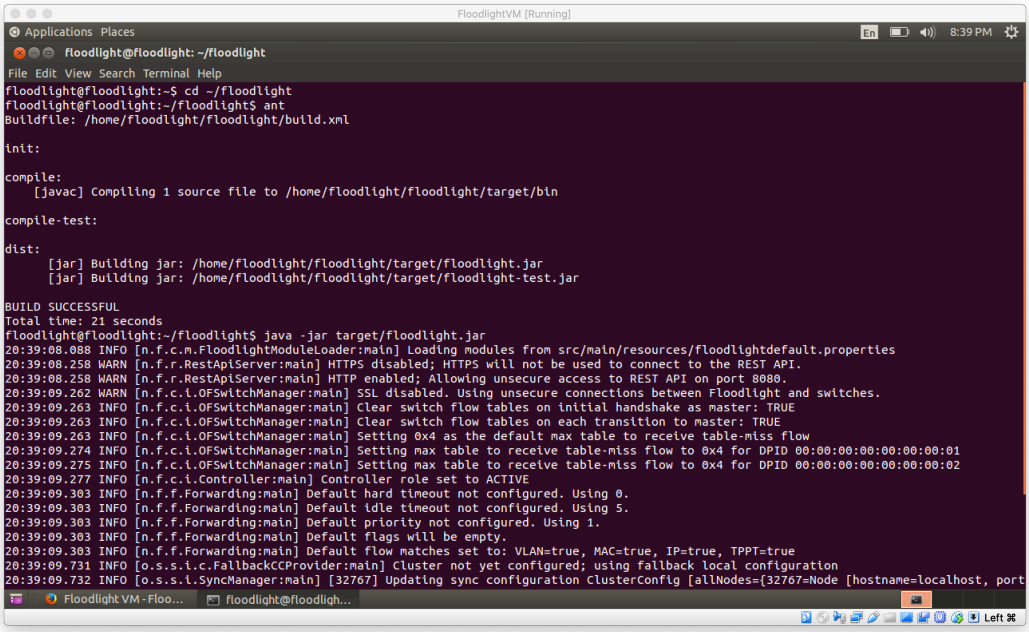
PROJECT 2: Floodlight Firewall App

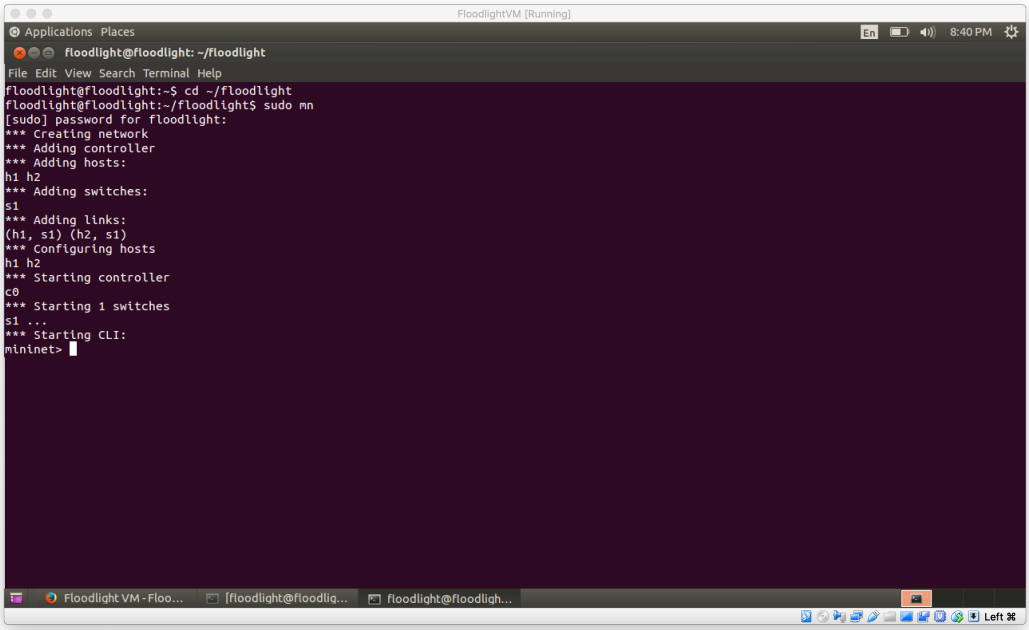
submitted by Christin Wilson

Inorder to setup the SDN environment, we first download the Floodlight VM and run it on the virtual box. After setting up the Virtual machine we do the following steps:

