Security APAche Web Server

Connection Limit Apache

membatasi jumlah koneksi per klien, untuk mengatasi Internet Download Manager. Kita berikan satu IP hanya bisa melakukan maksimum koneksi 5 http.

```
root@ubuntu:~# vim /etc/apache2/apache2.conf
<IfModule mpm_prefork_module>
    StartServers          5
    MinSpareServers       5
    MaxSpareServers      10
    MaxClients          150
#Maksimum 5 koneksi HTTP & HTTPS per satu alamat IP
    MaxRequestsPerChild   5
</IfModule>
```

Restart apache

```
service apache2 restart
```

Test koneksi Apache dengan 20 koneksi dan 100 request

```
ab -n 100 -c 20 http://192.168.20.20/  <-- ab tools bawaan dari apache2,
iftop -i eth0 -pP (dijalankan di server linux untuk memantau koneksi) <-- install tols iftop dulu (apt-get install iftop)
```

Disable Info Versi Apache

Melakukan disable versi apache sehingga sistem operasi dan versi compile apache tidak terlihat oleh browser maupun scanner

```
root@ubuntu:~# vim /etc/apache2/conf.d/security
ServerTokens Prod
ServerSignature Off
```

```
root@ubuntu:~# service apache2 restart
```

Test dengan nmap

```
root@lks-Lenovo-B490:~# nmap -A -T4 192.168.56.77 -p 80

Starting Nmap 5.21 ( http://nmap.org ) at 2014-08-15 13:20 WIB
Nmap scan report for 192.168.56.77
Host is up (0.00050s latency).
PORT   STATE SERVICE VERSION

### Sebelum nya 80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
80/tcp open  http    Apache httpd (Versi apache tidak muncul)
```

Membatasi Bandwidth Apache ke Klien

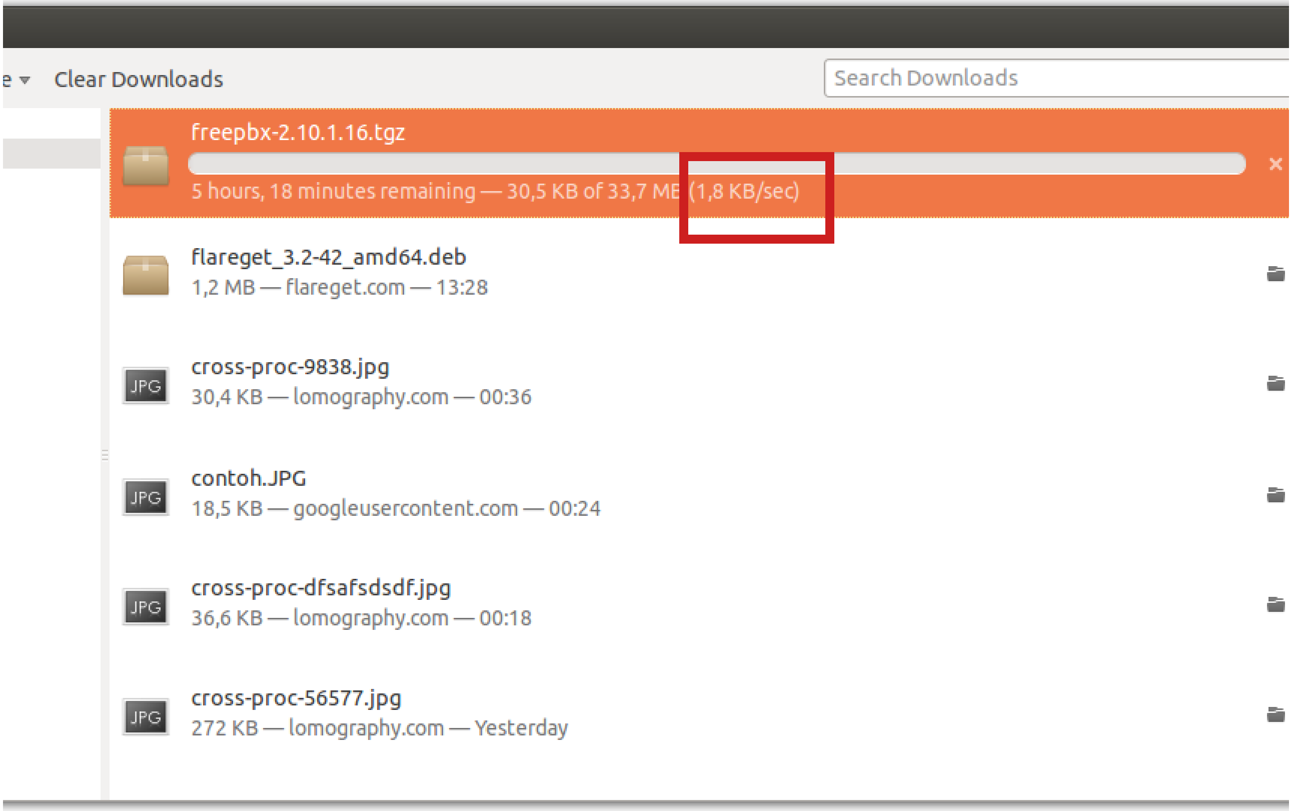
```
root@ubuntu:~# apt-get install libapache2-mod-bw
root@ubuntu:~# a2enmod bw
root@ubuntu:~# vim /etc/apache2/sites-enabled/000-default
<VirtualHost *:80>
        ServerAdmin webmaster@localhost

        DocumentRoot /var/www

#Tambahkan
        BandWidthModule On
        ForceBandWidthModule On   <--- di test error, bagian ini hapus / di tandai #
        #Maksimum Transfer Rate 2KByte /sec untuk semua klien
        BandWidth all 2000
        <Directory />
                Options FollowSymLinks
                AllowOverride None
        ......................
             .........
             etc

</VirtualHost>
```

Test dengan Firefox download file dari web server



freepbx-2.10.1.16.tgz
5 hours, 18 minutes remaining — 30,5 KB of 33,7 MB (1,8 KB/sec)

flareget_3.2-42_amd64.deb
1,2 MB — flareget.com — 13:28

cross-proc-9838.jpg
30,4 KB — lomography.com — 00:36

contoh.JPG
18,5 KB — googleusercontent.com — 00:24

cross-proc-dfsafsdsdf.jpg
36,6 KB — lomography.com — 00:18

cross-proc-56577.jpg
272 KB — lomography.com — Yesterday

BIND9 DNS Security

Disable Versi DNS
Disable Versi bertujuan agar versi BIND9 DNS kita tidak bisa dilihat oleh orang lain

```
root@lks-Lenovo-B490:~# vim /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";
        // Tambahkan
        version "LKS SMK 2014";

...
..
}
```

Restart DNS

```
root@lks-Lenovo-B490:~# service bind9 restart
```

Test DNS Version

```
root@lks-Lenovo-B490:~# dig @localhost version.bind chaos txt

; <<>> DiG 9.8.1-P1 <<>> @localhost version.bind chaos txt
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8180
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "LKS SMK 2014"

;; AUTHORITY SECTION:
version.bind.           0       CH      NS      version.bind.
```

Disable Recursion dan Transfer domain

disable recursion dan transfer domain untuk mencegah user di internet melakukan rekursi yaitu melihat isi domain yg ada di dns. Dan user di internet tidak bisa melakukan backup isi dns kita ke dns user tersebut.
User tetap dapat mendapatkan translasi alamat text www.lks2014budut.com ke alamat ip publik budut 192.168.20.20

```
root@lks-Lenovo-B490:~# vim /etc/bind/named.conf.options
// tambahkan
  allow-recursion { none; };
  allow-transfer { none; };
```

Restart Bind9

```
root@lks-Lenovo-B490:~# service bind9 restart

root@lks-Lenovo-B490:~# nslookup lks2014budut.com (resolve nama ke IP bisa sesuai fungsi dns)
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   lks2014budut.com
Address: 192.168.20.20

root@lks-Lenovo-B490:~# dig lks2014budut.com axfr (proteksi recursion & transfer domain gagal )

; <<>> DiG 9.8.1-P1 <<>> lks2014budut.com axfr
;; global options: +cmd
; Transfer failed.
```

Security SSH Server

Konfigurasi Server SSH

```
# What ports, IPs and protocols we listen for
#Remote ssh ke port 2244
Port 22 44
```

```
#tidak mengizinkan melakukan remote ssh dengan user root
PermitRootLogin no

#hanya izinkan user lks dan odik melakukan remote ssh
AllowUsers lks odik
```

Restart SSH Server

```
root@ubuntu:~# service ssh restart
```

Test Remote SSH dari client

```
root@lks-Lenovo-B490:~# ssh 192.168.20.20 -l odik -p 22 44
```

Security MySQL

Konfigurasi MySQL Server

```
root@ubuntu:~# vim /etc/mysql/my.cnf
#Bind hanya ke IP localhost
bind-address           = 127.0.0.1

#Maksimum koneksi per klien 10
max_connections        = 10
```

Berikan password root MySQL

Masuk ke Database MySQL

```
#Berikan password baru 123456 ke root MySQL Server
root@ubuntu:~# mysqladmin -u root PASSWORD 123456
```

```
#tanpa password
root@ubuntu:~# mysql -u root
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: NO)

#dengan password
root@ubuntu:~# mysql -u root -p
Enter password: <---- masukan 123456
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 88
Server version: 5.5.37-0ubuntu0.12.04.1 (Ubuntu)

Copyright (c) 2000, 2014, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```