LABORATORIUM PEMBELAJARAN ILMU KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA

BAB : 4 – FIREWALL
NAMA : MOH. ARIF ANDRIAN
NIM : 156250600111002
TANGGAL : 14/11/2017
ASISTEN : ATIKAH FEBRIANTI NASTITI
SRI WULAN UTAMI VITANDY

1.1. FIREWALL

1.1.1. PERCOBAAN

1. Lakukan langkah-langkah berikut untuk menghentikan ufw dan mengaktifkan iptables!
   a. Bukalah terminal di komputer anda; pastikan bahwa anda menggunakan komputer dengan sistem operasi Ubuntu 16.04.

```
andrian@156150600111002:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04.3 LTS
Release:        16.04
```

   Memastikan bahwa linux yang kita pakai benar-benar versi 16.04.

   b. Jalankan perintah **`sudo ufw reset`** dan **`sudo ufw disable`** untuk menghentikan ufw.

```
andrian@156150600111002:~$ sudo ufw reset
[sudo] password for andrian:
Resetting all rules to installed defaults. Proceed with operation (y|n)? y
Backing up 'before.rules' to '/etc/ufw/before.rules.20171114_123255'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20171114_123255'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20171114_123255'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20171114_123255'
Backing up 'after.rules' to '/etc/ufw/after.rules.20171114_123255'
Backing up 'user.rules' to '/etc/ufw/user.rules.20171114_123255'

andrian@156150600111002:~$ sudo ufw disable
Firewall stopped and disabled on system startup
```

   Melakukan perintah `uwf`, uwf adalah set perintah yang bisa digunakan untuk mengkonfigurasi iptables di Ubuntu. UFW tersedia mulai dari Ubuntu versi 8.04 dan terinstall secara default. UFW cocok untuk mengkonfigurasi firewall dengan mudah dan sederhana.

   c. Jalankan printah beriktu untuk mereset rule iptables.

```
sudo iptables --policy INPUT ACCEPT
sudo iptables --policy FORWARD ACCEPT
sudo iptables --policy OUTPUT ACCEPT
sudo iptables --flush
sudo iptables --delete-chain
```

```
andrian@156150600111002:~$ sudo iptables --policy INPUT ACCEPT
andrian@156150600111002:~$ sudo iptables --policy FORWARD ACCEPT
andrian@156150600111002:~$ sudo iptables --policy OUTPUT ACCEPT
andrian@156150600111002:~$ sudo iptables --flush
andrian@156150600111002:~$ sudo iptables --delete-chain
```

Ada tiga "rantai". Setiap rantai adalah daftar aturan untuk paket (traffic) yang diikuti secara berurutan:
INPUT - Aturan untuk menentukan lalu lintas masuk yang akan diterima atau ditolak
OUTPUT - Aturan untuk menentukan lalu lintas keluar yang akan diterima atau ditolak
FORWARD - Aturan untuk menentukan lalu lintas mana yang akan diteruskan akan diterima atau ditolak.
Kita dapat menentukan perilaku default untuk setiap rantai - baik untuk ACCEPT semua lalu lintas, atau DENY semua lalu lintas.

FLUSH - Perintah ini mengosongkan aturan pada sebuah chain. Apabila chain tidak disebutkan, maka semua chain akan di-flush.
DELETE-CHAIN - Perintah ini akan menghapus chain yang disebutkan. Agar perintah di atas berhasil, tidak boleh ada aturan lain yang mengacu kepada chain tersebut.

d. Jalankan perintah **`sudo iptables --list --numeric`** untuk menampilkan rule dalam iptables. Bila anda berhasil, maka anda akan mendapatkan output sperti pada tabel berikut ini.

```
Chain INPUT (policy ACCEPT)
target                      prot     opt     source
destination

Chain FORWARD (policy ACCEPT)
target                      prot     opt     source
destination

Chain OUTPUT (policy ACCEPT)
target                      prot     opt     source
destination
```

```
andrian@156150600111002:~$ sudo iptables --list --numeric
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
andrian@156150600111002:~$
```

Hasil dari konfigurasi yang telah dilakukan berisikan rule dalam iptables.

e. Perintah yang anda jalankan pada langkah 1.c. akan mengijinkan semua paket untuk keluar, masuk, dan diteruskan dari komputer anda.
Jawaban:
Iya benar, karena kita telah mengkonfigurasi paket traffic dengan mengijinkan semua lalu lintas(INPUT, OUTPUT, FORWARD) yaitu dengan perintah ACCEPT.

