IT-EXPLORE
Jurnal Penerapan Teknologi Informasi dan Komunikasi
ISSN 2828-7940, e-ISSN 2829-1727
Volume 02 Nomor 01 Tahun 2023

PERANCANGAN SISTEM KEAMANAN JARINGAN BERBASIS *HIERARCHICAL NETWORK DESIGN*

Milleano Jody Alfredo Walimema[1], Wiwin Sulistyo[2]

[1,2] Program Studi Teknik Informatika, FTI UKSW,
SalatigaJl. Diponegoro 52-60, Salatiga 50711, Indonesia
Email : 672018141@student.uksw.edu[1], wiwin.sulistyo@uksw.edu[2]

Riwayat artikel:
Submitted: 18-11-2022 *Revised: 06-01-2022* *Published: 04-02-2023*

Abstrak **–** Keamanan jaringan menjadi suatu hal yang sangat penting, terutama untuk sebuah organisasi yang menerapkan teknologi dan sistem informasi di dalamnya. Seperti halnya yang terjadi di Fakultas Teknologi Informasi Universitas Kristen Satya Wacana (FTI UKSW). Saat ini FTI UKSW menggunakan topologi jaringan dengan perangkat *MikroTik* dan dinilai belum cukup terstruktur. Penelitian ini merekomendasikan perancangan desain topologi berbasis *Hierarchical Network Design* dan dirancang dengan menggunakan *pfSense Router Firewall*. Perancangan sistem difokuskan pada bagian *traffic* antara *Distribution Layer* dan *Access Layer*. Hal tersebut dilakukan untuk mengamankan *traffic* jaringan dan memberikan proteksi secara langsung melalui *Web Service pfSense*. Di dalam *pfSense Router Firewall*, terdapat *tools* yaitu *Intrusion Prevention System (IPS) Snort* yang berfungsi untuk membantu dalam memberikan *action* dan *blocking* jika terjadi ancaman pada jaringan. Dengan desain topologi yang diusulkan tersebut diharapkan dapat menghasilkan peningkatan keamanan jaringan komputer di FTI UKSW.

Kata Kunci **–** *Hierarchical Network Design, IPS Snort, pfSense Firewall.*

Abstract **–** *Network security is very important, especially for an organization that implements information technology and systems in it. This is what happened at the Information Technology Faculty of Satya Wacana Christian University (FTI UKSW). Currently FTI UKSW uses a network topology with MikroTik devices. This study recommends designing a topology design based on Hierarchical Network Design and designed using pfSense Router Firewall. System design is focused on the traffic section between the Distribution Layer and Access Layer. This is done to secure network traffic and provide protection directly through the pfSense Web Service. Inside the pfSense Router Firewall, there are tools, namely the Intrusion Prevention System (IPS) Snort which functions to assist in providing action and blocking if a threat occurs on the network. With the proposed topology design, it is hoped that it will result in increased computer network security at FTI UKSW.*

Keywords **–** *Hierarchical Network Design, IPS Snort, pfSense Firewall.*

.

I. PENDAHULUAN

Keamanan jaringan merupakan hal yang sangat penting di era teknologi saat ini. Walau demikian, banyak lembaga dan organisasi yang kurang menghiraukan masalah ini. Akan tetapi, jika suatu saat jaringan diserang dan sistemnya rusak, banyak biaya yang harus dikeluarkan untuk memperbaiki sistem tersebut. Dengan demikian sistem keamanan jaringan menjadi hal yang perlu diutamakan untuk mencegah terjadinya ancaman serangan yang saat ini berkembang pesat baik jenis maupun tingkat risikonya [1].

Fakultas Teknologi Informasi Universitas Kristen Satya Wacana (FTI UKSW) merupakan lembaga yang banyak menggunakan sarana dan prasarana di bidang teknologi informasi. Perancangan, implementasi sampai dengan pengelolaan perlu dilakukan dengan dasar-dasar metode atau pendekatan yang kuat khususnya untuk membangun sistem keamanan yang memadai. Saat ini, belum semua desain jaringan komputer di Fakultas Teknologi Informasi menggunakan pendekatan yang sesuai dengan kebutuhan. Oleh sebab itu, penelitian ini melakukan perancangan dengan menggunakan pendekatan *Hierarchical Network Design* pada jaringan komputer di FTI UKSW tersebut.

Penelitian ini merancang sistem keamanan jaringan komputer di FTI UKSW pada topologi yang berbasiskan *Hierarchical Network Design.* Dengan demikian akan dapat dibangun model keamanan jaringan yang lebih terstruktur dengan mengikuti pola yang ada pada pendekatan tersebut. Penelitian ini menghasilkan skema penempatan sistem keamanan pada jaringan pada *layer* yang terdapat pada model *hierarchical.*

Desain *Hierarchical Network Design* bertujuan untuk membentuk topologi jaringan yang terstruktur. Perancangan yang dilakukan memfokuskan sistem keamanan jaringan pada *traffic* diantara *Distribution Layer* dan *Access Layer* saja, dan tidak meneliti area *Core Layer.* Hal itu dikarenakan *Core Layer* adalah salah satu zona *Hierarchical Network Design* yang memiliki sumber daya jaringan (*network resource*) yang sangat besar [2]. Dengan penerapan desain tersebut dapat meningkatkan keamanan jaringan di FTI UKSW dan mengurangi kerentanan terhadap upaya-upaya serangan yang merugikan.

II. KAJIAN PUSTAKA

2.1. Penelitian Terdahulu

Berdasarkan penelitian terdahulu yang berjudul *High Availability Network Design University Campus Network* [3], dapat dipelajari penyelesaian permasalahan terkait desain topologi jaringan dengan menggunakan *Hierarchical Network Design.* Hal tersebut sangat berpengaruh terhadap kualitas internet dengan jumlah pengguna yang sangat besar. Dengan menggunakan desain tersebut terbukti dapat menciptakan rancangan jaringan yang handal dan efisien untuk penggunaan topologi jaringan berskala besar.

Selanjutnya pada penelitian terdahulu yang berjudul Pemodelan *Hierarchical Network Design* pada Instalasi Rawat Jalan Rumah Sakit Umum [4] mengemukakan bahwa pemodelan dengan desain *Hierarchical Network Design* sangat efisien. Untuk itu peneliti merekomendasikan kepada pihak rumah sakit untuk melakukan pembaharuan

lalu lintas jaringan agar lebih cepat dapat memproses data pasien dan mempermudah dalam *administrator* jaringan melakukan *monitoring* lalu lintas jaringan.

