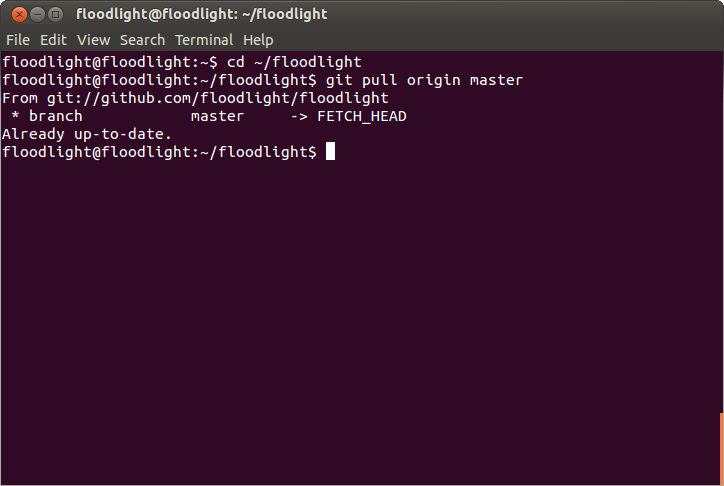


Fig 1.

1. The floodlight is built and run within the VM using the following commands as shown in Figure 2 and Figure 3.

$ ant

$ java –jar target/floodlight.jar

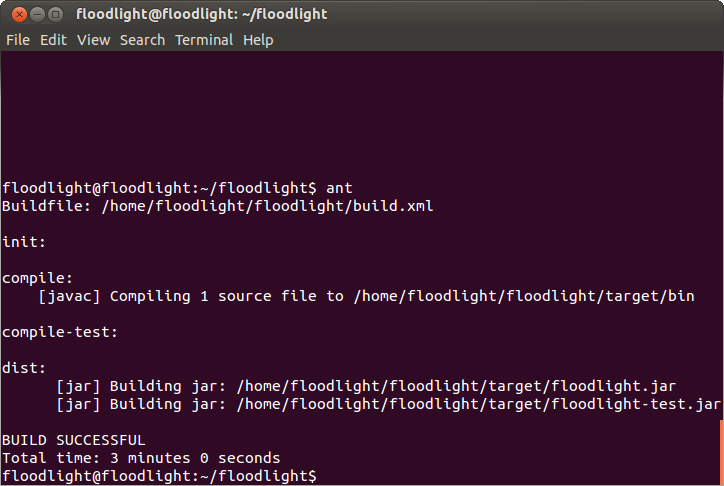


Fig 2

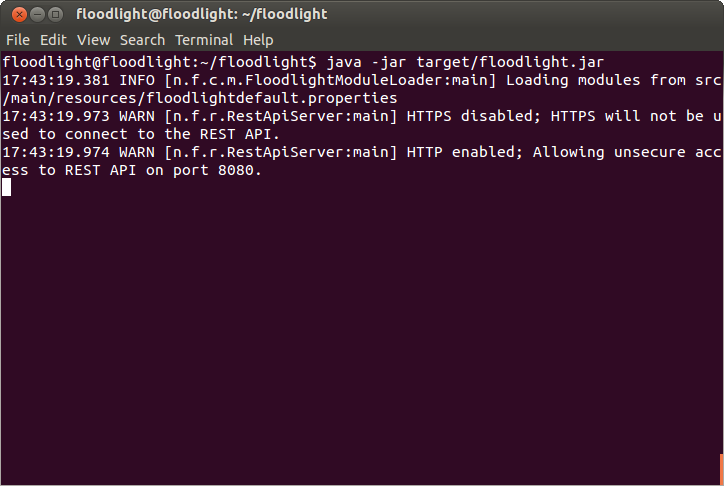


Fig 3

* To develop applications on top of Floodlight, REST API is the interface that is commonly used.
* The REST API is available at port 8080 of the controller
* A new terminal is opened as the Floodlight is running at the background and the following curl examples are tried using the steps below.

**STEP 1:**

To show whether the firewall is enabled or not, the command is typed as follows and the Figure 4 shows that the firewall is disabled.

