

MANUAL BOOK

IMPLEMENTASI FIREWALL DENGAN OPNSENSE DAN ZENARMOR PADA WEB SERVER



Oleh :

Naufal Ishomi Akbar

E32222915

**PROGRAM STUDI TEKNIK KOMPUTER
JURUSAN TEKNOLOGI INFORMASI
POLITEKNIK NEGERI JEMBER**

2025

1. Pendahuluan

Buku manual ini dibuat sebagai panduan untuk mengimplementasikan firewall menggunakan OPNsense dan Zenarmor pada server web, dengan tujuan untuk meningkatkan keamanan jaringan dan melindungi data sensitif dari ancaman siber. OPNsense adalah platform firewall

Open-source berbasis FreeBSD, sementara Zenarmor adalah plugin tambahan yang menyediakan fitur keamanan canggih seperti inspeksi paket mendalam (deep packet inspection) dan analitik jaringan.

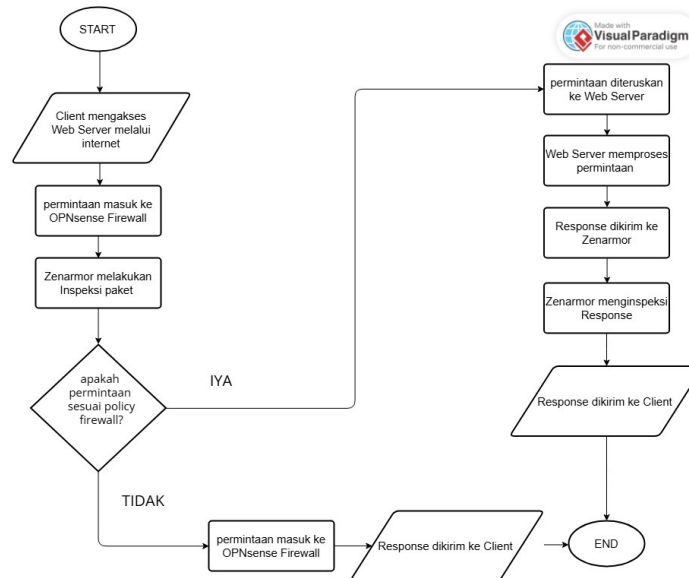
2. Perangkat yang Dibutuhkan

- **Perangkat Keras:** Laptop Asus dengan spesifikasi minimum CPU Intel Core i3-10110U, RAM 12 GB, dan penyimpanan 256 GB SSD & 500 GB HDD.
- **Perangkat Lunak:**
 - **OPNsense:** Sistem operasi firewall utama
 - **Zenarmor:** Plugin firewall tambahan untuk OPNsense
 - **VirtualBox:** Alat mesin virtualisasi
 - **OWASP ZAP:** Perangkat lunak penguji firewall
 - **Visual Paradigm:** Aplikasi untuk membuat flowchart
 - **Microsoft:** Untuk pembuatan laporan

3. Metode Kegiatan

- **Studi Literatur:** Mengumpulkan informasi dan pengetahuan teoritis dari literatur, jurnal, dan buku yang relevan.
- **Perancangan Skema:** Membuat gambaran sistem yang akan dibangun.
- **Pembuatan Sistem:** Melakukan instalasi dan konfigurasi perangkat lunak.
- **Uji Coba & Hasil:** Melakukan pengujian untuk memverifikasi fungsionalitas dan efektivitas sistem.
- **Penyusunan Laporan:** Mendokumentasikan seluruh proses dan hasil.

4. Alur Skema Sistem



Alur dari sistem yang ada, akan bermula ketika klien mengakses web server melalui jaringan internet, lalu jaringan yang berasal dari akses client akan masuk ke sistem firewall OPNsense. Setelah itu zenarmor akan memeriksa lebih mendalam sesuai konfigurasi, zenarmor juga akan memeriksa lagi apakah lalu lintas yang ada sudah sesuai dengan konfigurasi firewall. Dari proses tersebut maka zenarmor akan mencatat log aktivitas pengguna serta dapat memblokir. Jika proses yang terjadi dianggap aman maka proses akan berlangsung ke web server lalu akan menampilkan ke client.