Penelitian lain yang berjudul Perancangan *Blueprint* Jaringan *Intervlan Routing* menggunakan *Hirarki Desain Jaringan pada STMIK Lombok* menjelaskan bahwa *Hierarchical Network Design* sangat dibutuhkan mengingat adanya permasalahan kualitas koneksi jaringan yang tidak baik. Hal itu dikarenakan infrastruktur jaringan *STMIK* yang sebelumnya tidak maksimal sehingga proses bisnis dan pengaksesan untuk semua kegiatan menjadi terganggu. Sehingga desain tersebut akan digunakan untuk meminimalisir semua gangguan dan hambatan sekaligus mengkombinasikan dengan konsep *Inter-VLAN Routing* untuk pembagian akses jaringan [5].

Penelitian yang berjudul Perancangan Jaringan Komputer Lokal Menggunakan Model Hierarki di Kampus [6] menjelaskan bahwa penggunaan *Hierarchy Network Design* sangat berpengaruh terhadap suatu instansi yaitu kampus. Kampus yang terdiri dari berbagai macam gedung, terhubung satu sama lain melalui perangkat jaringan, membutuhkan desain jaringan yang terstruktur. Sebelumnya konsep desain jaringan kampus ini sangat sederhana dan belum bisa memenuhi kebutuhan kampus secara maksimal. Dengan melakukan perancangan desain tersebut, *administrator* jaringan lebih mudah dalam melakukan *monitoring* lalu lintas jaringan dan mengestimasi interkoneksi antar gedung sehingga kinerja pengaksesan jaringan menjadi lebih maksimal [6].

2.2. Hierarchical Network Design

Hierarchical Network Design merupakan salah satu rancangan jaringan efisien untuk diterapkan dalam jaringan berskala besar. Setiap *layer* akan dimaksimalkan penggunaannya dalam melakukan *management* suatu jaringan. Terdapat 3 tiga lapisan pada *Hierarchical Network Design* yang diantaranya adalah *Core Layer, Distribution Layer,* dan *Access Layer*. *Core Layer* berfungsi sebagai lapisan sumber daya jaringan seperti perangkat *Router, Mikrotik, Server*, dan lain sebagainya.

Sedangkan *DistributionLayer* berfungsi sebagai media perangkat yang berfungsi untuk mendistribusikan atau membagikan sumber daya jaringan ke perangkat yang dituju seperti *Switch, Hub, AccessPoint.* Yang terakhir yaitu *Access Layer* yang berfungsi sebagai lapisan penerima sumber daya jaringan yang dapat digambarkan seperti *PC* (*Personal Computer*), *Laptop*, dan perangkat *end user* lainnya.

2.3. Intrusion Prevention System Snort

Intrusion Prevention System Snort adalah *tools* yang bekerja untuk me-*monitoring traffic* suatu jaringan, mendeteksi aktivitas sebuah serangan atau aktivitas yang mencurigakan dengan cara memberikan notifikasi berupa *alert*, dan pencegahan dengan cara melakukan *blocking*. *Action* ini dapat berjalan dikarenakan berisi *rules – rules* dan paket *IPS Snort* yang secara otomatis mendeteksi bermacam – macam jenis serangan terhadap *protocol* jaringan seperti *HTTP, SNMP, SMTP, DOS, DDOS,* dan lain sebagainya. *Snort* ini juga bersifat *open-source* dan sangat relevan untuk digunakan sebagai proteksi keamanan untuk saat ini.

2.4. MikroTik CRS

MikroTik Cloud Router Switch (CRS) merupakan sebuah perangkat *Switch* yang menggunakan sistem operasi *RouterOS MikroTik* di dalamnya dan mampu melakukan manajemen *traffic layer 3 (Routing)*. *MikroTik CRS* ini sering disebut sebagai *Switch*

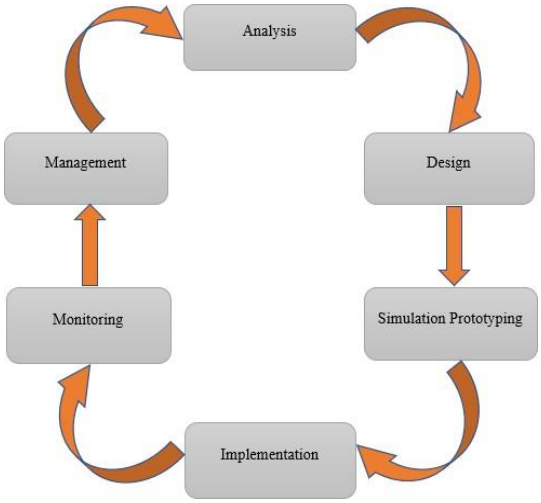
Layer 3. Uniknya *MikroTik CRS* juga menggunakan *RouterOS* sehingga semua fitur pada *RouterOS* juga bisa diterapkan di perangkat ini. Dalam hal ini, *MikroTik CRS* berfungsi sebagai *Switch* pada *Distribution Layer*.

2.5. pfSense Router Firewall

pfSense Router Firewall adalah suatu perangkat lunak yang berbasis *FreeBSD* yang disesuaikan untuk kebutuhan *Router* dan *Firewall*. *pfSense* ini menyediakan beberapa paket yang sering dibutuhkan untuk kebutuhan *Gateway* dan berbagai jenis layanan kepada *client*. Dalam hal ini, *pfSense Router Firewall* berfungsi sebagai perangkat untukmenjalankan *tools Intrusion Prevention System Snort* yang nantinya akan digunakan untuk sistem keamanan jaringan.

III. METODE PENELITIAN

Metode yang digunakan untuk melakukan penelitian ini adalah yaitu *Network Development Life Cycle* (NDLC). Metode ini digunakan untuk mendukung pembaharuan topologi jaringan FTI yang semula tidak terstruktur menjadi terstruktur dengan berbasiskan *Hierarchical Network Design.* Metode ini juga sekaligus digunakan untuk perencanaan dan daur ulang perancangan sebuah sistem keamanan jaringan yang disesuaikan terhadap topologi jaringan yang ada. Tahapan dari metode *NDLC* dapat dilihat pada Gambar 1.



Gambar 1. *Flowchart* Tahapan Penelitian *NDLC*.

Tahapan penelitian ini menggambarkan langkah – langkah untuk melakukan perancangan sistem keamanan jaringan Fakultas Teknologi Informasi, diantaranya [7]:

1. *Analysis*

   Tahapan awal ini menganalisis kebutuhan penelitian untuk menghasilkan data yang berkaitan dengan topologi jaringan dan skema sistem keamanan jaringan yang akan dibuat pada Fakultas Teknologi Informasi UKSW. Perangkat pendukung perancangan seperti *hardware* dan *software* diperlukan guna melakukan perancangan sistem keamanan jaringan dengan pendekatan berbasis *Hierarchical Network Design.*

2. *Design*

Tahap berikutnya adalah membuat desain atau skema sistem keamanan jaringan komputer yang akan dirancang di Fakultas Teknologi Informasi berbasis *Hierarchical Network Design*.

