

LAB PROJECT 2: Floodlight Firewall App

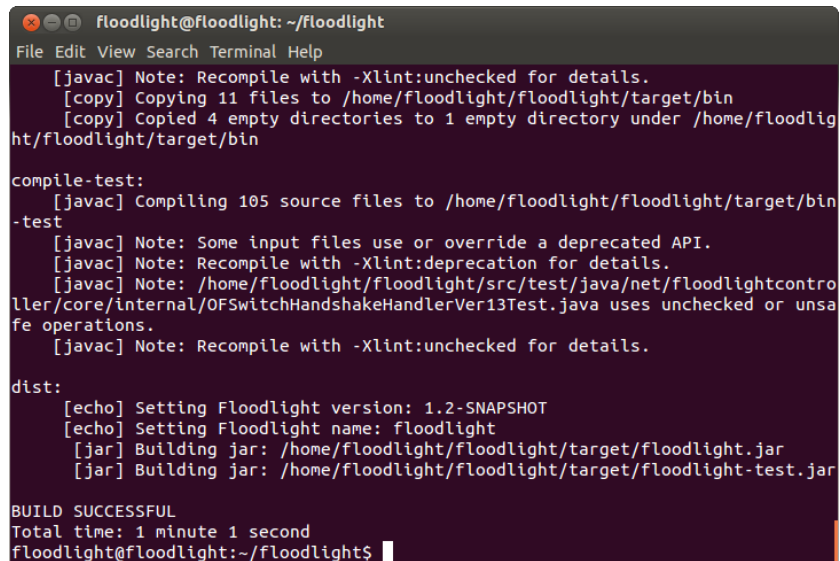
Kushal Hebbar | C13031425 | khebbar@g.clemson.edu

- ❖ Build SDN environment, enable firewall application (ACL REST API) and test (Firewall REST API)
- ❖ Provide screenshots in your report when you test "Examples using curl"

Download and install Oracle VirtualBox from <https://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html>

Next, download the pre-loaded image of Floodlight VM from <http://www.projectfloodlight.org/download/>

- Load the downloaded floodlight image into VirtualBox
- Run the following command
git clone git://github.com/floodlight/floodlight.git
- cd into the floodlight folder: **cd floodlight**
- Execute **sudo apt-get update** to update all the packages cloned from github
- Execute **sudo apt-get install curl** to install ant which will be used to build the solution
- Install Oracle Java 8 for Ubuntu
sudo add-apt-repository ppa:webupd8team/java
sudo apt-get update
sudo apt-get install oracle-java8-installer
- Set Oracle Java 8 as default
sudo apt-get install oracle-java8-set-default
- Test Java installation: **javac -version**
- Run **ant** command



```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help

[javac] Note: Recompile with -Xlint:unchecked for details.
[copy] Copying 11 files to /home/floodlight/floodlight/target/bin
[copy] Copied 4 empty directories to 1 empty directory under /home/floodlight/floodlight/target/bin

compile-test:
[javac] Compiling 105 source files to /home/floodlight/floodlight/target/bin
-test
[javac] Note: Some input files use or override a deprecated API.
[javac] Note: Recompile with -Xlint:deprecation for details.
[javac] Note: /home/floodlight/floodlight/src/test/java/net/floodlightcontroller/core/internal/OFSwitchHandshakeHandlerVer13Test.java uses unchecked or unsafe operations.
[javac] Note: Recompile with -Xlint:unchecked for details.

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: 1 minute 1 second
floodlight@floodlight:~/floodlight$
```

- Execute the following command to run the REST API
java -jar target/floodlight.jar

```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
2018-10-22 16:58:50.470 INFO [n.f.h.HAController] HAController is starting...
2018-10-22 16:58:50.484 INFO [n.f.h.ControllerLogic] [ControllerLogic] Running.
..
2018-10-22 16:58:50.500 INFO [n.f.h.HAServer] Starting HAServer...
2018-10-22 16:58:50.818 INFO [o.r.C.I.Server] Starting the Simple [HTTP/1.1] se
rver on port 8080
2018-10-22 16:58:50.819 INFO [org.restlet] Starting net.floodlightcontroller.re
stserver.RestApiServer$RestApplication application
2018-10-22 16:58:59.323 INFO [n.f.j.JythonServer] Starting DebugServer on :6655
2018-10-22 16:59:05.339 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2018-10-22 16:59:20.344 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2018-10-22 16:59:35.348 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2018-10-22 16:59:50.352 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
2018-10-22 16:59:50.532 INFO [n.f.h.ControllerLogic] [ControllerLogic] Election
timed out, setting Controller 1 as LEADER!
2018-10-22 16:59:50.535 INFO [n.f.h.ControllerLogic] [ControllerLogic] Getting
Leader: 1
2018-10-22 17:00:05.357 INFO [n.f.l.i.LinkDiscoveryManager] Sending LLDP packet
s out of all the enabled ports
```

• FIREWALL REST API:

- Open another terminal and execute the “Examples using curl”
- Check whether the firewall is enabled or disabled