5. Konfigurasi OPNsense dan Zenarmor

- **Konfigurasi OPNsense**

Proses pembuatan sistem ini melibatkan beberapa langkah utama yakni menginstal sistem operasi OPNsense pada virtualbox yang telah disiapkan. Setelah proses instalasi selesai dilakukan konfigurasi pada interfaces serta IP address. Proses dimulai dengan login root pada console virtualbox lalu terdapat beberapa opsi, enter an option: 1 yakni pada opsi assign interfaces.

Ubah interfaces yang default sebagai antisipasi salah dalam konfigurasi, yakni untuk interface **WAN:em0** dan **LAN:em1**.

```
Valid interfaces are:
em0          08:00:27:24:1c:45 Intel(R) Legacy PRO/1000 MT 82540EM
em1          08:00:27:2b:98:35 Intel(R) Legacy PRO/1000 MT 82540EM
zen0        00:00:00:00:00:00

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em1

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:
WAN -> em0
LAN -> em1

Do you want to proceed? [y/N]: y
```

Selanjutnya konfigurasi ip address pada interface LAN pada console Virtualbox yang mana terdapat pada opsi 2 set interface IP address lalu pilih interface LAN dan terdapat opsi Configure IPv4 address LAN interface via DHCP [y/N] N karena pada interface LAN menggunakan host only adapter maka perlu memberikan ip address statik dari blok ip tersebut, yakni bisa dilihat dari ipconfig laptop host.

```
C:\WINDOWS\system32\cmd. x + v
C:\Users\faris>ipconfig

Windows IP Configuration

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::ac2f:f206:5167%19
    IPv4 Address. . . . . : 192.168.56.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Enter the number of the interface to configure: 1
Configure IPv4 address LAN interface via DHCP? [y/N] n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.56.104

Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
    255.255.0.0 = 16
    255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 192.168.56.103
> 24

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
Configure IPv6 address LAN interface via DHCP6? [y/N] n
```

Ketika konfigurasi sudah selesai maka akses opnsensei via web UI dilakukan dengan ip address dari interface LAN tersebut (**192.168.56.104**).

```
Configuring firewall.....done.
Starting web GUI...done.

You can now access the web GUI by opening
the following URL in your web browser:

    https://192.168.56.104

*** OPNsense.localdomain: OPNsense 25.1.12 (amd64) ***

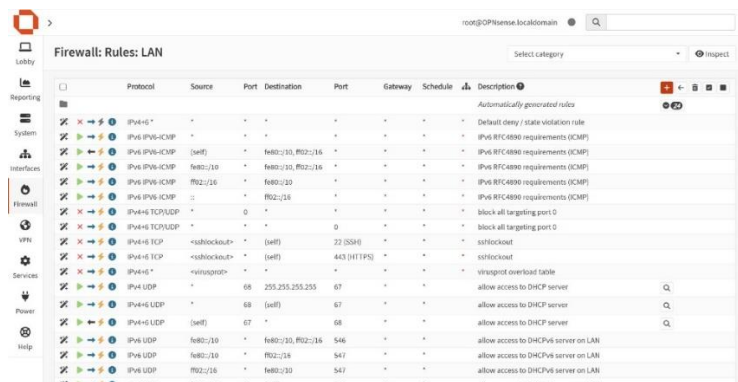
LAN (em1)      -> v4: 192.168.56.104/24
WAN (em0)      -> v4/DHCP4: 192.168.0.109/24

HTTPS: sha256 1E BF AC E6 00 5D B9 0E D7 E1 0E E2 F4 EC 01 35
              17 27 20 2D 10 7A 61 D9 3A B2 99 AA 69 F1 34 2B

0) Logout
1) Assign interfaces
2) Set interface IP address
3) Reset the root password
4) Reset to factory defaults
5) Power off system
6) Reboot system
7) Ping host
8) Shell
9) pfTop
10) Firewall log
11) Reload all services
12) Update from console
13) Restore a backup

Enter an option: █
```

Ketika sudah mengakses OPNsense via Web UI akan terdapat banyak informasi serta menu untuk konfigurasi firewall lebih lanjut, seperti pada menu rules pada opnsense yang mana ini merupakan inti dari pengelolaan firewall, yang berfungsi untuk mengatur lalu lintas jaringan (traffic) berdasarkan berbagai parameter. Rules ini menentukan apakah suatu koneksi diizinkan (allow), ditolak (block). Berikut ini merupakan rules yang terdapat pada OPNsense.