3. *Simulation Prototyping*

   Simulation Prototyping dibuat untuk memudahkan dalam memahami penggunaan *software* yang akan dikembangkan. Selain itu, *prototyping* juga berguna sebagai alat untuk mendesain sebuah sistem serta bagaimana sistem tersebut akan terlihat dan dapat dipahami oleh orang-orang yang menggunakannya. Beberapa pekerja jaringan akan membuat dalam bentuk simulasi dengan bantuan aplikasi khusus dibidang *network* seperti *Graphical Network Simulator 3, Packet Tracert, EVE-NG*, dan sebagainya. Dalam penelitian ini penulis menggunakan *tools* yang sudah ditentukan pada tahap sebelumnya.

4. *Implementation*

   Tahap ini membahas tentang implementasi sistem keamanan jaringan yang sudahdirancang ke dalam *Hierarchical Network Design* khususnya sistem yang akan difokuskan antara *Distribution Layer* dan *Access Layer* saja. Dalam hal ini, sistem keamanan jaringan yang dibangun hanyalah perancangan saja. Untuk tahap ini belum sepenuhnya dilakukan dan selanjutnya akan menuju ke tahapan berikutnya.

5. *Monitoring*

   Tahapan berikutnya adalah *monitoring*. Pada tahap ini, perlu dilakukan pemantauan terhadap performansi dan keakuratan sistem terhadap lalu lintas jaringan antara *Distribution Layer* dan *Access Layer*.

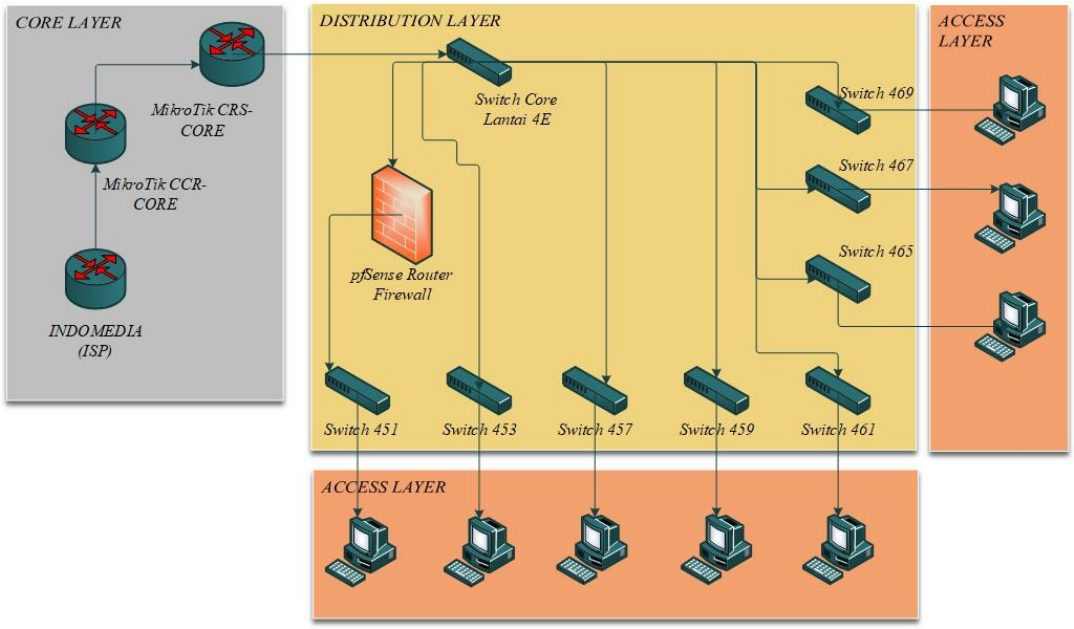
6. *Management*

   Setelah melewati tahap *monitoring*, langkah terakhir adalah tahapan *management*.Pada langkah terakhir ini, sistem keamanan jaringan yang berhasil dirancang dan disimulasikan di Fakultas Teknologi Informasi harus melakukan *maintenance* dan pemeliharaan supaya sistem tersebut selalu *update* dan tidak akan mengalami masalah pada saat digunakan.

IV. HASIL DAN PEMBAHASAN

4.1. Analisis Kebutuhan Perancangan Sistem Keamanan Jaringan

Berdasarkan data topologi yang didapat, tidak akan merubah bentuk dari topologi jaringan pada Fakultas Teknologi Informasi. Di bawah ini merupakan bentuk dari topologi jaringan awal sebelum diberikan sistem keamanan. Topologi jaringan ini menggunakan semua perangkat dari *MikroTik.* Untuk topologi *logic* Fakultas Teknologi Informasi dapat dilihat pada Gambar 2.



Gambar 2. Topologi *logic* Fakultas Teknologi Informasi UKSW saat ini.

Selanjutnya akan dilihat tingkatan kebutuhan *user* untuk sistem keamanan jaringan FTI UKSW. Tingkatan kebutuhan user tersebut dapat dikelompokkan pada Tabel 1 di bawah ini.

Tabel 1. Tingkatan *user* terhadap sistem keamanan jaringan.

User	Prioritas	Keterangan
Level Pimpinan • Dekan • Wakil Dekan • Dekan Departemen • Sekretaris Fakultas • Kaprodi	Tinggi	Mendapatkan perlindungan *user* dan prioritas akses yangtinggi (yang disesuaikan dengan wewenangnya).
Kepala Bagian • Kabag Lab Komputer • Kabag Administrasi • Kepala bagian TU	Tinggi	Mendapatkan perlindungan user dan prioritas akses yang tinggi sesuai dengan wewenangnya.
Dosen	Tinggi	Mendapatkan perlindungan user dan prioritas akses yang tinggi untuk bidang yang berhubungan dengan akademik (pengajaran dan lain - lain).
Staff dan Pegawai	Tinggi	Mendapatkan perlindungan user dan prioritas akses yang tinggi untuk bidang masing – masing yang telah ditentukan.
Mahasiswa	Menengah	Mendapatkan perlindungan user tinggi dan prioritas akses yang terbatas untuk pembelajaran

Konsep perancangan *Firewall* ini bertujuan untuk melindungi, menyaring, membatasi, dan menolak suatu kegiatan pada jaringan pribadi/privat dengan jaringan luar yang bukan merupakan ruang lingkupnya. Berkaitan dengan hal tersebut, konsep *firewall* ini menggunakan pendekatan *Arsitektur Screened Subnet*. Cara kerja *firewall* ini menutup *traffic* yang keluar (*outgoing network traffic*) berdasarkan sumber atau tujuan dari *traffic* tersebut. Selain itu, *Firewall* ini juga menyaring *traffic* yang berasal dari jaringan internal ke internet, misalnya ketika ingin mencegah *user* dari mengakses *situs-situs* yang tidak diinginkan. Lebih tepatnya, *firewall* ini bekerja dari lingkup jaringan internal terhadap *user* yang terhubung langsung ke jaringan FakultasTeknologi Informasi.

