# 2.6 Layanan Pusat Data

- Kompilasi Konfigurasi Mikrotik
  - Konfig NAT Mikrotik Agar Dapat Melihat IP Publik Visitor
  - Membuat Akses VPN dengan L2TP/IPsec
  - Konfigurasi Open VPN Server Mikrotik Dengan Mikrotik
- Pengelola Layanan Pusat Data
- Pengamanan Server
  - Pengamanan Server Menggunakan Fail2Ban
  - App Logwebmin
  - Monitoring Koneksi Aktif ke Server
  - Cek Lokasi File Exploit pada Root Web
  - Mengamankan PHP
- Optimalisasi Server
  - Konfigurasi MPM Event Apache
  - Konfigurasi Apache MPM Prefork + PHP (mod_php)

# Kompilasi Konfigurasi Mikrotik

# Konfig NAT Mikrotik Agar Dapat Melihat IP Publik Visitor

untuk mengatasi masalah agar web server atau web dapat melihat IP publik visitor yang ditempatkan pada jaringan mikrotik denga konfigurasi NAT maka dapat menggunakan fitur **Hairpin NAT atau NAT Reflection.**

Skenarionya sebagaimana contoh berikut:

server 1: 36.67.22.18 -> 192.168.80.50 port 80
server 2: 36.67.22.19 -> 192.168.80.51 port 80
server 3: 36.67.22.20 -> 192.168.80.52 port 80

permasalahnya adalah saat cek ip lewat internet di server 1, server 2 dan server 3 yang terbaca adalah ip 36.67.22.18. Artinya ip publik pertama saja yang terbaca, sedangkan ip pengunjung server yang terdeteksi hanya ip gateway nya saja:
server 1: 36.67.22.18 -> 192.168.80.50 port 80 -> terdeteksi ip pengunjung 192.168.80.1
server 2: 36.67.22.19 -> 192.168.80.51 port 80 -> terdeteksi ip pengunjung 192.168.80.1
server 3: 36.67.22.20 -> 192.168.80.52 port 80 -> terdeteksi ip pengunjung 192.168.80.1

sedangkan solusi yang diinginkan adalah ketika cek ip lewat internet setiap server terdeteksi ip publiknya masing-masing:
server 1: cek ip lewat internet -> 36.67.22.18
server 2: cek ip lewat internet -> 36.67.22.19
server 3: cek ip lewat internet -> 36.67.22.20

tujuannya adalah agar dapat melihat ip visitor yang mengunjungi website pada server:
server 1: 36.67.22.18 -> 192.168.80.50 port 80 -> terdeteksi ip publik pengunjung
server 2: 36.67.22.19 -> 192.168.80.51 port 80 -> terdeteksi ip publik pengunjung
server 3: 36.67.22.20 -> 192.168.80.52 port 80 -> terdeteksi ip publik pengunjung

nah untuk itu konfigurasinya adalah sebagai berikut:

buat rule

/ip firewall nat
add chain=srcnat src-address=192.168.80.0/24 dst-address=192.168.80.0/24 out-interface=ether8-SERVER action=masquerade

add chain=dstnat dst-address=36.67.22.18 protocol=tcp dst-port=80 action=dst-nat to-addresses=192.168.80.50 to-ports=80

add chain=dstnat dst-address=36.67.22.19 protocol=tcp dst-port=80 action=dst-nat to-addresses=192.168.80.51 to-ports=80

add chain=dstnat dst-address=36.67.22.20 protocol=tcp dst-port=80 action=dst-nat to-addresses=192.168.80.52 to-ports=80

add chain=srcnat src-address=192.168.80.50 protocol=tcp out-interface=ether8-SERVER action=masquerade

add chain=srcnat src-address=192.168.80.51 protocol=tcp out-interface=ether8-SERVER action=masquerade

add chain=srcnat src-address=192.168.80.52 protocol=tcp out-interface=ether8-SERVER action=masquerade

add chain=srcnat out-interface=ether3-WAN-ASTINET action=masquerade

# Membuat Akses VPN dengan L2TP/IPsec

Kami akan memberikan panduan untuk membuat akses VPN Server untuk jaringan internet rumah/kantor (indihome). Akses user menggunakan VPN Windows 11.

**A. Konfigurasi Mikrotik**

1. Buat IP pool untuk klien VPN

*/ip pool add name=pool-vpn ranges=192.168.89.10-192.168.89.250*

2. Buat profile PPP untuk L2TP

*/ppp profile add name=profile-vpn local-address=192.168.89.1 dns-server=8.8.8.8 remote-address=pool-vpn use-encryption=yes*

3. Tambah user (secret) -> Bisa ditambah sesuai kebutuhan

*/ppp secret add name=opd1 password=Dishub2025! service=l2tp profile=profile-vpn*

4. Aktifkan L2TP server

*/interface l2tp-server server set enabled=yes authentication=mschap2 default-profile=profile-vpn use-ipsec=required ipsec-secret=Kominfo-Hebat2025! max-mtu=1460 max-mru=1460*

5. Konfigurasi IPsec (policy/proposal)

*/ip ipsec proposal set [find default=yes] auth-algorithms=sha1 enc-algorithms=aes-128-cbc,aes-256-cbc pfs-group=none*

6. Firewall: izinkan paket IPsec & L2TP (UDP 500, UDP 1701, UDP 4500, ESP)

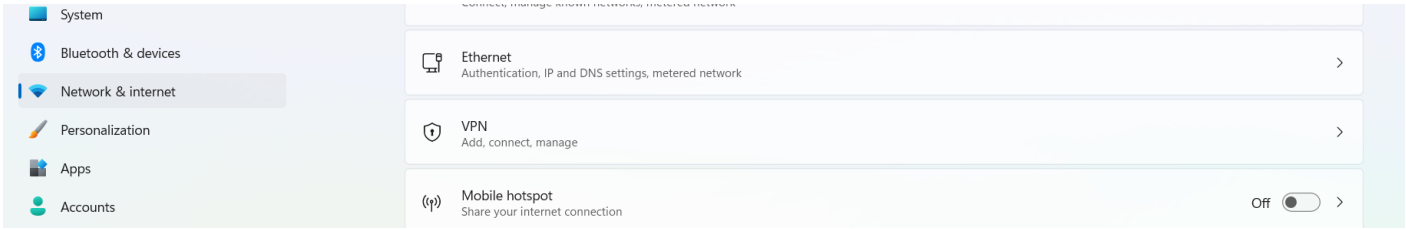
*/ip firewall filter add chain=input protocol=udp dst-port=500,1701,4500 action=accept comment="Allow IPsec/L2TP UDP"*
*# Allow ESP (protocol 50)*
*/ip firewall filter add chain=input protocol=ipsec-esp action=accept comment="Allow ESP"*
*# Allow established/related (biasanya sudah ada)*

7. NAT: masquerade agar client bisa akses internet melalui router

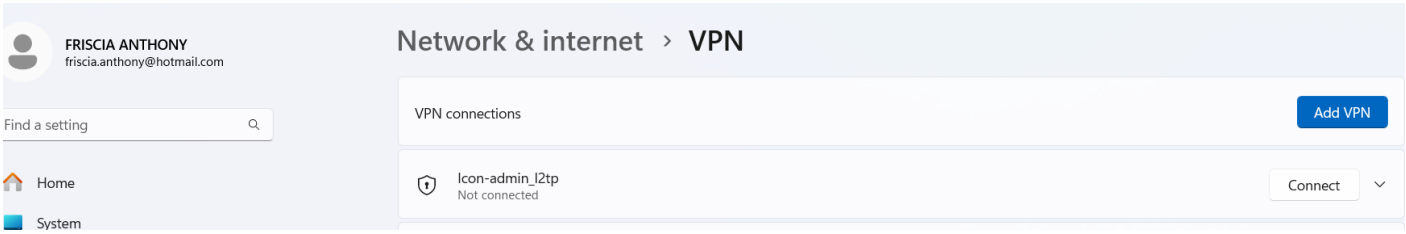
*/ip firewall nat add chain=srcnat src-address=192.168.89.0/24 out-interface=<WAN-INTERFACE-NAME> action=masquerade comment="NAT VPN clients"*