2. Lakukan langkah-langkah berikut untuk menguji input chain dari iptables!
   a. Install apache web server dalam komputer anda dengan menjalankan perintah **`sudo apt install -y apache2`**.

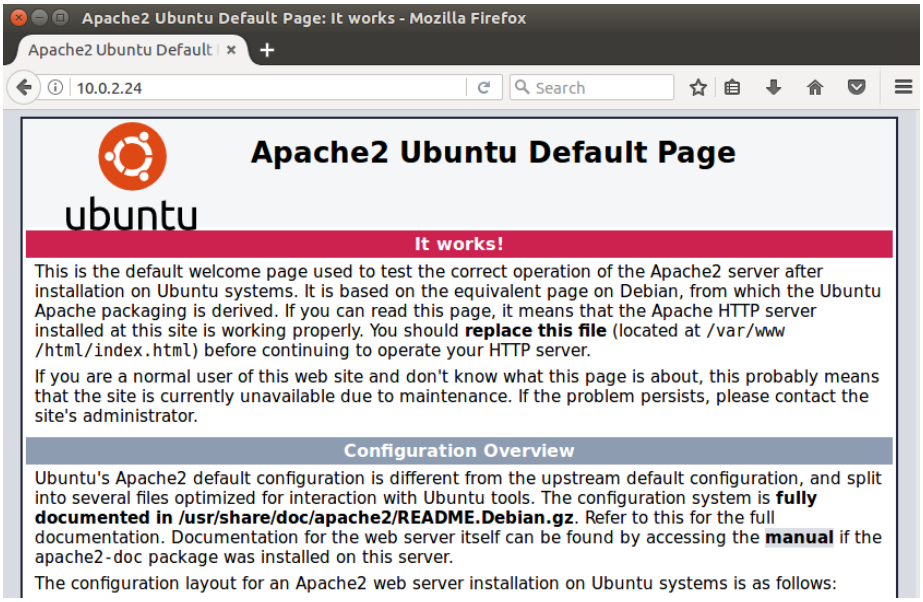
```
andrian@156150600111002:~$ sudo apt install -y apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0
0 upgraded, 9 newly installed, 0 to remove and 117 not upgraded.
Need to get 1.634 kB of archives.
After this operation, 6.268 kB of additional disk space will be used.
Get:1 http://security.ubuntu.com/ubuntu xenial-security/main i386 apache2-bin i3
86 2.4.18-2ubuntu3.5 [986 kB]
Get:2 http://id.archive.ubuntu.com/ubuntu xenial/main i386 libapr1 i386 1.5.2-3
[95,1 kB]
Get:3 http://id.archive.ubuntu.com/ubuntu xenial/main i386 libaprutil1 i386 1.5.
4-1build1 [82,7 kB]
Get:4 http://id.archive.ubuntu.com/ubuntu xenial/main i386 libaprutil1-dbd-sqlit
e3 i386 1.5.4-1build1 [10,9 kB]
Get:5 http://id.archive.ubuntu.com/ubuntu xenial/main i386 libaprutil1-ldap i386
 1.5.4-1build1 [8.916 B]
Get:6 http://id.archive.ubuntu.com/ubuntu xenial/main i386 liblua5.1-0 i386 5.1.
5-8ubuntu1 [114 kB]
Get:7 http://security.ubuntu.com/ubuntu xenial-security/main i386 apache2-utils
i386 2.4.18-2ubuntu3.5 [86,9 kB]
Get:8 http://security.ubuntu.com/ubuntu xenial-security/main i386 apache2-data a
ll 2.4.18-2ubuntu3.5 [162 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/main i386 apache2 i386 2
.4.18-2ubuntu3.5 [86,7 kB]
```

Melakukan instalasi paket `apache2`. Apache digunakan untuk untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas web/www ini menggunakan HTTP.

b. Bukalah web browser kemudian akseslah IP dari komputer anda dan rekan praktikum anda.

```
andrian@156150600111002:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:5a:22:64
          inet addr:10.0.2.24  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5a:2264/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:6046 (6.0 KB)
```