1. On the terminal, we cd into the floodlight directory and run the `ant` command which is a java library to build the java files in the directory. After this we run `java -jar target/floodlight.jar` to run floodlight and get our localhost setup in the VM.
   Screenshot:



2. Next a virtual network is setup using mininet . Thus the floodlight is attached to the OpenFlow network.



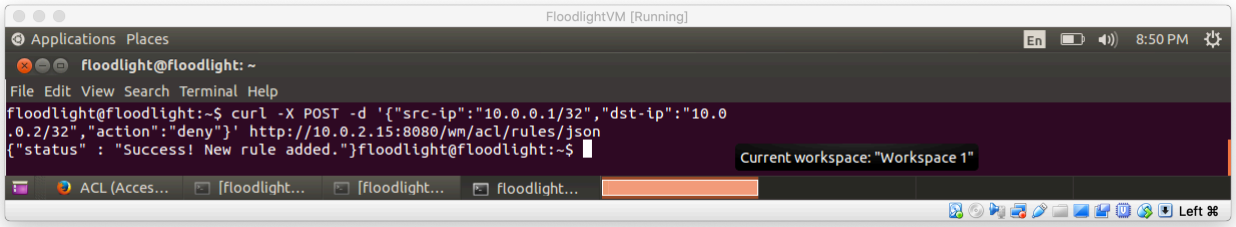
ACL REST API

1. Add an ACL rule:

command:

```
curl -X POST -d '{"src-ip":"10.0.0.1/32","dst-ip":"10.0.0.2/32","action":"deny"}' http://10.0.2.15:8080/wm/acl/rules/json
```

Screenshot:

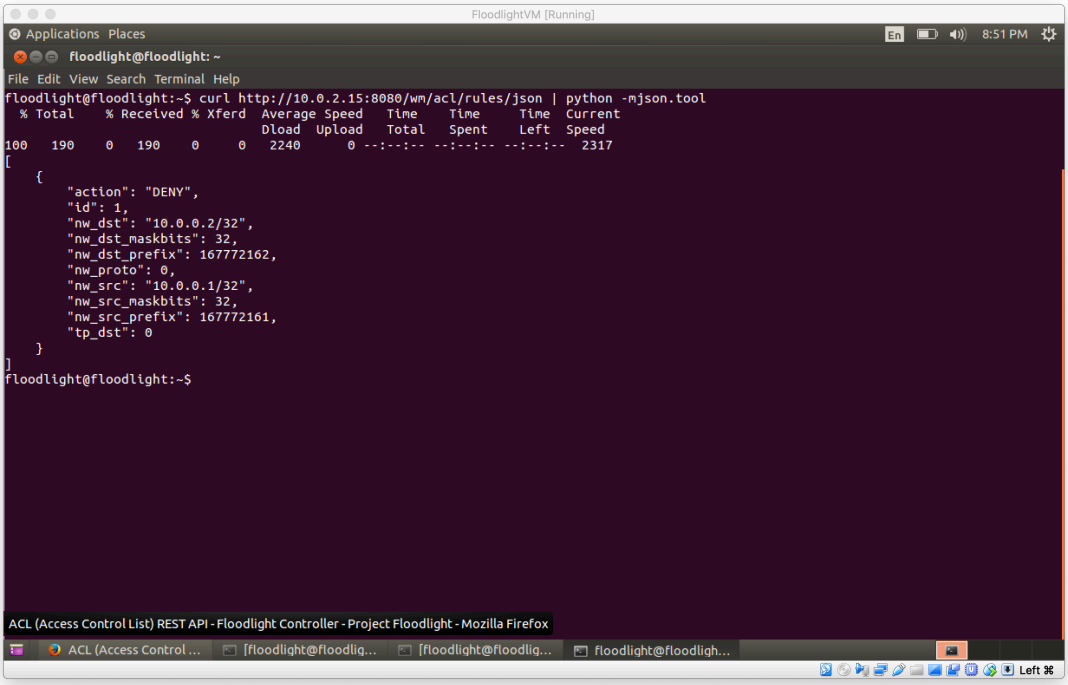


2. Listing all ACL rules

Command:

```
curl http://10.0.2.15:8080/wm/acl/rules/json | python -mjson.tool
```

Screenshot:

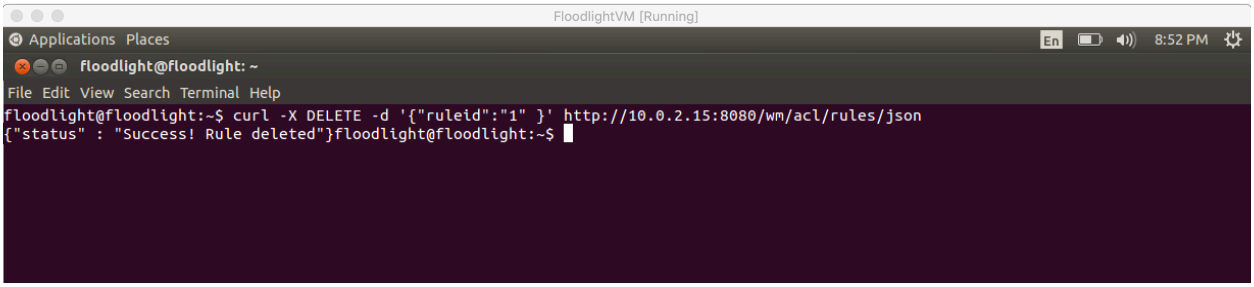


3. Remove an ACL rule:

Command:

```
curl -X DELETE -d '{"ruleid":"1" }' http://10.0.2.15:8080/wm/acl/rules/json
```

Screenshot:

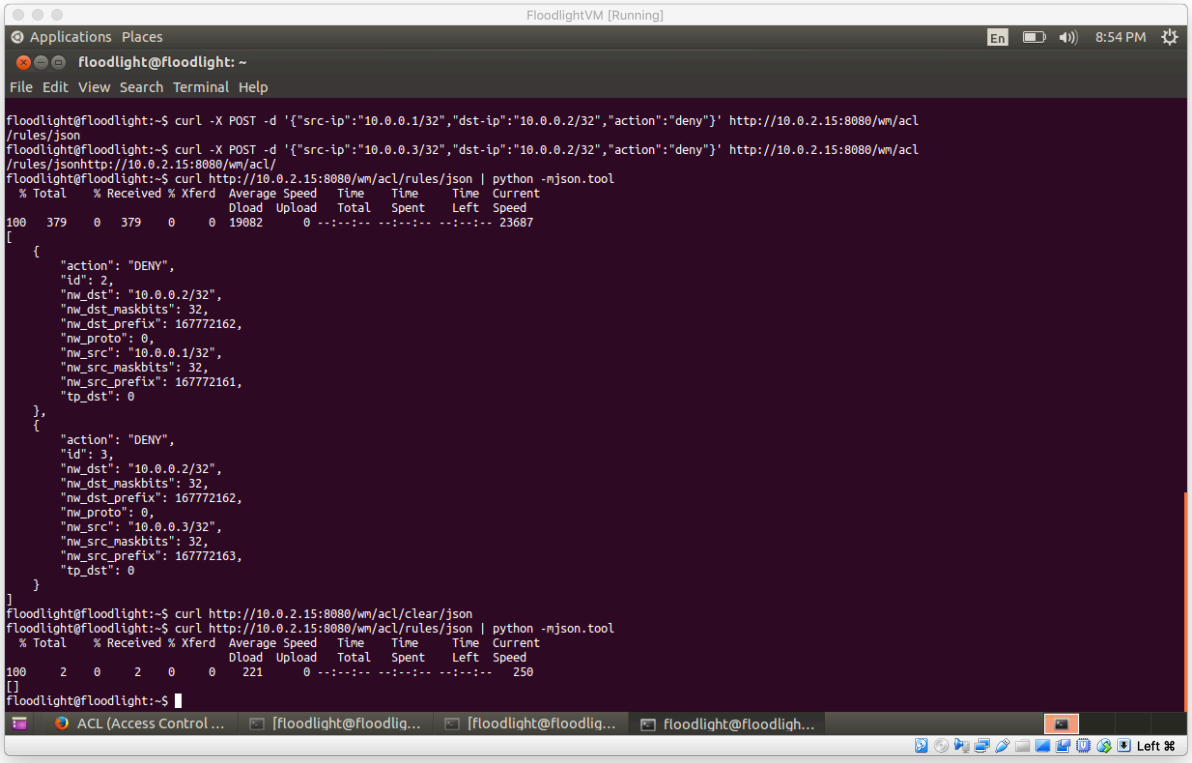


4. Remove all ACL rules:

Command:

```
curl http://10.0.2.15:8080/wm/acl/clear/json
```

Screenshot:



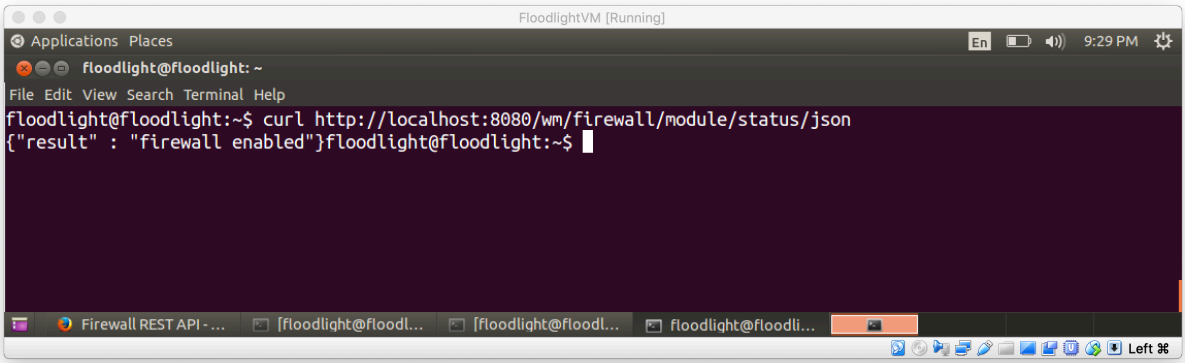
Firewall REST API

1. Check status of firewall (enabled/disabled).

Command:

```
curl http://localhost:8080/wm/firewall/module/status/json
```

Screenshot:

