# MEMBANGUN SISTEM KEAMANAN JARINGAN BERBASIS FIREWALL DAN IDS MENGGUNAKAN TOOLS OPNSENSE

**Reza Rizky Adha[1], Mochammad Fahru Rizal[2], Setia Juli Irzal Ismail[3]**

[1, 2,3] Universitas Telkom, Bandung
**rezarizkyadha@student.telkomuniversity.ac.id[1]**, **mfrizal@telkomuniversity.ac.id[2]**,
**julismail@telkomuniversity.ac.id[3]**

**Abstrak**

**Internet membuat komunikasi informasi saat ini menjadi sangat mudah dan cepat, kemudahan itu juga menyebabkan banyak kejahatan yang melibatkan internet. contoh kejahatan yang terjadi seperti kasus peretasan spionase cina yang diduga menyusup ke dalam jaringan BIN dan 9 lembaga negara lainnya dengan cara mengirimkan malware pada target. namun, metode pengiriman malware dan titik intrusi masih belum ditemukan. Maka diperlukan sistem yang aman, yang dapat mencegah serangan tersebut. Untuk mencegah serangan tersebut, diperlukan sistem yang dilengkapi dengan fitur firewall dan Intrusion Detection System (IDS). Fitur Firewall dan Intrusion Detection system (IDS) dapat diterapkan pada Tools OPNSense. Dalam menerapkan Firewall dan Intrusion Detection System(IDS) dengan Tools OPNSense dapat memberikan solusi untuk melindungi server dan memblokir serangan. Pada saat melakukan Scanning, pengujian DDOS dan sniffing maka sistem dapat mencatat log serangan, mengirimkan notifikasi serangan, memblokir serangan, serta melakukan pengujian URL Filter pada website.**

**Kata Kunci :Firewall, Intrusion Detection System, OPNSense, Jaringan, Intrusi.**

***Abstract***

***The internet makes communication of information today very easy and fast, this convenience also causes many crimes involving the internet. examples of cyber crimes that occurred such as the case of hacking Chinese espionage which allegedly infiltrated the BIN network and 9 other state institutions by sending malware to the target. However, the malware delivery method and the intrusion point are still not found. So we need a safe system, that it can prevent Hacking and attack. To prevent these attack, a system equipped with firewall and Intrusion Detection System (IDS) features is required. Firewall and Intrusion Detection system (IDS) features can be applied with OPNSense Tools. Implementing a Firewall and Intrusion Detection System (IDS) with OPNSense Tools can provide solutions to protect servers and block attacks. When scanning, testing DDOS and sniffing, the system can record attack logs, send attack notifications, block attacks, and test URL Filters on websites.***

***Keywords: Firewall, Intrusion Detection System, OPNSense, Network, Intrusion.***

## 1. Pendahuluan

### 1.1 Latar Belakang

Perkembangan teknologi infomasi merupakan hal yang penting bagi masyarakat saat ini dalam internet. Dengan adanya internet membuat komunikasi dan informasi sangat mudah didapatkan. Kemudahan ini menyebabkan terjadinya kejahatan di dunia maya. Kejahatan cyber dapat menyerang jaringan komputer, menyusup kedalam jaringan mengambil data – data rahasia dan melumpuhkan sistem jaringan komputer. Dalam mengatasi kejahatan yang akan terjadi, dibutuhkan sistem yang dilengkapi firewall dan Intrusion Detection System(IDS). Firewall dan Intrusion Detection System(IDS) sebagai fiitur keamanan jaringan yang dapat melindungi server, melindungi jaringan internal, dan memblok serangan. Fitur Firewall dan Intrusion Detection System(IDS) dapat diterapkan dalam Tools OPNSense. OPNsense merupakan operating system yang bersifat open source yang digunakan untuk konfigurasi firewall dan Routing. OPNSense memberikan kemudahan dalam melakukan berbagai macam pengaturan melalui antarmuka web (web GUI / graphical users interface). Dengan demikian Proyek Akhir ini berjudul "Membangun Sistem Keamanan Jaringan Berbasis Firewall dan IDS Menggunakan Tools OPNSense ". Dengan tools OPNSense memberikan solusi melindungi server dan memblokir serangan, mencatat

log serangan. ketika terjadi serangan berupa Serangan Port Scanning, Denial of Service(DOS).

