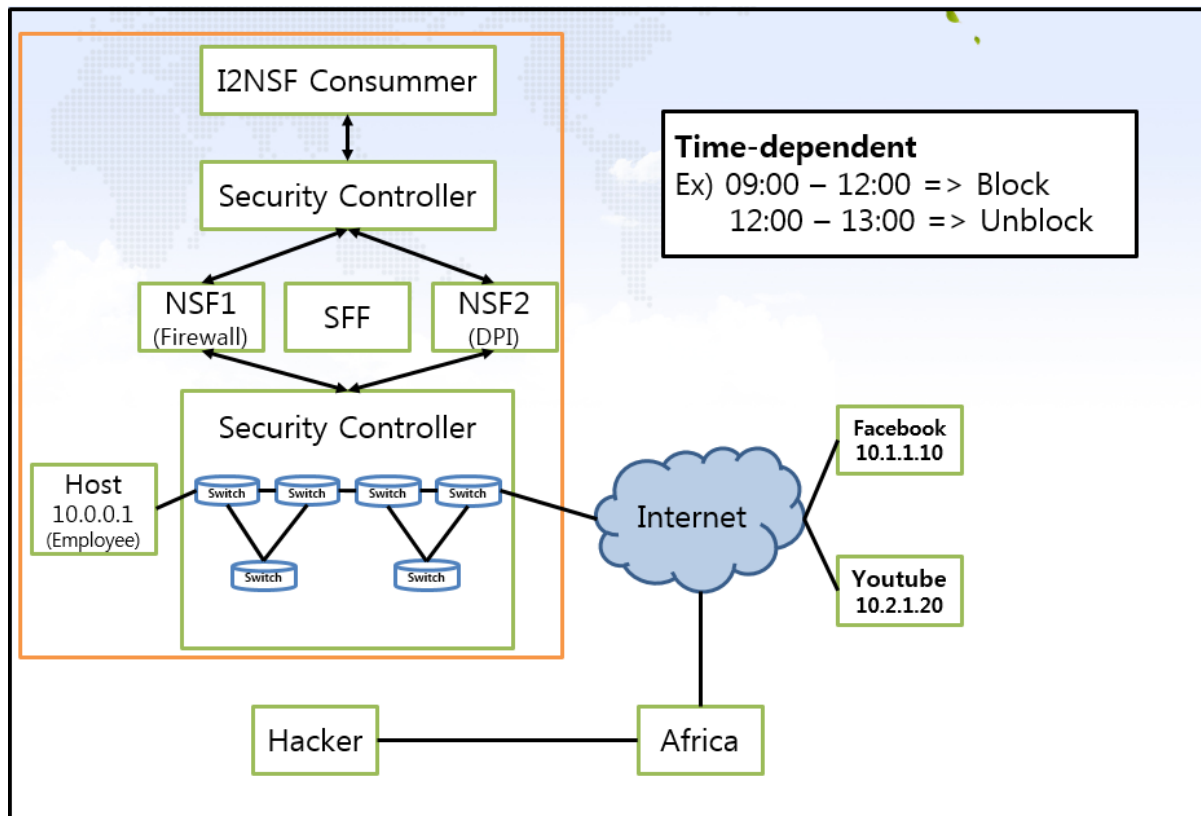


Hackathon Scenario

We assume that you have set up your system as suggested in the Hackathon Manual, so please go back and make sure everything is set up properly. If you encounter any problems, please do not hesitate to ask the Hackathon staff.

This document describes a real world scenario and explains each step involved in setting up the firewall and dpi in the scenario.

Topology



Scenario

Several studies suggest that companies that allow employees to use SNS (Social Network Services) during their working hours lose productivity. SNS can affect the relations within a company as employees can harass one another by sending or posting negative messages using the service. Moreover, SNS also has effects on confidentiality and company image in a long term. For example, an employee might post a progress of a project he is involved in his company which should be considered as confidential, or he might post business information that is not yet ready to be publicly available. Therefore, a company owner needs to take appropriate measures for such actions which may damage the company in any ways.

The owner (president) of SKKU co. ltd decided to limit the access to social network services or irrelevant websites during working hours as those may negatively affect his company's productivity. He asks his security administrator to provide a network solution to block employee's access to certain websites for a certain period time.


