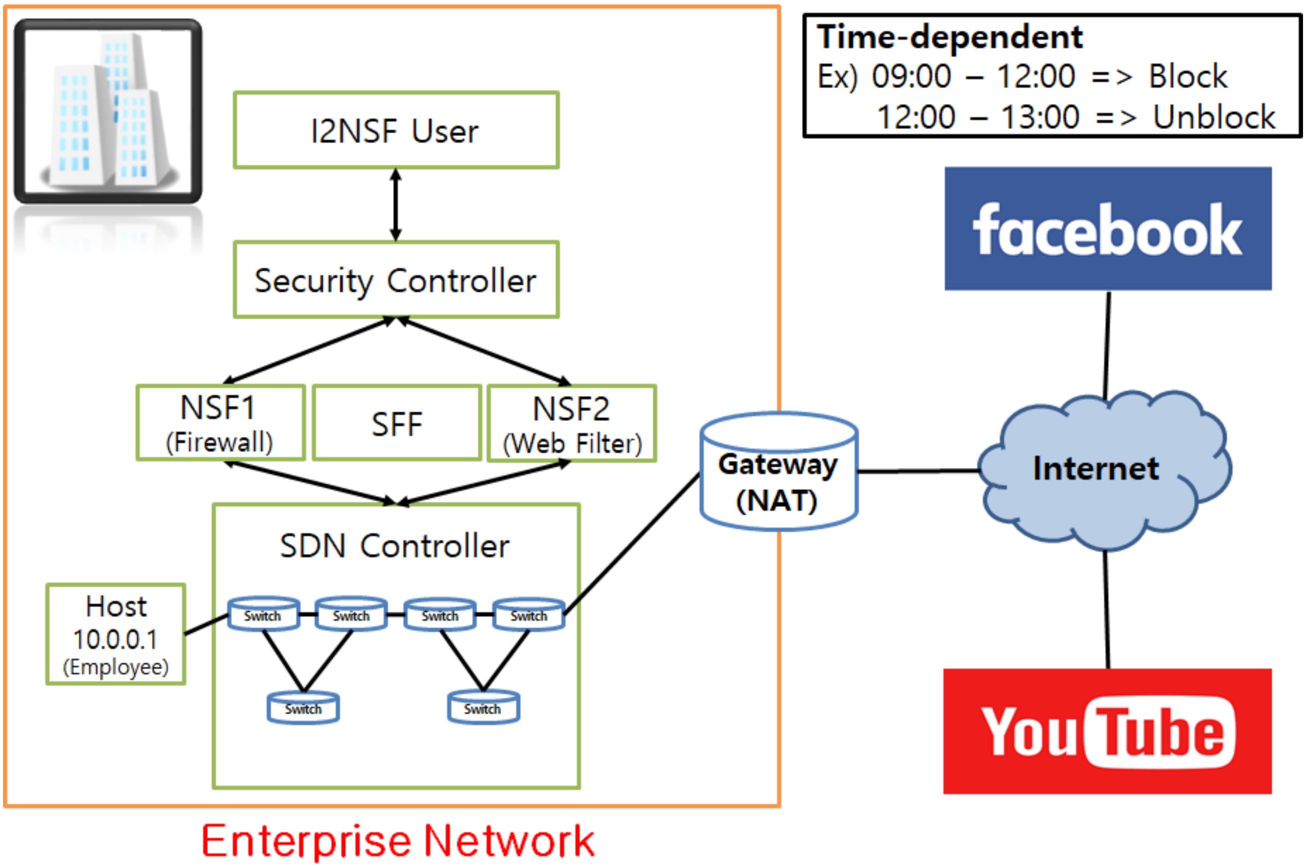
Hackathon Scenario

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 web filter in the scenario.

Topology



Scenario 1

Many enterprises and institutions use policy that blocks all port and allows only few ports. According to this policy, we divided 3 cases. First, the level-1 allows the ports for FTP, SSH, Telent, SMTP, POP2, POP3, IMAP4, HTTP, and HTTPS. Secondary, level-2 narrows down the boundary level-1 to SSH, POP2, POP3, IMAP4, and HTTS. Finally, all of port are blocked.

Scenario 2

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 and so on 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. He also asks administrator to allow only few ports.

Firewall and Web Filter set up

1. Our goal is to build a web based user interface to create, update, read, and delete the policies (CURD of rules) and send them to the security management system so that SNS and websites are blocked or allowed by a web filter as desired during a certain period time. Also, only few port allowed by firewall. 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

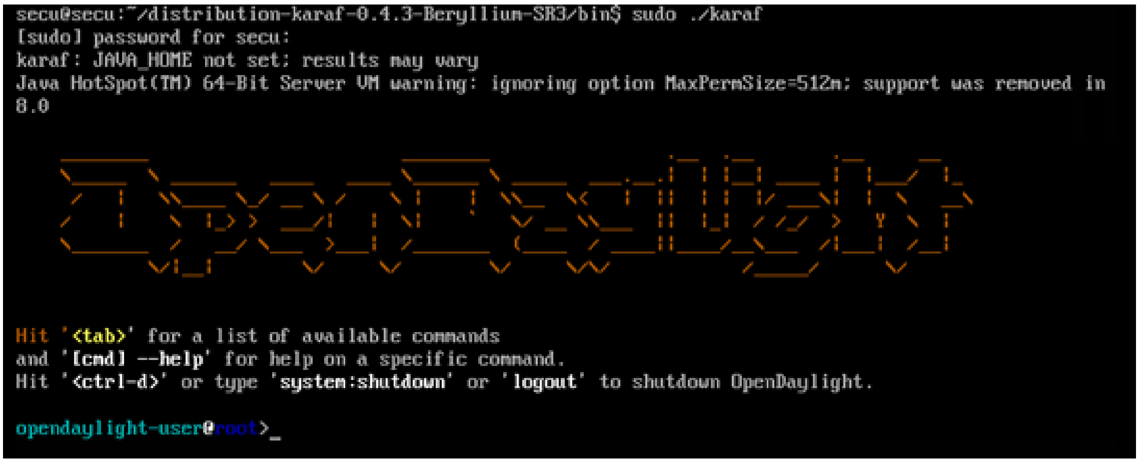
   A. When asked, use "secu" as the password.