### 1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka dapat dirumuskan permasalahan sebagai berikut.

1. Bagaimana cara konfigurasi firewall dan IDS menggunakan tools OPNSense ?
2. Bagaimana cara melakukan pengujian Scanning port, Serangan (DDoS), Web Filter?
3. Bagaimana cara memonitoring jaringan pada saat terjadinya aktifitas peretasan?

### 1.3 Tujuan

Adapun tujuan yang ingin dicapai dalam pembuatan laporan tugas akhir ini adalah:

1. Konfigurasi Firewall dan IDS dilakukan dengan cara mengkonfigurasi rules pada Firewall dan IDS.
2. Pengujian scanning port menggunakan tools Masscan, untuk DoS menggunakan LOIC, dan Web filter menggunakan rules yang ada pada Firewall.
3. Untuk Memonitoring jaringan pada saat terjadinya peretasan bisa dilihat pada menu Log.

### 1.4 Batasan Masalah

Untuk menghindari luasnya pembahasan masalah yang akan di teliti maka terdapat beberapa Batasan yaitu :

1. Menggunakan Aplikasi VirtualBox sebagai media pengerjaan Proyek Akhir.
2. Tidak menggunakan aplikasi Firewall lain selain OPNSense.
3. Menggunakan fitur Masscan untuk melakukan scanning port pada web server yang akan di retas.
4. Menggunakan 1 buah laptop.
5. Menggunakan aplikasi LOIC untuk melakukan penyerangan berupa DDOS.
6. Menggunakan firmware suricata untuk Intrusion Detection System(IDS) pada Tools OPNSense.
7. Menggunakan layanan Web pada Sistem Operasi Ubuntu 21.04.

## 2. Tinjauan Pustaka

### 2.1 Tinjauan Pustaka

Tijauan Pustaka digunakan sebagai referensi umtuk pembuatan proyek akhir ini .

Penelitian sebelumnya yang berjudul "IMPLEMENTASI FIREWALL DAN INTRUSION PREVENTION SYSTEM (IPS) DENGAN SISTEM OPERASI IPFIRE". Penelitian tersebut membangun system yang akan digunakan sebagai acuan system Firewall dan Intrusion Detection System. Tujuan Penelitian ini adalah untuk mencegah kejahatan cyber yang sering terjadi di internet menggunakan tool IPFire, namun pada system saat ini menggunakan Tools OPNSense untuk melakukan pertahanan terhadap serangan. [1]

Penelitian sebelumnya yang berjudul "ANALISIS KEAMANAN WEBSITE MENGGUNAKAN METODE SCANNING DAN PERHITUNGAN SECURITY METRIKS". Penelitian tersebut bertujuan untuk menguji keamanan suatu website dengan menggunakan metode scanning dan perhitungan security matriks.[2]

Penelitian sebelumnya yang berjudul "MENGATASI SERANGAN PORT SCANNING DAN WEB SERVER VULNERABILITY SCANNING MENGGUNAKAN PORTSENTRY DAN MODSECURITY". Tujuan penelitian ini adalah untuk mengatasi serangan Port scanning menggunakan PortSentry, namun pada system saat ini menggunakan Tools OPNSense untuk mengatasi port scanning tersebut.[3]

### 2.2 Dasar Teori

#### 2.2.1 OPNsense

OPNsense adalah aplikasi open source, firewall dan platform routing berbasis FreeBSD yang open source, mudah digunakan dan mudah dikofigurasi.[4]