Firewall set up

1. Our goal is to build a web based user interface to set policies (set of rules) and send them to the security management system so that SNS and websites are blocked or allowed by a firewall as desired during a certain period time. The network is set up as shown in the topology figure shown above, and we will follow bellow steps to achieve this goal.

OpenDayLight Setup

1. Start a virtual machine
 - A. When asked, use “secu” as the password.
2. Run OpenDayLight.
 - A. Open a terminal and enter the following command in the home directory as shown in the below figure:
sudo ./distribution-karaf-0.4.3-Beryllium-SR3/bin/karaf
 - B. When asked, use “secu” as the password.

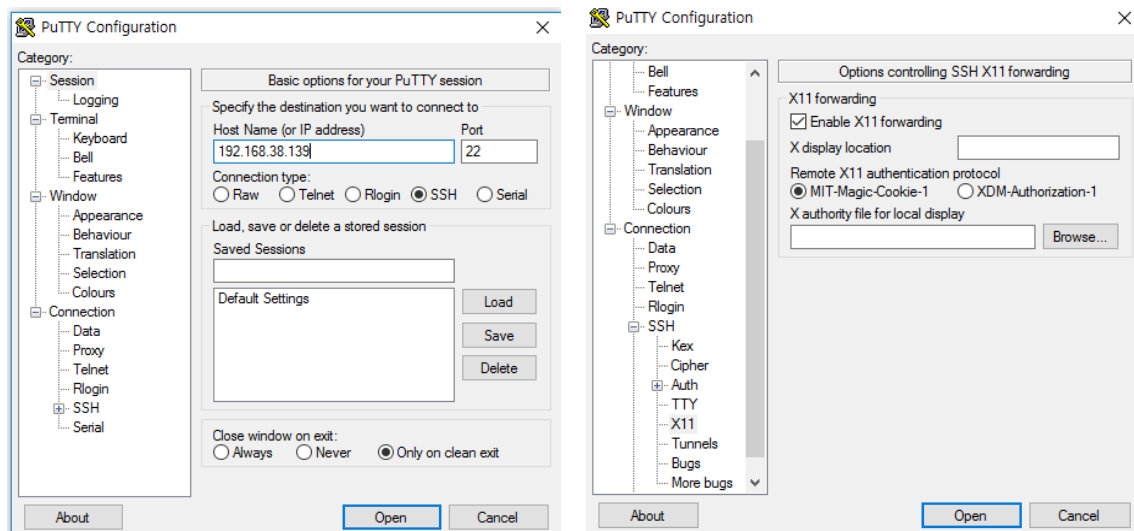
```
secu@secu:~/distribution-karaf-0.4.3-Beryllium-SR3/bin$ sudo ./karaf
[sudo] password for secu:
karaf: JAVA_HOME not set; results may vary
Java HotSpot(TM) 64-Bit Server VM warning: ignoring option MaxPermSize=512m; support was removed in
8.0
```



```
Hit '<tab>' for a list of available commands
and '[cmd] --help' for help on a specific command.
Hit '<ctrl-d>' or type 'system:shutdown' or 'logout' to shutdown OpenDaylight.
```

```
opendaylight-user@root>
```

3. Run new terminal through **Putty program**.
 - A. Go to the **Connection** category, extend the **SSH** tree and select **X11**.
 - B. Tick in the box to **Enable the X11 forwarding**.
 - C. Click on the Session Category and type in the IP address of a virtual machine.
 - D. When asked, use “**secu**” as the password.