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

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

- Enabling the firewall is done using the following command
curl http://localhost:8080/wm/firewall/module/enable/json -X PUT -d ''

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

- 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: ~/floodlight
File Edit View Search Terminal Help
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" : "864317309"}floodlight@floodlight:~/floodlight$
```

- Adding an ALLOW rule for all flows between IP host 10.0.0.3 and host 10.0.0.7

```
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
```

```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
floodlight@floodlight:~$ cd floodlight/
floodlight@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" : "765598214"}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
```

```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
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" : "1986077958"}floodlight@floodlight:~/floodlight$
```

- 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": "00:00:00:00:00:0a"}'
http://localhost:8080/wm/firewall/rules/json
```

```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
floodlight@floodlight:~$ cd floodlight/
floodlight@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" : "2096535958"}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
```

```
floodlight@floodlight: ~/floodlight  
File Edit View Search Terminal Help  
floodlight@floodlight:~$ cd 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" : "428667318" }floodlight@floodlight:~/floodlight$
```

- 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

```
floodlight@floodlight: ~/floodlight  
File Edit View Search Terminal Help  
floodlight@floodlight:~$ cd floodlight/  
floodlight@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" : "1492377087" }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
```

```
floodlight@floodlight: ~/floodlight  
File Edit View Search Terminal Help  
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" : "1827169727" }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
```

```
floodlight@floodlight: ~/floodlight  
File Edit View Search Terminal Help  
floodlight@floodlight:~$ cd 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" : "647328017" }floodlight@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
```

```

floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
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": "1577005052"}floodlight@floodlight:~/floodlight$

```

- Adding an ALLOW rule for UDP to work between IP hosts 10.0.0.4 and 10.0.0.10
`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`

```

floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
cd floodlight@floodlight:~$ cd floodlight/
floodlight@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": "1063545826"}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

```

```

floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
floodlight@floodlight:~$ cd 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": "464968620"}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

```

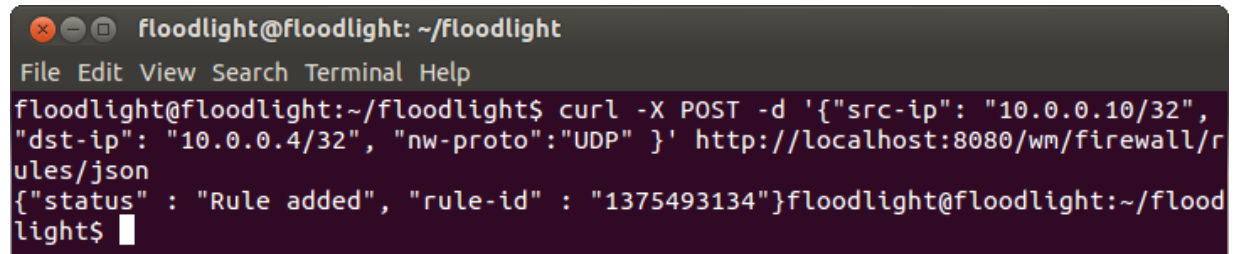
```

floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
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": "1692257166"}floodlight@floodlight:~/floodlight$

```



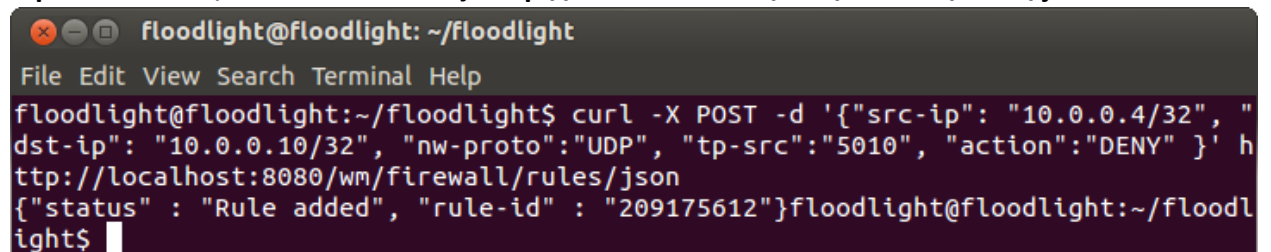
```
curl -X POST -d '{"src-ip": "10.0.0.10/32", "dst-ip": "10.0.0.4/32", "nw-proto": "UDP" }' http://localhost:8080/wm/firewall/rules/json
```



```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
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": "1375493134"}floodlight@floodlight:~/floodlight$
```

