

CPSC 8570: SECURITY IN ADVANCED NETWORKING TECHNOLOGIES

PROJECT 2

STATELESS FIREWALL USING FLOODLIGHT

Description:

In this project, we are asked to setup FloodLight, which is used to build ACL Stateless Firewall System. And then run the curl examples on Floodlight to add ACL rules to the Firewall

Initial Setup of FloodLight:

1. The Oracle VirtualBox VM was downloaded from <https://www.virtualbox.org/wiki/Downloads> and installed it on my Windows machine
2. The FloodLight VM was downloaded from <https://floodlight.atlassian.net/wiki/spaces/floodlightcontroller/pages/8650780/Floodlight+VM>
3. Once the download was complete, the 'floodlight-vm.zip' was extracted.
4. Floodlight VM was setup on VirtualBox using the 'Floodlight-v1.1+Mininet.vmdk' which was extracted in the previous step.
5. The username and password are both 'floodlight'.
6. Java 8 was updated using the following commands

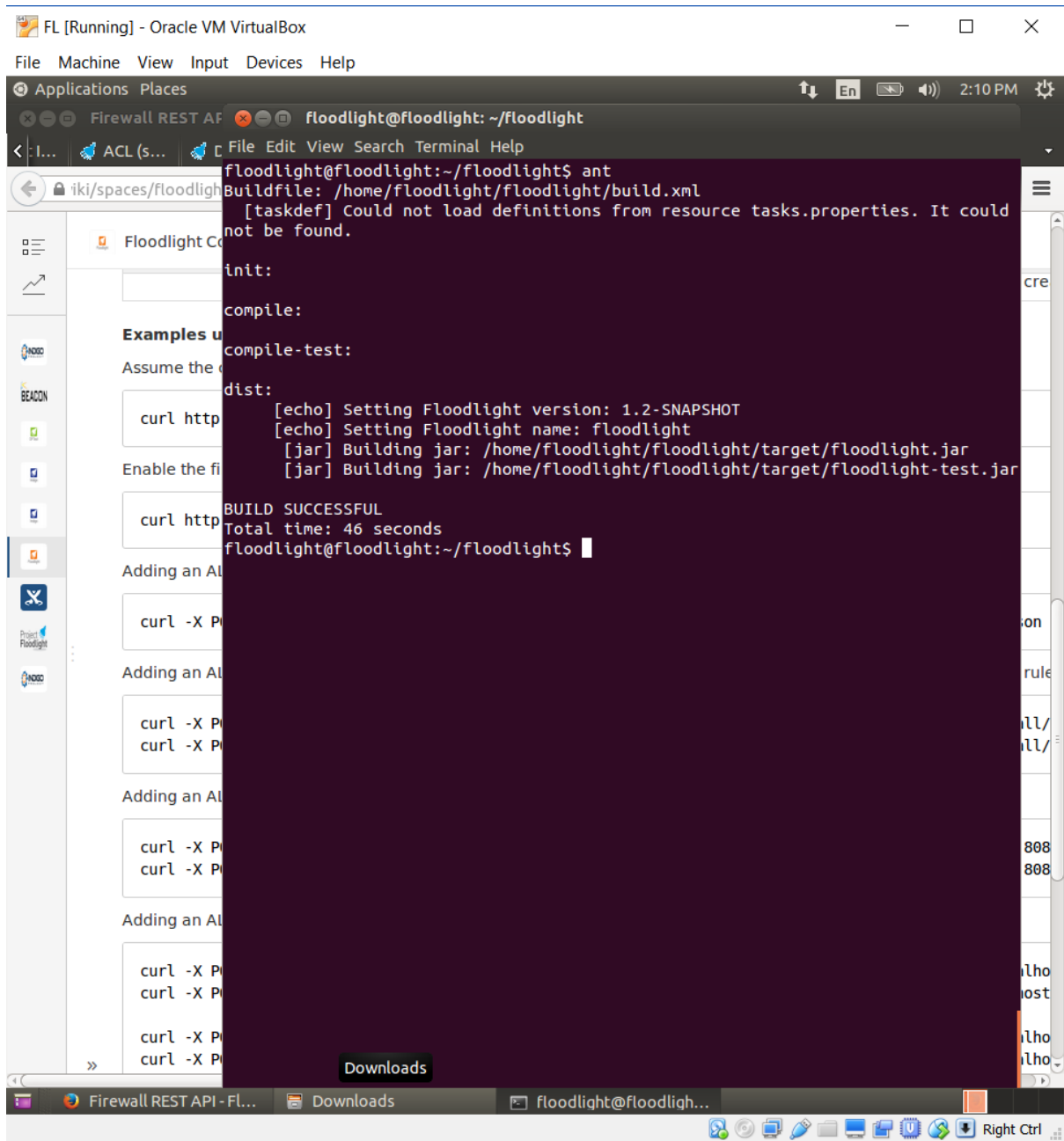
```
sudo add-apt-repository ppa:webupd8team/java
sudo apt-get update
sudo apt-get install oracle-java8-installer
```
7. To update Eclipse, it is downloaded from its official website – <https://eclipse.org/downloads/> and installed using the following command

```
cd /opt/ && sudo tar -zxvf ~/Downloads/eclipse-*.tar.gz
```
8. Floodlight was updated using the following commands

```
cd ~/floodlight
git pull origin master
git submodule init
git submodule update
```

Building and running FloodLight:

1. Floodlight was built command – *ant*



The screenshot shows a VirtualBox window titled "FL [Running] - Oracle VM VirtualBox". Inside the window, there is a terminal window titled "floodlight@floodlight: ~/floodlight". The terminal shows the following commands and output:

```
floodlight@floodlight:~/floodlight$ ant
Buildfile: /home/floodlight/floodlight/build.xml
[taskdef] Could not load definitions from resource tasks.properties. It could
not be found.

init:

compile:

compile-test:

dist:
[echo] Setting Floodlight version: 1.2-SNAPSHOT
[echo] Setting Floodlight name: floodlight
[jar] Building jar: /home/floodlight/floodlight/target/floodlight.jar
[jar] Building jar: /home/floodlight/floodlight/target/floodlight-test.jar

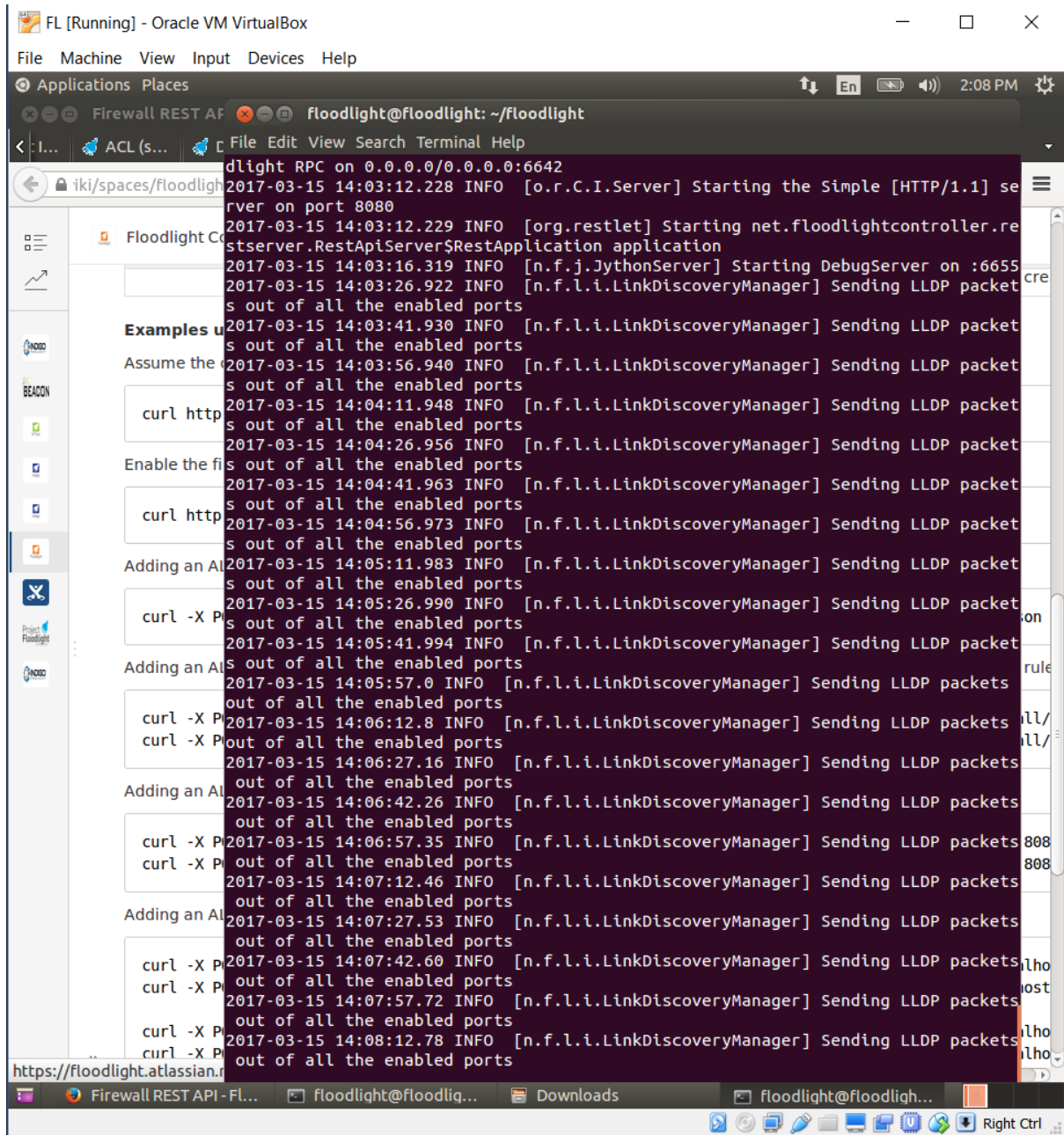
BUILD SUCCESSFUL
Total time: 46 seconds
floodlight@floodlight:~/floodlight$
```

The background of the terminal window shows a web browser with the URL "iki/spaces/floodlight" and a sidebar with various icons and a "Downloads" button.