* $ curl http://localhost:8080/wm/firewall/module/status/json

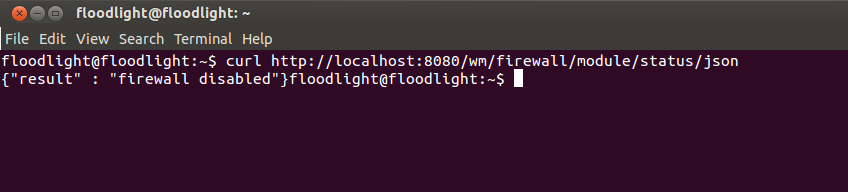


Fig 4

**STEP 2:**

Next, the firewall is enabled using the following command and the result is shown in Figure 5, where it displays that the firewall is running.

* $ curl http://localhost:8080/wm/firewall/module/enable/json -X PUT -d ''

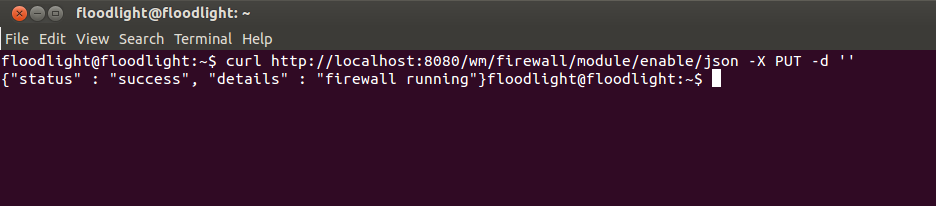


Fig 5

**STEP 3:**

This command adds ALLOW rule for all flows to pass through switch 00:00:00:00:00:00:00:01 as shown in Figure 6.

* curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:01"}' <http://localhost:8080/wm/firewall/rules/json>

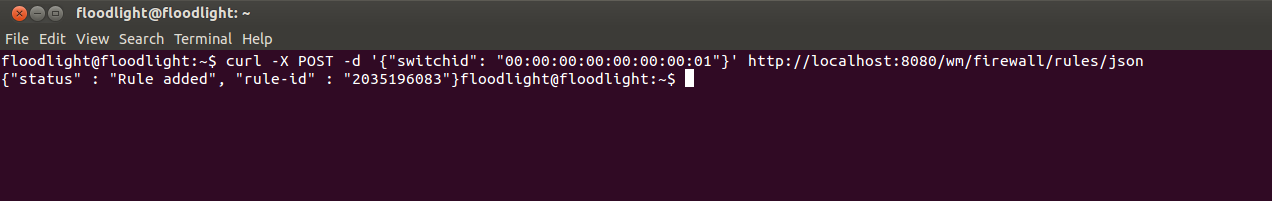


Fig 6

**STEP 4:**

These commands add an ALLOW rule for all flows between IP host 10.0.0.3 and host 10.0.1.5. Not specifying action implies ALLOW rule. The results are shown in Figure 7 and 8.

* curl -X POST -d '{"src-ip": "10.0.0.3/32", "dst-ip": "10.0.0.7/32"}' <http://localhost:8080/wm/firewall/rules/json>
* curl -X POST -d '{"src-ip": "10.0.0.7/32", "dst-ip": "10.0.0.3/32"}' <http://localhost:8080/wm/firewall/rules/json>

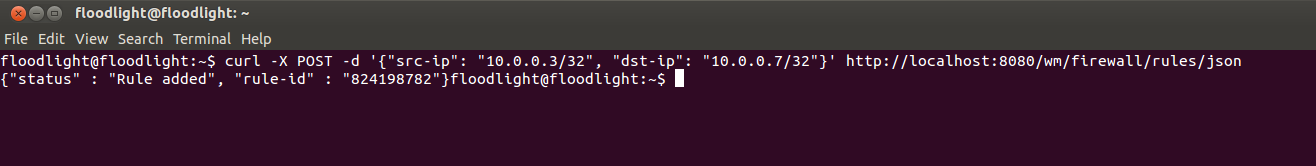


Fig 7

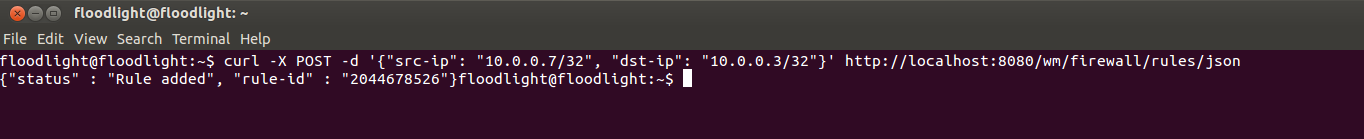


Fig 8

**STEP 5:**

These commands add an ALLOW rule for all flows between host mac 00:00:00:00:00:0a and host 00:00:00:00:00:0b. The results are shown in Figure 9 and 10.

* curl -X POST -d '{"src-mac": "00:00:00:00:00:0a", "dst-mac": "00:00:00:00:00:0a"}' <http://localhost:8080/wm/firewall/rules/json>
* curl -X POST -d '{"src-mac": "00:00:00:00:00:0b", "dst-mac": "00:00:00:00:00:0b"}' <http://localhost:8080/wm/firewall/rules/json>

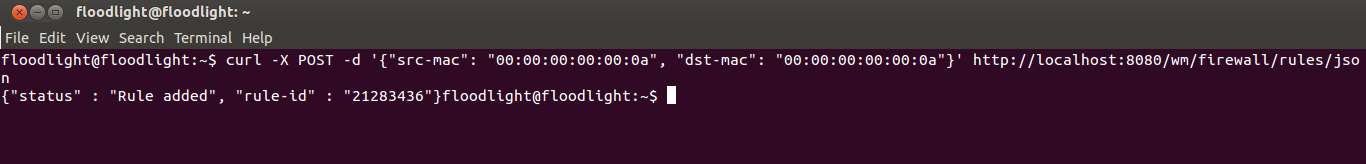


Fig 9

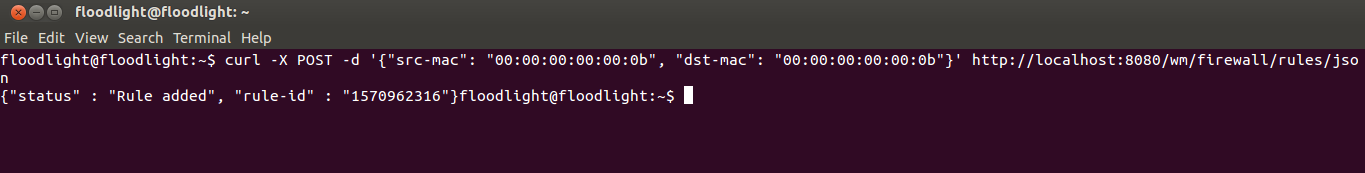


Fig 10

**STEP 6:**

These commands add an ALLOW rule for ping to work between IP hosts 10.0.0.3 and 10.0.0.7. The results are shown in Figure 11,12,13 and 14.

* curl -X POST -d '{"src-ip": "10.0.0.3/32", "dst-ip": "10.0.0.7/32", "dl-type":"ARP" }'   <http://localhost:8080/wm/firewall/rules/json>
* curl -X POST -d '{"src-ip": "10.0.0.7/32", "dst-ip": "10.0.0.3/32", "dl-type":"ARP" }' <http://localhost:8080/wm/firewall/rules/json>
* curl -X POST -d '{"src-ip": "10.0.0.3/32", "dst-ip": "10.0.0.7/32", "nw-proto":"ICMP" }' <http://localhost:8080/wm/firewall/rules/json>
* curl -X POST -d '{"dst-ip": "10.0.0.7/32", "dst-ip": "10.0.0.3/32", "nw-proto":"ICMP" }' <http://localhost:8080/wm/firewall/rules/json>