Gambar 2. 1 OPNSense

#### 2.2.2 Firewall

Firewall adalah suatu aturan yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri

dengan tujuan untuk melindungi, baik dengan melakukan filterisasi, membatasi ataupun menolak suatu koneksi pada jaringan yang dilindunginya dengan jaringan luar lainnya seperti internet.[5]

### 2.2.3 Intrusion Detection System

Intrusion detection system (IDS) adalah suatu teknik atau metode yang digunakan untuk mendeteksi ancaman yang mencurigakan pada jaringan. IDS memiliki dua kategori dasar yaitu signature-based dan anomaly detection system.[6]

### 2.2.4 Denial-of-Service

Denial-of-Service merupakan sebuah metode serangan di dunia maya di mana si pelaku penyerangan berupaya membuat sumber daya jaringan atau suatu server tidak tersedia bagi client yang dituju dengan cara mengganggu layanan host yang terhubung dengan internet untuk sementara atau jangka waktu yang sudah di tentukan.[7]

### 2.2.5 Suricata

Suricata merupakan sebuah system pendeteksi dan pencegah gangguan atau Intrusion Detection and Prevention System (IDPS) berbasis open source yang merupakan generasi lanjutan dari IDS/IPS.[8]

### 2.2.6 Virtual Box

VirtualBox adalah aplikasi opne source yang berhubungan dengan Virtualisasi, Virtualisasi yang di maksud adalah menjalankan system operasi lain secara independen di atas system operasi utama.[9]


Gambar 2. 2 Virtual Box

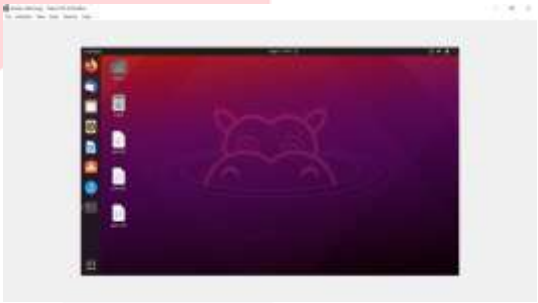
### 2.2.7 Kali Linux

Kali linux adalah salah satu Distribusi Linux turunan dari Debian linux yang dikembangkan dengan tujuan sebagai system operasi yang dapat digunakan untuk Testing keamanan suatu jaringan .[10]

Gambar 2. 3 Kali Linux

### 2.2.8 Ubuntu

Ubuntu adalah salah satu dari sekian banyak distro linux yang berbasis Debian dan bersifat Open Source.



Gambar 2. 4 Ubuntu 21.04

### 2.2.9 LOIC

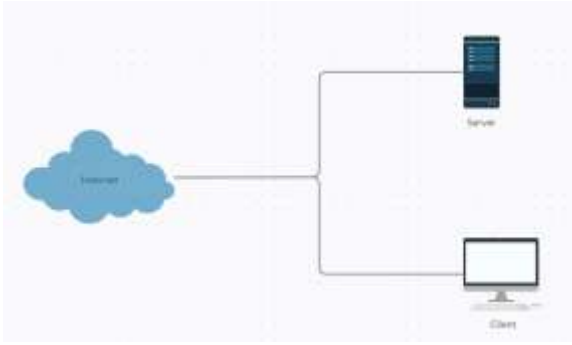
LOIC (Low Orbit Ion Cannon) merupakan salah satu Tools atau aplikasi yang digunakan untuk melakukan serangan DDoS pada sebuah jaringan atau website tertentu. [11]


Gambar 2. 5 Tools DoS LOIC

## 3. Analisis dan perancangan

### 3.1 Gambaran Sistem Saat Ini (atau produk)

Pada sistem saat ini tanpa adanya firewall dan Intruction Detection System, penyerang atau pengguna lain dari luar jaringan dapat mengakses semua file atau konten yang ada pada server tanpa ada nya proses filtering terlebih dahulu. Sehingga jika terjadi penyerangan server bisa saja mendapat malware atau virus, ataupun penyerang dapat melakukan aktivitas yang dapat merugikan server seperti hacking.



