

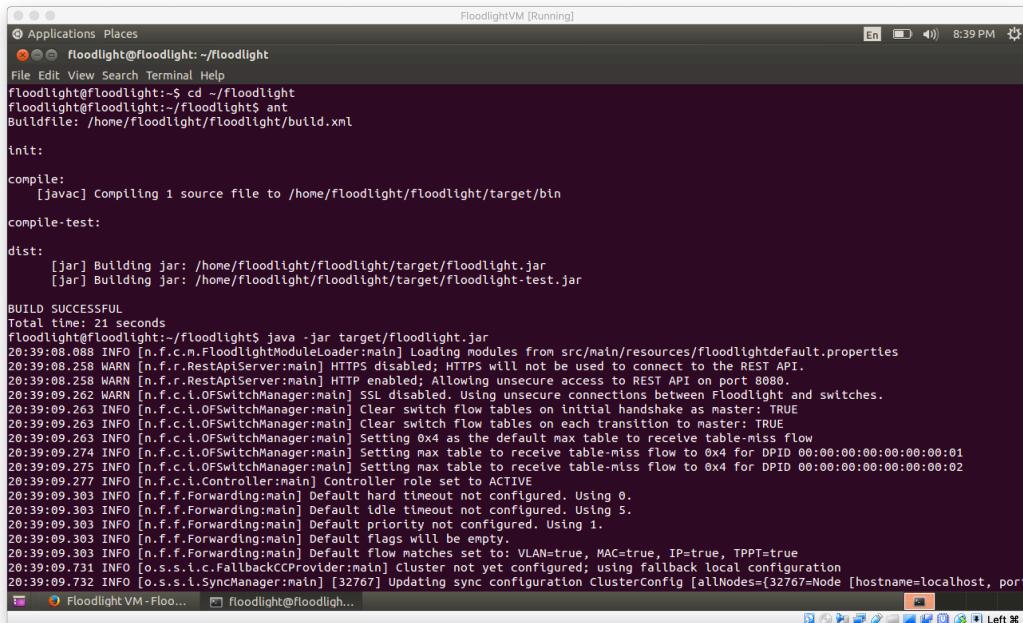
PROJECT 2: Floodlight Firewall App

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:

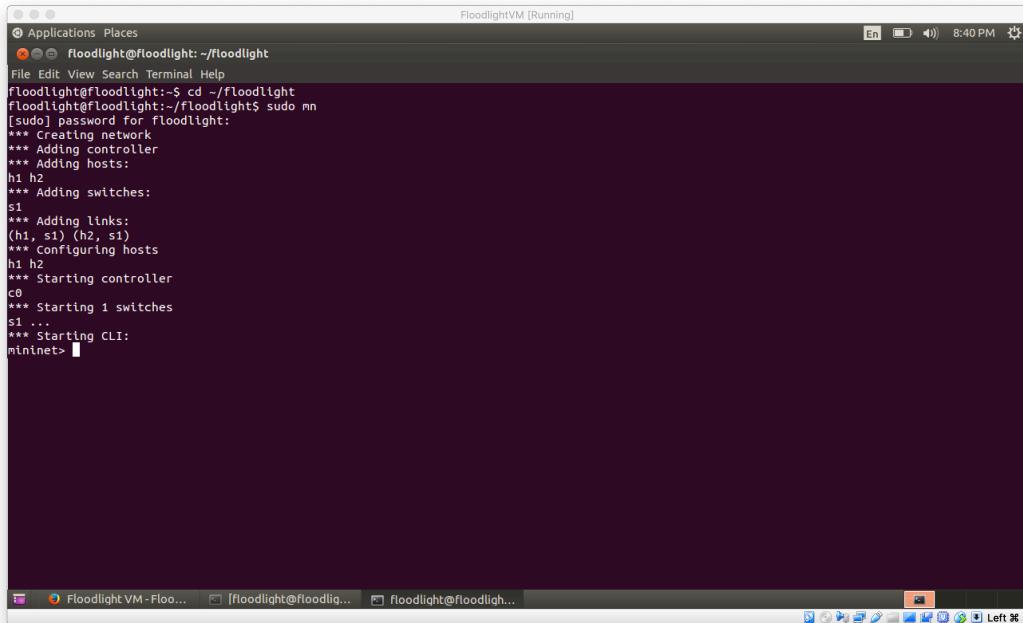


```
FloodlightVM [Running]
File Edit View Search Terminal Help
floodlight@floodlight:~$ cd ~/floodlight
floodlight@floodlight:~/floodlight$ ant
Buildfile: /home/floodlight/floodlight/build.xml

init:
compile:
[javac] Compiling 1 source file to /home/floodlight/floodlight/target/bin
compile-test:
dist:
[jar] Building jar: /home/floodlight/floodlight/target/floodlight.jar
[jar] Building jar: /home/floodlight/floodlight/target/floodlight-test.jar

BUILD SUCCESSFUL
Total time: 21 seconds
floodlight@floodlight:~/floodlight$ java -jar target/floodlight.jar
20:39:08.088 INFO [n.f.c.m.FloodlightModuleLoader:main] Loading modules from src/main/resources/floodlightdefault.properties
20:39:08.258 WARN [n.f.r.RestApiServer:main] HTTPS disabled; HTTPS will not be used to connect to the REST API.
20:39:08.258 WARN [n.f.r.RestApiServer:main] HTTP enabled; Allowing unsecure access to REST API on port 8080.
20:39:09.262 WARN [n.f.c.i.OFSwitchManager:main] SSL disabled. Using unsecure connections between Floodlight and switches.
20:39:09.263 INFO [n.f.c.i.OFSwitchManager:main] Clear switch flow tables on initial handshake as master: TRUE
20:39:09.263 INFO [n.f.c.i.OFSwitchManager:main] Clear switch flow tables on each transition to master: TRUE
20:39:09.263 INFO [n.f.c.i.OFSwitchManager:main] Setting 0x4 as the default max table to receive table-miss flow
20:39:09.274 INFO [n.f.c.i.OFSwitchManager:main] Setting max table to receive table-miss flow to 0x4 for DPID 00:00:00:00:00:00:00:01
20:39:09.275 INFO [n.f.c.i.OFSwitchManager:main] Setting max table to receive table-miss flow to 0x4 for DPID 00:00:00:00:00:00:00:02
20:39:09.277 INFO [n.f.c.i.Controller:main] Controller role set to ACTIVE
20:39:09.303 INFO [n.f.f.Forwarding:main] Default hard timeout not configured. Using 0.
20:39:09.303 INFO [n.f.f.Forwarding:main] Default idle timeout not configured. Using 5.
20:39:09.303 INFO [n.f.f.Forwarding:main] Default priority not configured. Using 1.
20:39:09.303 INFO [n.f.f.Forwarding:main] Default flags will be empty.
20:39:09.303 INFO [n.f.f.Forwarding:main] Default flow matches set to: VLAN=true, MAC=true, IP=true, TPPT=true
20:39:09.731 INFO [o.s.s.i.c.FallbackCCProvider:main] Cluster not yet configured; using fallback local configuration
20:39:09.732 INFO [o.s.s.i.SyncManager:main] [32767=Node [hostname=localhost, port=6653]] Updating sync configuration clusterConfig [allNodes={32767=Node [hostname=localhost, port=6653]}]
```

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



```
FloodlightVM [Running]
File Edit View Search Terminal Help
floodlight@floodlight:~$ cd ~/floodlight
floodlight@floodlight:~/floodlight$ sudo mn
[sudo] password for floodlight:
*** Creating network
*** Adding controller
*** Adding hosts:
h1 h2
*** Adding switches:
s1
*** Adding links:
(h1, s1) (h2, s1)
*** Configuring hosts
h1 h2
*** Starting controller
c0
*** Starting 1 switches
s1 ...
*** Starting CLI:
mininet>
```

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:

```
FloodlightVM [Running]
Applications Places
floodlight@floodlight:~ 
File Edit View Search Terminal Help
floodlight@floodlight:~$ 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
{"status": "Success! New rule added."}floodlight@floodlight:~$ 
Current workspace: "Workspace 1"

```

2. Listing all ACL rules

Command:

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

Screenshot:

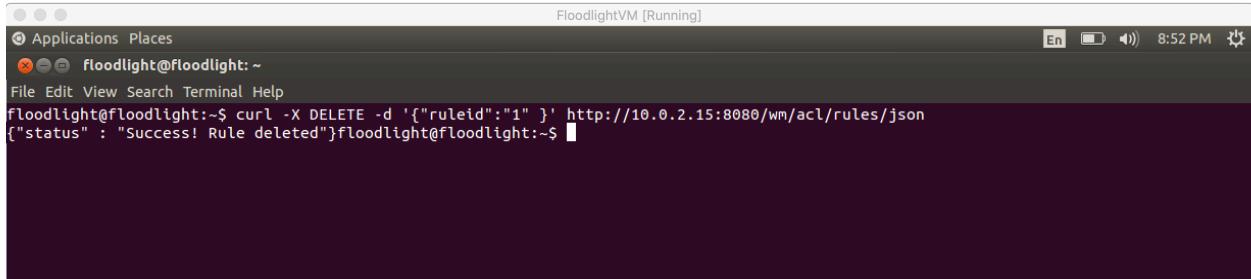
```
FloodlightVM [Running]
Applications Places
floodlight@floodlight:~ 
File Edit View Search Terminal Help
floodlight@floodlight:~$ curl http://10.0.2.15:8080/wm/acl/rules/json | python -mjson.tool
% Total    % Received % Xferd  Average Speed   Time   Time  Current
          0     0      0      0      0      0      0      0 --:--:-- --:--:-- --:--:-- 2317
[{"action": "DENY", "id": 1, "nw_dst": "10.0.0.2/32", "nw_dst_maskbits": 32, "nw_dst_prefix": 167772162, "nw_proto": 0, "nw_src": "10.0.0.1/32", "nw_src_maskbits": 32, "nw_src_prefix": 167772161, "tp_dst": 0}
]
floodlight@floodlight:~$ 
```

3. Remove an ACL rule:

Command:

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

Screenshot:



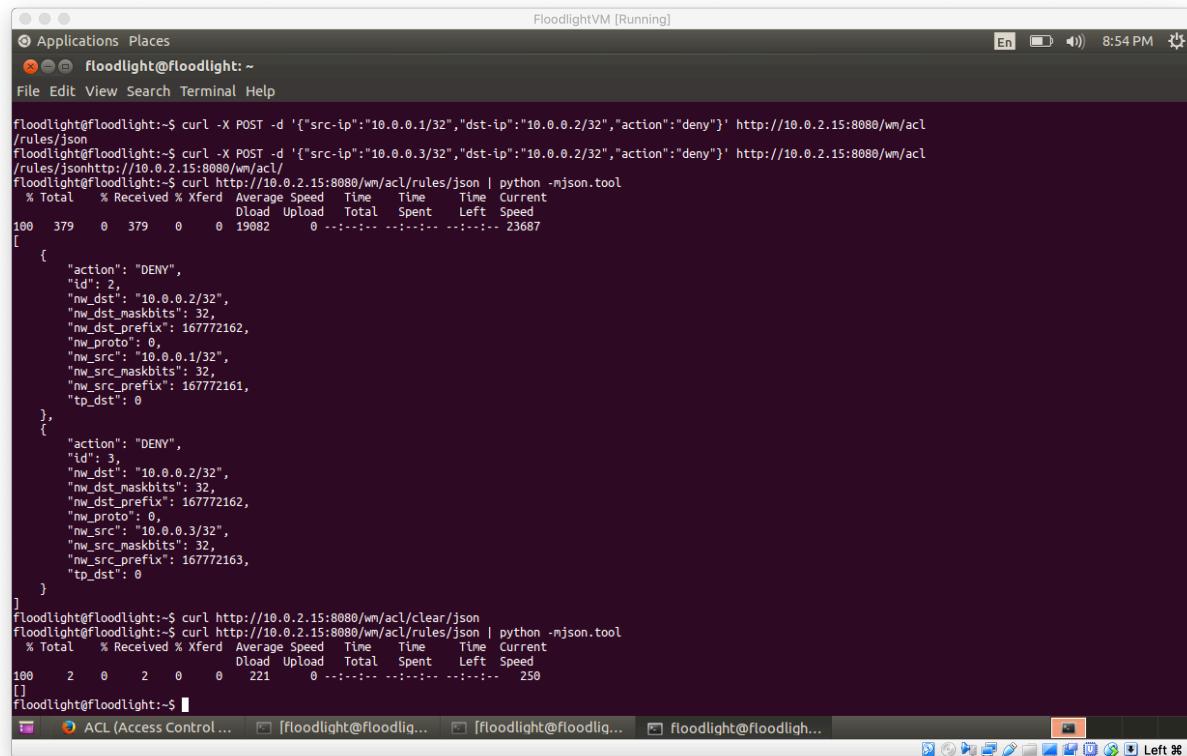
```
FloodlightVM [Running]
Applications Places
floodlight@floodlight: ~
File Edit View Search Terminal Help
floodlight@floodlight:~$ curl -X DELETE -d '{"ruleid":"1"}' http://10.0.2.15:8080/wm/acl/rules/json
{"status" : "Success! Rule deleted"}floodlight@floodlight:~$
```