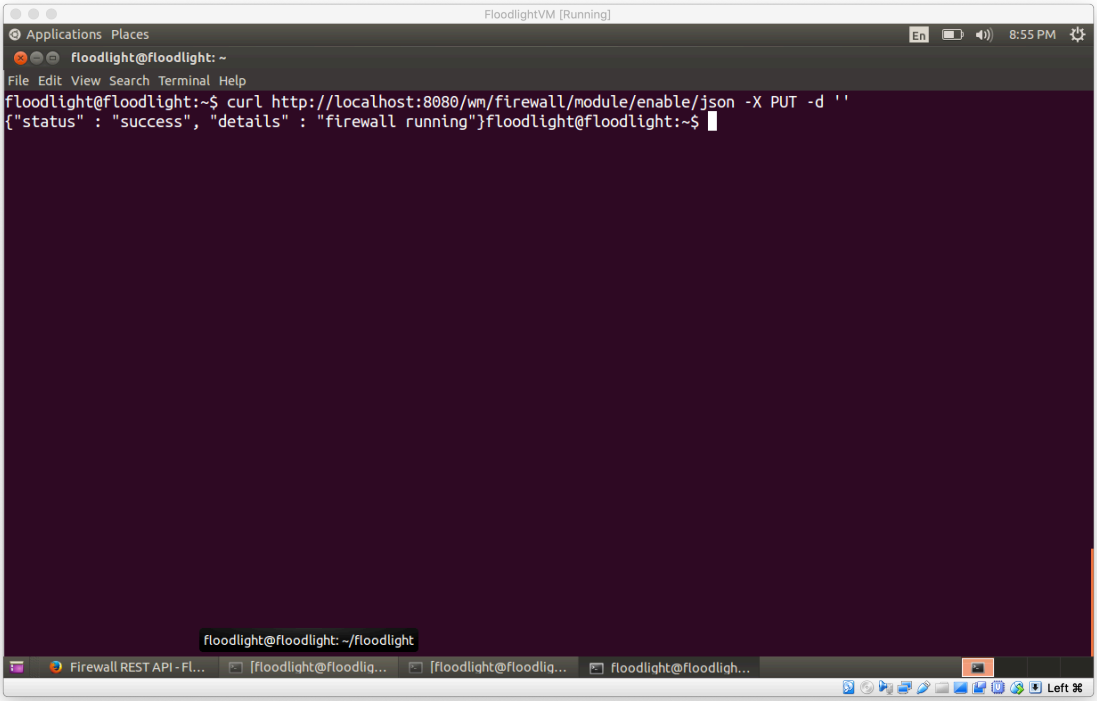


2. Enable the firewall.

Command:

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

Screenshot:

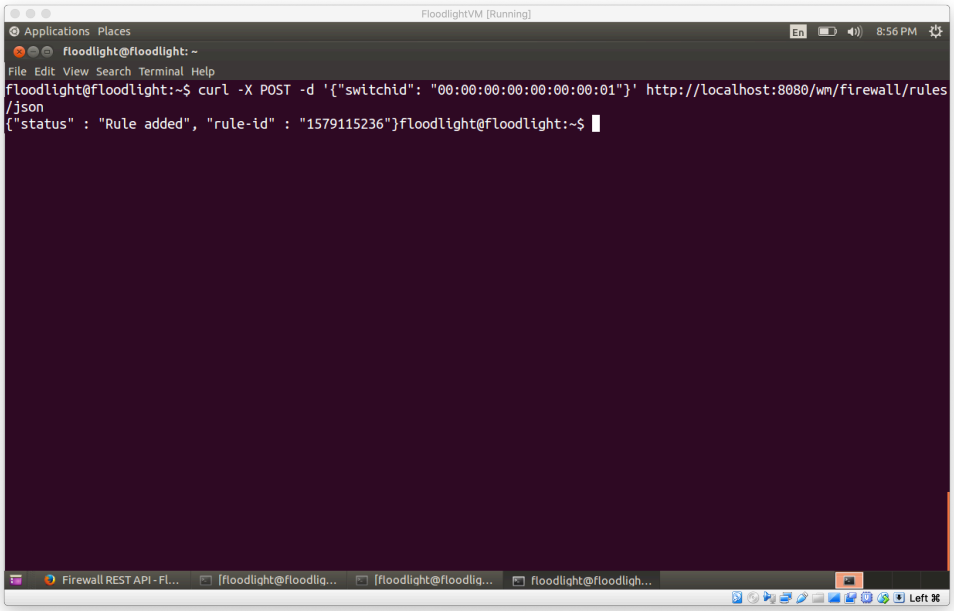


3. Adding an ALLOW rule for all flows to pass through switch 00:00:00:00:00:00:00:01.

Command:

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

Screenshot:

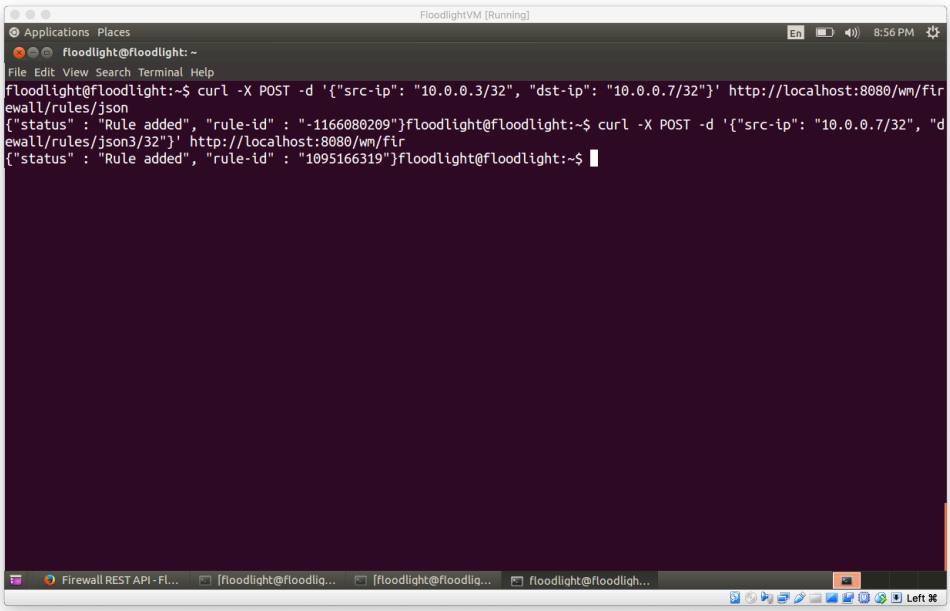


4. Adding an ALLOW rule for all flows between IP host 10.0.0.3 and host 10.0.1.5.

Command:

```
 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
```

Screenshot:

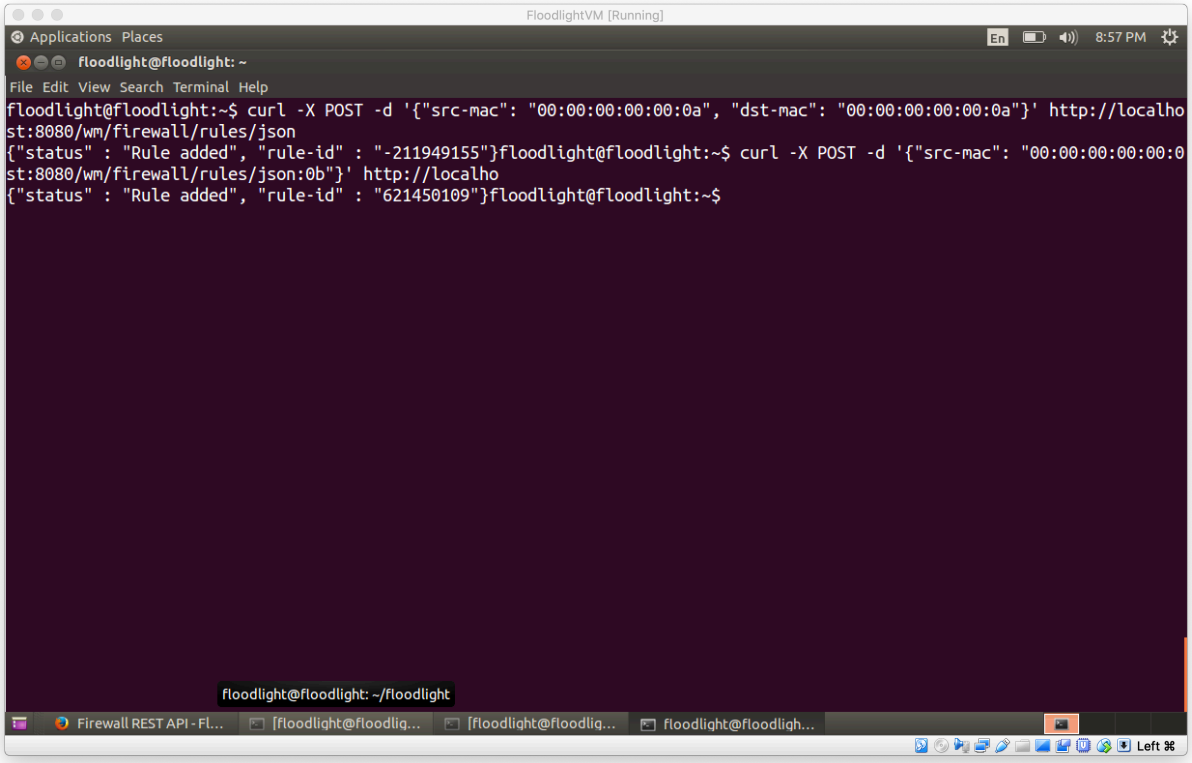


5. Adding an ALLOW rule for all flows between host mac 00:00:00:00:00:0a and host 00:00:00:00:00:0b.

Command:

```
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
```

Screenshot:



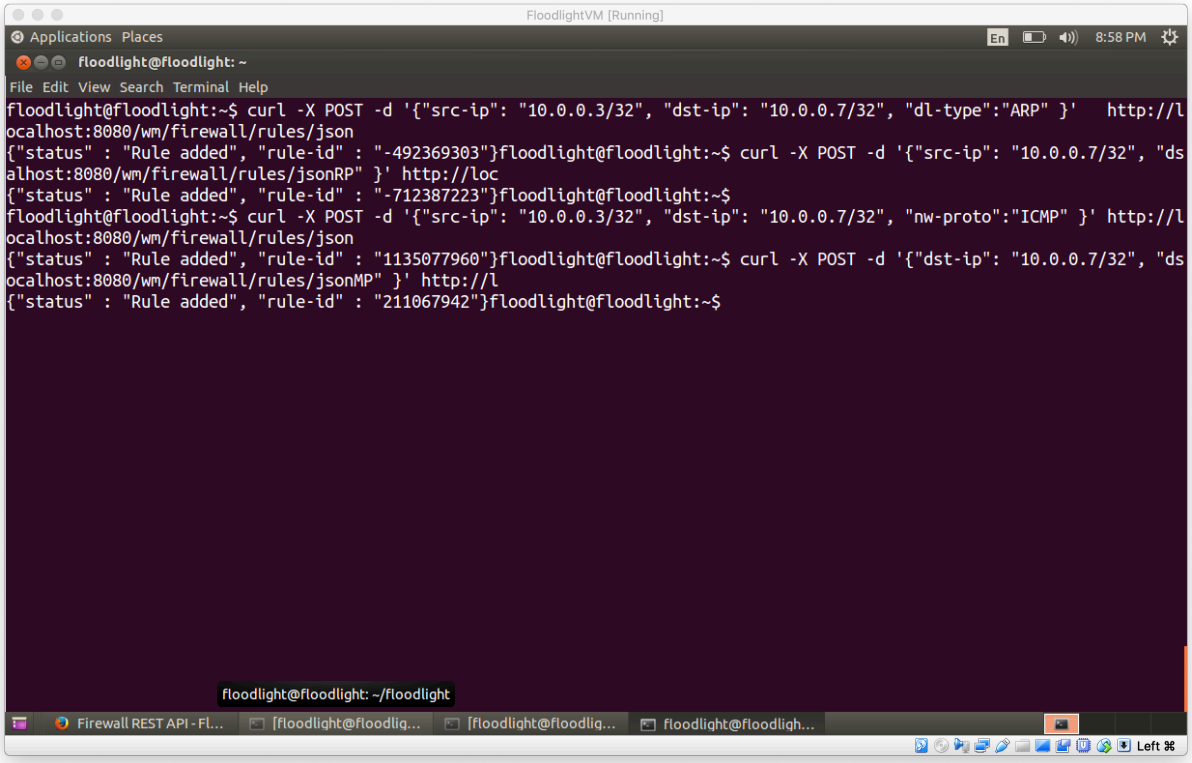
6. Adding an ALLOW rule for ping to work between IP hosts 10.0.0.3 and 10.0.0.7.

Command:

```
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
```

Screenshot:



7. Adding an ALLOW rule for UDP to work between IP hosts 10.0.0.4 and 10.0.0.10, and then blocking port 5010.

Command:

```
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
```

Screenshot: