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
```

Revisi #17
Dibuat 16 Mei 2025 22:34:17 oleh Friscia Anthony
Diperbaharui 12 Oktober 2025 00:14:58 oleh Friscia Anthony