Gambar 3. 1 Gambaran system tanpa Firewall

### 3.2 Identifikasi Kebutuhan Sistem (atau Produk)

#### 3.2.1. Analisis Kebutuhan Fungsional Dan Non-Fungsional

Analisi kebutuhan fungsional dapat dilihat pada Tabel 3. 1 dan analisis kebutuhan non-fungsional dapat dilihat pada Tabel 3. 2.

| No | Kebutuhan Fungsional |
|---|---|
| 1 | Menggunakan software OPNsense untuk monitoring, *Web Filtering*, dan *Intrution Detection System* |
| 2 | Menggunakan OPNsense untuk filtering paket data |
| 3 | Penggunaan VirtualBox sebagai tempat konfigurasi server dan OPNSense. |

Tabel 3. 1 Tabel Kebutuhan Fungsional

| No | Kebutuhan Non-Fungsional |
|---|---|
| 1 | Penggunaan Laptop sebagai client dan Server |
| 2 | Penggunaan Adapter NAT Network pada Vbox sebagai penghubung ke jaringan |
| 3 | Menggunakan Kali Linux sebagai penyerang terhadap server |

Tabel 3. 2 Kebutuhan Non-Fungsional

### 3.3 Perancangan Sistem

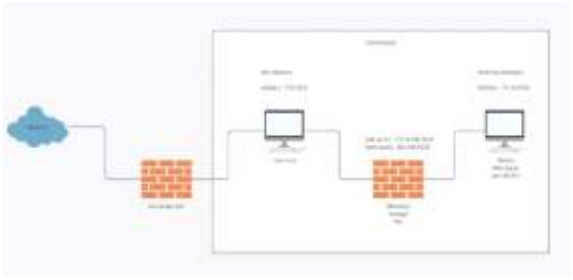
Dalam perancangan sistem akan diuraikan tentang software yang akan di install atau konfigurasi. software tersebut adalah sebagai berikut :

1. VirtualBox 6.1 digunakan sebagai media virtualisasi untuk menjalankan sistem operasi yang akan digunakan dalam proyek akhir ini.
2. Sistem Operasi Ubuntu 21.04 sebagai sistem operasi yang akan menjadi client sekaligus menjadi web server.
3. OPNSense yang akan digunakan sebagai perantara antara internet dan client ubuntu, yang akan bertugas sebagai penyedia layanan firewall dan Detection Intruction System(IDS).
4. Suricata adalah sebuah program pendeteksi sekaligus pencegah gangguan atau Intrution Detection dan Prevention System berbasis Open source yang akan digunakan untuk melindungi server dari ancaman penyerang.
5. Kali Linux sistem operasi yang akan digunakan sebagai penyerang.

Perancangan sistem dapat dilihat pada blok diagram di bawah ini :

Gambar 3. 2 Blok Diagram

### 3.3.1 Gambaran Sistem Usulan



Gambar 3. 3 Topologi Sistem Usulan

Pada Topologi gambaran sistem usulan , Virtual OPNsense akan terhubung ke internet melalui Virtual Kali Linux menggunakan adapter NAT Network, Virtual OPNSense akan meneruskan data ke server menggunakan adapter jaringan Host Only Network yang sudah di konfigurasi, pada server terdapat layanan Web server.

Pada Virtual OPNSense akan dikonfigurasi Firewall dan Intrution Detection System serta Webfilter. Firewall dan IDS akan melindungi server, memblokir serangan dan mencatat log serangan. Kemudian Kali Linux akan melakukan pengujian port scanning dan serangan DDoS.