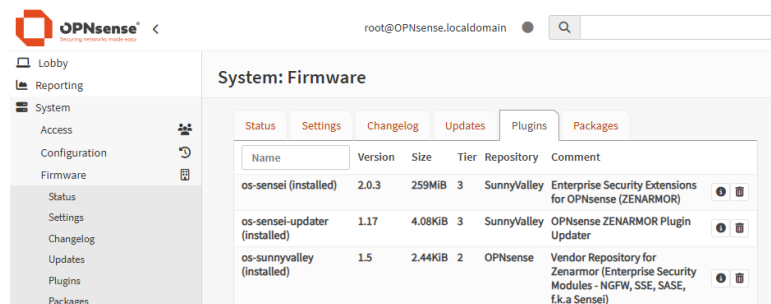


Untuk rules pada OPNsense seperti gambar diatas, ada beberapa rules yang mana itu default rules dari interface LAN yang ada setelah proses instal OPNsense itu sendiri. Terdapat satu aturan pada baris ke-9 dari atas, bahwa akan terjadi tindakan block yang berarti setiap traffic yang cocok dengan kriteria aturan akan secara aktif ditolak oleh firewall. Aturan ini berlaku untuk koneksi yang menggunakan protokol TCP, mencakup baik IPv4 maupun IPv6,

yang merupakan protokol dasar yang digunakan oleh SSH. Inti dari aturan ini terletak pada bagian Source-nya yang merujuk pada alias `<sshlockout>`. Alias ini merupakan sebuah tabel dinamis yang secara otomatis diisi dan dikelola oleh layanan sshguard di OPNsense. Ketika sistem mendeteksi percobaan login SSH yang gagal secara berulang dari suatu IP address, sshguard akan segera menambahkan IP tersebut ke dalam alias `<sshlockout>`. Hal ini dirancang untuk menandai IP yang menunjukkan perilaku mencurigakan atau berpotensi melakukan serangan *brute-force*. Selanjutnya, aturan ini secara khusus menetapkan *Destination* sebagai (self), yang mengindikasikan bahwa target perlindungan adalah firewall OPNsense itu sendiri. Dan port yang menjadi fokus adalah 22 (SSH), yang secara jelas menargetkan upaya koneksi ke layanan Secure Shell.

- **Konfigurasi Zenarmor**

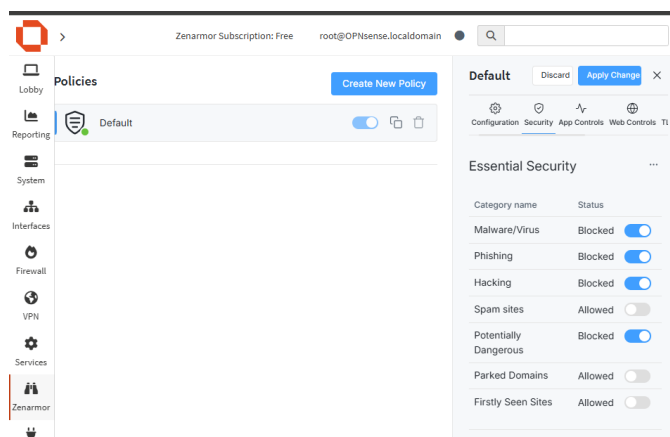
Zenarmor sendiri di instal pada OPNsense yakni pada menu **system, firmware, plugins**. Yang mana terdapat os yang perlu di instal yakni `os-sunnyvalley` serta `os-sensei`.



Setelah instal OS maka terdapat konfigurasi awal dari Zenarmor yakni mulai dari instal database yang ingin digunakan untuk menyimpan data log maupun statistik aktivitas jaringan mengingat fungsi Zenarmor yaitu dapat memberikan statistik lalu lintas jaringan secara realtime serta menyimpan log jaringan. Serta konfigurasi pada pemilihan interface yang akan di proteksi yaitu pada interface LAN.

Pada Zenarmor ini dilakukan konfigurasi pada menu *policies* yang di suguhkan sebagai value Zenarmor versi *essential security* atau versi gratis,

yakni pada opsi blokir kategori *malware/virus*, *phishing*, *hacking*, serta *potentially dangerous*. Hal tersebut memicu tujuan untuk meningkatkan stabilitas jaringan serta perlindungan ancaman lebih luas.