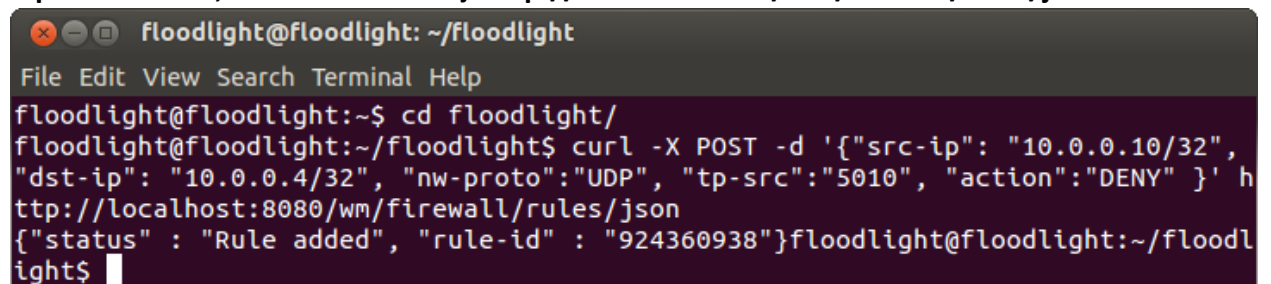
- Adding an ALLOW rule for UDP to work between IP hosts 10.0.0.4 and 10.0.0.10, and then blocking port 5010

```
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
```



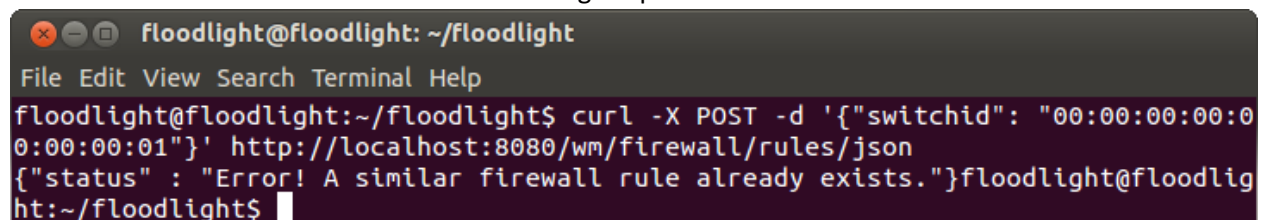
```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
floodlight@floodlight:~/floodlight$ curl -X POST -d '{"src-ip": "10.0.0.4/32", "dst-ip": "10.0.0.10/32", "nw-proto": "UDP", "tp-src": "5010", "action": "DENY" }' http://localhost:8080/wm/firewall/rules/json
{"status": "Rule added", "rule-id": "209175612"}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
```



```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
floodlight@floodlight:~$ cd 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": "924360938"}floodlight@floodlight:~/floodlight$
```

- Addition of the same rule results in the following output



```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
floodlight@floodlight:~/floodlight$ curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:00:01"}' http://localhost:8080/wm/firewall/rules/json
{"status": "Error! A similar firewall rule already exists."}floodlight@floodlight:~/floodlight$
```

• ACL REST API:

- Adding an ACL rule is done using the below command

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

```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
floodlight@floodlight:~/floodlight$ curl -X POST -d '{"src-ip":"10.0.0.1/32","dst-ip":"10.0.0.2/32","action":"deny"}' http://localhost:8080/wm/acl/rules/json
{"status": "Success! New rule added."}floodlight@floodlight:~/floodlight$
```

- A list of all ACL rules can be displayed using the following command
curl http://localhost:8080/wm/acl/rules/json | python -mjson.tool

```
floodlight@floodlight: ~/floodlight
File Edit View Search Terminal Help
floodlight@floodlight:~/floodlight$ curl http://localhost:8080/wm/acl/rules/json
| python -mjson.tool
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
100    568    0    568    0     0   5866      0  --:--:-- --:--:-- --:--:--   5916
[
  {
    "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
  },
  {
    "action": "DENY",
    "id": 2,
    "nw_dst": "10.0.0.4/32",
    "nw_dst_maskbits": 32,
    "nw_dst_prefix": 167772164,
    "nw_proto": 0,
    "nw_src": "10.0.0.1/32",
    "nw_src_maskbits": 32,
    "nw_src_prefix": 167772161,
    "tp_dst": 0
  }
]
```

- Copy paste <http://localhost:8080/wm/acl/rules/json> in Firefox browser to see the following

```
Mozilla Firefox
http://local...l/rules/json x
localhost:8080/wm/acl/rules/json
[{"id":1,"nw_src":"10.0.0.1/32","nw_dst":"10.0.0.2/32","nw_src_prefix":167772161,"nw_src_maskbits":32,"nw_dst_prefix":167772162,"nw_dst_maskbits":32,"nw_proto":0,"tp_dst":0,"action":"DENY"},{"id":2,"nw_src":"10.0.0.1/32","nw_dst":"10.0.0.4/32","nw_src_prefix":167772161,"nw_src_maskbits":32,"nw_dst_prefix":167772164,"nw_dst_maskbits":32,"nw_proto":0,"tp_dst":0,"action":"DENY"},{"id":3,"nw_src":"10.0.0.7/32","nw_dst":"10.0.0.4/32","nw_src_prefix":167772167,"nw_src_maskbits":32,"nw_dst_prefix":167772164,"nw_dst_maskbits":32,"nw_proto":0,"tp_dst":0,"action":"DENY"}]
```