- The floodlight.jar file, which is present in the floodlight/target folder was run using the command –

java -jar target/floodlight.jar

It enables all the ports and starts sending LLDP packets from all the enabled ports as shown in the screen dump below.



The screenshot shows a terminal window titled "floodlight@floodlight: ~/floodlight". The terminal output displays the following logs:

```
floodlight RPC on 0.0.0.0/0.0.0.0:6642
2017-03-15 14:03:12.228 INFO [o.r.C.I.Server] Starting the Simple [HTTP/1.1] se
server on port 8080
2017-03-15 14:03:12.229 INFO [org.restlet] Starting net.floodlightcontroller.re
stserver.RestApiServer$RestApplication application
2017-03-15 14:03:16.319 INFO [n.f.j.JythonServer] Starting DebugServer on :6655
2017-03-15 14:03:26.922 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 14:03:41.930 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 14:03:56.940 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 14:04:11.948 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 14:04:26.956 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 14:04:41.963 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 14:04:56.973 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 14:05:11.983 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 14:05:26.990 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 14:05:41.994 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 14:05:57.0 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packets
out of all the enabled ports
2017-03-15 14:06:12.8 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packets
out of all the enabled ports
2017-03-15 14:06:27.16 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packets
out of all the enabled ports
2017-03-15 14:06:42.26 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packets
out of all the enabled ports
2017-03-15 14:06:57.35 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packets
out of all the enabled ports
2017-03-15 14:07:12.46 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packets
out of all the enabled ports
2017-03-15 14:07:27.53 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packets
out of all the enabled ports
2017-03-15 14:07:42.60 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packets
out of all the enabled ports
2017-03-15 14:07:57.72 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packets
out of all the enabled ports
2017-03-15 14:08:12.78 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packets
out of all the enabled ports
```

Examples using curl:

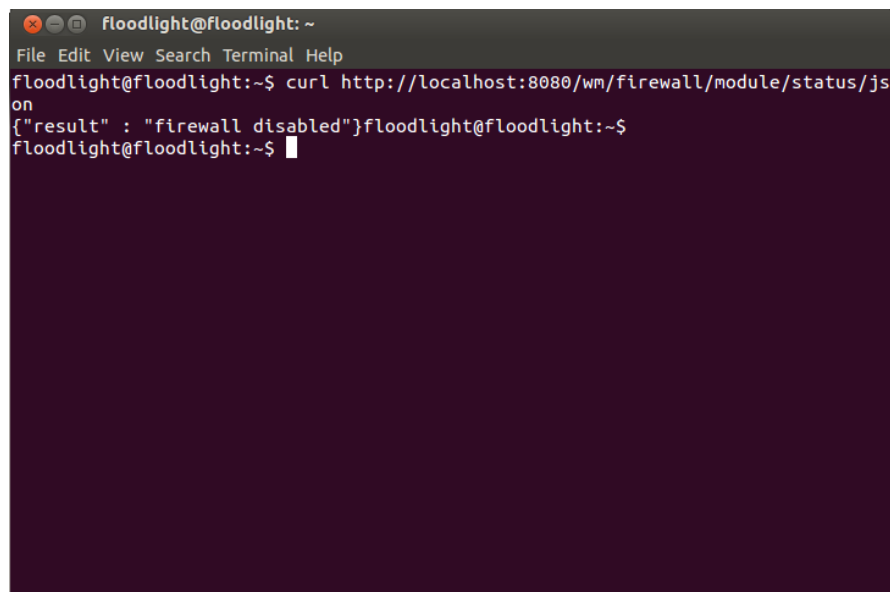
I opened a new terminal for running the curl examples, while the floodlight.jar was running on the other terminal to keep all the ports open.

1. To check whether the firewall is enabled or not:

To check whether the firewall is enabled or not, I ran the following command.