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>_
```

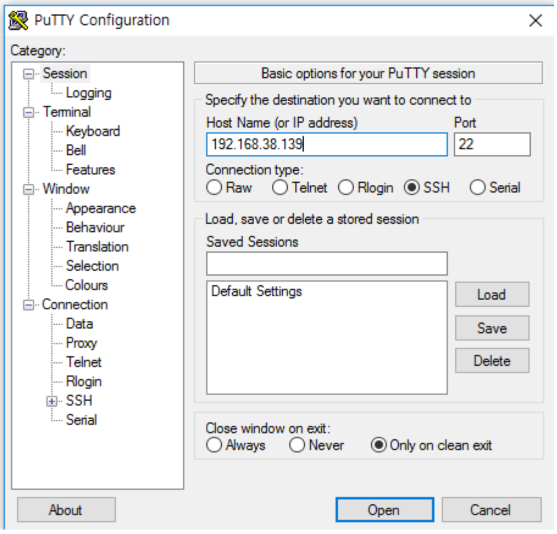
3. Run new terminal through **Putty program**.

   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.



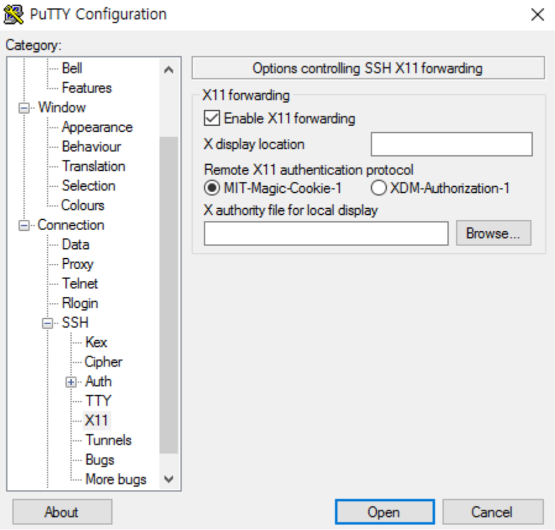
Specify the destination you want to connect to

Host Name (or IP address): 192.168.38.139

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit



X11 forwarding

☑ Enable X11 forwarding

X display location:

Remote X11 authentication protocol: ● MIT-Magic-Cookie-1 ○ XDM-Authorization-1

X authority file for local display:

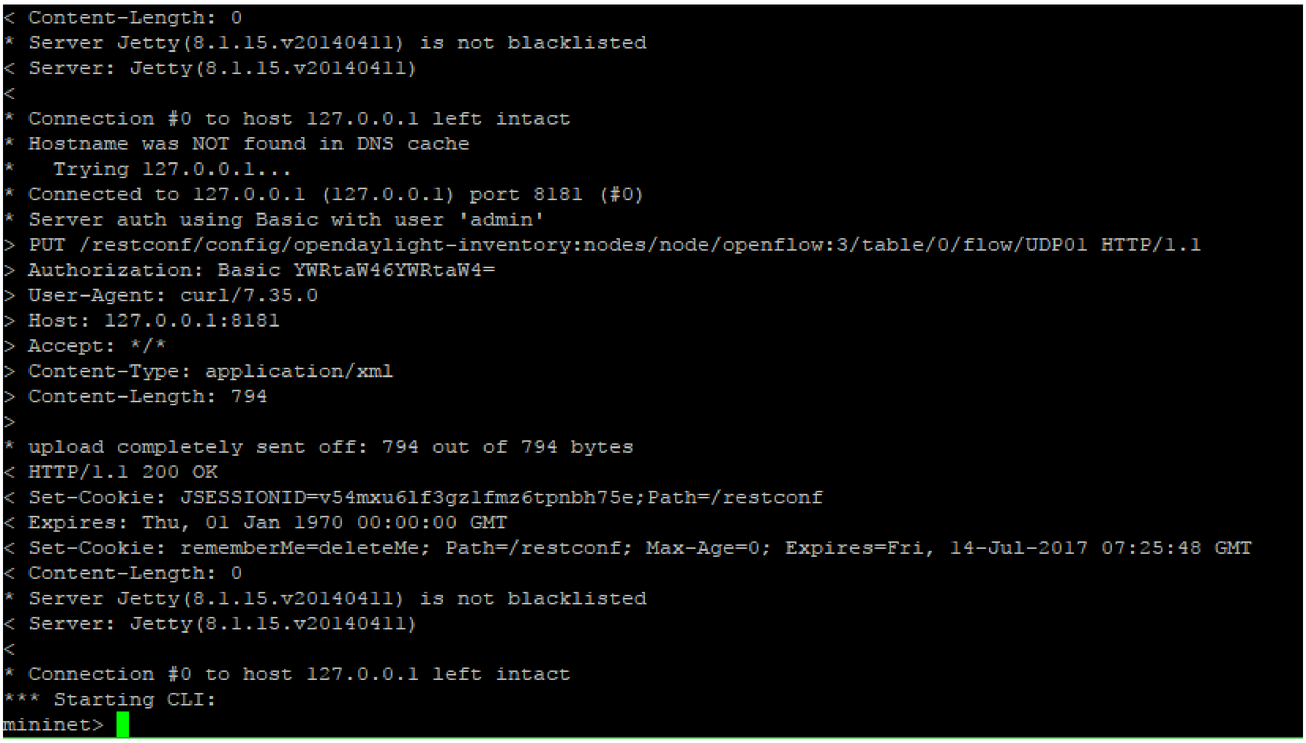
4. **In the Putty terminal**, type in the following command to move to the following directory:

   A. cd Hackathon/Hackathon-99/FullVersion/Scripts.

5. From the Scripts directory, run the python script “topology.py” using the following command (This is the virtual network on mininet).

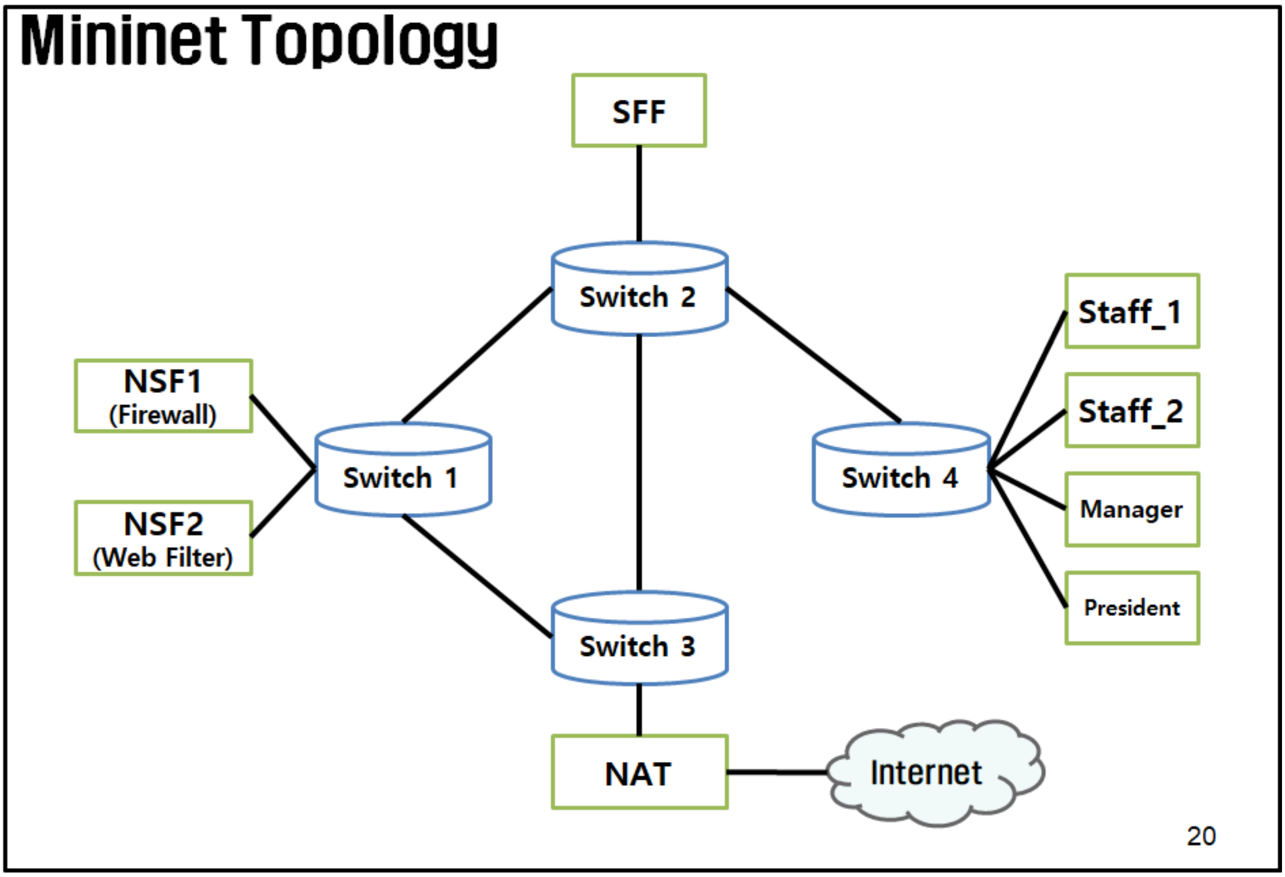
   A. sudo python topology.py.

   B. When asked, use “secu” as the password.