### 3.3.2 Metode Pengerjaan

Metode pengerjaan proyek akhir ini menggunakan metodologi pengembangan Network Development Life Cycle (NDLC) yang merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya. Adapun tahapannya adalah sebagai berikut:

1. Analisis
   Melakukan analisis kebutuhan hardware dan software untuk membangun Firewall dan IDS menggunakan OPNSense.
2. Desain
   Melakukan perancangan Topologi sistem.
3. Prototype
   Membangun Sistem Firewall dan IDS menggunakan OPNSense
4. Implementasi
   Melakukan konfigurasi Rules Firewall dan Rules IDS.
5. Monitoring
   Melakukan pengujian Firewall dan IDS.

## 3.4 Kebutuhan Perangkat Keras dan Perangkat Lunak

### 3.4.1 Perangkat Keras

Perangkat keras yang digunakan yaitu

| No. | Perangkat Keras | Jumlah | Spesifikasi |
|---|---|---|---|
| 1 | Laptop | 1 Buah | Intel Core i7 9750HF CPU 2.6GHz; RAM 16 DDR 4; SSD 512 GB |

Tabel 3. 3 Perangkat keras

### 3.4.2 Perangkat Lunak

Membahas kebutuhan perangkat lunak (minimal) dalam PA ini.

| No | Perangkat Lunak | Jumlah | Spesifikasi |
|---|---|---|---|
| 1 | OPNSense | 1 Buah | OPNSense 21.7.1 |
| 2 | VirtualBox | 1 Buah | VirtualBox 6.1 |
| 3 | Kali Linux | 1 Buah | Kali Linux 2020.3 |
| 4 | Ubuntu | 1 Buah | Ubuntu 20.04 |

Tabel 3. 4 Perangkat Lunak

## 4. Implementasi dan Pengujian

### 4.1 Implementasi

Bagian ini menjelaskan mengenai Langkah-langkah dalam implementasi Firewall dan Intrution Detection System dengan Tools OPNSense. Langkah-langkah pengerjaan terdiri dari Setting adapter untuk OPNSense, installasi OPNSense, Konfigurasi Jaringan pada Kali Linux, OPNSense, dan Ubuntu, Konfigurasi Web Server pada Ubuntu, Konfigurasi WebFilter dan Suricata sebagai Software untuk

Intrution Detection System, dan Pengujian Port Scanning, Denial of Service(DoS).

### 4.2 Langkah Pengerjaan

#### 4.2.1. Setting Adapter untuk OPSense

Pada bagian ini akan dijelaskan Langkah-langkah Setting Adapter yang akan digunakan pada OPNSense :

1. Sebelum menginstall OPNSense, buat Virtual NAT Network sebagai adapter yang akan digunakan OPNSense untuk terhubung ke internet dengan network 10.0.100.0/24 . kemudian centang pada “Supports DHCP”.

Gambar 4. 1 Setting Virtual NAT

2. Setelah itu buat Virtual adapter Host Only network adapter untuk OPNSense agar terhubung dengan Server. Dengan ip adapter 172.16.100.1/24, kemudian enable DHCP Server.

Gambar 4. 2 Setting IPv4 Host-only Adapter

Gambar 4. 3 DHCP Setting Host-only ADAPTER

#### 4.2.2. Installasi OPNSense

Untuk tahap ini akan menjelaskan tahapan instalasi OPNSense yang akan digunakan, Langkah-langkah nya sebagai berikut :

1. Pastikan ISO dan pengaturan Network adapter yang digunakan untuk instalasi sudah benar.

Gambar 4. 4 Input CD untuk install OPNSense

Gambar 4. 5 Adapter 1 (NAT Network)

Gambar 4. 6 Adapter 2 (Host-Only Adapter)

2. Kemudian klik start, tunggu sampai muncul tampilan berikut. Karena status nya sekarang masih live cd maka diperlukan menyimpan data instalan nya dengan cara login menggunakan user : installer dan Password : opnsense