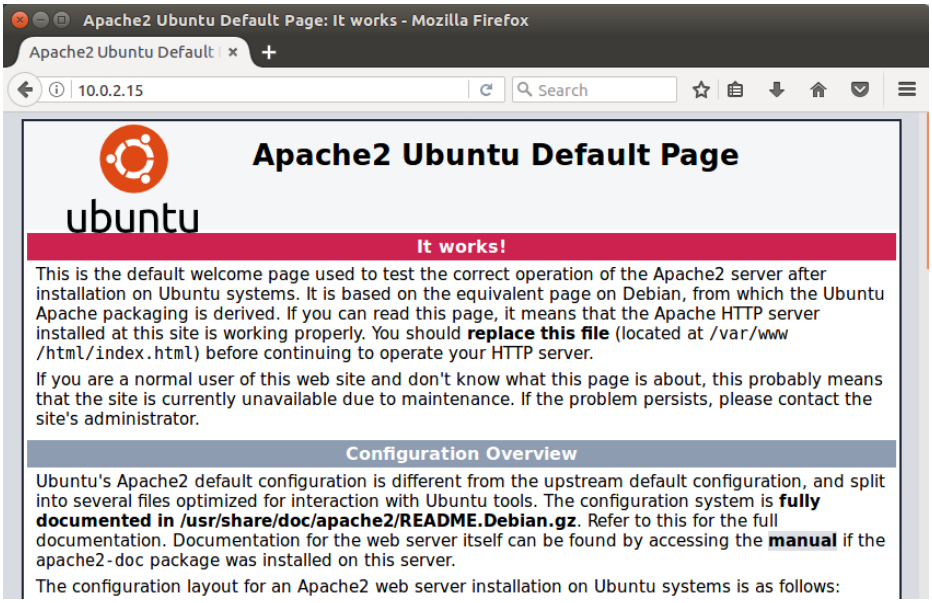
Melakukan pemerikasan untuk mengetahui berapa alamat IP komputer yang kita gunakan. Alamat IP yang didapat adalah 10.0.2.24.



Memastikan paket `apache2` yang telah kita instal berhasil, dengan cara melakukan akses alamat IP kita pada broswer. IP address komputer yang saya pakai adalah 10.0.2.24.

```
indah@156150600111008:~$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:b1:38:51
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::5a1e:f59:150:781/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:170680 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46870 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:231420258 (231.4 MB)  TX bytes:2860899 (2.8 MB)
```

Melakukan pemerikasan untuk mengetahui berapa IP address komputer yang dipakai teman saya Indah Puspitasari. Alamat IP yang didapat adalah 10.0.2.15.



Memastikan paket `apache2` yang telah kita instal berhasil, dengan cara melakukan akses alamat IP kita pada broswer. IP address komputer yang dipakai teman saya Indah Puspitasari adalah 10.0.2.15.

c. Kembalilah ke terminal dan jalankan perintah **`curl`** ***`alamat-IP-komputer`*** anda, misal **`curl http://192.168.56.101/`**. Bagaimana hasilnya? Simpulkan kegunaan dari perintah curl.

```
The program 'curl' is currently not installed. You can install it by typing:
sudo apt install curl
andrian@156150600111002:~$ sudo apt install curl
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libcurl3-gnutls
The following NEW packages will be installed:
  curl
The following packages will be upgraded:
  libcurl3-gnutls
1 upgraded, 1 newly installed, 0 to remove and 116 not upgraded.
Need to get 347 kB of archives.
After this operation, 334 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://security.ubuntu.com/ubuntu xenial-security/main i386 libcurl3-gnutl
s i386 7.47.0-1ubuntu2.4 [205 kB]
Get:2 http://security.ubuntu.com/ubuntu xenial-security/main i386 curl i386 7.47
.0-1ubuntu2.4 [142 kB]
Fetched 347 kB in 18s (18,7 kB/s)
(Reading database ... 175910 files and directories currently installed.)
Preparing to unpack .../libcurl3-gnutls_7.47.0-1ubuntu2.4_i386.deb ...
Unpacking libcurl3-gnutls:i386 (7.47.0-1ubuntu2.4) over (7.47.0-1ubuntu2.2) ...
Selecting previously unselected package curl.
```

Pastikan sebelumnya bahwa komputer kita telah terinstal paket CURL, jika belum silahkan lakukan isntalasi dengan cara `sudo apt install curl`. Curl adalah alat untuk mentransfer data dari atau ke server, menggunakan salah satu protokol yang didukung (HTTP, HTTPS, FTP, SFTP, LDAP, TELNET, IMAP, POP3, SMTP, dll.). Curl menawarkan fasilitas yang berguna seperti dukungan proxy, otentikasi pengguna, ftp upload, posting HTTP, SSL (https:) koneksi, cookies, transfer file, resume dan banyak lagi.

```
andrian@156150600111002:~$ curl http://10.0.2.24/

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.or
g/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2014-03-19
    See: https://launchpad.net/bugs/1288690
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }

  body, html {
    padding: 3px 3px 3px 3px;

    background-color: #D8DBE2;

    font-family: Verdana, sans-serif;
    font-size: 11pt;
    text-align: center;
  }

  div.main_page {
    position: relative;
    display: table;
```

Karena protokol yang kita gunakan adalah HTTP. Hasilnya setelah perintah dijalankan adalah menampilkan seluruh source code HTML dan CSS yang ada pada halaman IP yang telah kita akses. Cara ini sama seperti saat kita melakukan CTRL+U pada suatu halaman website pada broswer.

d. Jalankan perintah **`sudo iptables --append INPUT --match state --state NEW --protocol tcp --dport 80 --jump REJECT`**

```
andrian@156150600111002:~$ sudo iptables --append INPUT --match state --state NE
W --protocol tcp --dport 80 --jump REJECT
```

Menambahkan konfigurasi pada iptables.

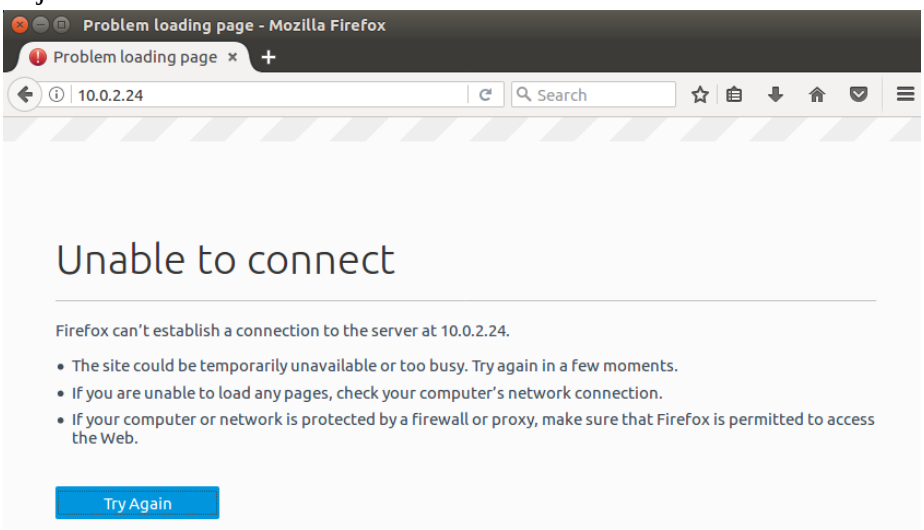
Jadi, perintah yang telah kita lakukan diatas digunakan untuk menambahkan kriteria baru pada iptables pada jalur lalu linta INPUT dengan melakukan REJECT pada protokol TCP dengan port 80(HTTP PORT).

e. Jalankan perintah **`sudo iptables --list --numeric`** untuk menampilkan rule dalam iptables. Bagimana hasilnya?

```
andrian@156150600111002:~$ sudo iptables --list --numeric
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:
80 reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Hasil dari konfigurasi yang telah dilakukan berisikan rule dalam iptables. Rule telah berubah sesuai dengan perintah yang telah dilakukan pada point 2.d yaitu menambahkan keriterian baru pada paket trafict INPUT dengan melakukan REJECT pada protokol TCP dengan port 80 (HTTP PORT).

f. Bukalah web browser dalam komputer anda kemudian akseslah kembali IP dari komputer anda dan rekan praktikum anda. Apa yang terjadi?



Koneksi yang kita lakukan menuju http://10.0.2.24 gagal/ditolak.

Koneksi yang kita lakukan menuju http://10.0.2.15 gagal/ditolak.

g. Kembalilah ke terminal dan jalankan perintah **`curl`** ***`alamat-IP-komputer`*** anda, misal **`curl http://192.168.56.101/`**. Bagaimana hasilnya?

```
andrian@156150600111002:~$ curl http://10.0.2.24/
curl: (7) Failed to connect to 10.0.2.24 port 80: Connection refused
andrian@156150600111002:~$
```

Koneksi yang kita lakukan menuju http://10.0.2.24 akan gagal/ditolak.

h. Buatkah kesimpulan mengapa kejadian pada langkah 2.f. dan 2.g. terjadi!

Jawaban:

Jadi, karena port 80 telah diblok pada iptables pada jalur lalu lintas INPUT maka akses yang kita lakukan pada semua aktifitas yang berhubungan protokol HTTP ditolak.

i. Jelaskan fungsi tiap perintah yang digunakan pada langkah 2.d.! Anda boleh menggunakan bantuan dengan menggunakan webiste https://explainshell.com/.

Jawaban:

```
andrian@156150600111002:~$ sudo iptables --append INPUT --match state --state NE
W --protocol tcp --dport 80 --jump REJECT
```

Penjelasan dari fungsi-fungsi yang digunakan pada perintah 2.d diatas:

APPEND - Perintah ini menambahkan aturan pada akhir chain. Aturan akan ditambahkan di akhir baris pada chain yang bersangkutan, sehingga akan dieksekusi terakhir.

INPUT - Aturan untuk menentukan lalu lintas masuk yang akan diterima atau ditolak

MATCHES - Artinya pendefinisian kriteria yang berlaku secara umum. Match ini mendefinisikan state apa saja yang cocok. Ada 4 state yang berlaku, yaitu NEW, ESTABLISHED, RELATED dan INVALID. NEW digunakan untuk paket yang akan memulai koneksi baru. ESTABLISHED digunakan jika koneksi telah tersambung dan paket-paketnya merupakan bagian dari koneki tersebut. RELATED digunakan untuk paket-paket yang bukan bagian dari koneksi tetapi masih berhubungan dengan koneksi tersebut, contohnya adalah FTP data transfer yang menyertai sebuah koneksi TCP atau UDP. INVALID adalah paket yang tidak bisa diidentifikasi, bukan merupakan bagian dari koneksi yang ada.

JUMP - Adalah perlakuan yang diberikan terhadap paket-paket yang memenuhi kriteria atau match. Jump memerlukan sebuah chain yang lain dalam tabel yang sama. Chain tersebut nantinya akan dimasuki oleh paket yang memenuhi kriteria.

REJECT bekerja seperti DROP, yaitu memblok paket dan menolak untuk memproses lebih lanjut paket tersebut. Tetapi, REJECT akan mengirimkan error message ke host pengirim paket tersebut. REJECT bekerja pada chain INPUT, OUTPUT dan FORWARD atau pada chain tambahan yang dipanggil dari ketiga chain tersebut.

3. Lakukan langkah-langkah berikut untuk menguji output chain dari iptables!
   a. Reset kembali iptables menggunakan langkah 1.c, kemudian jalankah langkah 1.d. Pastikan hasilnya sesuai dengan tabel pada langkah 1.d.

```
andrian@156150600111002:~$ sudo iptables --policy INPUT ACCEPT
andrian@156150600111002:~$ sudo iptables --policy FORWARD ACCEPT
andrian@156150600111002:~$ sudo iptables --policy OUTPUT ACCEPT
andrian@156150600111002:~$ sudo iptables --flush
andrian@156150600111002:~$ sudo iptables --delete-chain
andrian@156150600111002:~$
andrian@156150600111002:~$ sudo iptables --list --numeric
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
andrian@156150600111002:~$
```

   Melakukan reset pada IPTABLES.

   b. Jalankan perintah ***sudo iptables --append OUTPUT --match state --state NEW --protocol tcp --dport 80 --jump DROP***

```
andrian@156150600111002:~$ sudo iptables --append OUTPUT --match state --state N
EW --protocol tcp --dport 80 --jump DROP
andrian@156150600111002:~$
```

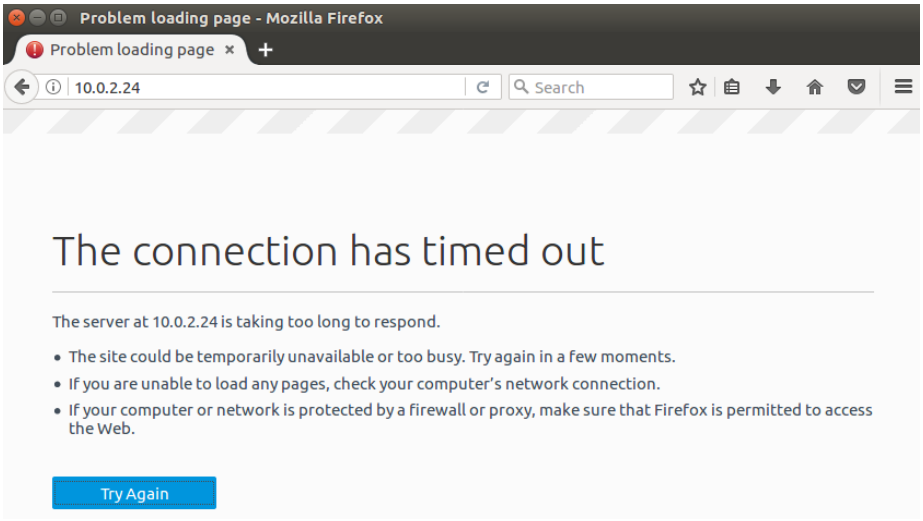
   Menambahkan keriteria baru pada iptables dengan melakukan DROP port 80, dimana port 80 adalah port untuk protokol HTTP. Pada paket traffic OUTPUT atau lalu lintas keluar.

   c. Jalankan perintah **`sudo iptables --list --numeric`** untuk menampilkan rule dalam iptables. Bagimana hasilnya?

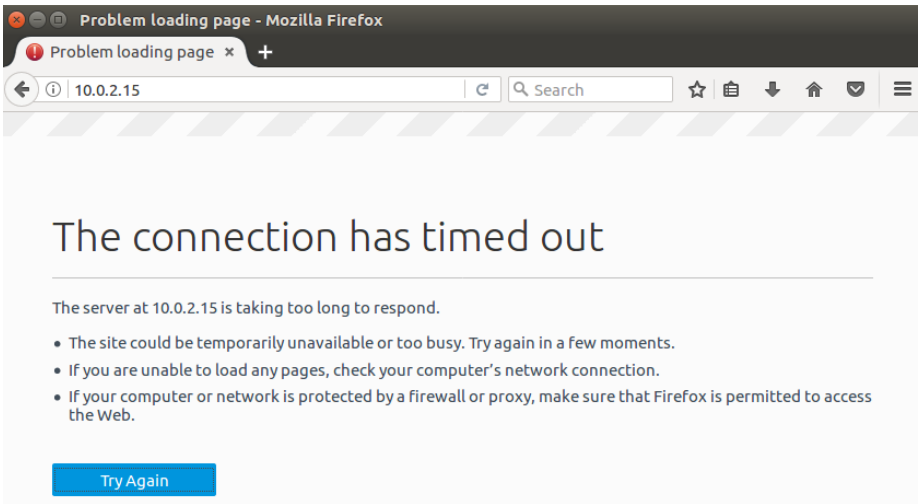
```
andrian@156150600111002:~$ sudo iptables --list --numeric
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:
80
```

   Memastikan perintah 3.b yang telah kita lakukan berhasil, dengan melihat pada list role IPTABLES.

   d. Bukalah web browser dalam komputer anda kemudian akseslah kembali IP dari komputer anda dan rekan praktikum anda. Apa yang terjadi?

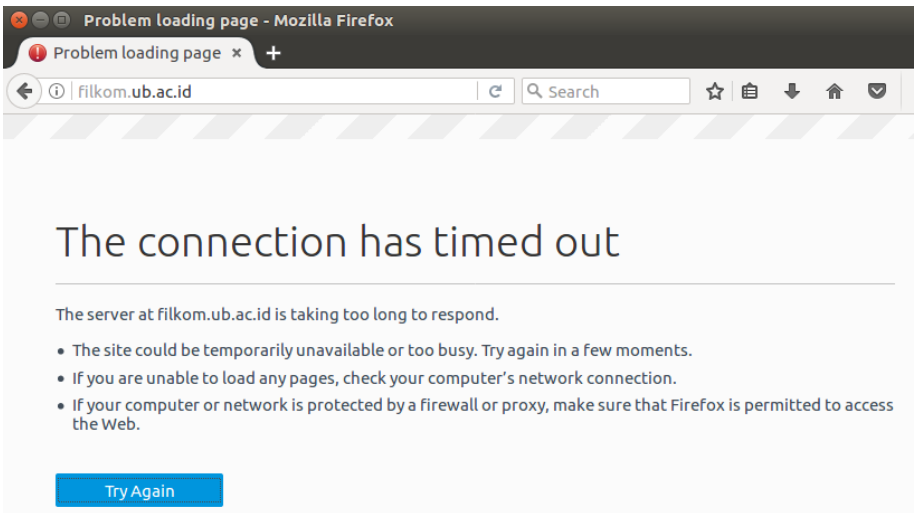


Koneksi yang kita lakukan menuju http://10.0.2.24 gagal/timed out.



Koneksi yang kita lakukan menuju http://10.0.2.15 gagal/timed out.

e. Bukalah web browser dalam komputer anda kemudian akseslah http://filkom.ub.ac.id/. Apa yang terjadi?



Koneksi yang kita lakukan menuju http://filkom.ub.ac.id gagal/timed out.

f. Kembalilah ke terminal dan jalankan perintah **`curl` *`alamat-IP-komputer`*** anda, misal **`curl http://192.168.56.101/`**. Bagaimana hasilnya?

```
andrian@156150600111002:~$ curl http://10.0.2.24/
curl: (7) Failed to connect to 10.0.2.24 port 80: Connection timed out
andrian@156150600111002:~$
```

Koneksi yang kita lakukan menuju http://10.0.2.24 gagal/timed out.

g. Jalankan perintah **`curl http://filkom.ub.ac.id/`**. Bagaimana hasilnya?

```
andrian@156150600111002:~$ curl http://filkom.ub.ac.id/
curl: (7) Failed to connect to filkom.ub.ac.id port 80: Connection timed out
andrian@156150600111002:~$
```

Koneksi yang kita lakukan menuju http://filkom.ub.ac.id gagal/timed out.

h. Buatkah kesimpulan mengapa kejadian pada langkah 3.d. hingga 3.g. terjadi!

Jawaban:

Jadi, karena port 80 telah diblok pada iptables pada jalur lalu lintas OUTPUT maka akses yang kita lakukan pada semua aktifitas yang berhubungan protokol HTTP ditolak.

i. Jelaskan fungsi tiap perintah yang digunakna pada langkah 3.b.! Anda boleh menggunakan bantuan dengan menggunakan webiste https://explainshell.com/.

Jawaban:

```
andrian@156150600111002:~$ sudo iptables --append OUTPUT --match state --state N
EW --protocol tcp --dport 80 --jump DROP
andrian@156150600111002:~$
```

Penjelasan dari fungsi-fungsi yang digunakan pada perintah 3.b diatas:

APPEND - Perintah ini menambahkan aturan pada akhir chain. Aturan akan ditambahkan di akhir baris pada chain yang bersangkutan, sehingga akan dieksekusi terakhir.

OUTPUT - Aturan untuk menentukan lalu lintas keluar yang akan diterima atau ditolak .

MATCHES - Artinya pendefinisian kriteria yang berlaku secara umum. Match ini mendefinisikan state apa saja yang cocok. Ada 4 state yang berlaku, yaitu NEW, ESTABLISHED, RELATED dan INVALID. NEW digunakan untuk paket yang akan memulai koneksi baru. ESTABLISHED digunakan jika koneksi telah tersambung dan paket-paketnya merupakan bagian dari koneki tersebut. RELATED

digunakan untuk paket-paket yang bukan bagian dari koneksi tetapi masih berhubungan dengan koneksi tersebut, contohnya adalah FTP data transfer yang menyertai sebuah koneksi TCP atau UDP. INVALID adalah paket yang tidak bisa diidentifikasi, bukan merupakan bagian dari koneksi yang ada.
JUMP - Adalah perlakuan yang diberikan terhadap paket-paket yang memenuhi kriteria atau match. Jump memerlukan sebuah chain yang lain dalam tabel yang sama. Chain tersebut nantinya akan dimasuki oleh paket yang memenuhi kriteria.
REJECT bekerja seperti DROP, yaitu memblok paket dan menolak untuk memproses lebih lanjut paket tersebut. Tetapi, REJECT akan mengirimkan error message ke host pengirim paket tersebut. REJECT bekerja pada chain INPUT, OUTPUT dan FORWARD atau pada chain tambahan yang dipanggil dari ketiga chain tersebut.

j. Apa perbedaan pesan error yang muncul pada langkah 2.g dengan 3.f? Jelaskan sebabnya!

Jawaban:

Pada langkah 2.g.

```
andrian@156150600111002:~$ curl http://10.0.2.24/
curl: (7) Failed to connect to 10.0.2.24 port 80: Connection refused
andrian@156150600111002:~$
```

Connection Refused terjadi pada saat aplikasi client membuat koneksi ke aplikasi server melalui nomor port tertentu, komputer server dalam keadaan aktif namun ternyata port tersebut tertutup, tidak menerima koneksi.

Penyebab Connection:

- Refused Aplikasi server belum dijalankan.
- Aplikasi server atau port tersebut diblokir oleh firewall di server.
- Client belum dikonfigurasi/setting koneksi salah. Setting koneksi di aplikasi client menuju ke IP server dan port yang salah.

Pada masalah diatas kesalah terjadi karena port HTTP(80) diblokir.

Pada langkah 3.f.