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

Since, we are yet to start the firewall, it gives back a message saying that the firewall is disabled.



```
floodlight@floodlight: ~  
File Edit View Search Terminal Help  
floodlight@floodlight:~$ curl http://localhost:8080/wm/firewall/module/status/json  
{"result" : "firewall disabled"}floodlight@floodlight:~$  
floodlight@floodlight:~$
```

2. Enable the Firewall

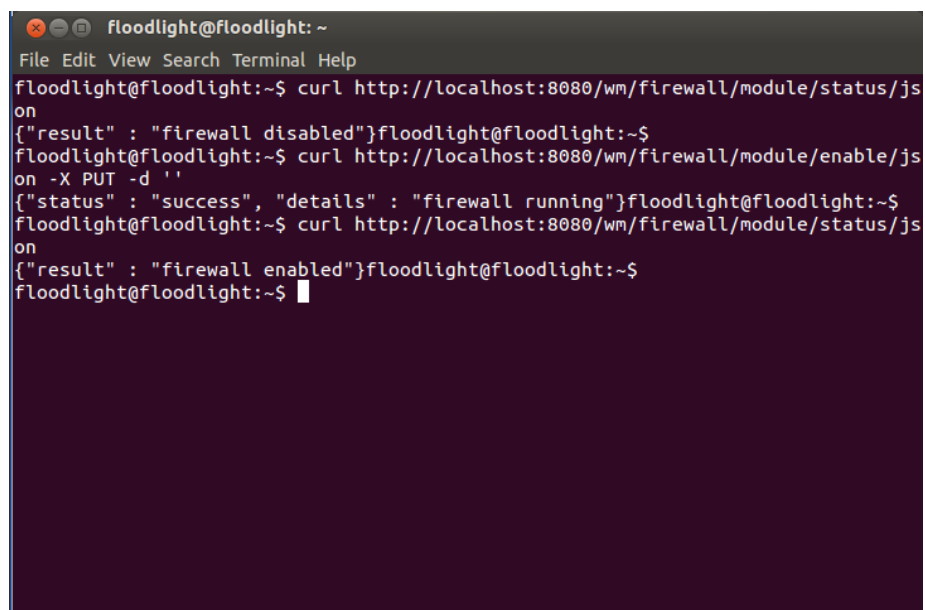
By default, firewall denies all traffic unless an explicit ALLOW rule is created.

The following command is used to enable the firewall

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

After enabling the firewall, again we check the status of the firewall using

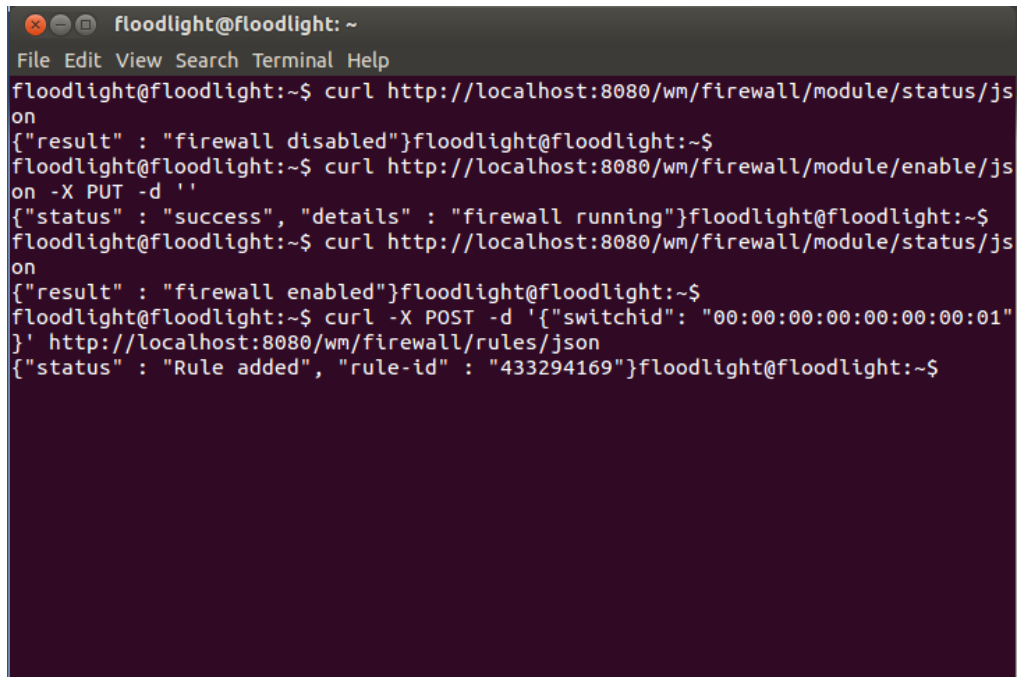
```
curl http://localhost:8080/wm/firewall/module/status/json
```



```
floodlight@floodlight: ~  
File Edit View Search Terminal Help  
floodlight@floodlight:~$ curl http://localhost:8080/wm/firewall/module/status/json  
{"result" : "firewall disabled"}floodlight@floodlight:~$  
floodlight@floodlight:~$ curl http://localhost:8080/wm/firewall/module/enable/json -X PUT -d ''  
{"status" : "success", "details" : "firewall running"}floodlight@floodlight:~$  
floodlight@floodlight:~$ curl http://localhost:8080/wm/firewall/module/status/json  
{"result" : "firewall enabled"}floodlight@floodlight:~$  
floodlight@floodlight:~$
```

```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
ion ClusterConfig [allNodes={1=Node [hostname=192.168.1.100, port=6642, nodeId=1
, domainId=1], 2=Node [hostname=192.168.1.100, port=6643, nodeId=2, domainId=1]}
, authScheme=CHALLENGE_RESPONSE, keyStorePath=/etc/floodlight/key2.jceks, keySto
rePassword is set]
2017-03-15 16:16:26.532 INFO [o.s.s.i.r.RPCService] Listening for internal floo
dlight RPC on 0.0.0.0/0.0.0.0:6642
2017-03-15 16:16:26.798 INFO [o.r.C.I.Server] Starting the Simple [HTTP/1.1] se
rver on port 8080
2017-03-15 16:16:26.803 INFO [org.restlet] Starting net.floodlightcontroller.re
stserver.RestApiServer$RestApplication application
2017-03-15 16:16:30.575 INFO [n.f.j.JythonServer] Starting DebugServer on :6655
2017-03-15 16:16:41.610 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:16:56.617 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:17:11.625 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:17:26.636 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:17:41.643 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:17:56.654 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:18:11.663 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:18:26.673 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:18:41.686 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:18:56.695 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:19:11.703 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:19:26.712 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:19:41.723 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:19:49.879 INFO [n.f.f.Firewall] Setting firewall to true
2017-03-15 16:19:56.732 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:20:11.744 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2017-03-15 16:20:26.751 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
```