4. Remove all ACL rules:

Command:

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

Screenshot:



```
FloodlightVM [Running]
Applications Places
floodlight@floodlight: ~
File Edit View Search Terminal Help
floodlight@floodlight:~$ 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
floodlight@floodlight:~$ curl -X POST -d '{"src-ip":"10.0.0.3/32","dst-ip":"10.0.0.2/32","action":"deny"}' http://10.0.2.15:8080/wm/acl/rules/json
floodlight@floodlight:~$ curl http://10.0.2.15:8080/wm/acl/rules/json | python -mjson.tool
% Total    % Received % Xferd  Average Speed   Time   Time Current
          Dload Upload Total Spent   Left Speed
100  379     0  379     0      0  19082   0 ---:--- ---:--- 23687
[
  {
    "action": "DENY",
    "id": 2,
    "nw_dst": "10.0.0.2/32",
    "nw_dst_maskbits": 32,
    "nw_dst_prefix": 167772162,
    "nw_proto": 0,
    "nw_src": "10.0.0.1/32",
    "nw_src_maskbits": 32,
    "nw_src_prefix": 167772161,
    "tp_dst": 0
  },
  {
    "action": "DENY",
    "id": 3,
    "nw_dst": "10.0.0.2/32",
    "nw_dst_maskbits": 32,
    "nw_dst_prefix": 167772162,
    "nw_proto": 0,
    "nw_src": "10.0.0.3/32",
    "nw_src_maskbits": 32,
    "nw_src_prefix": 167772163,
    "tp_dst": 0
  }
]
floodlight@floodlight:~$ curl http://10.0.2.15:8080/wm/acl/clear/json
floodlight@floodlight:~$ curl http://10.0.2.15:8080/wm/acl/rules/json | python -mjson.tool
% Total    % Received % Xferd  Average Speed   Time   Time Current
          Dload Upload Total Spent   Left Speed
100      2     0      2     0      0  221   0 ---:--- ---:--- 250
[]
floodlight@floodlight:~$
```

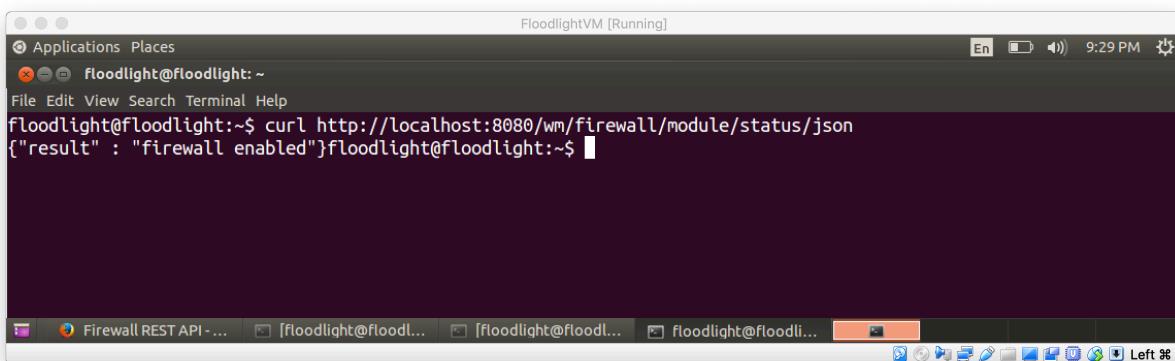
Firewall REST API

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

Command:

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

Screenshot:



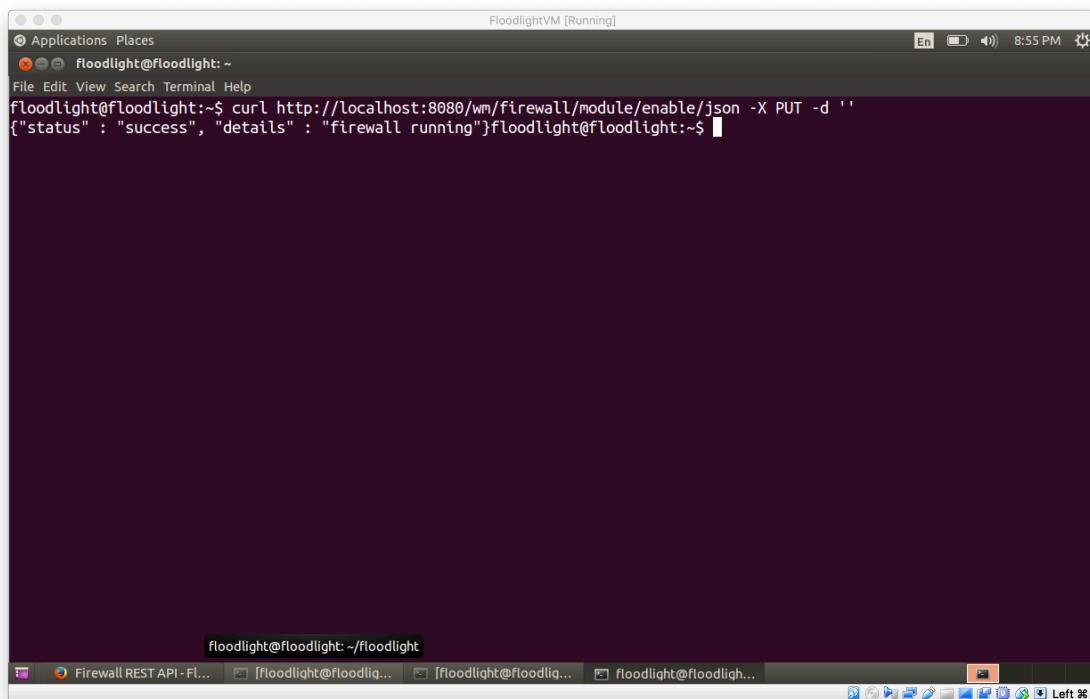
```
FloodlightVM [Running]
Applications Places
En 9:29 PM
floodlight@floodlight: ~
File Edit View Search Terminal Help
floodlight@floodlight:~$ curl http://localhost:8080/wm/firewall/module/status/json
{"result" : "firewall enabled"}floodlight@floodlight:~$ 
```

2. Enable the firewall.

Command:

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

Screenshot:



```
FloodlightVM [Running]
En 8:55 PM
Applications Places
floodlight@floodlight: ~
File Edit View Search Terminal Help
floodlight@floodlight:~$ curl http://localhost:8080/wm/firewall/module/enable/json -X PUT -d ''
{"status" : "success", "details" : "firewall running"}floodlight@floodlight:~$ 
```