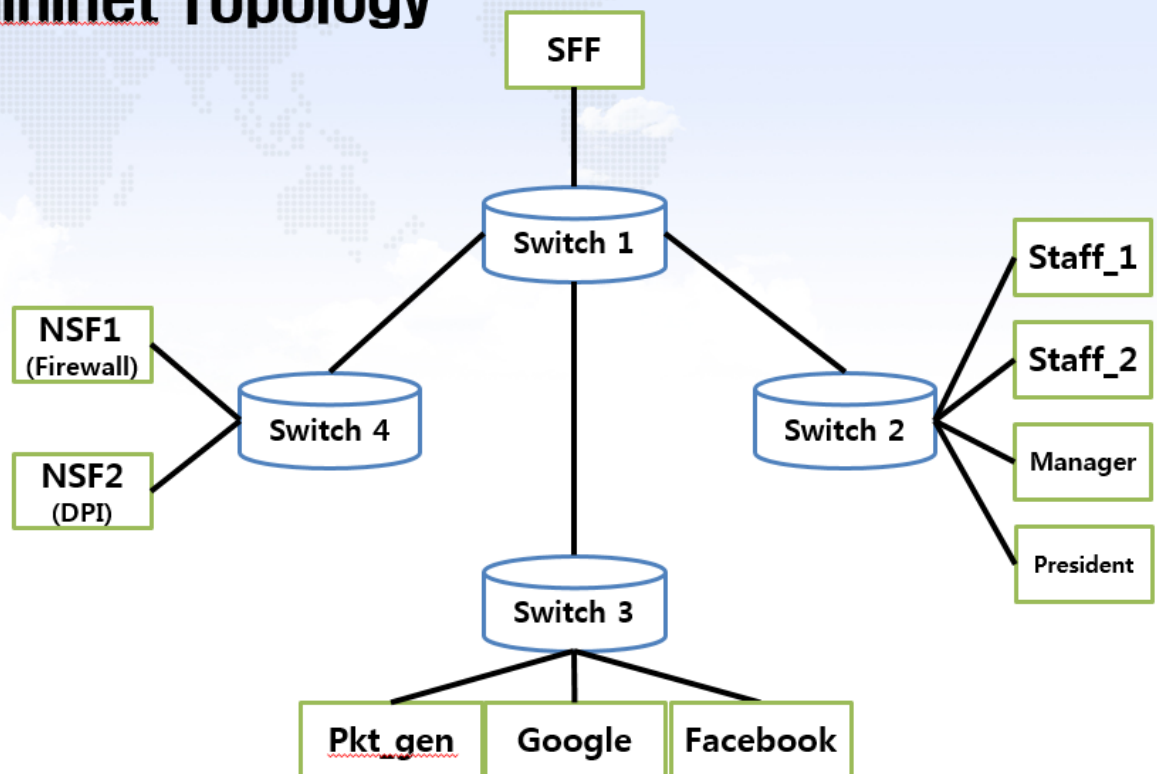


4. **In the Putty terminal**, type in the following command to move to the following directory:
 - A. `cd Hackathon/Scripts.`
5. From the Scripts directory, run the python script “topology.py” using the following command (This is the virtual network on mininet).
 - A. `sudo python topology.py.`
 - B. When asked, use “secu” as the password.

```
secu@secu:~/Hackathon/Scripts$ sudo python topology.py
[sudo] password for secu:
Enter password:
*** Creating network
*** Adding controller
*** Adding hosts:
admin facebook firewall google instagram manager naver president sff1 staff_1 staff_2
*** Adding switches:
switch1 switch2 switch3 switch4
*** Adding links:
(admin, switch1) (facebook, switch3) (firewall, switch1) (google, switch3) (instagram, switch3) (manager, switch4) (naver, switch3) (president, switch4) (sff1, switch2) (staff_1, switch4) (staff_2, switch4) (switch1, switch2) (switch2, switch3) (switch2, switch4)
*** Configuring hosts
admin facebook firewall google instagram manager naver president sff1 staff_1 staff_2
*** Starting controller
c0
*** Starting 4 switches
switch1 switch2 switch3 switch4 ...
*** Ping: testing ping reachability
admin -> X X X X X X X X X X
```

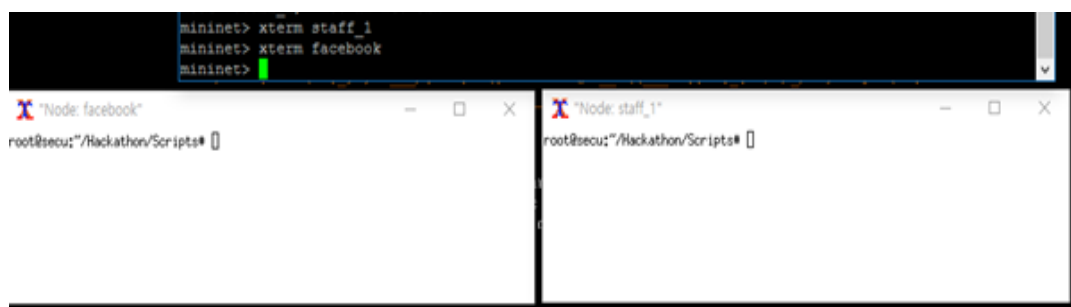
- C. This is the mininet topology.