Untuk mendukung perancangan dan uji coba sistem keamanan jaringan ini, perangkat keras (*hardware*) sangat ditentukan berdasarkan kemampuan sistem nantinya. Untuk *hardware* yang digunakan dan spesifikasi secara *detail* dapat dilihat pada Tabel 2. Sedangkan untuk perangkat tambahan yaitu perangkat jaringan dapat dilihat pada Tabel 3 di bawah ini.

Tabel 2. *Detail* mengenai perangkat keras yang digunakan.

Perangkat Keras	Spesifikasi
Laptop sebagai *RouterFirewall*	• Processor : Intel Core i3 – 6006U. • VGA Card : NVIDIA GeForce MX 110. • RAM : 12 GB DDR4. • HDD : 1 TB. • Merk : ASUS VivoBook Max X441UB.
Laptop sebagai *PCClient*	• Processor : Intel Core i7 8550U. • VGA Card : NVIDIA GeForce MX 150. • RAM : 16 GB DDR4. • HDD : 1 TB. • Merk : Acer E5 476G.

Tabel 3. *Detail* mengenai perangkat jaringan tambahan yang digunakan.

Perangkat Jaringan
MikroTik CRS (*Cloud Router Switch*)
Kabel *LAN (Ethernet)*
Adapter LAN Network Hub 1 port
MikroTik HAP 4 Port Switch

Untuk *software* yang akan digunakan untuk melakukan perancangan sistem keamanan jaringan disajikan dalam bentuk tabel. Untuk lebih lanjut dapat dilihat pada Tabel 4.

Tabel 4. *Detail* mengenai perangkat lunak yang digunakan.

Nama *Tools*	Jenis *Tools*	Versi
FreeBSD pfSense	*Router Firewall + Web Services*	*2.6.0*
Snort	*Intrusion Prevention System (IPS)*	*4.1.6*

Perancangan sistem keamanan jaringan ini menggunakan pendekatan berbasis *Hierarchical Network Des5ign.* Di bawah ini adalah zona keamanan yang akan difokuskan untuk sistem keamanan jaringan. Untuk lebih jelasnya dapat dilihat pada Tabel 5.

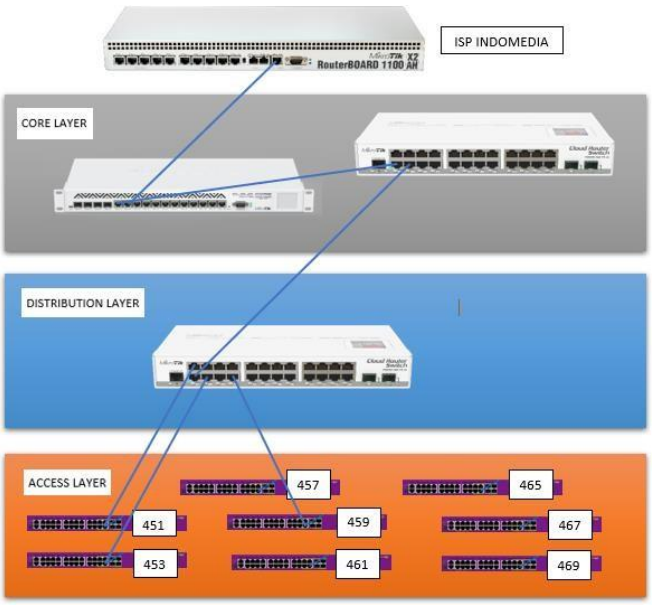
Tabel 5. *Detail* Informasi mengenai zona keamanan.

Zona	Keterangan
Core Layer	Tidak difokuskan dikarenakan memiliki sumber daya yang sangat besar sehingga penulis tidak memiliki perangkat pendukung yang memadai.
Distribution Layer	Memberikan perlindungan pada *traffic* jaringan yang menuju ke *Access Layer*.
Access Layer	Memberikan perlindungan penggunaan jaringan pada *user*.

4.2. Perancangan Sistem Keamanan Jaringan FTI UKSW

4.2.1. Topologi Jaringan Berbasis *Hierarchical Network Design*

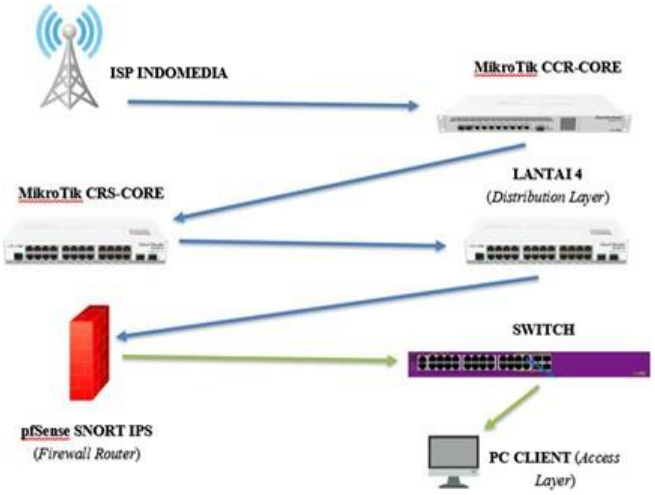
Topologi jaringan tanpa adanya fitur keamanan sangatlah rentan terhadap serangan yang berasal dari luar. Selain itu, *administrator* jaringan juga sangatsulit ketika ingin mendeteksi adanya serangan tersebut. Untuk itu, diperlukan langkah pengambilan dari salah satu topologi yang akan dirancang untuk pendekatan desain berbasis *Hierarchical Network Design*. Untuk hasilnya dapat dilihat pada Gambar 3.



Gambar 3. Perubahan topologi yang sudah berbasis *Hierarchical Network Design*.

Setelah topologi jaringan FTI dirancang ke desain topologi *Hierarchical Network Design*, maka langkah berikutnya adalah membuat skema sistem keamanan untuk memudahkan perancangan sistem keamanan jaringan pada *Distribution Layer* dan *Access Layer*. Selanjutnya diambil salah satu bagian topologi yang vital. Salah satu perangkat *Distribution Layer* yaitu *MikroTik Cloud Router Switch*. Pada skema ini,

hanya difokuskan untuk bagian antara *Distribution Layer* dan *Access Layer* saja. Skema tersebut dapat digambarkan seperti Gambar 4.