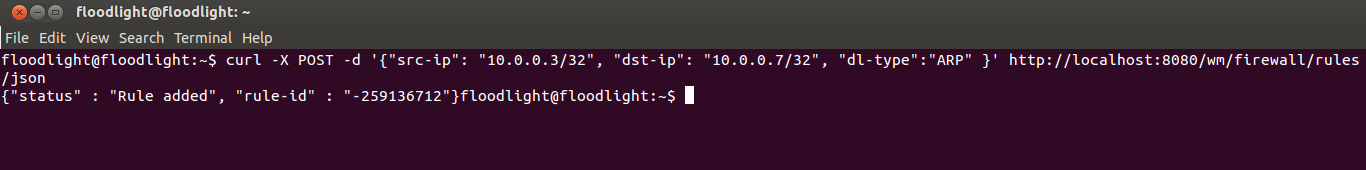


Fig 11

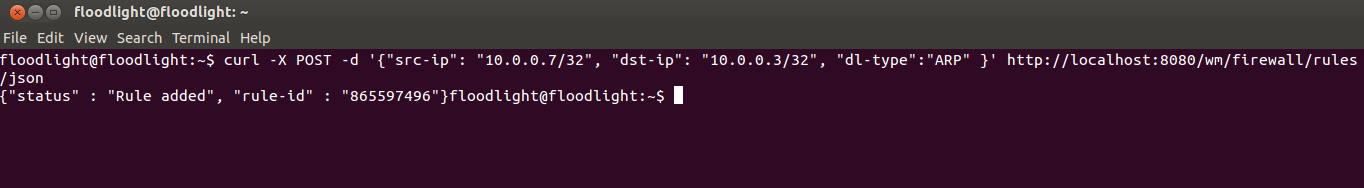


Fig 12

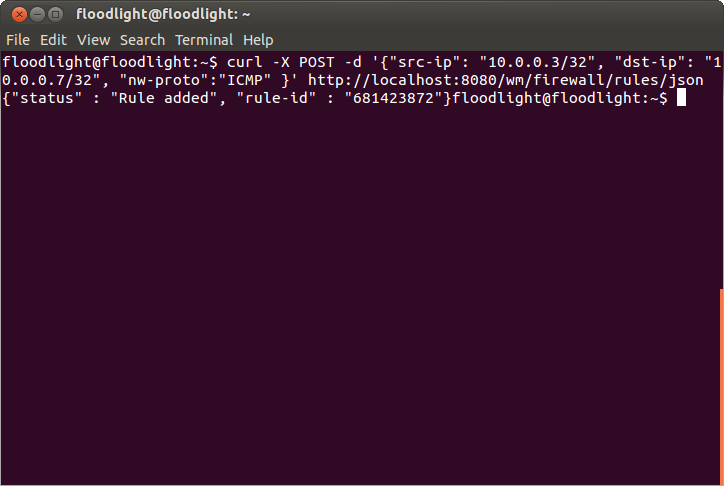


Fig 13

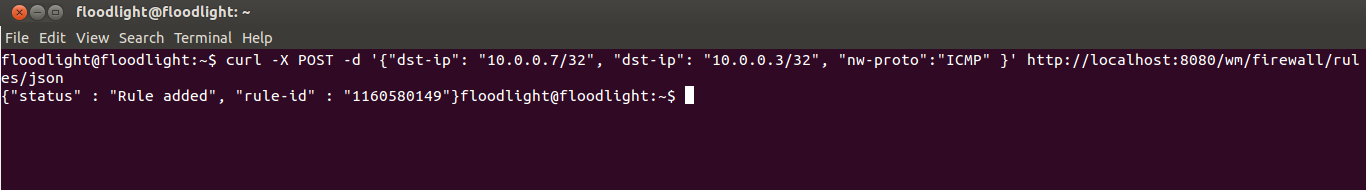


Fig 14

**STEP 7:**

These commands add an ALLOW rule for UDP (such as iperf) to work between IP hosts 10.0.0.4 and 10.0.0.10, and then blocking port 5010. The results are shown in Figure 15,16,17,18,19 and 20.

* curl -X POST -d '{"src-ip": "10.0.0.4/32", "dst-ip": "10.0.0.10/32", "dl-type":"ARP" }' <http://localhost:8080/wm/firewall/rules/json>
* curl –X POST –d ‘{“dst-ip”: “10.0.0.10/32”, “dst-ip”: “10.0.0.4/32”, “dl-type”:”ARP” }’ <http://localhost:8080/wm/firewall/rules/json>
* curl -X POST -d '{"src-ip": "10.0.0.4/32", "dst-ip": "10.0.0.10/32", "nw-proto":"UDP" }' <http://localhost:8080/wm/firewall/rules/json>
* curl -X POST -d '{"src-ip": "10.0.0.10/32", "dst-ip": "10.0.0.4/32", "nw-proto":"UDP" }' <http://localhost:8080/wm/firewall/rules/json>
* curl -X POST -d '{"src-ip": "10.0.0.4/32", "dst-ip": "10.0.0.10/32", "nw-proto":"UDP", "tp-src":"5010", "action":"DENY" }' <http://localhost:8080/wm/firewall/rules/json>
* curl -X POST -d '{"src-ip": "10.0.0.10/32", "dst-ip": "10.0.0.4/32", "nw-proto":"UDP", "tp-src":"5010", "action":"DENY" }' <http://localhost:8080/wm/firewall/rules/json>