## B. Akses Pengguna VPN

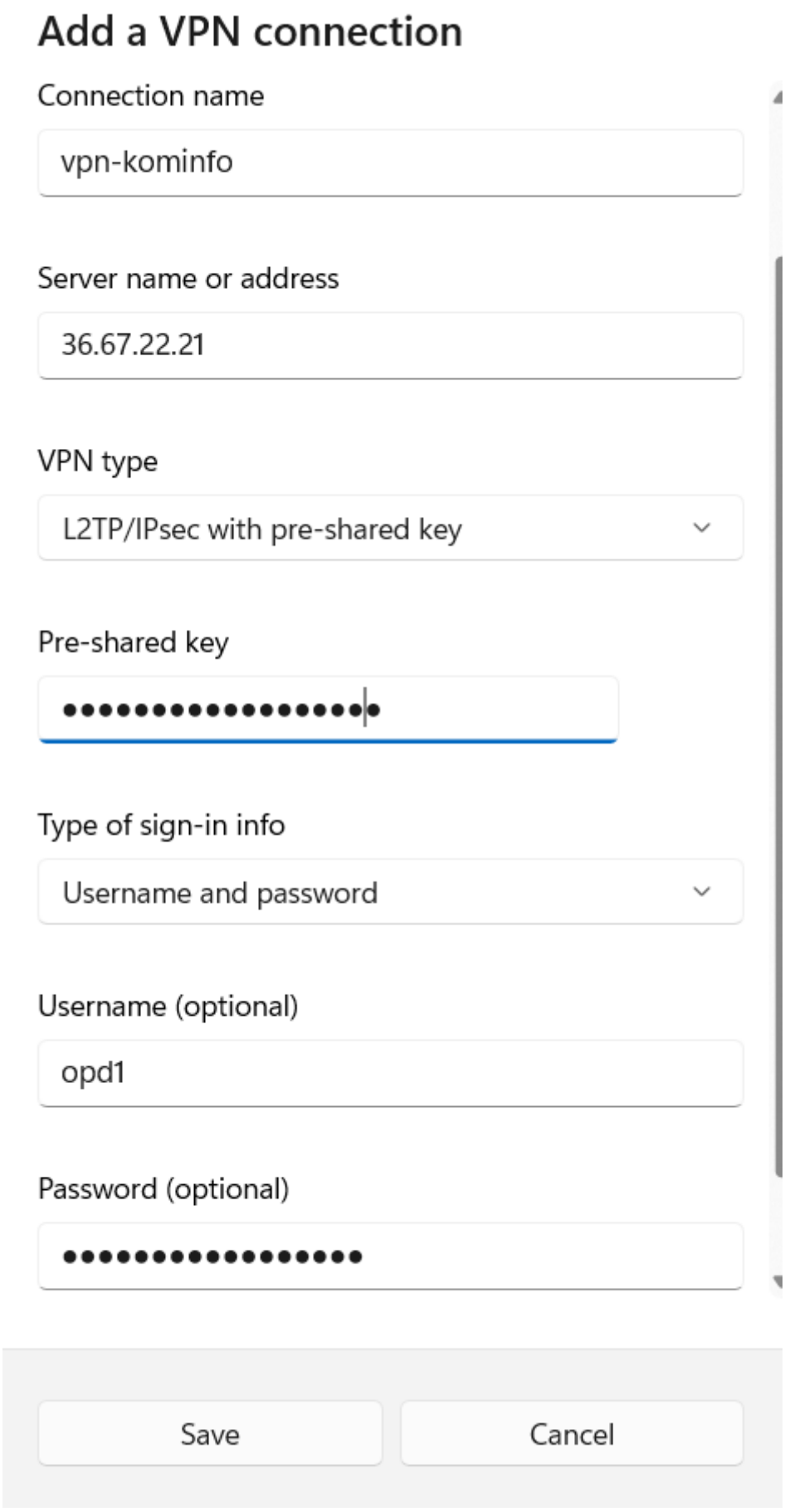
1. Buka Setting - Network & Internet




2. Buka VPN

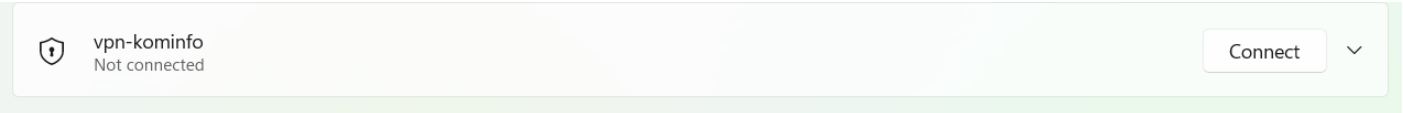



3. Add VPN -> isi sesuai password ipsec, username dan passwordnya.

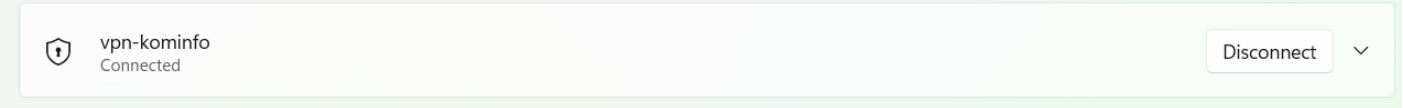

Add a VPN connection
Connection name
vpn-kominfo
Server name or address
36.67.22.21
VPN type
L2TP/IPsec with pre-shared key
Pre-shared key
Type of sign-in info
Username and password
Username (optional)
opd1
Password (optional)
Save
Cancel