6. Hasil Pengujian

- **Pengujian dengan rules OPNsense**

Pengujian ini dilakukan pada salah satu rules default pada OPNsense yaitu pada rules *sshlockout*. Pengujian ini dilakukan untuk memverifikasi fungsionalitas aturan *sshlockout* di OPNsense, yang berfungsi sebagai mekanisme pertahanan otomatis terhadap serangan *brute-force* pada layanan SSH (Secure Shell) OPNsense. Aturan ini bertujuan untuk memblokir alamat IP yang terdeteksi melakukan percobaan *login* yang gagal secara berulang kali.

Pada pengujian ini, sebuah skenario simulasi serangan *brute-force* sederhana dilakukan dari *client* (laptop) dengan IP address 192.168.56.103 yang terhubung ke *interface* LAN OPNsense. Proses dilakukan dengan mengakses layanan SSH dari *client* (laptop) ke OPNsense (**IP LAN: 192.168.56.104**) menggunakan *SSH client* (Command Prompt).percobaan *login* SSH dengan *username* root namun dengan *password* yang salah secara berulang kali sampai tertera bahwa *connection time out*.

```

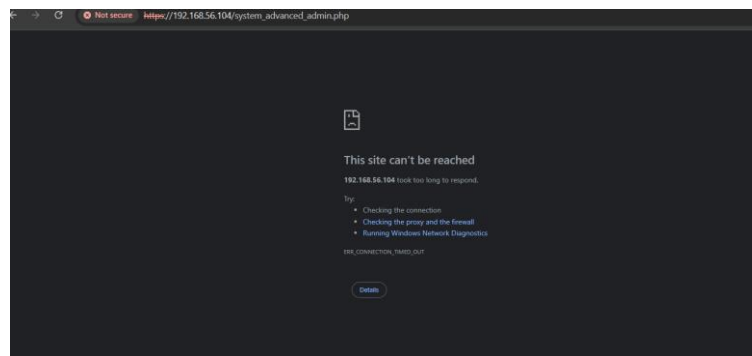
C:\Users\faris>ssh root@192.168.56.104 -p 22
(root@192.168.56.104) Password:
(root@192.168.56.104) Password:
(root@192.168.56.104) Password:
root@192.168.56.104's password:
Permission denied, please try again.
root@192.168.56.104's password:
Permission denied, please try again.
root@192.168.56.104's password:
Received disconnect from 192.168.56.104 port 22:2: Too many authentication failures
Disconnected from 192.168.56.104 port 22

C:\Users\faris>ssh root@192.168.56.104 -p 22
(root@192.168.56.104) Password:
(root@192.168.56.104) Password:
(root@192.168.56.104) Password:
root@192.168.56.104's password:
Permission denied, please try again.
root@192.168.56.104's password:
Permission denied, please try again.
root@192.168.56.104's password:
Received disconnect from 192.168.56.104 port 22:2: Too many authentication failures
Disconnected from 192.168.56.104 port 22

C:\Users\faris>ssh root@192.168.56.104 -p 22
ssh: connect to host 192.168.56.104 port 22: Connection timed out

```

Setelah itu, ketika akses kembali Web UI OPNsense (<https://192.168.56.104>) dari browser di client (laptop) tidak akan bisa. Karena berdasarkan skenario pengujian yang dilakukan, ditemukan bahwa upaya akses SSH yang gagal secara berulang dari IP address (192.168.56.103) memicu aturan sshlockout OPNsense. Secara bersamaan, akses Web UI OPNsense pada port 443 (HTTPS) dari client yang sama (192.168.56.103) juga tidak dapat dilakukan. Ini menunjukkan bahwa rule sshlockout yang terkait dengan HTTPS juga ikut aktif.