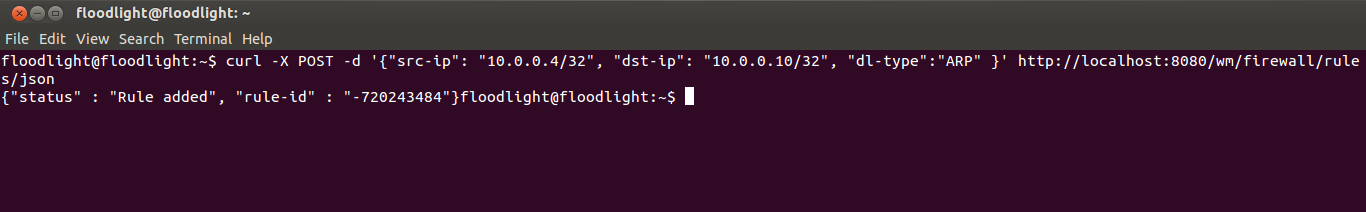


Fig 15

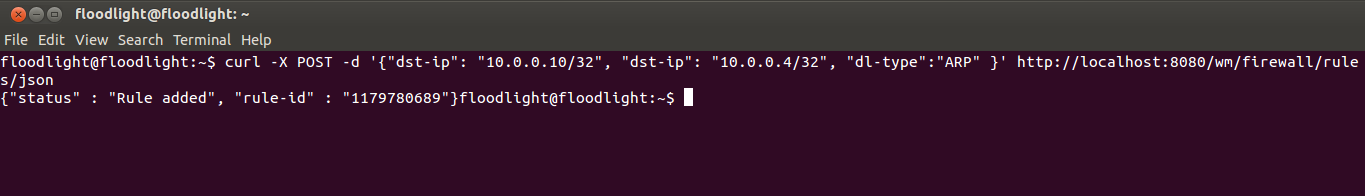


Fig 16

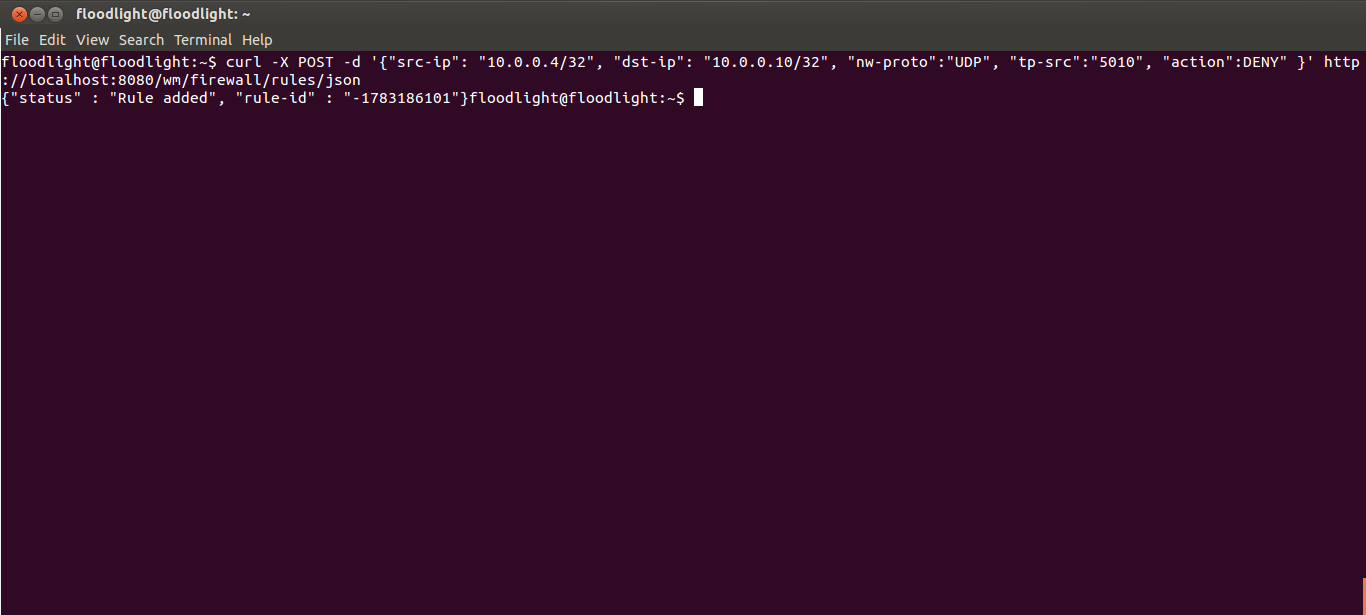


Fig 17