4. Save

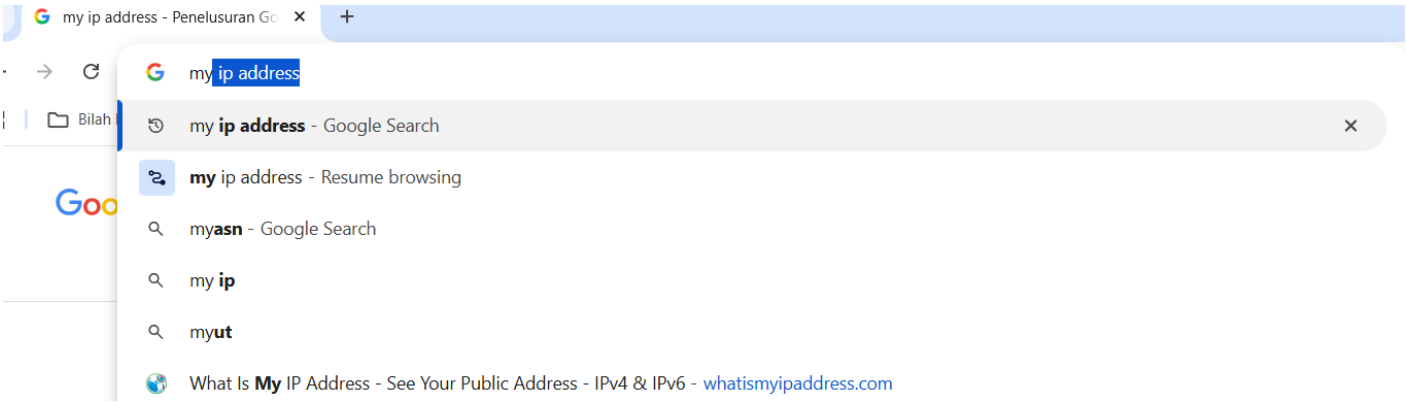
5. Connect

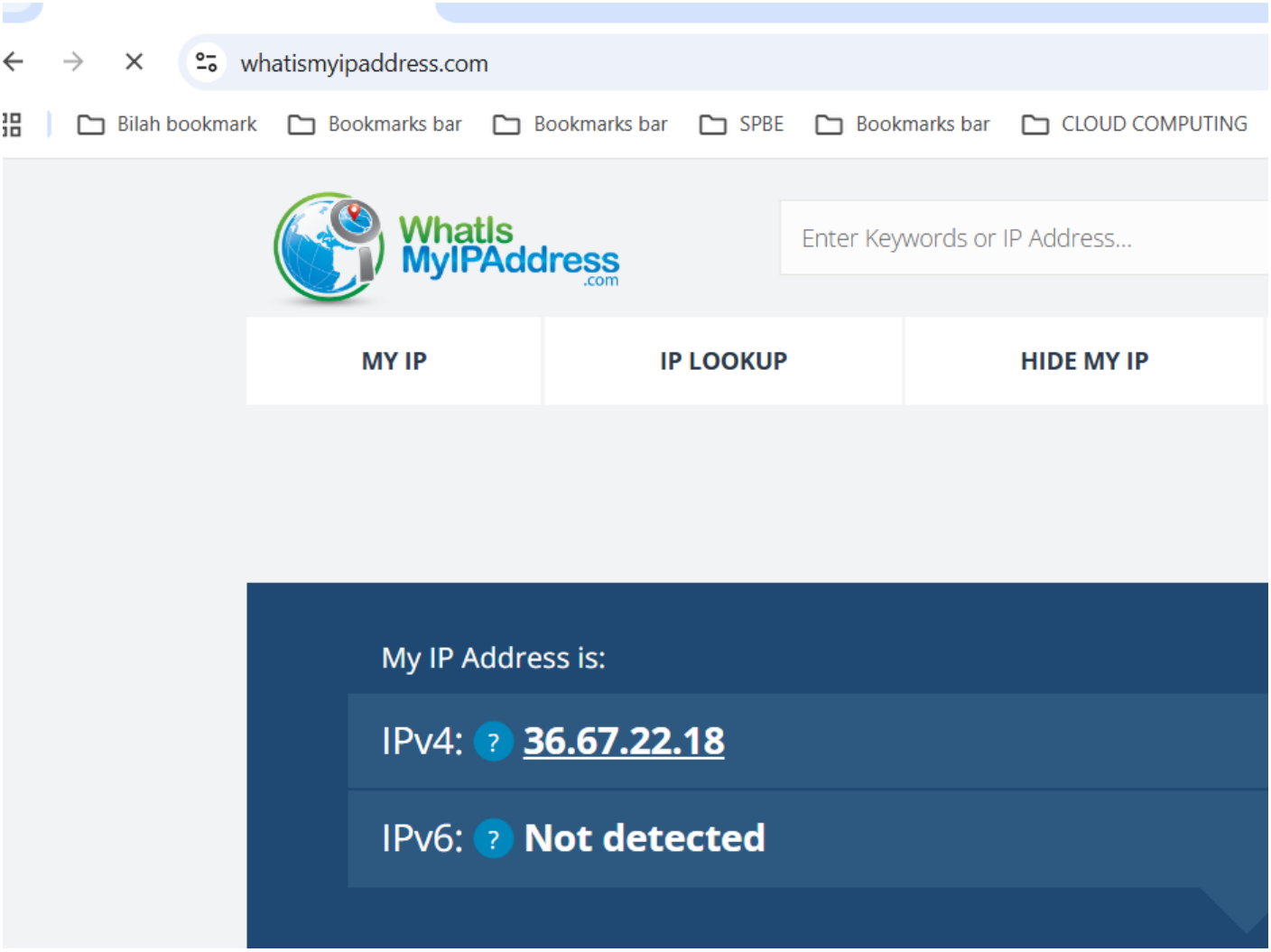



6. Jika berhasil maka status Connected




7. coba akses browser dan ketikan my ip address. jika berhasil maka ip publik terdeteksi sama dengan ip publik pada VPN Server.






**Video Tutorial**

https://www.youtube.com/embed/evgP7zvdvas

# Konfigurasi Open VPN Server Mikrotik Dengan Mikrotik

Tujuan : agar client terhubung secara lokal pada jaringan 192.168.80.0/24

**1. Informasi Sistem**

- Router: **MikroTik RouterOS**
- VPN Protocol: **OpenVPN**
- LAN Server: 192.168.80.0/24
- Gateway LAN: 192.168.80.1
- Subnet VPN: 10.10.10.0/24
- Port OVPN: 1194 (TCP)

**2. Pembuatan Sertifikat di MikroTik**

**2.1 Buat CA (Certificate Authority)**

Buka terminal mikrotik:

```
/certificate
add name=ca-template common-name=MyCA key-usage=key-cert-sign,crl-sign
sign ca-template name=MyCA
```

Cek status Pastikan CA statusnya: `trusted=yes`

```
/certificate print
```

Jika belum:

```
/certificate set MyCA trusted=yes
```

**2.2 Buat Sertifikat Server**

```
/certificate
add name=server-template common-name=ovpn-server
sign server-template ca=MyCA name=ovpn-server
```

```
/certificate set ovpn-server trusted=yes
```

**2.3 Buat Sertifikat Client**

```
/certificate
add name=client1-template common-name=client1
```

```
sign client1-template ca=MyCA name=client1
```

### 2.4 Export Sertifikat ke Client

```
/certificate export-certificate client1 export-passphrase=1234
/certificate export-certificate MyCA
```

File yang akan muncul di Files:

- client1.crt
- client1.key
- MyCA.crt

Download file tersebut ke PC client.

## 3. Konfigurasi OVPN Server

### 3.1 Buat IP Pool

```
/ip pool
add name=ovpn-pool ranges=10.10.10.10-10.10.10.50
```

### 3.2 Buat PPP Profile

```
/ppp profile
add name=ovpn-profile \
local-address=10.10.10.1 \
remote-address=ovpn-pool \
dns-server=8.8.8.8
```

### 3.3 Buat User VPN

```
/ppp secret
add name=user1 \
password=123456 \
service=ovpn \
profile=ovpn-profile
```

### 3.4 Aktifkan OVPN Server

```
/interface ovpn-server server
set enabled=yes \
port=1194 \
mode=ip \
netmask=24 \
authentication=sha1 \
cipher=aes256 \
certificate=ovpn-server \
require-client-certificate=yes
```

## 4. Firewall

### 4.1 Allow Port OVPN

```
/ip firewall filter
add chain=input protocol=tcp port=1194 action=accept comment="Allow OVPN"
```

### 4.2 NAT Internet

```
/ip firewall nat
add chain=srcnat out-interface=ether3-WAN action=masquerade
```

## 5. Konfigurasi Client Windows

### 5.1 Install OpenVPN Client

Download pada https://openvpn.net/community/ atau untuk mencari repository lama pada https://build.openvpn.net/downloads/releases/?C=M&O=D

lalu Install OpenVPN GUI.

### 5.2 Copy File Sertifikat

File:

- **MyCA.crt**
- **client1.crt**
- **client1.key**

untuk dibuat **client1.ovpn** :

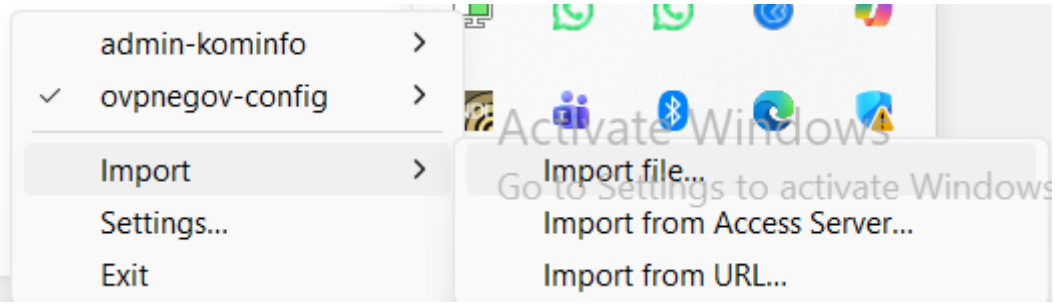
```
client
dev tun
proto tcp-client
remote 36.67.22.18 1194
route 192.168.80.0 255.255.255.0
resolv-retry infinite
nobind
persist-key
persist-tun

auth SHA1
cipher AES-256-CBC
data-ciphers AES-256-GCM:AES-128-GCM:AES-256-CBC
data-ciphers-fallback AES-256-CBC

remote-cert-tls server
auth-user-pass
auth-nocache

<ca>
sertifikat dalam MyCA.crt
```