Gambar 4. 7 Tampilan awal OPNSense (CLI)

3. Pilih “continue with default keymap”.

Gambar 4. 8 Pemilihan Keymap

4. Pilih “install (ZFS)” lalu “ok”.

Gambar 4. 9 Pemilihan Paket Installasi

5. Kemudian pilih “ok” pada pilihan “stripe”.

Gambar 4. 10 Pemilihan Paket Installasi

6. Beri tanda pada pilihan “ada0 VBOX HARDDISK” lalu “ok”.

Gambar 4. 11 Penggunaan Vbox Harddisk

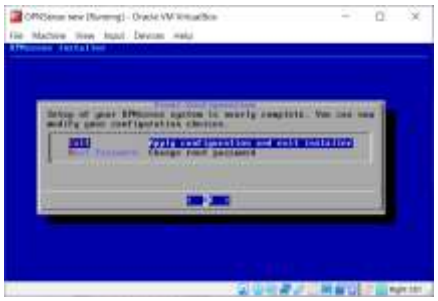
7. Pilih “YES” kemudian tunggu proses selesai.

Gambar 4. 12 Memastikan Paket yang akan di install

8. Buat password baru untuk root, lalu OK.

Gambar 4. 13 Setting Password baru

9. Kemudian apply configuration.

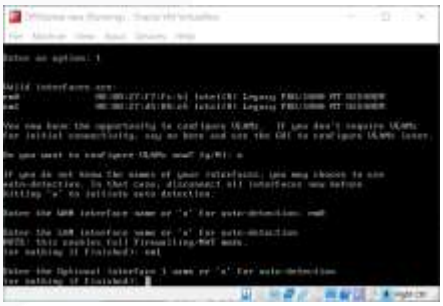


Gambar 4. 14 Terapkan Konfigurasi

10. Tunggu proses sampai selesai, lalu login menggunakan “root” dan password yang sudah disetting sebelumnya.

Gambar 4. 15 Tampilan awal setelah installasi paket

11. Karena interface dari OPNSense masih dalam keadaan default, maka diperlukan setting pada interface terlebih dahulu, ketik 1 pada console lalu enter. Atur interface untuk WAN nya ke “em0” dan LAN “em1”, setelah itu enter.



Gambar 4. 16 Setting Interface

Setelah selesai mengatur interface simpan pengaturan kemudian tunggu proses sampai selesai.

Gambar 4. 17 Simpan Pengaturan

12. Setelah selesai setting interface maka Langkah selanjutnya setting IP pada setiap interface, ketik 2 kemudian enter.

Gambar 4. 18 Setting IP Address interface

Ketik 1 untuk interface LAN dan 2 untuk WAN.

13. Disini kita atur LAN terlebih dahulu. Atur IPv4 pada LAN melalui protocol DHCP, untuk pengaturan IPv6 cukup ketik “N” saja karena kita tidak memerlukannya. Kemudian ketik “y” untuk “web GUI protocol from HTTPS to HTTP?”, agar admin bisa mengakses GUI dari OPNSense.

Gambar 4. 19 Setting IP & Web GUI

14. Setelah selesai maka kita bisa melihat IP dari interface LAN sudah berubah.

Gambar 4. 20 IP LAN

15. OPNSense sudah dapat digunakan, kita dapat mengakses OPNSense melalui web. Ketik IP Address interface LAN pada browser. Kemudian login menggunakan root dan password yang sedang di setting.

Gambar 4. 21 Tampilan Web GUI OPNSense

**4.2.3. Konfigurasi Layanan Web Server Pada Ubuntu 21.04**

1. Install paket web server.

#apt-get install apache2 lalu enter.

Gambar 4. 22 Install Paket Apache di ubuntu

2. Akses web apache dengan mengetikan IP Address dari Ubuntu.


Gambar 4. 23 Tampilan Web default apache2

**4.2.4. Konfigurasi IDS pada OPNSense**

Pada bagian ini menjelaskan mengenai tahapan konfigurasi IDS pada OPNSense, Langkah-langkahnya sebagai berikut :

1. klik pada menu “service” pilih sub menu “Intrusion Detection”. Kemudian pada bar menu, pilih “Download”, setelah itu beri tanda centang pada semua paket suricata yang akan di download. lalu klik “enable selected”. Kemudian klik “Download & Update Rules”

Gambar 4. 24 Download Paket Suricata

2. pada tab rules sudah terlihat paket suricata yang sudah terdownload.

Gambar 4. 25 Paket Suricata

3. kemudian beralih ke tab setting. Beri tanda centang pada “Enable”, “IPS Mode”, dan “Promiscuous mode”, pada bagian pattern matcher

lalu pilih “Hyperscan”, pada bagian interfaces pilih “LAN, WAN” lalu Apply. IDS Siap digunakan.

Gambar 4. 26 Enable IDS sistem

## 4.3 Pengujian

### 4.3.1 Pengujian Port Scanning

Pengujian port scanning dilakukan menggunakan tools Masscan pada kali linux menuju Virtual Ubuntu yang sudang terinstall Web Server. Langkah-Langkah pengujian sebagai berikut :

1. Untuk melakukan Port scanning menggunakan Masscan, Ketikan perintah # masscan -p [PORT] [IP target] pada terminal.

Gambar 4. 27 Port Scanning

Disini Serangan Port scanning berhasil mendeteksi port yang terbuka pada ubuntu, yaitu port 80.

4.3.2 Pengujian Denial Of Service (DoS)

Pengujian Denial of Service dilakukan menggunakan tools LOIC yang di install di dalam Kali linux menuju layanan Web yang ada pada Ubuntu 21.04. Langkah-langkah nya sbagai Berikut :

1. Untuk melakukan pengujian Denial of service (DoS) menggunakan tools LOIC, pada kolom IP, masukan IP Address dari web yang akan diserang. Lalu kklik “Lock on”


Gambar 4. 28 LOIC

2. Kemudian masukan port dan tipe serangan apakah itu TCP, UDP, atau HTTP, lalu set seberapa sering tools akan melakukan hit pada server. Kemudian Mulai Serangan.


Gambar 4. 29 Pilih jenis serangan

### 4.3.3 Web Filtering

Pengujian penyaringan web ini dilakukan menggunakan fitur firewall dengan membatasi client supaya tidak bisa mengakses web tertentu yang sudah di tentukan.

1. Buat aliases yang akan digunakan untuk memudahkan konfigurasi rules pada Firewall. Contoh Aliases disini seperti Domain dari suatu web, seperti youtube.com, facebook.com dan detik.com.

Gambar 4. 30 DNS Detik.com

Gambar 4. 31 DNS Youtube.com

Gambar 4. 32 DNS Facebook.com

2. Setelah itu lihat PfTables pada menu Firewall -> Diagnostics -> PfTables.

Gambar 4. 33 PfTables

3. Disana terdapat daftar ip yang sudah di terjemahkan OPNSense dari DNS yang sudah di daftarkan pada Aliases menjadi beberapa IP Address.

Gambar 4. 34 Daftar IP dari Aliases

Pada gambar di atas terdapat IP dari Aliases Youtube, hanya saja OPNSense tidak mampu menerjemahkan semua ip dari youtube karena terlalu banyak dan akan memakan waktu yang sangat lama.

4. Kemudian buat rules pada interface LAN yang akan digunakan untuk memblokir akses client menuju web facebook, youtube, dan detik.

Gambar 4. 35 Rules Youtube https

Pada rules ini actionyang di pakai adalah Block, agar client tidak dapat mengakses Youtube, interface LAN, Direction IN, Protocol yang digunakan adalah TCP/UDP, dan sumber nya dari LAN net.