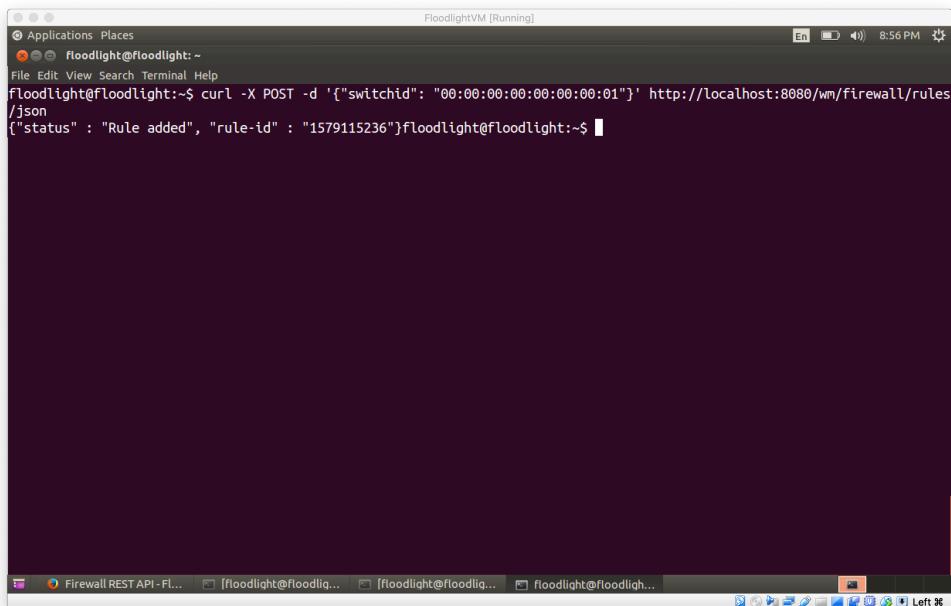
3. Adding an ALLOW rule for all flows to pass through switch

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:



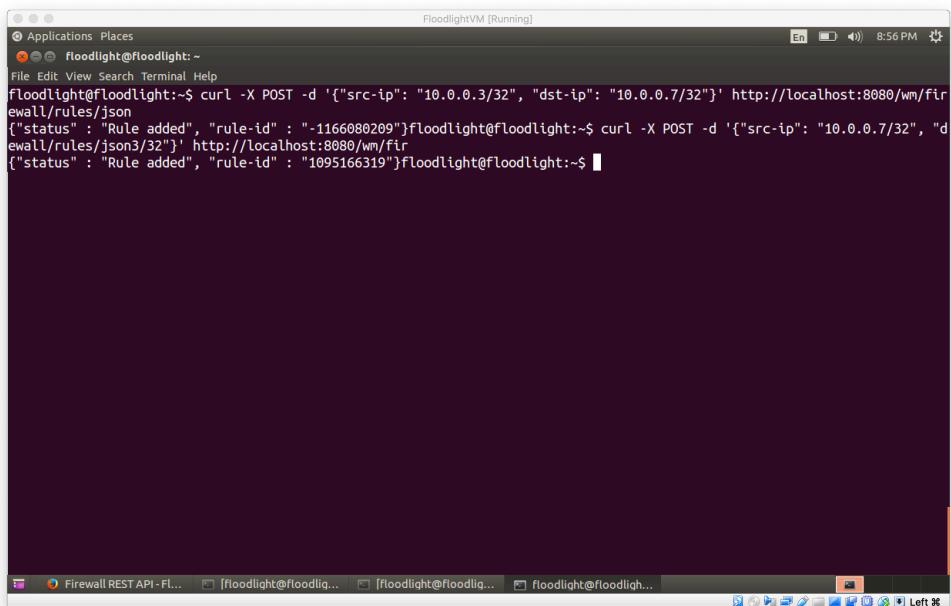
The screenshot shows a terminal window titled "FloodlightVM [Running]". The terminal session starts with the prompt "floodlight@floodlight:~". The user runs the command "curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:01"}' http://localhost:8080/wm/firewall/rules/json". The terminal then displays the JSON response: {"status": "Rule added", "rule-id": "1579115236"}. The terminal window has a dark background and white text. The title bar includes the window name and the current time, 8:56 PM. The bottom of the window shows the standard Linux desktop interface with icons for various applications.

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:



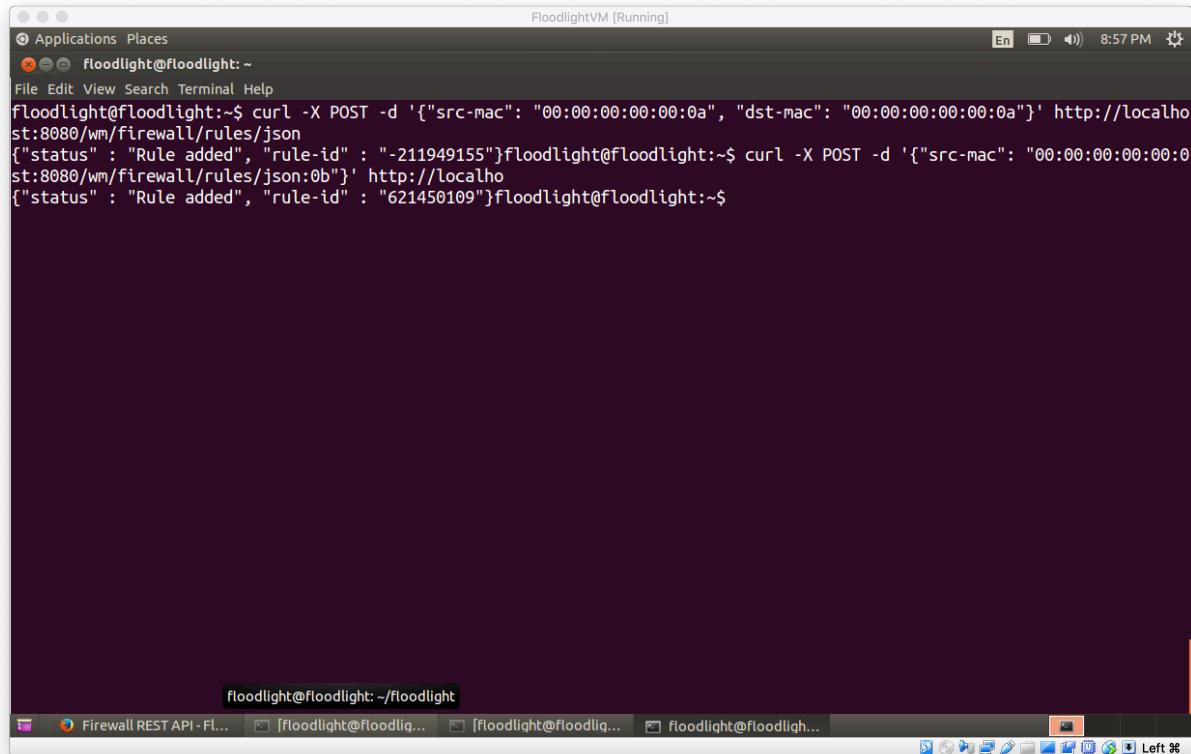
The screenshot shows a terminal window titled "FloodlightVM [Running]". The terminal session starts with the prompt "floodlight@floodlight:~". The user runs two commands, one for each direction of traffic. The first command is "curl -X POST -d '{"src-ip": "10.0.0.3/32", "dst-ip": "10.0.0.7/32"}' http://localhost:8080/wm/firewall/rules/json", resulting in a rule ID of "-1166080209". The second command is "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", resulting in a rule ID of "1095166319". Both commands return the message {"status": "Rule added"}. The terminal window has a dark background and white text. The title bar includes the window name and the current time, 8:56 PM. The bottom of the window shows the standard Linux desktop interface with icons for various applications.

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:



The screenshot shows a terminal window titled "FloodlightVM [Running]". The window contains the following text:

```
FloodlightVM [Running]  
Applications Places  
floodlight@floodlight: ~  
File Edit View Search Terminal Help  
floodlight@floodlight:~$ 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  
{"status" : "Rule added", "rule-id" : "-211949155"}floodlight@floodlight:~$ 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:  
{"status" : "Rule added", "rule-id" : "621450109"}floodlight@floodlight:~$
```

The terminal window has a dark background and light-colored text. The title bar says "FloodlightVM [Running]". The window title is "floodlight@floodlight: ~". The status bar at the bottom shows "floodlight@floodlight: ~/floodlight" and several other tabs are visible in the background.

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", "src-ip": "10.0.0.3/32",  
"nw Proto": "ICMP"}' http://localhost:8080/wm/firewall/rules/json
```

Screenshot:

```
FloodlightVM [Running]
File Edit View Search Terminal Help
floodlight@floodlight:~$ 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
{"status": "Rule added", "rule-id": "-492369303"}floodlight@floodlight:~$ 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
{"status": "Rule added", "rule-id": "-712387223"}floodlight@floodlight:~$ 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
{"status": "Rule added", "rule-id": "1135077960"}floodlight@floodlight:~$ curl -X POST -d '{"dst-ip": "10.0.0.7/32", "src-ip": "10.0.0.3/32", "nw Proto": "ICMP"}' http://localhost:8080/wm/firewall/rules/json
{"status": "Rule added", "rule-id": "211067942"}floodlight@floodlight:~$
```

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.

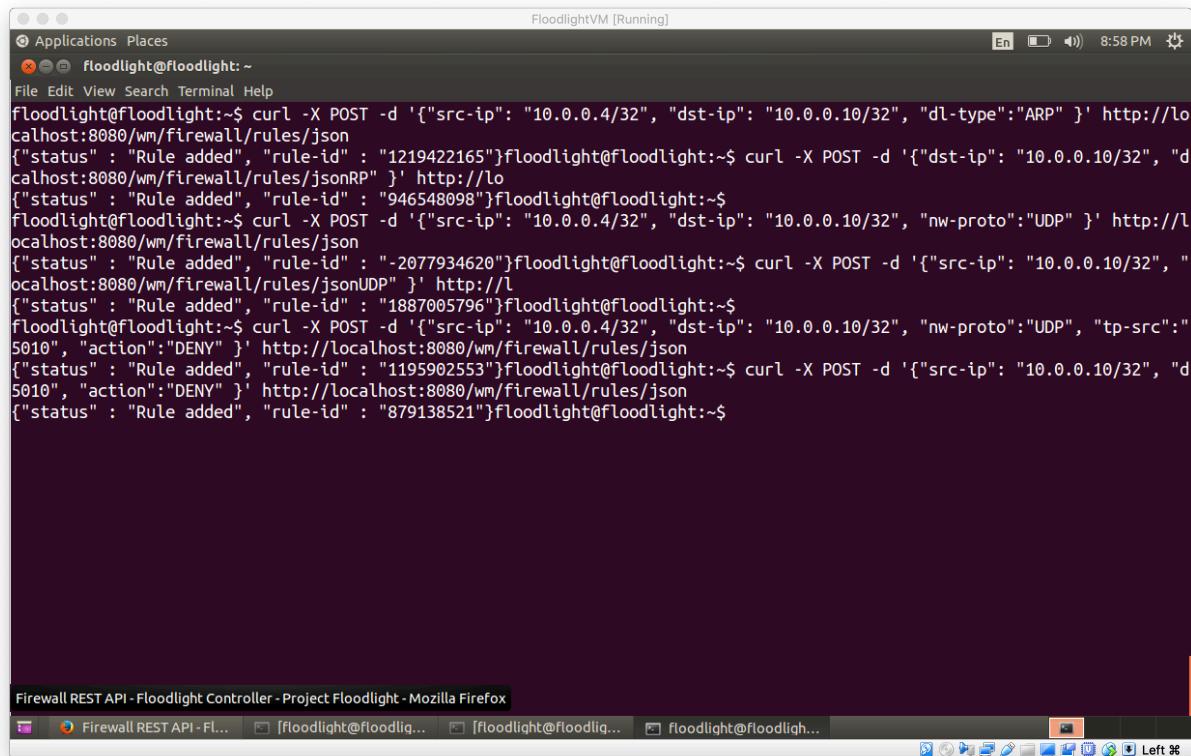
Command:

```
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", "src-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:



The screenshot shows a terminal window titled 'FloodlightVM [Running]' with a dark theme. The user is running several curl commands to manage firewall rules on a host with IP 10.0.0.4. The commands are as follows:

```
floodlight@floodlight:~$ 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
{"status": "Rule added", "rule-id": "1219422165"}floodlight@floodlight:~$ curl -X POST -d '{"dst-ip": "10.0.0.10/32", "src-ip": "10.0.0.4/32", "dl-type": "ARP"}' http://localhost:8080/wm/firewall/rules/jsonRP"
{"status": "Rule added", "rule-id": "946548098"}floodlight@floodlight:~$ 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
{"status": "Rule added", "rule-id": "-2077934620"}floodlight@floodlight:~$ 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
{"status": "Rule added", "rule-id": "1887005796"}floodlight@floodlight:~$ 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
{"status": "Rule added", "rule-id": "1195902553"}floodlight@floodlight:~$ 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
{"status": "Rule added", "rule-id": "879138521"}floodlight@floodlight:~$
```