</ca>

<cert>
sertifikat dalam client1.crt
</cert>

<key>
sertifikat dalam client1.key
</key>

### 5.3 Import File Sertifikat client1.ovpn pada OpenVPN GUI

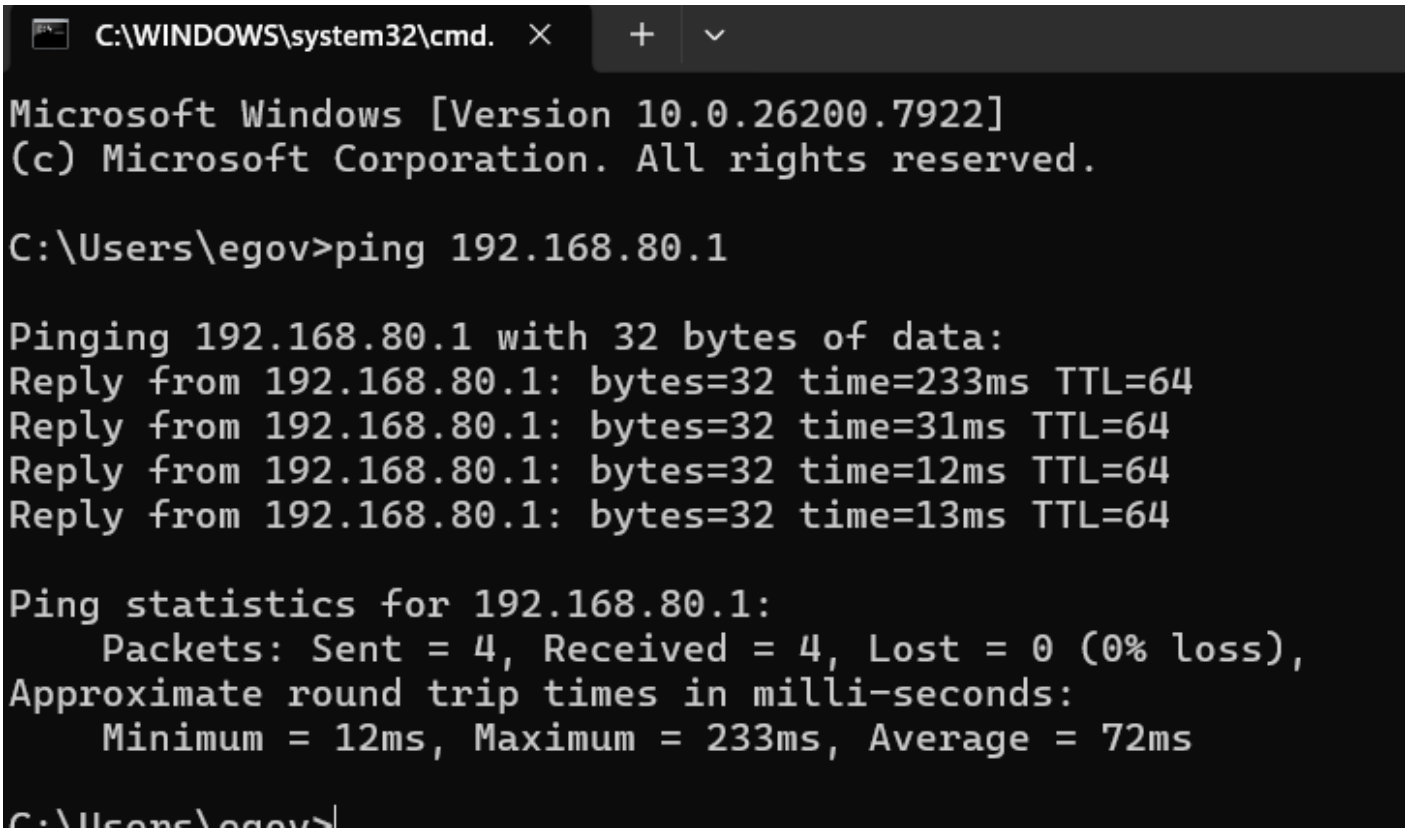



### 6. Connect VPN

- Jalankan OpenVPN GUI
- Klik kanan → Connect
- Masukkan username & password secret PPP

### 7. Verifikasi

Uji koneksi ke 192.168.80.1


C:\WINDOWS\system32\cmd.
Microsoft Windows [Version 10.0.26200.7922]
(c) Microsoft Corporation. All rights reserved.
C:\Users\egov>ping 192.168.80.1
Pinging 192.168.80.1 with 32 bytes of data:
Reply from 192.168.80.1: bytes=32 time=233ms TTL=64
Reply from 192.168.80.1: bytes=32 time=31ms TTL=64
Reply from 192.168.80.1: bytes=32 time=12ms TTL=64
Reply from 192.168.80.1: bytes=32 time=13ms TTL=64
Ping statistics for 192.168.80.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 12ms, Maximum = 233ms, Average = 72ms

# Pengelola Layanan Pusat Data

1. Penanggung jawab Pengelola Layanan Pusat Data Nasional untuk Pemerintah Kabupaten Barito Timur SK SEKDA PENANGGUNG JAWAB LAYANAN PUSAT DATA NASIONAL UNTUK KABUPATEN BARITO TIMUR
2. Tim Pengelola Layanan Pusat Data Kabupaten Barito Timur SK SEKDA PENGELOLA LAYANAN PUSAT DATA KABUPATEN BARITO TIMUR
3. Dalam mengelola Layanan Pusat Data Kabupaten Barito Timur memiliki SOP SK SEKDA BARTIM SOP LAYANAN PUSAT DATA

# Pengamanan Server

# Pengamanan Server Menggunakan Fail2Ban

Fail2Ban disini ditujukan untuk memblokir IP client yang melakukan aktivitas berbahaya pada aplikasi/website pada server.

**Installasi:**

```
sudo apt install fail2ban
```

**Konfigurasi Dasar untuk SSH**

```
sudo nano /etc/fail2ban/jail.local
```

**isi:**

```
[sshd]
enabled = true
port = ssh
filter = sshd
logpath = /var/log/auth.log
maxretry = 5
bantime = 1h
findtime = 10m

[apache-auth]
enabled = true
port = http,https
logpath = /var/log/apache*/*error.log
maxretry = 5
```

**Restart Fail2Ban**

```
sudo systemctl restart fail2ban
```

sudo systemctl enable fail2ban

**Cek Status Jail**

```
sudo fail2ban-client status
```

Metode pengamanan paling baik dengan Fail2Ban adalah dengan menyesuaikan perilaku atau aktivitas client dalam mengakses aplikasi/website pada server. Cara mudahnya adalah melihat error yang dihasil pada tail -f /var/log/apache2/error.log.

Dari error.log tersebut dihasilkan informasi aktivitas client yang melakukan upaya berbahaya yang menghasilkan error pada server apache.

Sebagai contoh saya mau memblokir IP client dengan aktivitas error berikut:
\[Fri May 16 19:32:01.013545 2025] \[proxy_fcgi\:error] \[pid 1496923] \[client 159.65.1.31:55208] AH01071: Got error 'PHP message: PHP Warning: Constant WP_MEMORY_LIMIT already defined in /var/www/html/dpmdsos/public_html/wp-config.php on line 98' \[Fri May 16 19:32:01.330516 2025] \[proxy_fcgi\:error] \[pid 1496903] \[client 159.65.1.31:55174] AH01071: Got error 'PHP message: PHP Warning: The magic method Vc_Manager::__wakeup() must have public visibility in /var/www/html/dpupkp/public_html/wp-content/plugins/js_composer/include/classes/core/class-vc-manager.php on line 203' \[Fri May 16 19:32:01.505303 2025] \[proxy_fcgi\:error] \[pid 1496930] \[client 159.65.1.31:55479] AH01071: Got error 'PHP message: PHP Warning: Constant WP_MEMORY_LIMIT already defined in /var/www/html/dpmdsos/public_html/wp-config.php on line 98' \[Fri May 16 19:32:01.726184 2025] \[proxy_fcgi\:error] \[pid 1497083] \[client 159.65.1.31:55322] AH01071: Got error 'PHP message: PHP Warning: The magic method Vc_Manager::__wakeup() must have public visibility in /var/www/html/disperpusip/public_html/wp-content/plugins/js_composer/include/classes/core/class-vc-manager.php on line 203' \[Fri May 16 19:32:01.773397 2025] \[autoindex\:error] \[pid 1487621] \[client 209.38.120.221:57305] AH01276: Cannot serve directory /var/www/html/inspektorat/public_html/.well-known/: No matching DirectoryIndex (index.html,index.cgi,index.pl,index.php,index.xhtml,index.htm) found, and server-generated directory index forbidden by Options directive \[Fri May 16 19:32:01.836303 2025] \[autoindex\:error] \[pid 1487621] \[client 209.38.120.221:57305] AH01276: Cannot serve directory /var/www/html/inspektorat/public_html/.well-known/pki-validation/: No matching DirectoryIndex (index.html,index.cgi,index.pl,index.php,index.xhtml,index.htm) found, and server-generated directory index forbidden by Options directive \[Fri May 16 19:32:01.907570 2025] \[autoindex\:error] \[pid 1487621] \[client 209.38.120.221:57305] AH01276: Cannot serve directory /var/www/html/inspektorat/public_html/.well-known/acme-challenge/: No matching DirectoryIndex (index.html,index.cgi,index.pl,index.php,index.xhtml,index.htm) found, and server-generated directory index forbidden by Options directive