Gambar 4. 36 Rules Youtube https

Ubah rentang port tujuan nya menjadi HTTPS kemudian isi deskripsi, deskripsi ini akan memberikan keterangan pada Log Firewall saat rules berjalan. Untuk facebook dab Detik pengaturannya juga seperti ini. Setelah itu simpan pengaturan.

5. Pada sisi client kita akan melakukan ujicoba dengan cara melakukan akses pada web yang sudah di pasangkan rules.

Gambar 4. 37 Pengujian Block Web

Terlihat pada gambar di atas pada saat ubuntu client mencoba mengakses Facebook maka OPNSense akan langsung melakukan blok dan menampilkan log yang memeberitahu bahwa web tersebut di block.

## 5. Kesimpulan dan Saran

### 5.1 Kesimpulan

Dari serangkaian pengujian dari Membangun Sistem Kemanan Jaringan Berbasis Firewall Dan IDS Menggunakan Tools Opnsense maka dapat disimpulkan bahwa sebagai berikut.

1. OPNSense mampu melakukan pencegahan pada client agar tidak dapat mengakses suatu web tertentu yang sudah ditentukan.
2. OPNSense mampu melakukan monitoring melalui menu log file.
3. OPNSense sudah mampu melakukan Blocking terhadap serangan DoS namun OPNSense masih belum mampu mencatat Log serangannya.

### 5.2 Saran

Untuk pengembangan lebih lanjut mengenai penelitian ini, disarankan membangun system firewall dan Intrusion Detection System(IDS) dengan menambahkan mikrotik sebagai router tambahan, agar system menjadi ebih komplek dari yang sebelumnya.

## REFERENSI

[1] S. Tumbuhan, B. Hutan, D. Sub, K. Bangsa, F. Marga, and B. Pohon, “Bab 2 tinjauan pustaka 2.1,” pp. 5–17, 1993.

[2] M. Wirdah, “Bab 1 pendahuluan,” *Pelayanan Kesehat.*, vol. 2016, no. 2014, pp. 1–6, 2010, [Online]. Available: http://library.oum.edu.my/repository/725/2/Chapter_1.pdf.

[3] L. Belakang and B. Masalah, “Pendahuluan,” pp. 3–4.

[4] “OPNsense.”

[5] Santo Faskafri, “Bab 1 pendahuluan,” *Pelayanan Kesehat.*, no. 2015, pp. 3–13, 2020, [Online]. Available: http://repository.usu.ac.id/bitstream/123456

789/23790/4/Chapter I.pdf.

[6] J. Gondohanindijo, “Sistem Untuk Mendeteksi Adanya Penyusup ( IDS : Intrusion Detection System ),” *Semarang*, vol. 2, pp. 46–54, 2011.

[7] بـ رر سیNo Title“ ,بـ اراد ی .ح .و .س .ع .ن .س
در گ یاهن جـغرافـ یایـ ی پـ راک نش و فـ لور
ایـ راد شهر مـ نط قه مراتـ ع در اق لـ یم بـ ا ارتـ باط
ا سـ تان,” vol. 148, pp. 148–162.

[8] S. Ramadhani, U. Sultan Syarif Kasim Alamat, J. Koto Kociak Kecamatan Latina Payakumbuh Sumatera Barat, J. H. Soebrantas Kelurahan Simpang Baru No, and K. Tampan, “Analisis Sistem Keamanan Web Server Dan Database Server Menggunakan Suricata,” *Semin. Nas. Teknol. Inf. Komun. dan Ind.*, vol. 0, no. 0, pp. 2579–5406, 2017, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/SNTIKI/article/view/3368.

[9] A. Haerani, “Pengertian Dan Fungsi Virtual Box.”

[10] D. P. C. C. L. E. Y. N. to K. in 20 Weeks, “Penerapan Watermark,” *Dk*, vol. 53, no. 9, pp. 1689–1699, 2015.