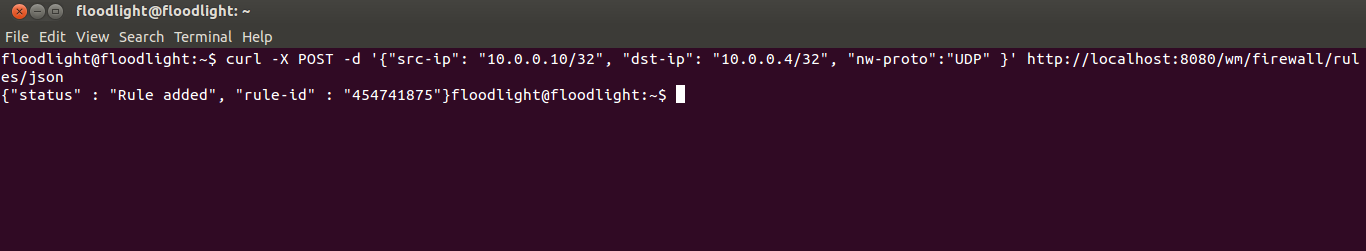


Fig 18

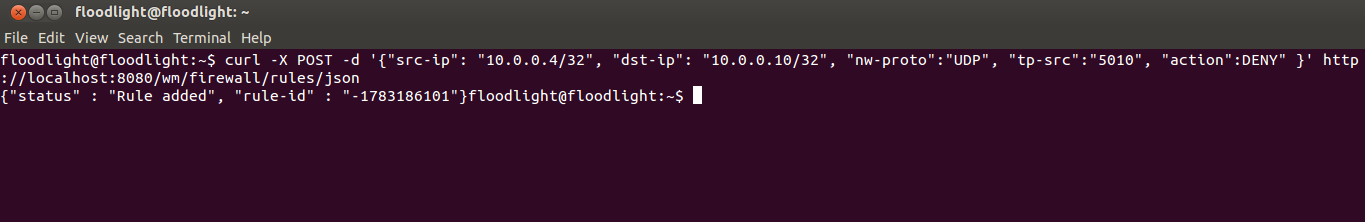


Fig 19

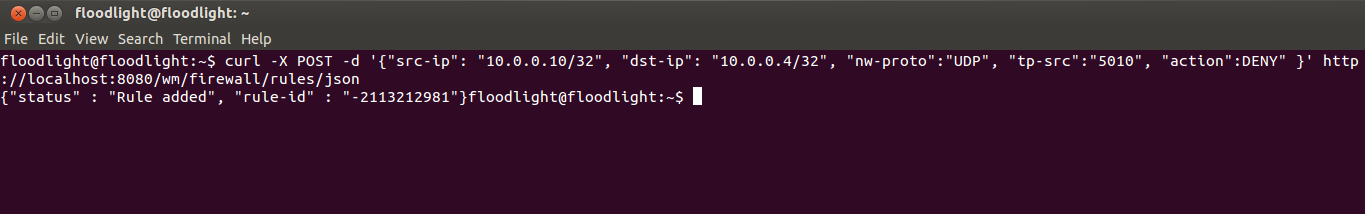


Fig 20