maka saya membuat file filter baru di `nano /etc/fail2ban/filter.d/apache-php-errors.conf`

**isi:**

```
[Definition]
failregex = ^\[[^\]]*\] \[[^\]]*\] \[pid [0-9]*\] \[client <HOST>:[0-9]*\] AH01071: Got error 'PHP message: PHP Warning:.*$
            ^\[[^\]]*\] \[autoindex:error\] \[pid [0-9]*\] \[client <HOST>:[0-9]*\] AH01276: Cannot serve directory.*$
ignoreregex =
```

***Note: gunakan Chatgpt atau Deepseek untuk membuat  koding filter***

Kemudian tambahkan jail baru di `/etc/fail2ban/jail.local`

Isi:

```
[apache-php-errors]
enabled  = true
port     = http,https
filter   = apache-php-errors
logpath  = /var/log/apache2/error.log
maxretry = 5
findtime = 10m
bantime  = 1h
```

Restart Fail2Ban

`sudo systemctl restart fail2ban`

Kemudian cek untuk melihat IP client sudah diblokir

`sudo fail2ban-client status apache-php-errors`

Silahkan tambahkan lagi filter lainnya sesuai dengan error.log yang diperoleh.

Apabila suatu waktu anda pun tidak dapat mengakses aplikasi/website pada server anda. Maka ada kemungkinan anda pun juga sudah diblokir oleh filter Fail2Ban yang anda buat sendiri. Maka kerjakan Tips berikut jika terjadi.

sudo fail2ban-client status <nama_jail>
# Contoh:

`sudo fail2ban-client status apache-php-errors`

Jika dipastikan memang IP anda yang diblokir maka lakukan seperti contoh berikut:

`sudo fail2ban-client set apache-wp-warnings unbanip 36.75.65.41`

dan cara paling aman adalah dengan membuat **Whitelist IP Anda** di `nano /etc/fail2ban/jail.local`

Isi:

```
[DEFAULT]
ignoreip = 127.0.0.1/8 ::1 36.75.65.41
```

atau kurangi agresivitas jail:

```
[apache-php-errors]
enabled  = true
port     = http,https
filter   = apache-php-errors
logpath  = /var/log/apache2/error.log
maxretry = 10            #ubah dari 5 jadi 10
findtime = 30m           #ubah dari 10 jadi 30
bantime  = 1h            #ubah dari 24h jadi 1h
```

Lakukan Monitoring lol Fail2Ban:

`sudo tail -f /var/log/fail2ban.log`

Cek daftar IP yang sudah diblokir fail2ban:

```
for jail in $(fail2ban-client status | grep 'Jail list' | cut -d: -f2 | tr ',' '\n' | tr -d ' '); do
    echo "== Jail: $jail ==";
    fail2ban-client status "$jail" | grep 'Banned IP list';
    echo;
done
```

Buka semua IP yang diblokir ada filter fail2ban:

```
for jail in $(fail2ban-client status | grep 'Jail list:' | cut -d: -f2 | tr -d ' ' | tr ',' ' '); do
  echo "Checking jail: $jail"
  banned_ips=$(fail2ban-client status "$jail" | grep 'Banned IP list' | cut -d: -f2)
  for ip in $banned_ips; do
    fail2ban-client set "$jail" unbanip "$ip" && echo "→ Unbanned $ip from $jail"
  done
done
```

Buka Blokir khusus Jail tertentu. ini misalnya modsecurity-aggressive:

```
for ip in $(sudo fail2ban-client status modsecurity-aggressive | grep 'Banned IP list:' | awk -F': ' '{print $2}'); do
    sudo fail2ban-client set modsecurity-aggressive unbanip $ip
done
```

Cara Membuka blokir IP tertentu pada semua jail:

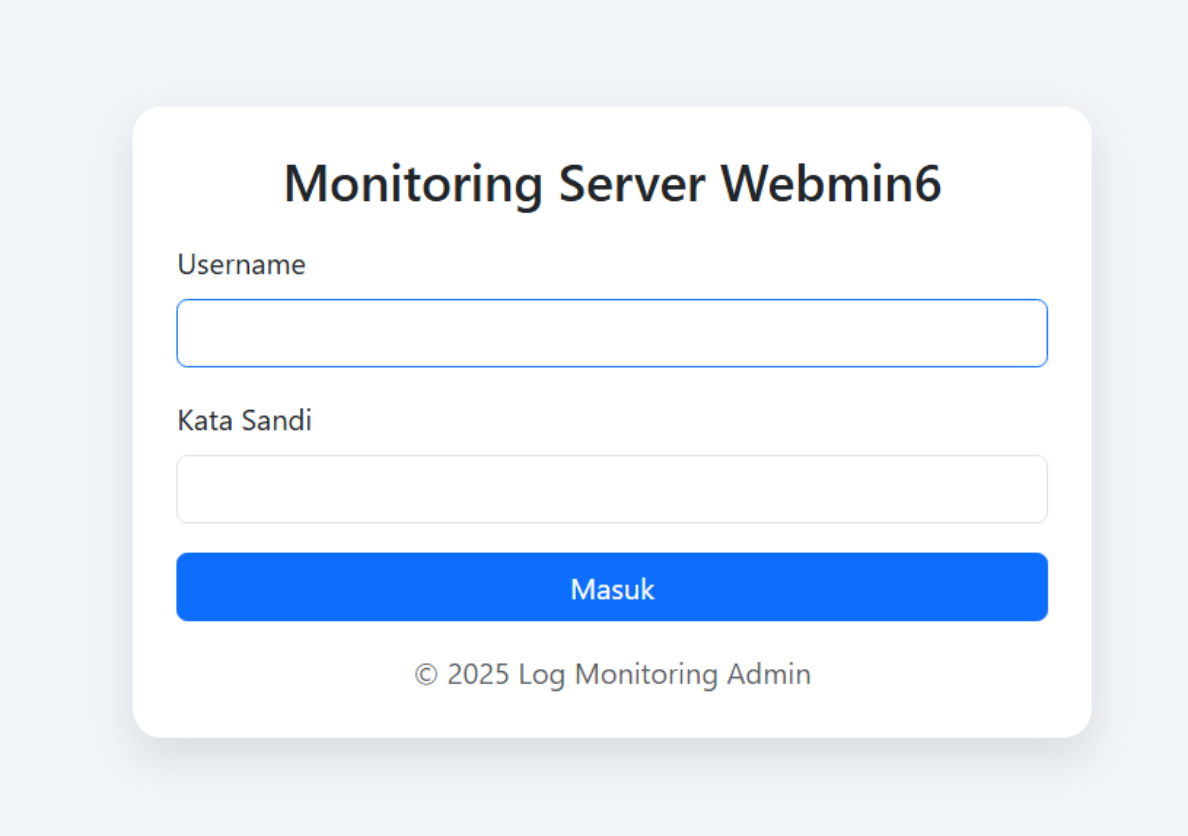
```
IP="182.8.131.150"
```

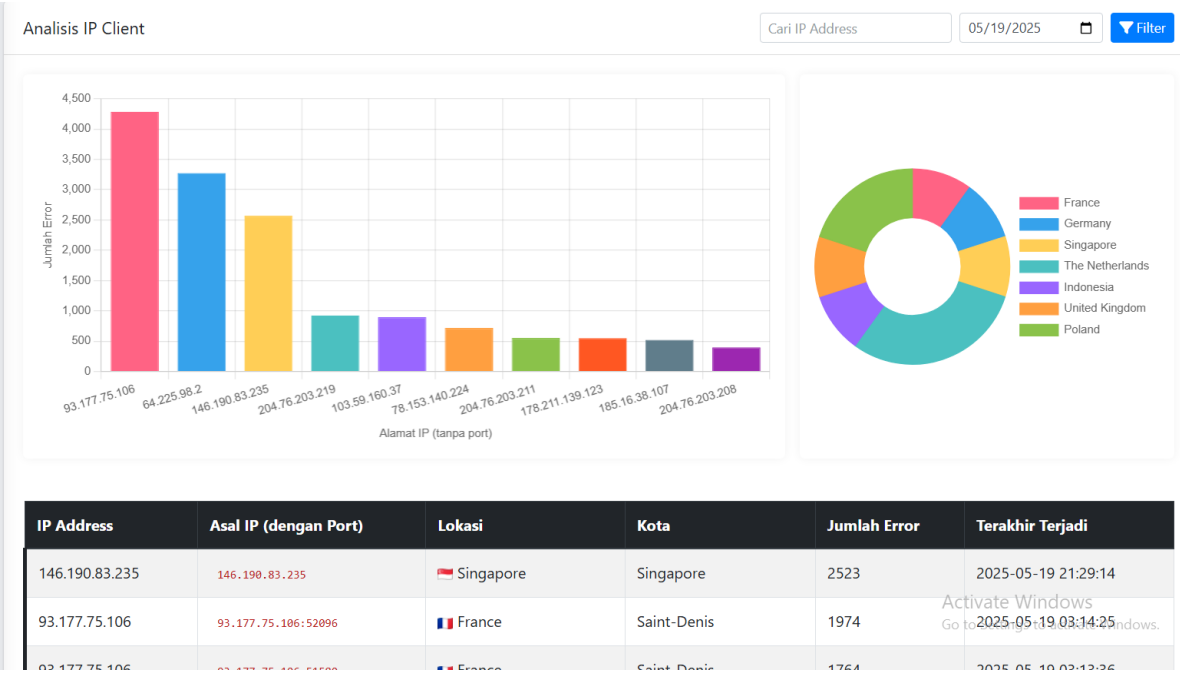
```
for jail in $(fail2ban-client status | grep 'Jail list:' | cut -d: -f2 | tr -d ' ' | tr ',' ' '); do
  echo "Checking jail: $jail"
  if fail2ban-client status "$jail" | grep -q "$IP"; then
    fail2ban-client set "$jail" unbanip "$IP" && echo "→ Unbanned $IP from $jail"
  else
    echo "No ban for $IP in $jail"
  fi
done
```

Pengamanan Server

# App Logwebmin

Aplikasi ini adalah hasil pengembangan mandiri Dinas Kominfo Bartim untuk memonitoring dan memblokir aktivitas client yang mencurigakan pada server webmin (server apache).



**Apikasi ini telah diinstall pada server Apache dengan spesifikasi:**

1. CPU 8x Intel(R) Xeon(R) Bronze 3206R CPU @ 1.90GHz (1 Socket)
2. RAM 32 GB
3. HDD 100GB
4. OS Linux Mint 20.2

Aplikasi dapat diunduh pada link **Cloud Repositori Bartim**.

**Petunjuk Instalasi:**

1. Upload file aplikasi pada /var/www/html/logwebmin

2. Buat konfigurasi virtual domain pada /etc/apache2/sites-available/000-default.conf

```
<VirtualHost *:80>
    ServerName log6.baritotimurkab.go.id
    DocumentRoot /var/www/html/logwebmin/public
    RewriteEngine on
    DocumentRoot /var/www/html/logwebmin/public
    RewriteCond %{SERVER_NAME} =www.log6.baritotimurkab.go.id [OR]
    RewriteCond %{SERVER_NAME} =log6.baritotimurkab.go.id
    RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R=permanent]
</VirtualHost>
```

3. Buat ssl dengan letsencrypt

4. Buat konfigurasi virtual domain ssl pada /etc/apache2/sites-available/default-ssl.conf

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
    ServerName log6.baritotimurkab.go.id
    DocumentRoot /var/www/html/logwebmin/public

    SSLEngine on
    SSLCertificateFile /etc/letsencrypt/live/log6.baritotimurkab.go.id/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/log6.baritotimurkab.go.id/privkey.pem
    Include /etc/letsencrypt/options-ssl-apache.conf

    ErrorLog ${APACHE_LOG_DIR}/logwebmin_error.log
    CustomLog ${APACHE_LOG_DIR}/logwebmin_access.log combined
</VirtualHost>
</IfModule>
```

5. Buat inisiasi fitur socket
**nano /etc/systemd/system/ipblock.service**

isi:

```
[Unit]
Description=IP Blocking Service
Requires=ipblock.socket

[Service]
Type=simple
ExecStart=/usr/local/bin/ipblock-daemon
User=www-data
Group=www-data
Restart=always
RestartSec=5
Environment="SOCKET_PATH=/var/www/html/logwebmin/storage/sockets/ipblock.sock"

[Install]
WantedBy=multi-user.target
```

**nano /etc/systemd/system/ipblock.socket**
isi:

```
[Unit]

Description=IP Blocking Socket

[Socket]
ListenStream=/var/www/html/logwebmin/storage/sockets/ipblock.sock
SocketUser=www-data
SocketGroup=www-data
SocketMode=0660

[Install]
WantedBy=sockets.target
```

**nano /usr/local/bin/ipblock-daemon** (berikan permissions 0755 dan ownership www-data)
isi:

```
#!/usr/bin/python3

import socket
import os
import subprocess
import re

SOCKET_PATH = '/var/www/html/logwebmin/storage/sockets/ipblock.sock'
```

```
# Setup socket directory
os.makedirs(os.path.dirname(SOCKET_PATH), exist_ok=True)

# Remove old socket if exists
try:
    os.unlink(SOCKET_PATH)
except FileNotFoundError:
    pass

# Create and bind socket
sock = socket.socket(socket.AF_UNIX, socket.SOCK_STREAM)
sock.bind(SOCKET_PATH)
sock.listen(1)
os.chmod(SOCKET_PATH, 0o660)
os.chown(SOCKET_PATH, 33, 33)  # www-data user and group ID

def validate_ip(ip):
    """Validate IPv4 address format"""
    pattern = r'^(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-
5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)$'
    return re.match(pattern, ip) is not None

while True:
    conn, _ = sock.accept()
    try:
        data = conn.recv(1024).decode().strip()
        if not data:
            continue

        # Handle unblock command
        if data.startswith('unblock:'):
            ip = data.split(':')[1]
            if validate_ip(ip):
                try:
                    subprocess.run(['sudo', '/usr/local/bin/unblock-ip.sh', ip], check=True)
                    conn.send(b"OK")
                except subprocess.CalledProcessError as e:
                    conn.send(f"ERROR: Unblock failed - {str(e)}".encode())
            else:
                conn.send(b"ERROR: Invalid IP format for unblock")

        # Handle block command (original functionality)
        else:
            ip = data
            if validate_ip(ip):
                try:
```

```
                subprocess.run(['sudo', '/usr/local/bin/block-ip.sh', ip], check=True)
                conn.send(b"OK")
            except subprocess.CalledProcessError as e:
                conn.send(f"ERROR: Block failed - {str(e)}".encode())
        else:
            conn.send(b"ERROR: Invalid IP format for block")

    except Exception as e:
        conn.send(f"ERROR: Server error - {str(e)}".encode())
    finally:
        conn.close()
```

**nano /usr/local/bin/block-ip.sh**
isi:
```
#!/bin/bash
IP=$1
iptables -A INPUT -s $IP -j DROP
```

**nano /usr/local/bin/unblock-ip.sh**
isi:
```
#!/bin/bash
IP=$1
iptables -D INPUT -s $IP -j DROP
```

6. Berikan akses www-data untuk menjalankan shell block-ip.sh dan unblock-ip.sh
**nano /etc/sudoers**
isi:
```
#

# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults    env_reset
Defaults    mail_badpass
Defaults    secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification
```

```
# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo    ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

#fungsi tambahan blokir lewa app logwebmin
www-data ALL=(ALL) NOPASSWD: /usr/local/bin/block-ip.sh
www-data ALL=(ALL) NOPASSWD: /usr/local/bin/unblock-ip.sh
```

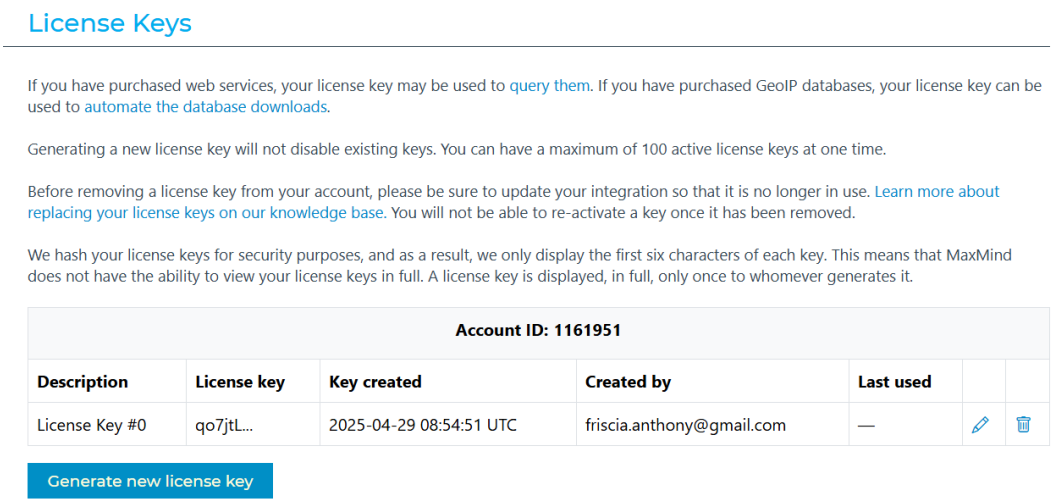
7. Jalankan service daemon

**sudo systemctl daemon-reload**
**sudo systemctl restart ipblock.socket ipblock.service**
**sudo systemctl enable ipblock.socket**

8. Verifikasi service

**sudo systemctl status ipblock.service**
**journalctl -u ipblock.service -f**

9. Pastikan anda telah mendaftar akun pada https://www.maxmind.com/ untuk mendapatkan license-key seperti pada contoh berikut:




agar dapat diinisiasikan pada .env

.env (/var/www/html/logwebmin)

```
APP_NAME=Laravel
APP_ENV=production
APP_KEY=base64:6Nfn6cKTJBemSHH99Cn5Kb7e8u0sVuYCGHjvtg0/rLQ=
APP_DEBUG=true
APP_URL=http://localhost
MAXMIND_LICENSE_KEY=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
```

# Monitoring Koneksi Aktif ke Server

Untuk melihat koneksi aktif ke server Anda, termasuk IP yang terhubung, gunakan `netstat`:
secara real time setiap 2 detik:

```
watch -n 2 netstat -ntu
```

contoh hasil:

```
Every 2.0s: netstat -ntu                                kominfos-0B: Tue Jun 24 21:28:23 2025  Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:3306          127.0.0.1:47308         ESTABLISHED
tcp        0      0 127.0.0.1:57164         127.0.0.1:556           ESTABLISHED
tcp        0      0 127.0.0.1:38366         127.0.0.1:3306          ESTABLISHED
tcp        0      0 127.0.0.1:556           127.0.0.1:57164         ESTABLISHED
tcp        0      0 192.168.80.51:22        196.251.70.166:57154    ESTABLISHED
tcp        0      0 192.168.80.51:41344     91.189.91.48:80         TIME_WAIT
tcp        0      0 192.168.80.51:2014      222.124.78.211:59143    ESTABLISHED
tcp        0      0 127.0.0.1:47308         127.0.0.1:3306          ESTABLISHED
tcp        0      0 127.0.0.1:3306          127.0.0.1:38366         ESTABLISHED
tcp        0      0 192.168.80.51:22        222.124.78.211:59160    ESTABLISHED
tcp6       0      0 192.168.80.51:443       114.125.120.16:41242    TIME_WAIT
tcp6       0      0 192.168.80.51:80        45.82.76.192:41150      SYN_RECV
tcp6       0     25 192.168.80.51:443       177.93.63.18:45129      CLOSING
udp        0      0 192.168.80.51:68        192.168.80.1:67         ESTABLISHED
udp        0      0 169.254.95.120:68       169.254.95.118:67       ESTABLISHED
```

## Daftar Status Koneksi TCP & Penjelasannya

| State | Penjelasan |
|---|---|
| **ESTABLISHED** | Koneksi telah terbentuk dan aktif digunakan untuk komunikasi data. Ini adalah koneksi yang “normal” dan siap untuk transfer data dua arah. |
| **SYN_SENT** | Klien telah mengirim paket SYN ke server dan sedang menunggu balasan (SYN-ACK). Ini adalah tahap awal dari koneksi outbound (keluar). |
| **SYN_RECV** | Server telah menerima SYN dari klien, membalas dengan SYN-ACK, dan sedang menunggu ACK dari klien untuk menyelesaikan proses handshake. |

| State | Penjelasan |
| --- | --- |
| **FIN_WAIT1** | Aplikasi telah menutup koneksi, dan sistem telah mengirim FIN (permintaan tutup koneksi) ke pihak lain. |
| **FIN_WAIT2** | Setelah menerima ACK dari FIN pertama, sistem menunggu FIN dari pihak lawan. |
| **TIME_WAIT** | Koneksi ditutup, tapi sistem menunggu selama periode waktu tertentu (biasanya 2x waktu maksimum segment life) untuk memastikan semua paket terlambat tidak akan menyebabkan kebingungan. |
| **CLOSE_WAIT** | Server menerima FIN dari klien, dan menunggu aplikasinya untuk menutup koneksi juga. |
| **CLOSING** | Kedua sisi telah mengirim FIN, tapi belum semua ACK diterima. |
| **LAST_ACK** | Sistem telah mengirim FIN (balasan), menunggu ACK dari pihak lain sebelum sepenuhnya menutup koneksi. |
| **CLOSED** | Koneksi telah ditutup sepenuhnya, tidak ada komunikasi lebih lanjut. |
| **LISTEN** | Server menunggu koneksi masuk pada port tertentu (passive open). Biasanya terlihat pada server seperti web server, SSH, dll. |

---

# Contoh Alur Normal TCP (3-way handshake + closing)

**Pembukaan koneksi:**

1. Klien: `SYN_SENT`
2. Server: `SYN_RECV`
3. Keduanya: `ESTABLISHED`

**Penutupan koneksi:**

1. Pengirim: `FIN_WAIT1`
2. Penerima: `CLOSE_WAIT`
3. Pengirim: `FIN_WAIT2`
4. Penerima: `LAST_ACK`
5. Keduanya: `TIME_WAIT`
6. Akhir: `CLOSED`

---

# Status yang Perlu Diwaspadai

- **SYN_RECV** banyak → kemungkinan *SYN flood attack*
- **TIME_WAIT** banyak → bisa akibat skrip web atau API client yang membuka-tutup koneksi terus-menerus

- **CLOSE_WAIT** menggantung → aplikasi Anda tidak menutup koneksi dengan benar (potensi memory leak)

Pengamanan Server

# Cek Lokasi File Exploit pada Root Web

Cek Lokasi file Exploit yang menggunakan **shell_exec**, **curl_exec** dan simpan hasilnya di hasil_scan.txt

```
cd /var/www/html/root_aplikasi
```

```
grep -RniE 'eval\s*\(|base64_decode\s*\(|assert\s*\(|shell_exec\s*\(|system\s*\(|passthru\s*\(|file_get_contents\s*\(' . > hasil_scan.txt
```