Karena akses Web UI juga terblokir maka untuk melihat serta menghapus IP address yang terblokir tersebut dilakukan melalui konsol menu *shell* pada mesin OPNsense. Untuk menampilkan IP address yang terblokir maka dengan menggunakan perintah `pfctl -t sshlockout -T show` dan akan menampilkan IP address yang terblokir. Serta dilakukan juga penghapusan IP address guna untuk bisa mengakses OPNsense via Web UI yakni dengan perintah `pfctl -t sshlockout -T delete 192.168.56.103`.

```

LAN (em1)      -> v4: 192.168.56.104/24
WAN (em0)      -> v4/DHCP4: 192.168.0.109/24

HTTPS: sha256 1E BF AC E6 80 5D B9 0E D7 E1 E0 E2 F4 EC 01 35
          17 27 20 2D 10 7A 61 D9 3A B2 99 AA 69 F1 34 2B
SSH:  SHA256 jCT5rFpBhG2SbJpdUNKl/NEsH7Im4iW+ndqx9CMcU+o (ECDSA)
SSH:  SHA256 Age5+DZf5m+NR8iihCBZseL9vf Ic7TrXlhaLgsHPsBc (ED25519)
SSH:  SHA256 g7lbQwEXuKgwPuudfm1L531BgpXZKMGMZSHm4SZHi/s (RSA)

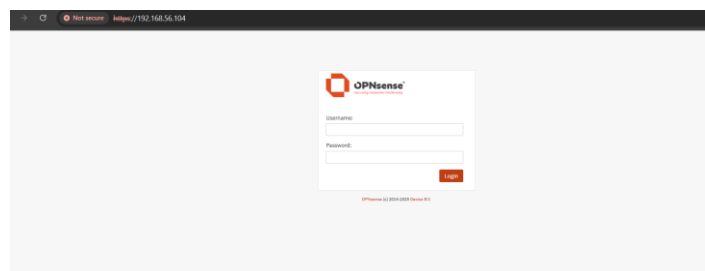
0) Logout                                7) Ping host
1) Assign interfaces                      8) Shell
2) Set interface IP address              9) pfTop
3) Reset the root password               10) Firewall log
4) Reset to factory defaults             11) Reload all services
5) Power off system                      12) Update from console
6) Reboot system                         13) Restore a backup

Enter an option: 8

root@OPNsense:~ # pfctl -t sshlockout -T show
192.168.56.103
root@OPNsense:~ # pfctl -t sshlockout -T delete 192.168.56.103
/1 addresses deleted.
root@OPNsense:~ #

```

Setelah dilakukan penghapusan IP address yang terblokir maka bisa mengakses OPNsense dengan browser kembali.

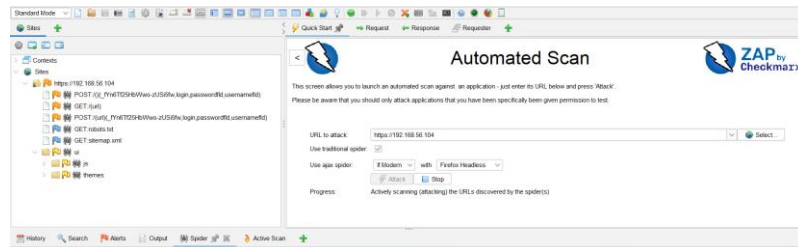


- **Pengujian menggunakan tools OWASP Zap**

Simulasi pengujian terhadap web dengan menggunakan tools OWASP ZAP, Pada bagian ini lebih bertujuan untuk menguji efektivitas dari konfigurasi keamanan jaringan yang telah dirancang menggunakan Zenarmor dalam menangkal berbagai jenis serangan yang umum terjadi pada web server.

Proses pengujian menggunakan metode firefox headless dengan Aotomated Scann, dalam pengertiannya Firefox Headless adalah mode tanpa antarmuka grafis (GUI) dari browser Mozilla Firefox. Dalam mode ini, Firefox berjalan di latar belakang tanpa menampilkan jendela browser, tetapi tetap berperan

seperti browser biasa. pengujian keamanan ini ditujukan untuk melakukan scanning terhadap endpoint situs <https://192.168.56.104>.



Menurut dari hasil pengujian terdapat beberapa alert yang masih menjadi celah dari sistem firewall ini, untuk mengetahui tentang pengertian maupun penjelasan dari berbagai alert yang tertera bisa di dapatkan dari situs web resmi dari Owasp ZAP sendiri yakni <https://www.zaproxy.org/docs/alerts/>. berikut merupakan hasil dari pengujian;

Generated on Sun, 3 Aug 2025 22:07:55

ZAP Version: 2.16.1

ZAP by [Checkmarx](https://www.checkmarx.com/)

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	6
Low	3
Informational	6

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	12
CSP: Failure to Define Directive with No Fallback	Medium	7
CSP: script-src unsafe-eval	Medium	7
CSP: script-src unsafe-inline	Medium	7
CSP: style-src unsafe-inline	Medium	7
Content Security Policy (CSP) Header Not Set	Medium	2