Gambar 4. Skema sistem keamanan jaringan Fakultas setelah diberikan *Firewall*

4.2.2. Perancangan Sistem Keamanan Jaringan

a. Melakukan perancangan *pfSense Firewall*

Pada tahap ini akan dilakukan perancangan menggunakan *pfSense Firewall* untuk *Intrusion Prevention System (IPS)* dengan *tools Snort.* Dalam hal ini digunakan perangkat dua *Laptop* sebagai *Firewall Router* dan *PC Client.* Sebelum melakukan pengujian, langkah awal yaitu melakukan konfigurasi pada *pfSense.* Konfigurasi ini bertujuan untuk menentukan arah *traffic* ke *WAN (Wide Area Network)* dan *LAN (Local Area Network)* dengan*network interface adapter* yang sudah tertera serta melakukan sedikit perubahan dan pengaturan *IP Address*.

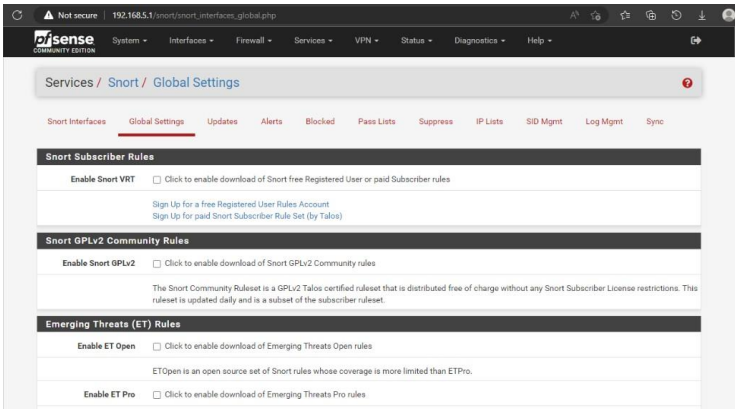
```
Starting webConfigurator...done.
Starting DHCP service...done.
Starting DHCPv6 service...done.
Configuring firewall...done.
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON...done.
pfSense 2.6.0-RELEASE amd64 Mon Jan 31 19:57:53 UTC 2022
Bootup complete
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
 pfSense - Serial : J2N0CV07U04308F - Netgate Device ID: 1de14bb143262ea0ea70
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***
WAN (wan)    -> re0       -> v4/DHCP4: 192.168.77.253/24
LAN (lan)    -> ue0       -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                  10) Filter Logs
 2) Set interface(s) IP address        11) Restart webConfigurator
 3) Reset webConfigurator password     12) PHP Shell + pfSense tools
 4) Reset to factory defaults          13) Update from console
 5) Reboot system                      14) Enable Secure Shell (sshd)
 6) Halt System                        15) Restore recent configuration
 7) Ping host                          16) Restart PHP-FPM
 8) Shell
```

Kode 1. Konfigurasi *Command Line Interface Router Firewall pfSense*

IP Address untuk membuka *Web Services pfSense* tersebut belum diubah sehingga diperlukan sedikit untuk perubahan untuk *IP Address* yang semula *192.168.1.1/24* menjadi *192.168.5.1/24* yang nantinya akan di-*remote* pada *PC / Laptop Client*. Untuk *Command Line* konfigurasi *pfSense Firewall Router* dapat dilihat pada Kode Program 1 di atas.

b. Konfigurasi *WAN* dan *LAN Snort Intrusion Prevention System*

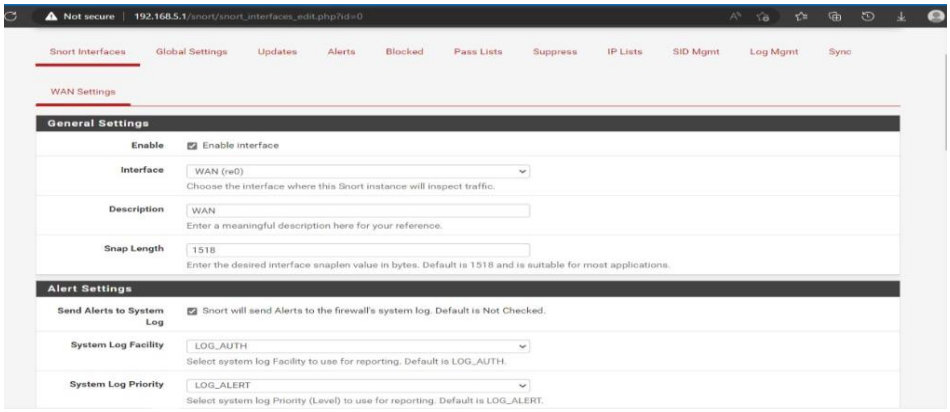
Sebelum melakukan konfigurasi 2 *network interfaces,* terlebih dahulumelakukan konfigurasi pada *Snort Services Settings.* Hal ini bertujuan untuk melakukan pengaturan *Snort Services* pada saat akan dijalankan sebagai *Intrusion Prevention System.* Konfigurasi ini berisi pilihan –pilihan yang harus ditandai untuk pengaturan *Snort Rules* dan *Emerging Threat Rules* yang akan ditampilkan sebagai *action Intrusion Prevention System* pada *pfSense*. Untuk hasil konfigurasi *Snort Services* dan *Update Global Settings* dapat dilihat pada Gambar 5.



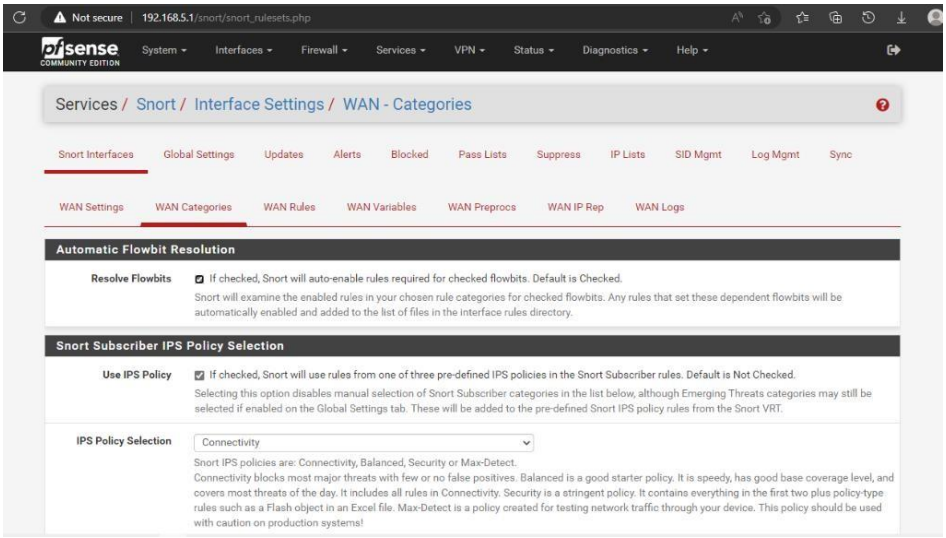
Gambar 5. Konfigurasi *menu Snort Service Global Settings*.