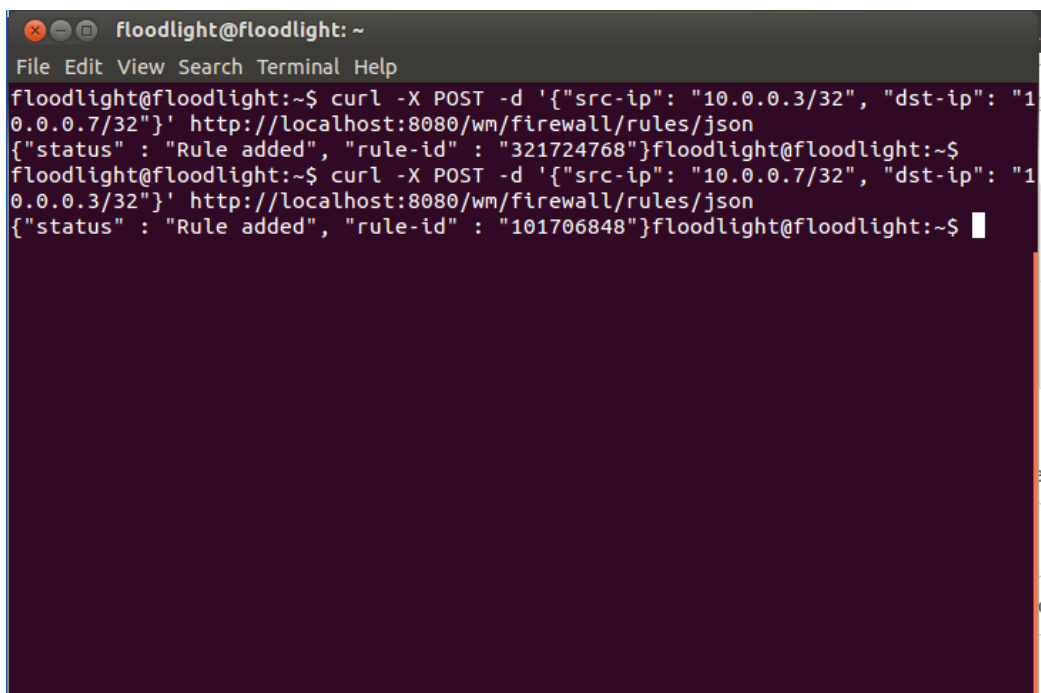
3. Adding an ALLOW rule for all flows to pass through switch 00:00:00:00:00:00:01.
`curl -X POST -d '{"switchid": "00:00:00:00:00:00:01"}' http://localhost:8080/wm/firewall/rules/json`



```
floodlight@floodlight: ~  
File Edit View Search Terminal Help  
floodlight@floodlight:~$ curl http://localhost:8080/wm/firewall/module/status/json  
{ "result" : "firewall disabled" }floodlight@floodlight:~$  
floodlight@floodlight:~$ curl http://localhost:8080/wm/firewall/module/enable/json -X PUT -d ''  
{ "status" : "success", "details" : "firewall running" }floodlight@floodlight:~$  
floodlight@floodlight:~$ curl http://localhost:8080/wm/firewall/module/status/json  
{ "result" : "firewall enabled" }floodlight@floodlight:~$  
floodlight@floodlight:~$ curl -X POST -d '{"switchid": "00:00:00:00:00:00:01"}' http://localhost:8080/wm/firewall/rules/json  
{ "status" : "Rule added", "rule-id" : "433294169" }floodlight@floodlight:~$
```