Mininet Topology

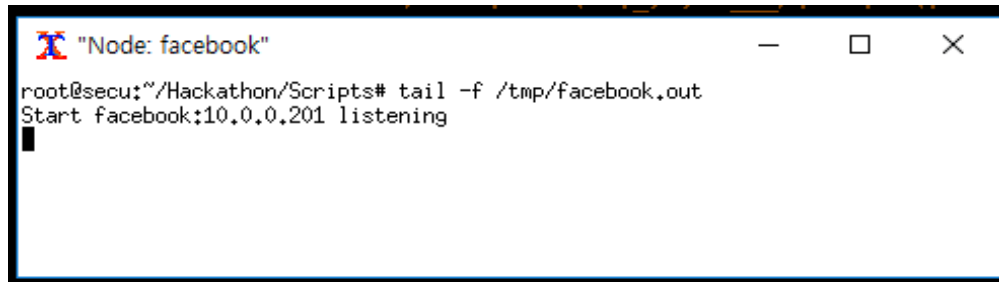


70

6. Open Xterm components for staff_1, facebook, admin, manager or whichever component if desired:
 - A. Input Xterm facebook as shown in the below figure, a separate Xterm window will open as shown in the below figure. Each component window can be opened this way.
 - B. Make sure Xterm is kept running in the background on your system for this to work.



7. Check the logs (facebook, naver, Instagram, google and etc) for each website components using the following command in the Xterm component window:



- A. Hackathon/bin/ipPacketGenerator name of website (e.g. facebook).

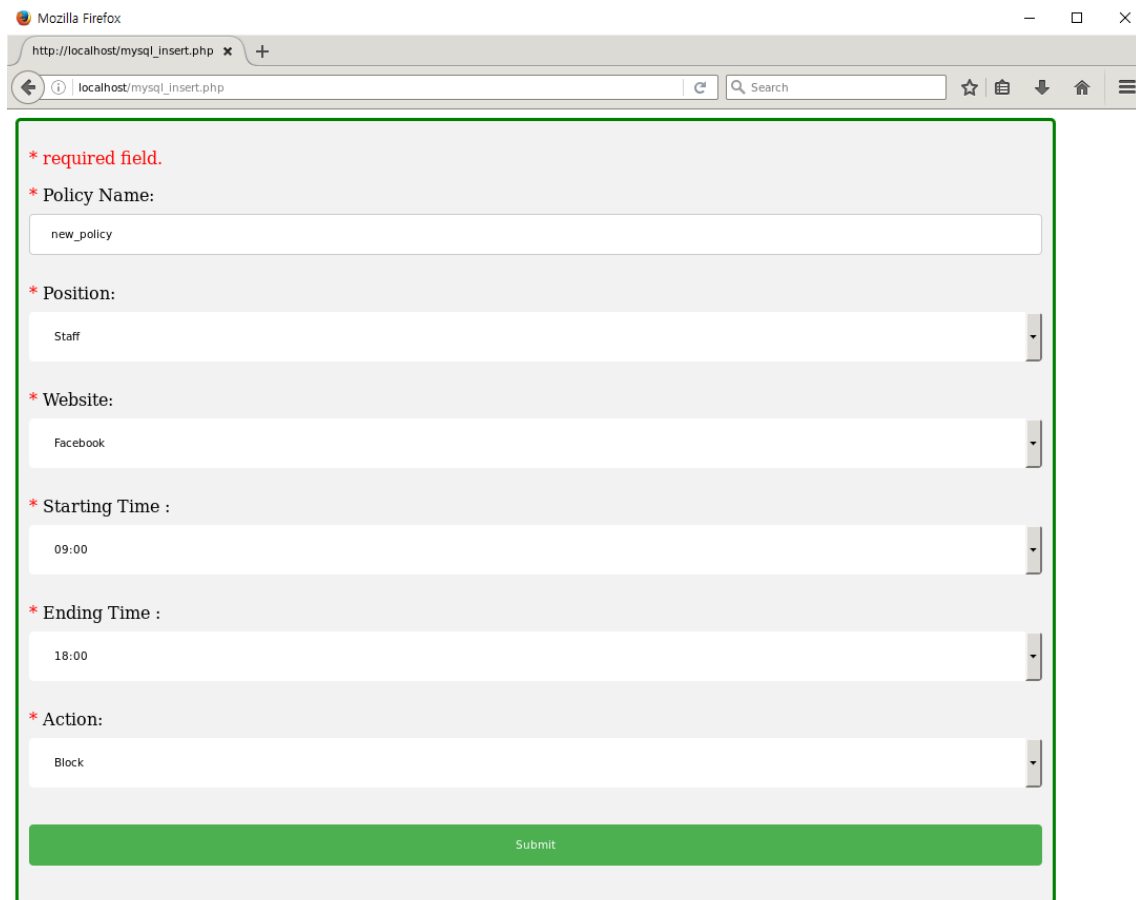
9. Open admin component and run Firefox by using the following command:

10. Go to the following website address for firewall configuration:

11. Use the following Username and Password:

- B. Password: skku.

12. Click on the Policy Set Up button to move to a page where you can set up a policy.
13. Set up a policy and click on the Submit button.



The screenshot shows a Mozilla Firefox browser window with the address bar displaying 'http://localhost/mysql_insert.php'. The page content is a form for setting up a policy. It includes several required fields, each marked with a red asterisk: 'Policy Name' (text input with 'new_policy'), 'Position' (dropdown menu with 'Staff'), 'Website' (dropdown menu with 'Facebook'), 'Starting Time' (dropdown menu with '09:00'), 'Ending Time' (dropdown menu with '18:00'), and 'Action' (dropdown menu with 'Block'). A green 'Submit' button is located at the bottom of the form.

14. When set up properly, your policy will be converted into an XML format document as shown below.

```
-<I2NSF>
-<Policies>
  <id>178</id>
  <Policy_name>new_policy</Policy_name>
  <Position>Staff</Position>
  <Website>Facebook</Website>
  <Start_time>09:00</Start_time>
  <End_time>18:00</End_time>
  <Action>Block</Action>
</Policies>
</I2NSF>
```

15. If you want to view the configured policy, input the following command in the admin component as shown in the below figure:

A. python show-firewall.py

```

"Node: admin"
root@secu:~/Hackathon/Scripts# ls
blacklist.xml          schema.sql
createVirtualNetworkInterface.sh  sendFlowScript.sh
FlowRuleToForwardIngressPacketToSFF.xml  show-firewall.py
install.sh             test.txt
mytopo.py             topology.py
removeVirtualNetworkInterface.sh
root@secu:~/Hackathon/Scripts# python show-firewall.py

Firewall Table

Rule ID    Src IP    Dest IP    Start Time    End Time    Action
1    10.0.0.1    10.0.0.201    9    18    Block
2    10.0.0.2    10.0.0.201    9    18    Block
3    10.0.0.3    10.0.0.201    9    18    Block
4    10.0.0.4    10.0.0.201    9    18    Block
5    10.0.0.5    10.0.0.201    9    18    Block
6    10.0.0.6    10.0.0.201    9    18    Block
7    10.0.0.7    10.0.0.201    9    18    Block
8    10.0.0.8    10.0.0.201    9    18    Block
9    10.0.0.9    10.0.0.201    9    18    Block
root@secu:~/Hackathon/Scripts#

```

Your Task sheet

Develop DPI (deep packet inspection) using the provided example architecture as a base. For this development, you need to build the following:

1. I2NSF User
 - A. Data transfer to security controller.
Work on the given bssp.php and uasp.php file.
2. Security Controller
 - A. Translation from a high-level policy to a low-level policy.
Work on the given server.py file located at ./SecurityController
 - B. YANG data model design for firewall policy.
Work on the given hst.yang file located at ./NSF/DPI
3. Network Security Functions & Security Function Forwarder
 - A. Implementation DPI for VoIP/VoLTE.
Work on the main.c file located at ./NSF/DPI

You can freely view and use the example, and its codes, as much as you like.