Selanjutnya dilakukan konfigurasi *Wide Area Network Interface Settings* pada *pfSense.* Pada tahap ini, dilakukan konfigurasi *menu Snort Interfaces WAN Settings*. Hal ini bertujuan untuk melakukan pengaturan *traffic WAN* yangberasal dari internet *ISP* yang terhubung ke perangkat *MikroTik CCR (Core Layer)*. Sekaligus melakukan konfigurasi lainnya seperti *General Setting* dan *Alert Setting*.

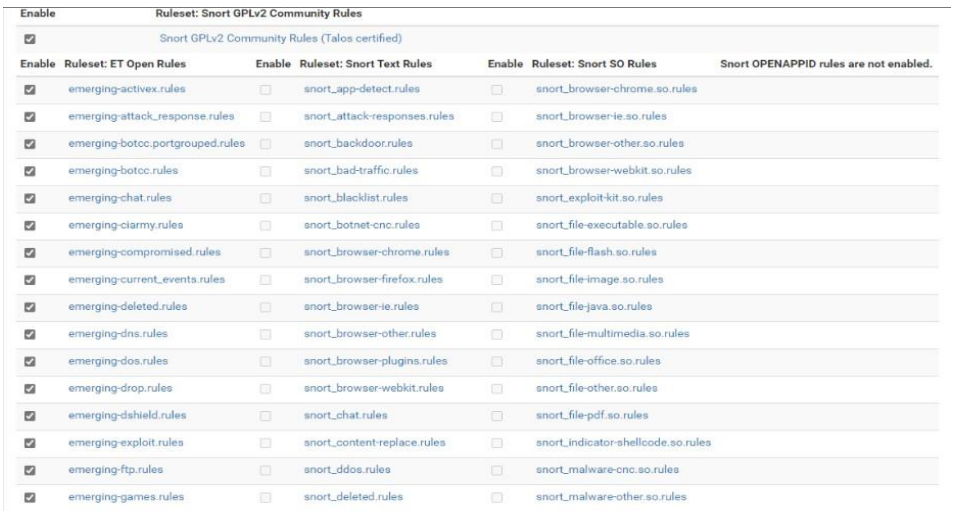
Konfigurasi ini bertujuan untuk menentukan jalannya *WAN interface* dan *Alert System* yang dimunculkan jika melewati*traffic* tersebut. Untuk *WAN network interface adapter* menggunakan *adapter (re0)*. Berikut adalah hasil konfigurasi pada *menu* di *Alert Settings*, *Block Settings*, dan *Detection Performance Settings*. Untuk hasilkonfigurasi menu *WAN Interface Settings* dapat dilihat pada Gambar 6. Sedangkan untuk hasil konfigurasi *WAN Categories Settings* dan*Emerging Threat Rules* untuk *Action Snort IPS* pada *WAN Interface* dapatdilihat pada Gambar 7 dan Gambar 8.



Gambar 6. Konfigurasi *menu WAN Interface Settings*.



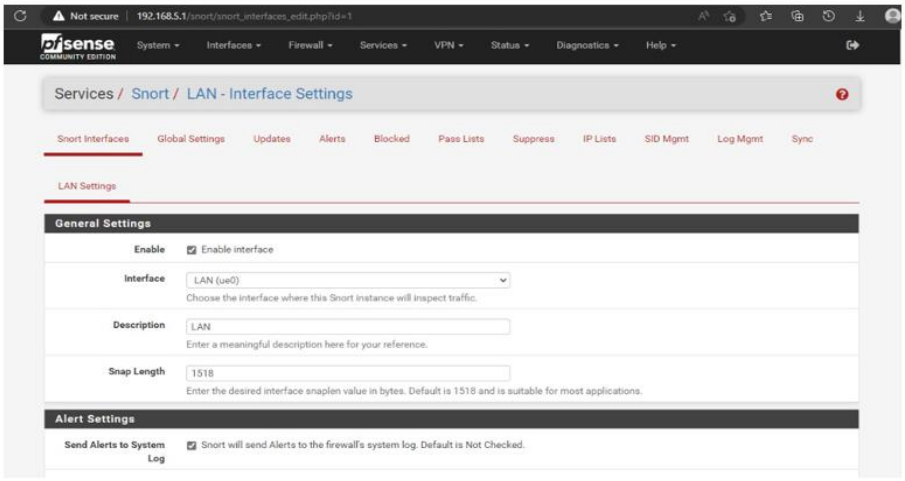
Gambar 7. Konfigurasi *menu WAN Categories Settings*.



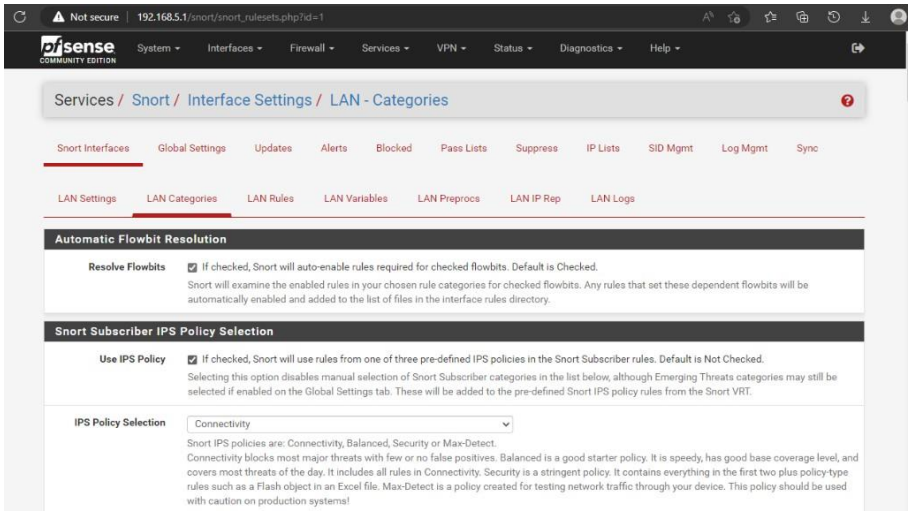
Gambar 8. Konfigurasi *Emerging Threat Rules*.