```
< Content-Length: 0
* Server Jetty(8.1.15.v20140411) is not blacklisted
< Server: Jetty(8.1.15.v20140411)
<
* Connection #0 to host 127.0.0.1 left intact
* Hostname was NOT found in DNS cache
*   Trying 127.0.0.1...
* Connected to 127.0.0.1 (127.0.0.1) port 8181 (#0)
* Server auth using Basic with user 'admin'
> PUT /restconf/config/opendaylight-inventory:nodes/node/openflow:3/table/0/flow/UDP01 HTTP/1.1
> Authorization: Basic YWRtaW46YWRtaW4=
> User-Agent: curl/7.35.0
> Host: 127.0.0.1:8181
> Accept: */*
> Content-Type: application/xml
> Content-Length: 794
>
* upload completely sent off: 794 out of 794 bytes
< HTTP/1.1 200 OK
< Set-Cookie: JSESSIONID=v54mxu61f3gz1fmz6tpnbh75e;Path=/restconf
< Expires: Thu, 01 Jan 1970 00:00:00 GMT
< Set-Cookie: rememberMe=deleteMe; Path=/restconf; Max-Age=0; Expires=Fri, 14-Jul-2017 07:25:48 GMT
< Content-Length: 0
* Server Jetty(8.1.15.v20140411) is not blacklisted
< Server: Jetty(8.1.15.v20140411)
<
* Connection #0 to host 127.0.0.1 left intact
*** Starting CLI:
mininet>
```

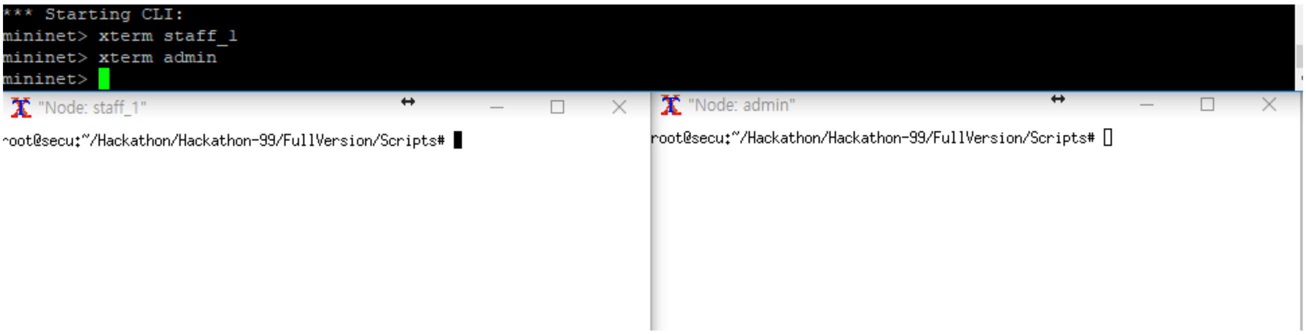
C. This is the mininet topology.



6. Open Xterm components for staff_1, admin or whichever component if desired:

A. Input Xterm staff_1 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.



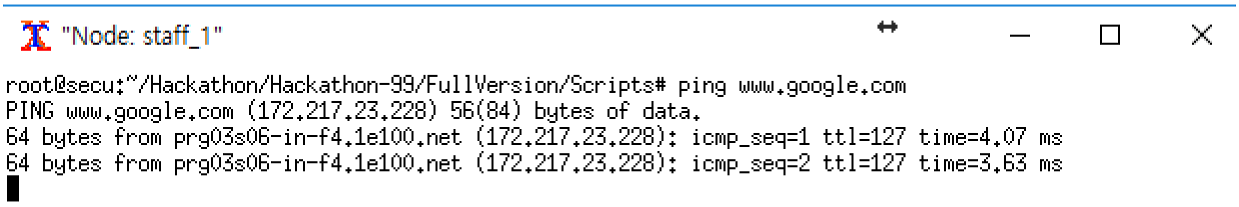
```
*** Starting CLI:
mininet> xterm staff_1
mininet> xterm admin
mininet> 
```