```
andrian@156150600111002:~$ curl http://10.0.2.24/
curl: (7) Failed to connect to 10.0.2.24 port 80: Connection timed out
andrian@156150600111002:~$
```

Connection Timeout terjadi pada saat aplikasi client sudah membuat koneksi ke aplikasi server melalui port yang dibuka oleh server, namun tidak ada respon dari aplikasi server setelah jangka waktu tertentu.

Penyebab Connection Timeout

- Aplikasi server sibuk.
- Aplikasi server mengalami overload atau kelebihan beban koneksi.
- Aplikasi server hang atau tidak merespon.

- Aplikasi client melakukan koneksi dengan waktu timeout yang sangat kecil (terlalu cepat).
- Koneksi jaringan atau internet Anda sangat lambat.

4. Berdarkan hasil latihan anda pada langkah 1 hingga 3, maka iptables tergolong firewall generasi keberapa? Jelaskan alasannya!

   Jawaban:

   Firewall Generasi Ketiga.

   Alasannya Application Layer Firewall generasi ketiga mampu memonitoring trafik hingga layer aplikasi dari OSI model seperti File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP). Firewall ini digunakan untuk mendeteksi aplikasi yang tak diinginkan yang mengganti protokol dan port standar yang seharusnya ia digunakan. Penjelasan diatas sangat sesuai dengan implementasi perintah-perintah yang telah kita lakukan pada langkah 1 sampai 3.

1.1.2. TUGAS

Buatlah sejumlah perintah iptables yang mengijinkan koneksi:

1. http (Port 80)

```
andrian@156150600111002:~$ sudo iptables --append INPUT --match state --state NE
W --protocol tcp --dport 80 --jump ACCEPT
[sudo] password for andrian:
```

```
andrian@156150600111002:~$ sudo iptables --list --numeric
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:
80

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

   Menambahkan role pada iptables untuk mengijinkan akses pada protocol http.

2. ssh dari subnet 10.0.1.150/28

```
andrian@156150600111002:~$ sudo iptables --append INPUT -s 10.0.1.150/28 --match
 state --state NEW --protocol tcp --dport 22 --jump ACCEPT
andrian@156150600111002:~$ sudo iptables --list --numeric
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:
80
ACCEPT     tcp  --  10.0.1.16/28         0.0.0.0/0            state NEW
ACCEPT     tcp  --  10.0.1.144/28        0.0.0.0/0            state NEW tcp dpt:
22

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

   Menambahkan role pada iptables untuk mengijinkan akses pada jalur ssh dari subnet 10.0.1.150/28.

3. tcp dari subnet 10.0.1.20/28

```
andrian@156150600111002:~$ sudo iptables --append INPUT -s 10.0.1.20/28 --match
state --state NEW --protocol tcp --jump ACCEPT
andrian@156150600111002:~$ sudo iptables --list --numeric
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:
80
ACCEPT     tcp  --  10.0.1.16/28         0.0.0.0/0            state NEW

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Menambahkan role pada iptables untuk mengijinkan akses pada jalur tcp dari subnet 10.0.1.20/28.

4. udp dari mac address 00:0F:EA:91:04:08

```
andrian@156150600111002:~$ sudo iptables -A INPUT -p udp -m mac -mac-source 00:0
F:EA:91:04:08 -j ACCEPT
[sudo] password for andrian:
```

Menambahkan role pada iptables untuk mengijinkan akses pada jalur udp dari mac address 00:0F:EA:91:04:08.

masuk ke dalam komputer anda;

Dan buatlah juga sejumlah perintah iptables yang menolak koneksi:

1. ke subnet 10.1.5.0/24

```
andrian@156150600111002:~$ sudo iptables --append OUTPUT -s 10.1.5.0/24 --match
state --state NEW --protocol tcp --dport 22 --jump REJECT
andrian@156150600111002:~$ sudo iptables --list --numeric
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     tcp  --  10.1.5.0/24          0.0.0.0/0            state NEW tcp dpt:
22 reject-with icmp-port-unreachable
```

Menambahkan role pada iptables untuk menolak akses ke jalur subnet 10.1.5.0/24.

2. ftp (Port 20)

```
andrian@156150600111002:~$ sudo iptables --append OUTPUT --match state --state N
EW --protocol tcp --dport 20 --jump REJECT
andrian@156150600111002:~$ sudo iptables --list --numeric
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     tcp  --  10.1.5.0/24          0.0.0.0/0            state NEW tcp dpt:
22 reject-with icmp-port-unreachable
REJECT     tcp  --  0.0.0.0/0            0.0.0.0/0            state NEW tcp dpt:
20 reject-with icmp-port-unreachable
```

Menambahkan role pada iptables untuk menolak akses ke protocol ftp.

keluar dari komputer anda!