```
grep -RniE 'eval\s*\(|base64_decode\s*\(|assert\s*\(|curl_exec\s*\(|system\s*\(|passthru\s*\(|file_get_contents\s*\(' . > hasil_scan2.txt
```

lihat hasilnya lalu hapus file tersebut (paling mencurigakan file .php yang berada di public atau storage)

# Mengamankan PHP

# Mengamankan PHP Apache

Untuk membatasi serangan hacker pada PHP dalam instalasi LAMPP (Linux, Apache, MySQL, PHP, PHPMyAdmin), Anda dapat mengambil beberapa langkah keamanan untuk melindungi aplikasi web Anda dari berbagai jenis serangan. Berikut adalah beberapa konfigurasi dan praktik keamanan umum yang dapat membantu Anda:

**Update PHP**
Pastikan Anda menjalankan versi PHP yang paling baru dan selalu diperbarui. Setiap pembaruan PHP biasanya mencakup perbaikan keamanan. Anda juga dapat mempertimbangkan untuk menggunakan PHP versi 8.x atau yang lebih baru, karena ini mendukung peningkatan keamanan dan kinerja.

**Konfigurasi PHP**
Edit file **php.ini** di **/etc/php/8.1/cli/php.ini** dan/atau **/etc/php/8.1/apache2/php.ini** dan terapkan konfigurasi keamanan berikut:

- Batasi maksimum ukuran upload file dengan parameter **upload_max_filesize** dan **post_max_size**.
- Matikan **register_globals**.
- Matikan **allow_url_fopen** dan **allow_url_include** untuk mencegah inklusi dan akses ke URL eksternal.
- Setel **display_errors** menjadi **Off** dalam produksi untuk menghindari menampilkan kesalahan PHP ke publik.
- Aktifkan disable_functions untuk memblokir fungsi-fungsi berbahaya jika Anda tahu apa yang Anda lakukan.
- Aktifkan open_basedir untuk membatasi direktori yang diizinkan PHP untuk mengakses.

Menggunakan opsi **disable_functions** dalam konfigurasi PHP dapat membantu mengurangi risiko keamanan dengan memblokir fungsi-fungsi tertentu yang dapat digunakan oleh penyerang untuk melakukan aktivitas berbahaya. Namun, penggunaan **disable_functions** harus dilakukan dengan hati-hati, karena mematikan fungsi-fungsi tertentu dapat mempengaruhi fungsi normal dari aplikasi PHP Anda. Beberapa fungsi yang sering kali dinonaktifkan karena potensi risiko keamanan termasuk:

1. **exec**: Fungsi `exec()` digunakan untuk menjalankan perintah shell dari dalam skrip PHP. Ini harus dinonaktifkan untuk mencegah penyerang menjalankan perintah shell di server

Anda.

2. **system**: Sama seperti `exec()`, `system()` juga digunakan untuk menjalankan perintah shell. Ini harus dinonaktifkan.
3. **shell_exec**: Fungsi `shell_exec()` juga digunakan untuk menjalankan perintah shell dan harus dinonaktifkan.
4. **passthru**: `passthru()` adalah fungsi lain yang dapat digunakan untuk menjalankan perintah shell. Ini juga harus dinonaktifkan.
5. **popen**: `popen()` memungkinkan skrip PHP untuk membuka pipe ke proses eksternal. Ini harus dinonaktifkan.
6. **proc_open**: Fungsi ini serupa dengan `popen()` dan juga digunakan untuk menjalankan proses eksternal. Ini harus dinonaktifkan.
7. **eval**: Fungsi `eval()` digunakan untuk mengeksekusi kode PHP dari string. Penyerang dapat memanfaatkannya dengan memasukkan kode berbahaya ke dalam string.
8. **assert:** Fungsi `assert()` juga dapat digunakan untuk mengeksekusi kode PHP dari string. Ini harus dinonaktifkan.
9. **system_popen**: Ini adalah alternatif lain untuk `popen()` dan harus dinonaktifkan.
10. **dl**: Fungsi `dl()` digunakan untuk memuat ekstensi PHP dinamis. Ini dapat membuka celah keamanan jika dinonaktifkan.
11. **proc_close:** Ini adalah fungsi terkait dengan `proc_open()` yang digunakan untuk menutup proses yang telah dibuka dengan `proc_open()`. Dinonaktifkan juga.
12. **pcntl_exec**: Fungsi ini memungkinkan penggunaan fungsi `exec()` dalam lingkungan PHP-FPM. Jika Anda tidak menggunakannya, disarankan untuk dinonaktifkan.

Cari baris yang mengandung **`disable_functions`**. Jika Anda tidak menemukannya, Anda dapat menambahkannya di bagian paling bawah file **php.ini**.

Tambahkan nama fungsi-fungsi yang ingin Anda nonaktifkan, dipisahkan oleh tanda koma. Misalnya, jika Anda ingin menonaktifkan fungsi exec, system, dan eval, tambahkan baris berikut:

```
disable_functions = exec, system, eval
```

Setelah menyimpan perubahan, Anda perlu merestart Apache agar perubahan ini berlaku:

**systemctl restart apache2**

**Catatan:**
**Pastikan bahwa Anda memeriksa bahwa aplikasi PHP Anda tetap berfungsi dengan baik setelah mengaktifkan disable_functions**, karena beberapa fungsi PHP mungkin diperlukan untuk fungsi normal aplikasi Anda. Selalu uji aplikasi Anda dengan cermat setelah mengubah pengaturan ini.

# Optimalisasi Server

Optimalisasi Server

# Konfigurasi MPM Event Apache

Setup Apache ke **MPM Event + PHP-FPM**

1⃣ Cek MPM Apache yang aktif

apachectl -V | grep -i mpm

- `mpm_prefork` ⃣ → harus diganti
- `mpm_event` ⃣ → sudah benar

2⃣ Nonaktifkan MPM Prefork dan PHP 8.1

sudo a2dismod mpm_prefork

sudo a2dismod php8.1

3⃣ Aktifkan MPM Event

sudo a2enmod mpm_event

4⃣ Aktifkan Integrasi Apache ↔ PHP-FPM

sudo a2enmod proxy_fcgi setenvif
sudo a2enconf php8.1-fpm

5⃣ Restart Apache & PHP-FPM

sudo systemctl restart php8.1-fpm
sudo systemctl restart apache2

6⃣ Pastikan MPM Event Aktif

apachectl -V | grep -i mpm

Output harus:
Server MPM:  event

7 Optimasi untuk Server Ram Besar

sudo nano /etc/apache2/mods-available/mpm_event.conf

```
<IfModule mpm_event_module>
    StartServers             2
    MinSpareThreads         25
    MaxSpareThreads         75
    ThreadLimit             64
    ThreadsPerChild         25
    MaxRequestWorkers      400
    MaxConnectionsPerChild 5000
</IfModule>
```

sudo systemctl restart apache2

# Konfigurasi Apache MPM Prefork + PHP (mod_php)

1⃣ Nonaktifkan PHP-FPM

sudo systemctl stop php8.1-fpm
sudo systemctl disable php8.1-fpm

Nonaktifkan konfigurasi Apache FPM:

sudo a2disconf php8.1-fpm
sudo a2dismod proxy_fcgi

2⃣ Aktifkan MPM Prefork

Matikan MPM Event:
sudo a2dismod mpm_event

Aktifkan Prefork:
sudo a2enmod mpm_prefork

## 3⃣ Pastikan **mod_php sesuai versi PHP** terpasang:

sudo apt install libapache2-mod-php8.1

sudo a2enmod php8.1

4⃣ Restart Apache Prefork

sudo systemctl restart php81.-fpm

sudo systemctl restart apache2

## 5⃣ Cek MPM:

apachectl -V | grep -i mpm

Harus muncul:
Server MPM: prefork

6 Optimasi Prefork

sudo nano /etc/apache2/mods-available/mpm_prefork.conf

```
<IfModule mpm_prefork_module>
    StartServers           5
    MinSpareServers        5
    MaxSpareServers       10
    MaxRequestWorkers    150
    MaxConnectionsPerChild 3000
</IfModule>
```

sudo systemctl restart apache2