Berikutnya adalah konfigurasi *LAN Interface Settings* pada *pfSense.* Sama seperti konfigurasi *network interface WAN* sebelumnya, diperlukan konfigurasi juga untuk *network interface adapter LAN*. Karena*LAN* disini berfungsi sebagai *network interfaces adapter* yang menerima *traffic* internet dari perangkat *MikroTik CCR (Core Layer).* Selanjutnya *traffic* jaringan tersebut akan menuju ke perangkat *MikroTik CRS* sebagai segmentasi jaringan yang akan diteruskan menuju ke *Switch* (*AccessLayer)*. Berkaitan dengan konfigurasinya hampir sama dengan *WAN* namun *LAN* ini menggunakan *network interfaces adapter* yang berbeda yaitu *adapter (ue0).*

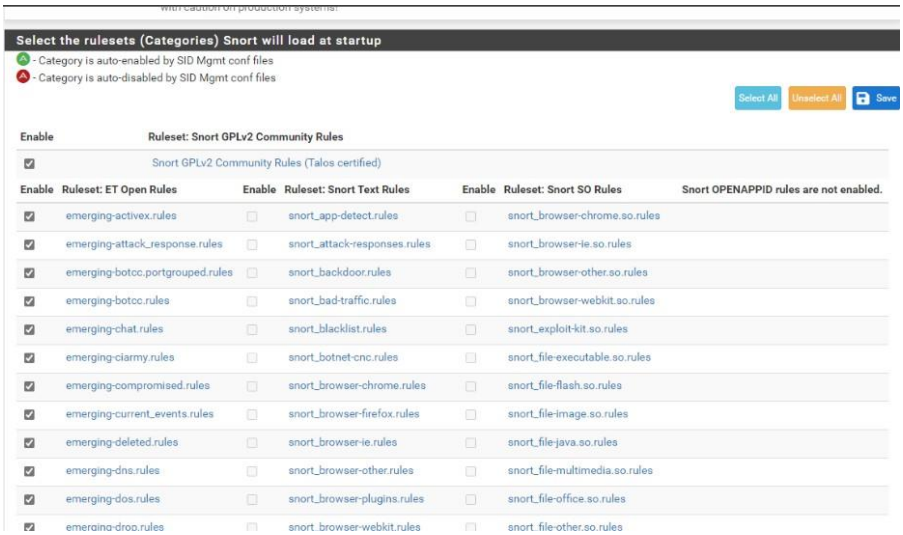
Berikutnya pada *Snort LAN Settings Interface* ini, terdapat *menu General Settings* dan *Alert Settings.* Dimana *menu* pada *LAN* ini digunakan juga sebagai *Action Snort IPS* untuk *traffic* dari*Distribution Layer* yang menuju ke *Access Layer*. Untuk pengaturan ancaman bisa dikonfigurasi pada menu *Emerging Threat Rules Sets* untuk*Snort IPS*. Untuk hasil *screenshot* konfigurasi *LAN Interface Settings* dapat dilihat pada Gambar 9. Sedangkan untuk hasil konfigurasi *LAN Categories Settings* dan *Emerging Threat Rules* untuk *Action Snort IPS* pada *LAN Interface* dapat dilihat pada Gambar 10 dan Gambar 11 berikut.



Gambar 9. Konfigurasi *LAN Interface Settings*.



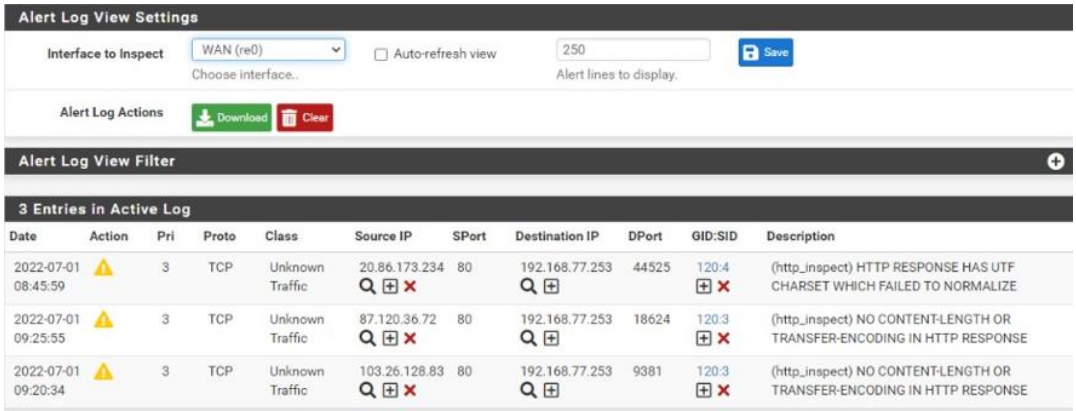
Gambar 10. Konfigurasi *LAN Categories Settings*



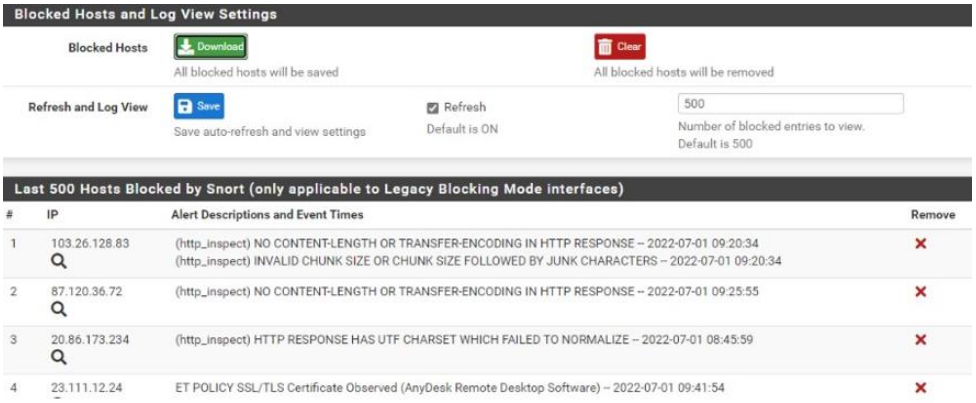
Gambar 11. Konfigurasi *Emerging Threat Rules* untuk *Action Snort IPS*

4.3. Hasil Pengujian Sistem

Untuk hasil pengujian sistem keamanan jaringan ini dapat dilihat dengan menggunakan *Snort IPS pfSense Web Services*. Dalam hal ini, sudah terlihatbahwa sistem *Snort IPS* akan memunculkan *alert* pada *monitoring* jika *web* atau *situs* tersebut telah dijalankan. Jika *alert* telah mendeteksi hal tersebut, artinya *web* atau *situs* tersebut telah dikategorikan dan dianggap sebagai sebuah serangan. Maka dari itu, secara otomatis juga *Snort IPS pfSense* akanmelakukan *action blocking situs* atau *web* yang dapat dilihat pada *Web Monitoring Blocked Host IP Address* sehingga *web* atau *situs* tersebut tidak dapat diakses secara langsung. Kecuali, penulis menonaktifkan *Alert* dengan*rules* tersebut maka kegiatan *blocking* tidak akan berjalan sebagaimanamestinya. Dibawah ini adalah bukti *screenshot* hasil pengujian *action alert* situs yang terdeteksi pada Gambar 12. Sedangkan untuk *action blocking* situspada Gambar 13.