4. Adding an ALLOW rule for all flows between IP host 10.0.0.3 and host 10.0.1.5. Not specifying an action implies ALLOW rule.
`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`

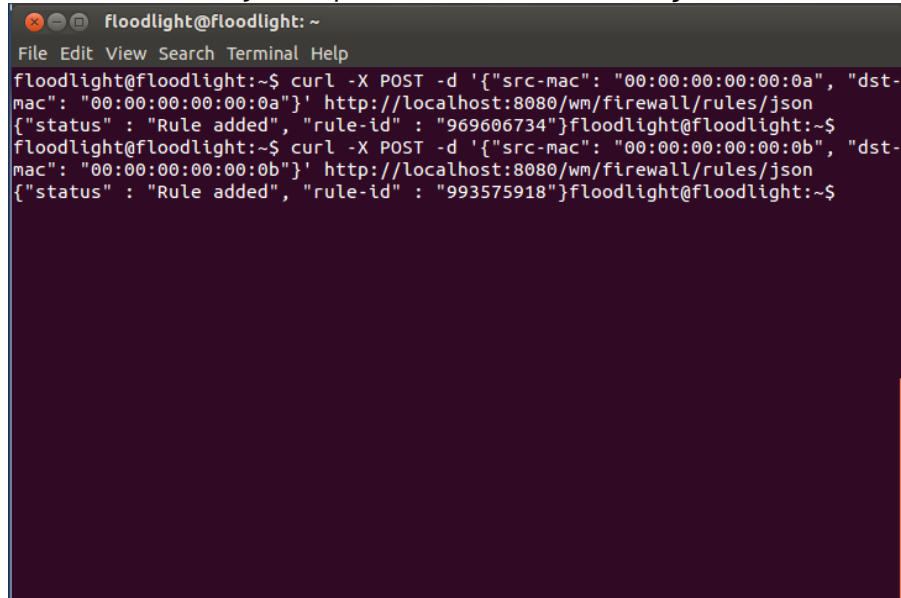
`curl -X POST -d '{"src-ip": "10.0.0.7/32", "dst-ip": "10.0.0.3/32"}' http://localhost:8080/wm/firewall/rules/json`



```
floodlight@floodlight: ~  
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"}' http://localhost:8080/wm/firewall/rules/json  
{ "status" : "Rule added", "rule-id" : "321724768" }floodlight@floodlight:~$  
floodlight@floodlight:~$ 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  
{ "status" : "Rule added", "rule-id" : "101706848" }floodlight@floodlight:~$
```

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

```
curl -X POST -d '{"src-mac": "00:00:00:00:00:0a", "dst-mac": "00:00:00:00:00:0b"}' 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
```

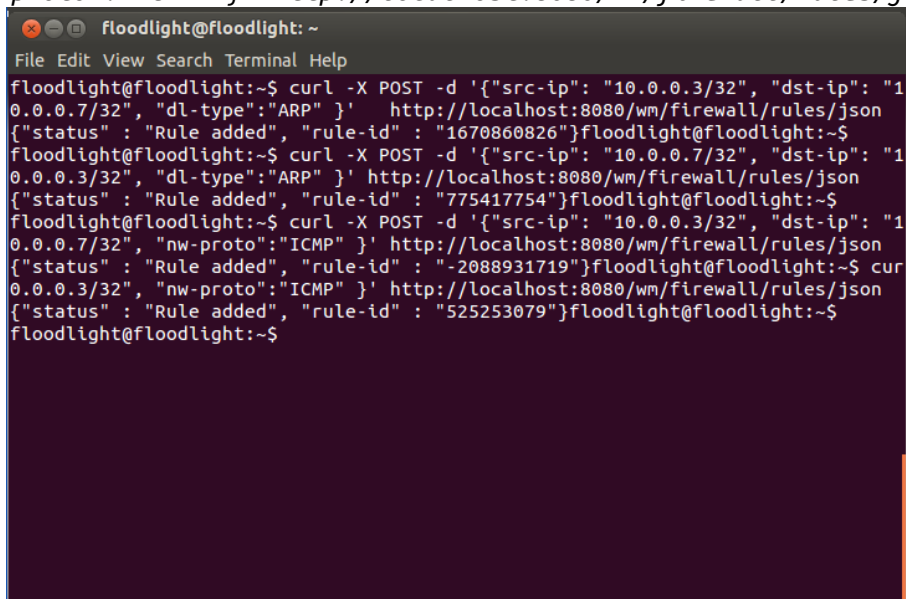


```
floodlight@floodlight: ~
File Edit View Search Terminal Help
floodlight@floodlight:~$ curl -X POST -d '{"src-mac": "00:00:00:00:00:0a", "dst-mac": "00:00:00:00:00:0a"}' http://localhost:8080/wm/firewall/rules/json
{"status": "Rule added", "rule-id": "969606734"}floodlight@floodlight:~$
floodlight@floodlight:~$ 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": "993575918"}floodlight@floodlight:~$
```

