Praarthana Ramakrishnan

C82908385

ADVANCED NETWORK SECURITY

PROJECT 3 - FLOODLIGHT FIREWALL APP

I. 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.

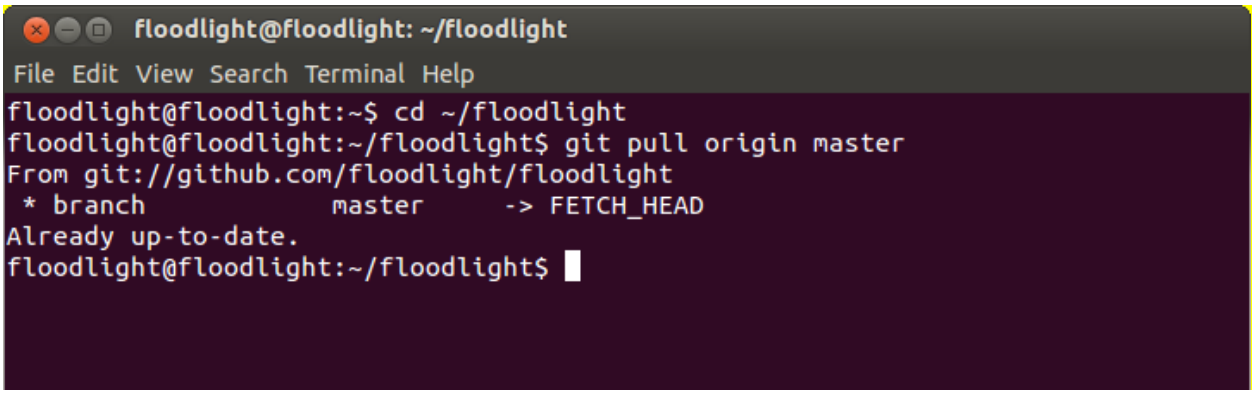

Fig 1.

2. 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

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

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: 3 minutes 0 seconds
floodlight@floodlight:~/floodlight$
```

Fig 2

```
floodlight@floodlight: ~/floodlight
File  Edit  View  Search  Terminal  Help
floodlight@floodlight:~/floodlight$ java -jar target/floodlight.jar
17:43:19.381 INFO [n.f.c.m.FloodlightModuleLoader:main] Loading modules from src
/main/resources/floodlightdefault.properties
17:43:19.973 WARN [n.f.r.RestApiServer:main] HTTPS disabled; HTTPS will not be u
sed to connect to the REST API.
17:43:19.974 WARN [n.f.r.RestApiServer:main] HTTP enabled; Allowing unsecure acc
ess to REST API on port 8080.
```

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`

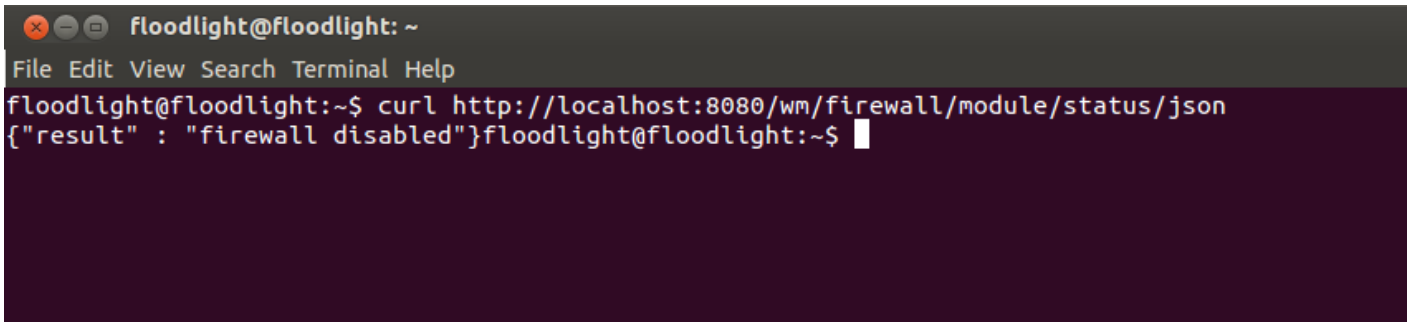

Fig 4

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 ''`

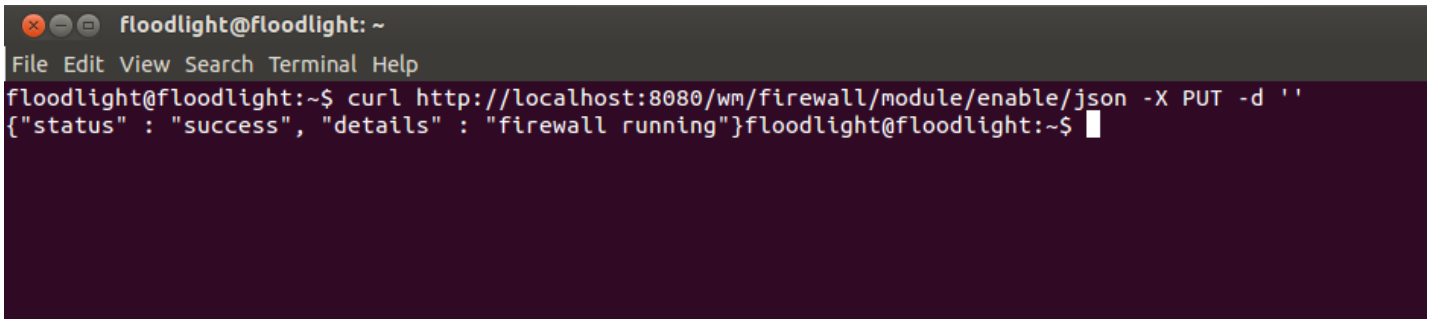

Fig 5

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`