```
root@secu:~/Hackathon/Hackathon-99/FullVersion/Scripts# 
```

```
root@secu:~/Hackathon/Hackathon-99/FullVersion/Scripts# 
```

7. Check the ping to google using the following command in the Xterm component window:

   A. Ping www.google.com



```
root@secu:~/Hackathon/Hackathon-99/FullVersion/Scripts# ping www.google.com
PING www.google.com (172.217.23.228) 56(84) bytes of data.
64 bytes from prg03s06-in-f4.1e100.net (172.217.23.228): icmp_seq=1 ttl=127 time=4.07 ms
64 bytes from prg03s06-in-f4.1e100.net (172.217.23.228): icmp_seq=2 ttl=127 time=3.63 ms
```

8. Use the following command on admin component and run browser to generate rule and configure firewall

   A. Sudo google-chrome-stable --no-sandbox

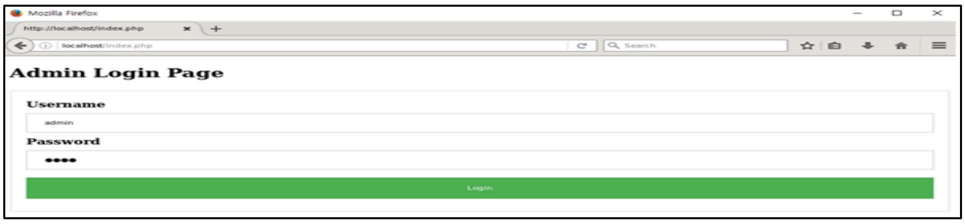
9. Go to the following website address for firewall configuration:

   A. localhost/index.php.

10. Use the following Username and Password:

   A. Username: admin.

   B. Password: skku.



Admin Login Page

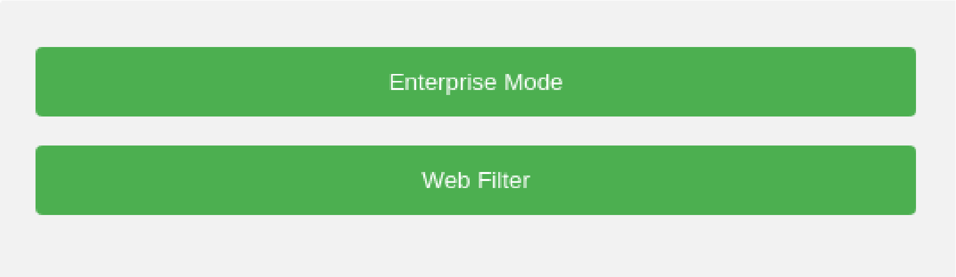
Username

admin