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

```
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
```



```
floodlight@floodlight: ~
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": "1670860826"}floodlight@floodlight:~$
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": "775417754"}floodlight@floodlight:~$
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": "-2088931719"}floodlight@floodlight:~$
floodlight@floodlight:~$ 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
{"status": "Rule added", "rule-id": "525253079"}floodlight@floodlight:~$
floodlight@floodlight:~$
```


7. Adding 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.

```
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
```

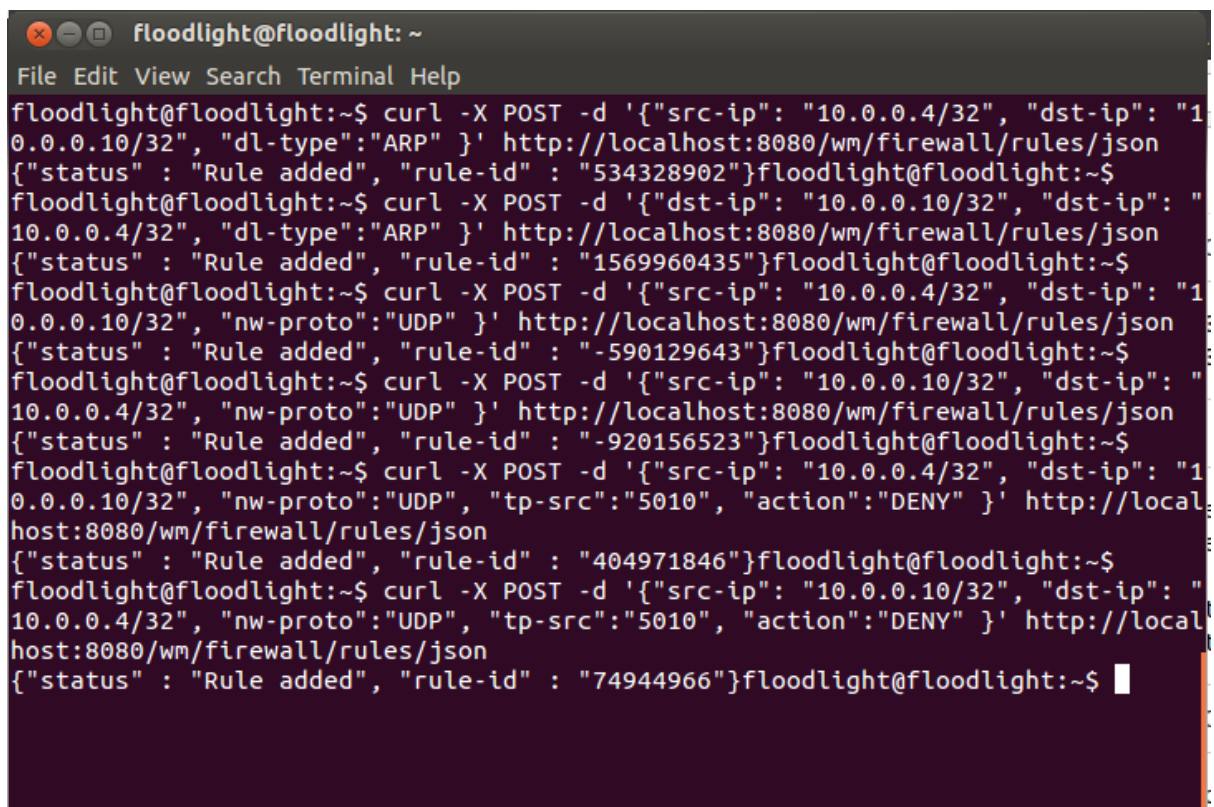
```
curl -X POST -d '{"dst-ip": "10.0.0.10/32", "dst-ip": "10.0.0.4/32",  
"dl-type": "ARP" }' http://localhost:8080/wm/firewall/rules/json
```

```
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
```