Gambar 12. *Situs* yang terdeteksi oleh *alert Snort IPS pfSense* pada *Alert LogView.*



Gambar 13. Hasil *action blocking situs* atau *web* pada *pfSense.*

Untuk tingkat keberhasilan pengujian ini, masih menemui permasalahan dan hasil pengujian dinyatakan kurang berhasil. Hal ini dikarenakan waktu pelaksanaan uji coba yang terbatas dan sistem *Snort IPS pfSense* ini hanya bisa mendeteksi *protocol* jaringan tertentu yaitu *protocol HTTP* dan *TCP*. Pendeteksian ini diujikan dan difungsikan pada *traffic* dari perangkat *Distribution Layer* yaitu *MikroTik CRS* yang akan menuju ke perangkat *Access Layer* yaitu e*ndpoint* (*user).* Untuk perbandingan dari kedua sistem tersebut, sistem ini sangat direkomendasikan karena tingkat keamanannya yang sangat tinggi. Sehinggasangat sesuai untuk *firewall* pada *traffic* diantara *Distribution Layer* dan *Access Layer*. Sedangkan, untuk sistem sebelumnya masih mengalami keterbatasan dalam melakukan pendeteksian. Hal ini dikarenakan hanya menggunakan fungsi *firewall* bawaan perangkat dari *MikroTik*.

V. SIMPULAN DAN SARAN

Berdasarkan dengan hasil perancangan dan pengujian sistem keamanan jaringan di FTI UKSW, dapat diketahui bahwa *pfSense Firewall* ini dapat dijadikan sebagai rekomendasi proteksi terhadap keamanan jaringan yang sesuai dengan desain topologinya yang terstruktur berbasiskan *Hierarchical Network Design*. Selain itu, sistem *pfSense Firewall* ini juga dapat memberikan informasi *detail* mengenai jenis serangan yang masuk ke *traffic* jaringan. Sistem ini juga didukung oleh *Snort Intrusion Prevention System* yang memberikan *action* berupa *alert* yang berupa notifikasi sehingga hasilnya dapat tersimpan pada *Log View* serta *blocking* atau penolakan terhadap suatu *situs* atau *web* karena terdeteksi sebagai sebuah serangan.

Dikarenakan waktu ujicoba yang terbatas, maka hasil *monitoring* menggunakan perangkat *Snort IPS pfSense* dirasakan kurang maksimal. Sehingga dalam mendeteksi serangan pada *traffic* antara *Distribution Layer* dan *Access Layer,* hanya dapat memberikan *detail* informasi yang terdeteksi serangan yaitu *protocol* jaringan *HTTP* dan *TCP* saja. Oleh karena itu, perlu dilakukan pengujian dengan menggunakan *situs* atau *web* lainnya.

DAFTAR PUSTAKA

[1] Wajong, A. M. R. “Kerentanan yang Dapat Terjadi di Jaringan Komputer Pada Umumnya,” *Jurnal ComTech*, vol. 3, no. 9, pp. 474–481, 2012.

[2] Anugrah I. dan Rahmanto, R. H., “Sistem Keamanan Jaringan Local Area Network

Menggunakan Teknik De-Militarized Zone," *PIKSEL Penelit. Ilmu Komput. Sist. Embed. Log.*, vol. 5, no. 2, pp. 91–106, 2018, doi: 10.33558/piksel.v5i2.271.

[3] Sulaiman, O. K. dkk, "High Availability Network Design University Campus Network Dengan Model Hirarki", *Jurnal Hirarki,* Vol. I, pp. 15–19, 2017.

[4] Atmaja, G. S. dan Sulistyo, W., "Pemodelan Hierarchical Network Design Pada Instalasi Rawat Jalan Rumah Sakit Umum Daerah Cibinong", *Infotech Journal Universitas Majalengka*, vol 02 no 01, 2021.

[5] Tantoni, A., "Perancangan Blueprint Jaringan INTERVLAN ROUTING Menggunakan Model Hirarki", *Jurnal Transformasi*, vol.15, no. 1, pp. 56–65, 2019.

[6] Novrian, F., "Perancangan Jaringan Komputer Lokal Menggunakan Model Hirarki", *Jurnal JARKOM,* vol. 7, no. 2, pp. 103–111, 2019.

[7] Sanjaya, T. dan Setiyadi, D., "Network Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim," *Mhs. Bina Insa.*, vol. 4, no. 1, pp. 1–10, 2019.

[8] Nurdadyansyah, N. dan Hasibuan, M. "Tampilan Perancangan Local Area Network Menggunakan NDLC Untuk Meningkatkan Layanan Sekolah," *Konf. Nas. Ilmu Komputer*, Agustus 2021.

[9] Dwiyatno, S. dkk. "Implemetation of Snort IPS Using PfSense as Network Forensic in SMK XYZ," *Proceedings of the 1st International Multidisciplinary Conference on Education, Technology, and Engineering* (IMCETE), 2019.

[10] Arman, M. dan Rachmat, N., "Implementasi Sistem Keamanan Web Server Menggunakan Pfsense," *Jusikom J. Sist. Komput. Musirawas*, vol. 5, no. 1, pp. 13–23, 2020.

[11] Laila, A.R. "Implementasi Intrusion Prevention System (IPS) Pada Keamanan Jaringan Dengan Notifikasi Berbasis Telegram di Jurusan Teknik Komputer," *J. Lap. Akhir Tek. Komput.*, vol. 1, no. 1, pp. 10–17, 2021

[12] Anggoro B.S., dan Sulistyo, W. "Implementasi Intrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi," *Semin. Nas. APTIKOM*, pp. 280–288, 2019, [Online]. Available: http://publikasi.dinus.ac.id/index.php/semnastik/article/view/2938

[13] Dasmen, dkk., "Penerapan Snort Sebagai Sistem Pendeteksi Serangan Keamanan Jaringan", [Online]. Available: https://tunasbangsa.ac.id/ejurnal/index.php/jurasi

[14] Anonim, "Ketentuan Program Multimedia dan Jaringan Jurusan Teknik Informatika dan Komputer", Politeknik Negeri Jakarta, 2021

[15] Dirgantara, R. R. C. "Implementasi ARP Watch Dengan PFSense untuk Mekanisme Pengamanan", *D3 Manaj. Inform. Fak. Tek. Univ. Negeri Surabaya*, pp. 67–76, 2020.