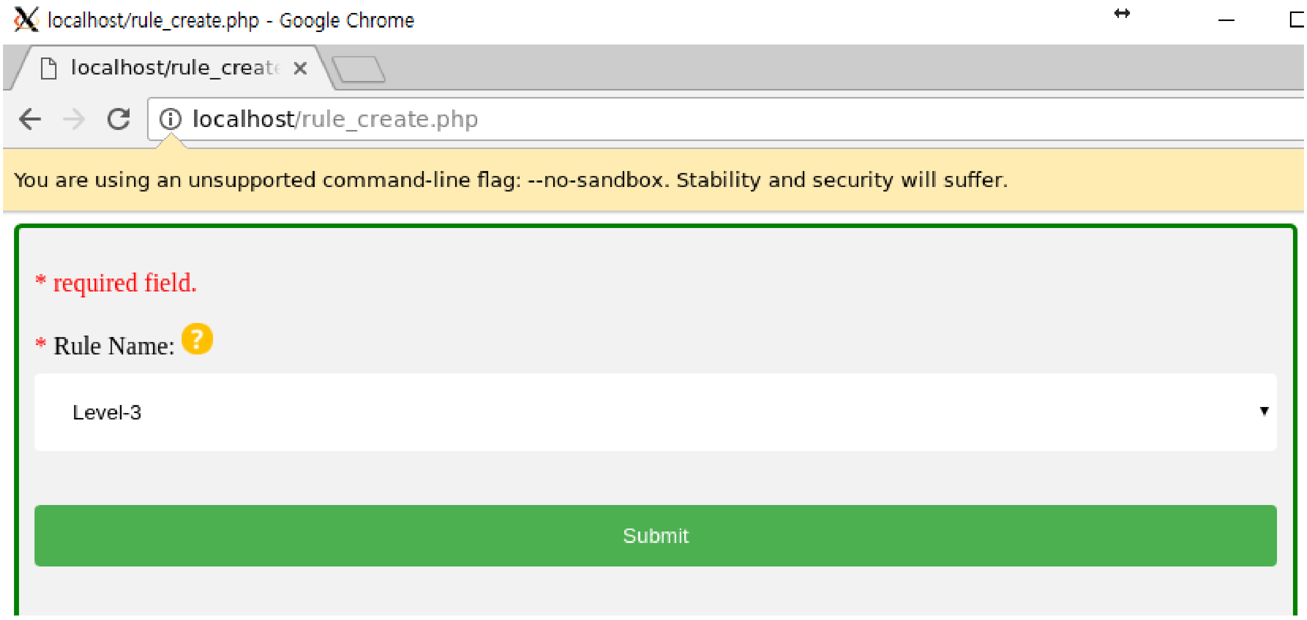
Password

••••

11. Click on the Enterprise Mode button to move to a page where you can choose CURD (create, update, read and delete).



12. Click on the Rule Create button to move to a page where you can create rule
13. Set up a rule for Level-3 and click on the Submit button.


localhost/rule_create.php - Google Chrome
localhost/rule_create
localhost/rule_create.php

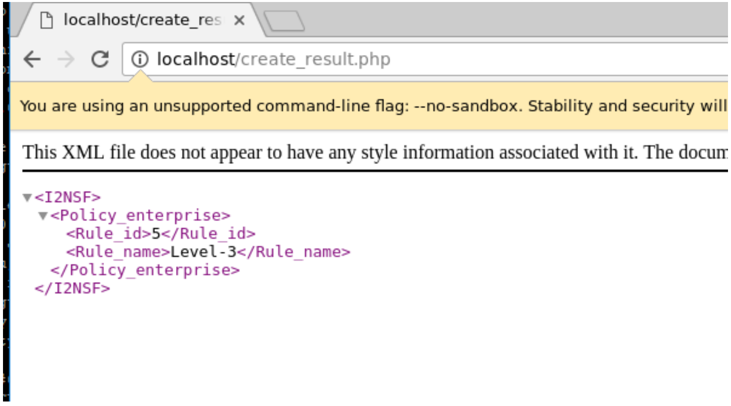
You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

* required field.

* Rule Name: ?

Level-3 ▾

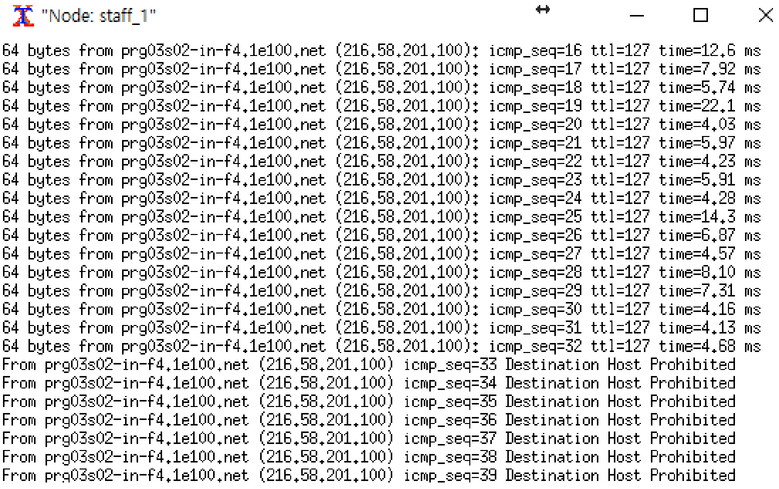
14. When set up properly, your policy will be converted into an XML format.
    After a while, you can see two buttons (Enterprise Mode, Web Filter) again.
    Then, you can check your staff_1 component ping does not work like below.



You are using an unsupported command-line flag: --no-sandbox. Stability and security will

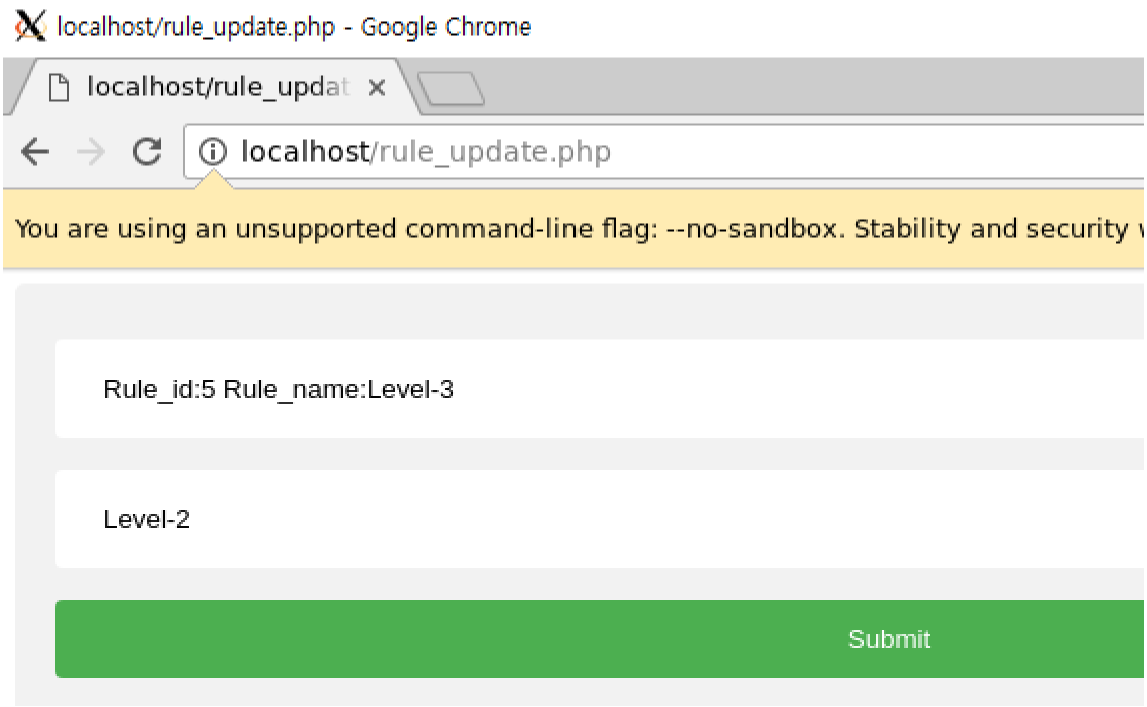
This XML file does not appear to have any style information associated with it. The docum