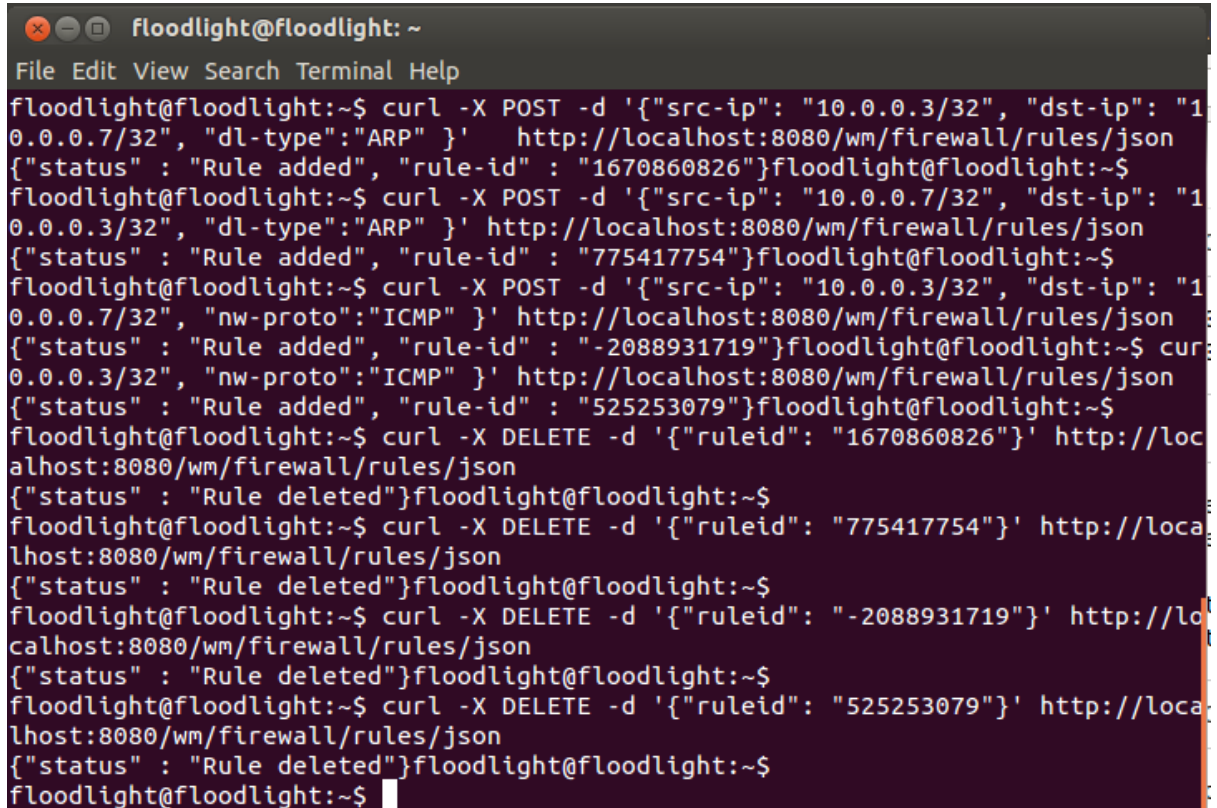
```
curl -X POST -d '{"src-ip": "10.0.0.10/32", "dst-ip": "10.0.0.4/32",  
"nw-proto": "UDP", "tp-src": "5010", "action": "DENY"  
}' http://localhost:8080/wm/firewall/rules/json
```



```
floodlight@floodlight: ~  
File Edit View Search Terminal Help  
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": "534328902"}floodlight@floodlight:~$  
floodlight@floodlight:~$ 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  
{"status": "Rule added", "rule-id": "1569960435"}floodlight@floodlight:~$  
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": "-590129643"}floodlight@floodlight:~$  
floodlight@floodlight:~$ 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  
{"status": "Rule added", "rule-id": "-920156523"}floodlight@floodlight:~$  
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": "404971846"}floodlight@floodlight:~$  
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": "74944966"}floodlight@floodlight:~$
```


8. After every test case, we delete the rule using the command
- ```
curl -X DELETE -d '{"ruleid":"- *****"}'
http://localhost:8080/wm/firewall/rules/json
```

For example: To delete all the rules added in example 7, we use

A terminal window titled 'floodlight@floodlight: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows a series of curl commands and their JSON responses. The first four commands are POST requests to add rules with specific parameters (src-ip, dst-ip, dl-type, nw-proto). The next four commands are DELETE requests to remove the rules by their rule-id. The responses for the DELETE requests are '{"status": "Rule deleted"}'.

```
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": "1670860826"}floodlight@floodlight:~$
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": "775417754"}floodlight@floodlight:~$
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": "-2088931719"}floodlight@floodlight:~$ curl -X POST -d '{"src-ip": "10.0.0.3/32", "nw-proto": "ICMP" }' http://localhost:8080/wm/firewall/rules/json
{"status": "Rule added", "rule-id": "525253079"}floodlight@floodlight:~$
floodlight@floodlight:~$ curl -X DELETE -d '{"ruleid": "1670860826"}' http://localhost:8080/wm/firewall/rules/json
{"status": "Rule deleted"}floodlight@floodlight:~$
floodlight@floodlight:~$ curl -X DELETE -d '{"ruleid": "775417754"}' http://localhost:8080/wm/firewall/rules/json
{"status": "Rule deleted"}floodlight@floodlight:~$
floodlight@floodlight:~$ curl -X DELETE -d '{"ruleid": "-2088931719"}' http://localhost:8080/wm/firewall/rules/json
{"status": "Rule deleted"}floodlight@floodlight:~$
floodlight@floodlight:~$ curl -X DELETE -d '{"ruleid": "525253079"}' http://localhost:8080/wm/firewall/rules/json
{"status": "Rule deleted"}floodlight@floodlight:~$
floodlight@floodlight:~$
```