```
floodlight@floodlight: ~
File Edit View Search Terminal Help
floodlight@floodlight:~$ curl -X POST -d '{"switchid": "00:00:00:00:00:00:00:01"}' http://localhost:8080/wm/firewall/rules/json
{"status" : "Rule added", "rule-id" : "2035196083"}floodlight@floodlight:~$
```

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`

```
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" : "824198782"}floodlight@floodlight:~$
```

Fig 7

```
floodlight@floodlight: ~
File Edit View Search Terminal Help
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" : "2044678526"}floodlight@floodlight:~$
```

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`

```
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/jso
n
{"status" : "Rule added", "rule-id" : "21283436"}floodlight@floodlight:~$
```

Fig 9

```
floodlight@floodlight: ~
File Edit View Search Terminal Help
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/jso
n
{"status" : "Rule added", "rule-id" : "1570962316"}floodlight@floodlight:~$
```

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

```
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" : "-259136712"}floodlight@floodlight:~$
```

Fig 11

```
floodlight@floodlight: ~
File Edit View Search Terminal Help
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" : "865597496"}floodlight@floodlight:~$
```

Fig 12

```
floodlight@floodlight: ~
File Edit View Search Terminal Help
floodlight@floodlight:~$ curl -X POST -d '{"src-ip": "10.0.0.3/32", "dst-ip": "1
0.0.0.7/32", "nw-proto":"ICMP" }' http://localhost:8080/wm/firewall/rules/json
{"status" : "Rule added", "rule-id" : "681423872"}floodlight@floodlight:~$
```

Fig 13

```
floodlight@floodlight: ~
File Edit View Search Terminal Help
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/rul
es/json
{"status" : "Rule added", "rule-id" : "1160580149"}floodlight@floodlight:~$
```

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

```
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/rule
s/json
{"status" : "Rule added", "rule-id" : "-720243484"}floodlight@floodlight:~$
```

Fig 15

```
floodlight@floodlight: ~
File Edit View Search Terminal Help
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/rule
s/json
{"status" : "Rule added", "rule-id" : "1179780689"}floodlight@floodlight:~$
```

Fig 16

```
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", "nw-proto":"UDP", "tp-src":"5010", "action":DENY" }' http
://localhost:8080/wm/firewall/rules/json
{"status" : "Rule added", "rule-id" : "-1783186101"}floodlight@floodlight:~$
```

Fig 17

```
floodlight@floodlight: ~
File Edit View Search Terminal Help
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/rul
es/json
{"status" : "Rule added", "rule-id" : "454741875"}floodlight@floodlight:~$
```

Fig 18

```
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", "nw-proto":"UDP", "tp-src":"5010", "action":DENY" }' http
://localhost:8080/wm/firewall/rules/json
{"status" : "Rule added", "rule-id" : "-1783186101"}floodlight@floodlight:~$
```

Fig 19

```
floodlight@floodlight: ~
File Edit View Search Terminal Help
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" : "-2113212981"}floodlight@floodlight:~$
```

Fig 20