```
▾<I2NSF>
  ▾<Policy_enterprise>
     <Rule_id>5</Rule_id>
     <Rule_name>Level-3</Rule_name>
   </Policy_enterprise>
 </I2NSF>
```



```
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=16 ttl=127 time=12.6 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=17 ttl=127 time=7.92 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=18 ttl=127 time=5.74 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=19 ttl=127 time=22.1 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=20 ttl=127 time=4.03 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=21 ttl=127 time=5.97 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=22 ttl=127 time=4.23 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=23 ttl=127 time=5.91 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=24 ttl=127 time=4.28 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=25 ttl=127 time=14.3 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=26 ttl=127 time=6.87 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=27 ttl=127 time=4.57 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=28 ttl=127 time=8.10 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=29 ttl=127 time=7.31 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=30 ttl=127 time=4.16 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=31 ttl=127 time=4.13 ms
64 bytes from prg03s02-in-f4.1e100.net (216.58.201.100): icmp_seq=32 ttl=127 time=4.68 ms
From prg03s02-in-f4.1e100.net (216.58.201.100) icmp_seq=33 Destination Host Prohibited
From prg03s02-in-f4.1e100.net (216.58.201.100) icmp_seq=34 Destination Host Prohibited
From prg03s02-in-f4.1e100.net (216.58.201.100) icmp_seq=35 Destination Host Prohibited
From prg03s02-in-f4.1e100.net (216.58.201.100) icmp_seq=36 Destination Host Prohibited
From prg03s02-in-f4.1e100.net (216.58.201.100) icmp_seq=37 Destination Host Prohibited
From prg03s02-in-f4.1e100.net (216.58.201.100) icmp_seq=38 Destination Host Prohibited
From prg03s02-in-f4.1e100.net (216.58.201.100) icmp_seq=39 Destination Host Prohibited
```

15. Click Enterprise Mode and click one more time for rule update.
    Then set Level-2 Enterprise Mode like below

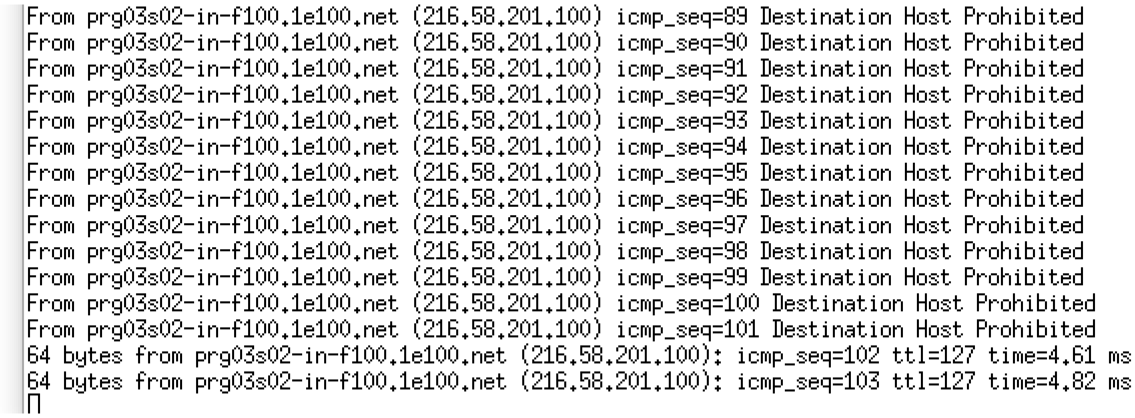

localhost/rule_update.php - Google Chrome
localhost/rule_updat
localhost/rule_update.php
Submit

You are using an unsupported command-line flag: --no-sandbox. Stability and security w

Rule_id:5 Rule_name:Level-3

Level-2

16. The ping from staff_1 work properly like below.



```
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=89 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=90 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=91 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=92 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=93 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=94 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=95 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=96 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=97 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=98 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=99 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=100 Destination Host Prohibited
From prg03s02-in-f100.1e100.net (216.58.201.100) icmp_seq=101 Destination Host Prohibited
64 bytes from prg03s02-in-f100.1e100.net (216.58.201.100): icmp_seq=102 ttl=127 time=4.61 ms
64 bytes from prg03s02-in-f100.1e100.net (216.58.201.100): icmp_seq=103 ttl=127 time=4.82 ms
```

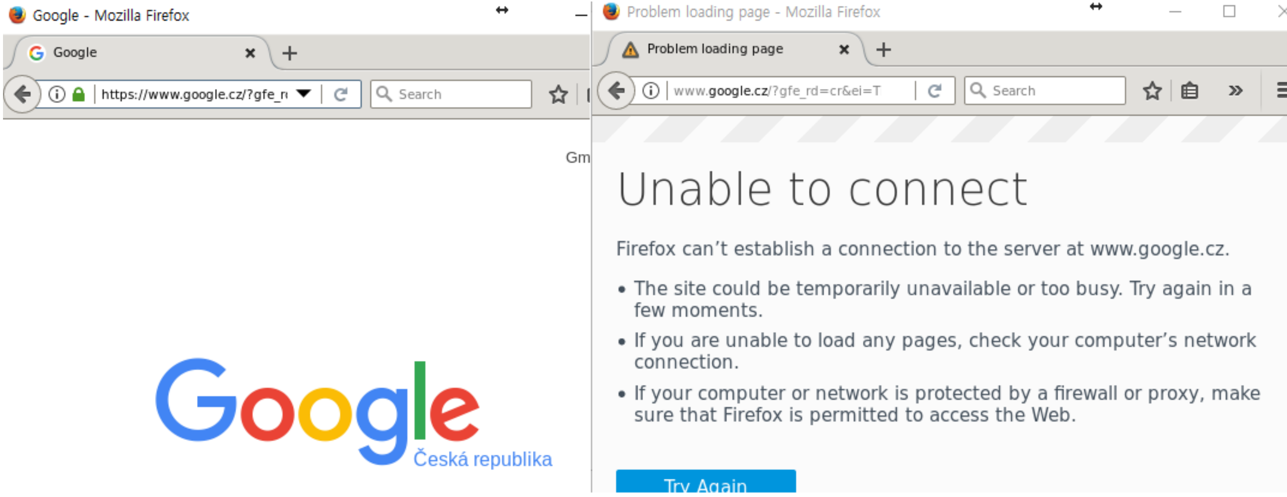
17. Using the following command on staff_1 component to check Enterprise Mode Level-2

A. sudo firefox

B. url : https://www.google.com

C. url : http://www.google.com

You can check we can use the https port to connect but cannot use http port to connect like below



https://www.google.cz/?gfe_r

www.google.cz/?gfe_rd=cr&ei=T

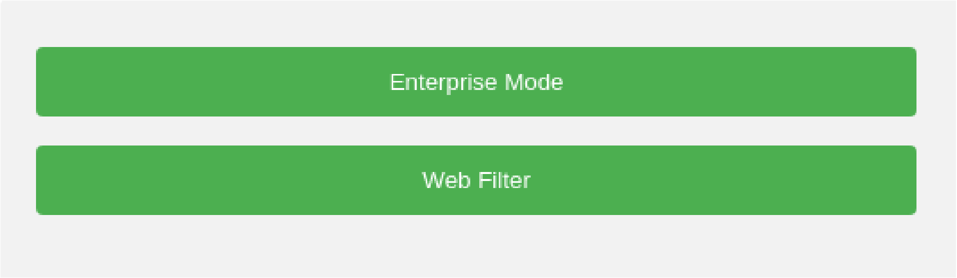
Unable to connect

Firefox can't establish a connection to the server at www.google.cz.

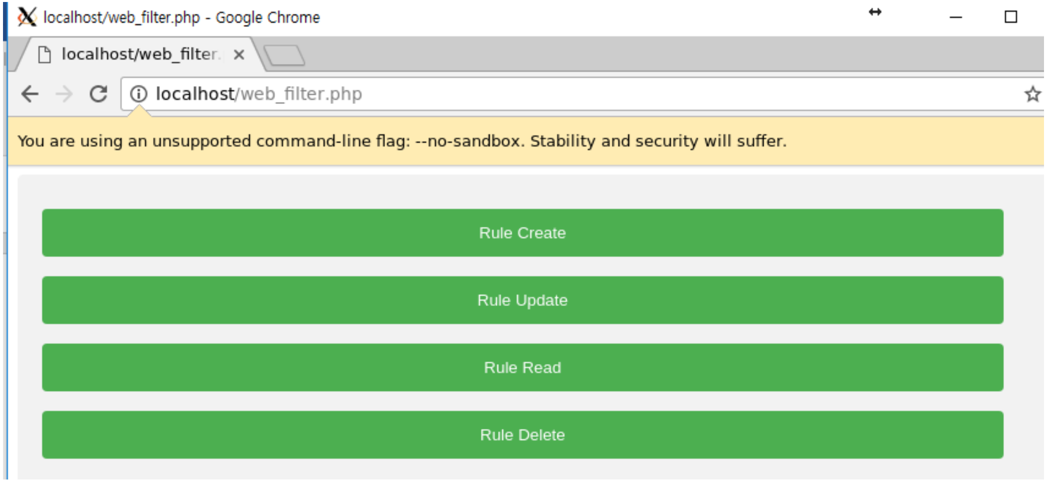
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

18. Follow instruction to use web filter for blocking www.google.com

A. Click web filter button on http://localhost/select_page.php



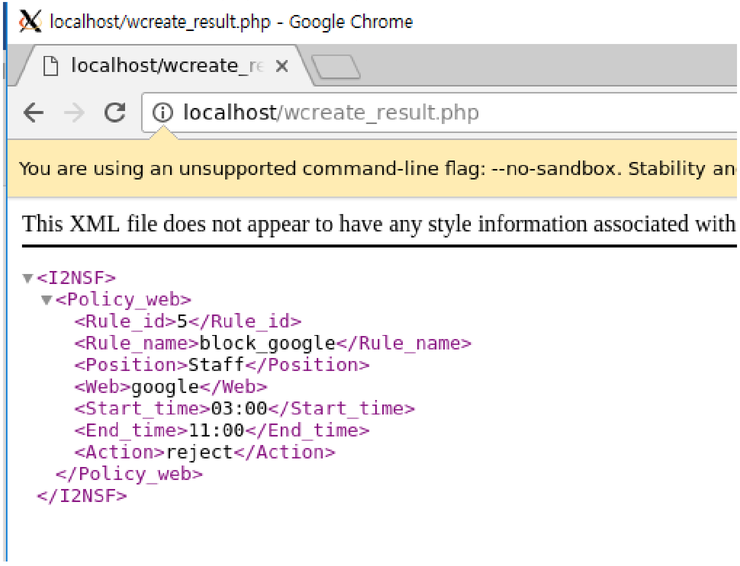
B. Click rule create button on http://localhost/web_filter.php



You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

C. Fill in the form to create rule. (You can check additional instruction by yellow question mark circle)

D. When set up properly, your policy will be converted into an XML format.


localhost/wcreate_result.php - Google Chrome
localhost/wcreate_re
localhost/wcreate_result.php

You are using an unsupported command-line flag: --no-sandbox. Stability an

This XML file does not appear to have any style information associated with

```
▼<I2NSF>
  ▼<Policy_web>
     <Rule_id>5</Rule_id>
     <Rule_name>block_google</Rule_name>
     <Position>Staff</Position>
     <Web>google</Web>
     <Start_time>03:00</Start_time>
     <End_time>11:00</End_time>
     <Action>reject</Action>
   </Policy_web>
 </I2NSF>
```

19. After a while, you can see two buttons (Enterprise Mode, Web Filter) again.

20. Using the following command on terminal that run mininet

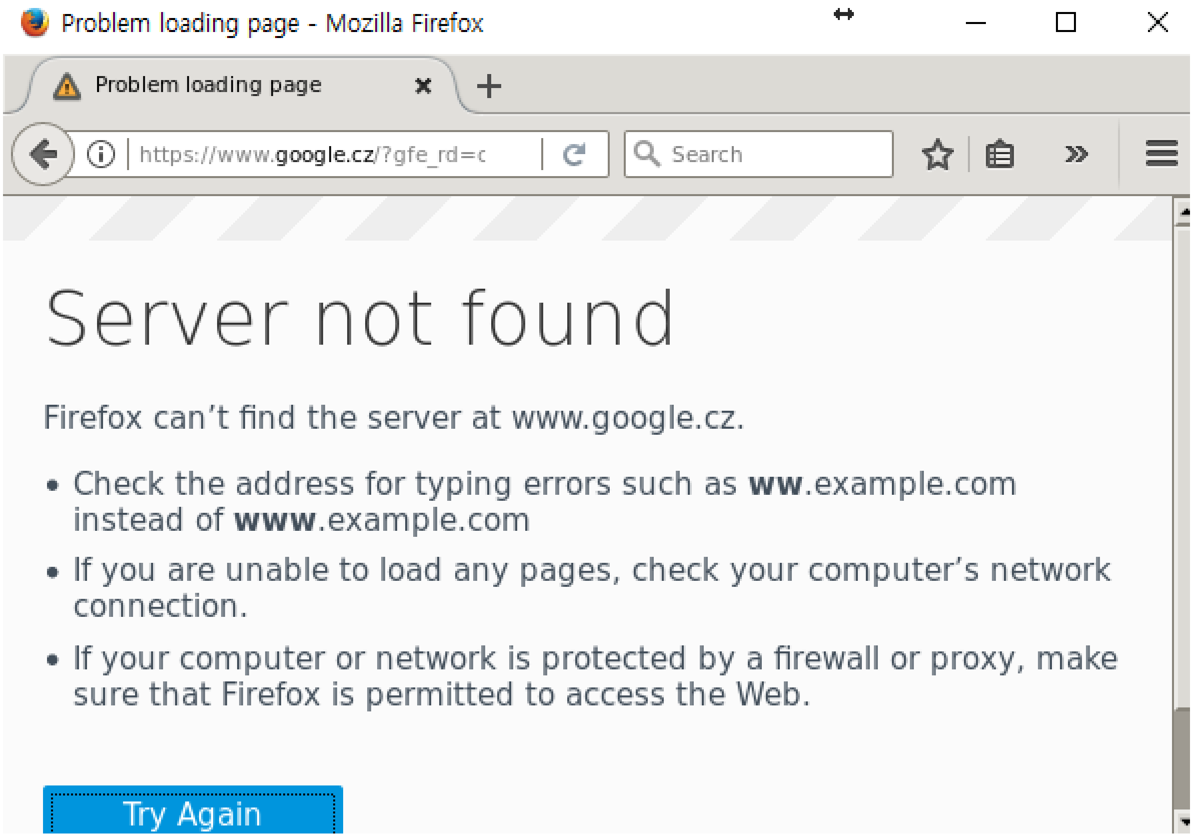
    A. Xterm staff_1
    You can use another staff_1 component to check web filter work properly.

21. Using the following command on staff_1component

    A. Sudo firefox

    B. url : https:www.google.com

22. You can check the web filter work properly.



Problem loading page - Mozilla Firefox
Problem loading page
https://www.google.cz/?gfe_rd=c
Search

Server not found

Firefox can’t find the server at www.google.cz.

- Check the address for typing errors such as **ww**.example.com instead of **www**.example.com
- If you are unable to load any pages, check your computer’s network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

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