PERANCANGAN FIREWALL ROUTER MENGGUNAKAN OPNSENSE UNTUK MENINGKATKAN KEAMANAN JARINGAN PT. PERTAMINA ASSET 2 PRABUMULIH

[1]Muhammad Afif Al Fauzan, [2]Timur Dali Purwanto
[1]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma, muhamadafif999@gmail.com
[2]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma, timurdalipurwanto@binadarma.ac.id

Abstract - *At PT. Pertamina Asset 2 Prabumulih uses a firewall from pfsense, but using this pfsense there is no improvement in securing the network because there are no new innovations or updates in securing the network because over time, a good firewall is needed and keeps up with the times. With these problems, the design is carried out using a firewall from Opnsense, because Opnsense has a newer firewall that develops with the times. By using action research research methods make diagnoses, make action plans, take action, evaluate, and learn. By designing a router firewall using Opnsense you get better results where using the firewall feature in Opnsense blocks attacks, spreading viruses on the network and blocking unauthorized access. Using this Opnsense network security will be safer because Opnsense updates or improves network security every week and it looks more modern and there are search navigation tools and the latest version of the firewall feature so that it can guarantee a safer network because it uses a newer and updated version of the firewall.*

Keywords: Firewall, OPNsense, Pfsense, Network Security, Router.

Abstrak - Di PT. Pertamina Asset 2 Prabumulih menggunakan firewall dari pfsense, tetapi menggunakan pfsense ini tidak adanya peningkatan dalam mengamankan jaringan dikarenakan tidak adanya inovasi baru atau pembaruan dalam mengamankan jaringan karena seiring perkembangan jaman maka diperlukannya firewall yang baik dan mengikuti perkembangan jaman. Dengan permasalahan tersebut maka dilakukan perancangan menggunakan firewall dari opnsense, karena opnsense memiliki firewall yang lebih baru berkembang seiring perkembangan jaman. Dengan menggunakan metode penelitian action research melakukan diagnosa, membuat rencana tindakan, melakukan tindakan, melakukan evaluasi, dan pembelajaran. Dengan melakukan perancangan firewall router menggunakan opnsense mendapatkan hasil yang lebih baik yang dimana menggunakan fitur firewall di opnsense melakukan pemblokiran terhadap penyerangan , penyebaran virus di jaringan dan pemblokiran akses yang tidak sah. Menggunakan opnsense ini keamanan jaringan akan lebih aman karena opnsense melakukan pembaruan atau meningkatkan keamanan jaringan setiap minggunya dan tampilannya lebih modern dan ada tools navigasi pencarian serta fitur firewall nya versi terbaru sehingga bisa menjamin jaringan lebih aman karena menggunakan firewall versi lebih baru dan ter-update.

Kata kunci: Firewall, OPNsense, Pfsense, Keamanan Jaringan, Router.

1. Pendahuluan

Di PT. Pertamina Asset 2 sendiri menggunakan dua ISP yaitu Icon+ dan Astinet Telkom yang memiliki *bandwidth* masing-masing icon+ 40MB dan Astinet Telkom 20MB. Dan menggunakan *firewall* dari *Pfsense* yang dimana *firewall* ini untuk mengamankan jaringan dari Serangan dari luar jaringan seperti serangan *DoS*, serta paket *terfragmentasi* & cacat, ancaman lainnya. Fitur *firewall* di *pfsense* sendiri yaitu *stateful firewall , networdk address translation*, penyaringan jaringan, rute fleksibel dan lain-lain. Tetapi dengan menggunakan *pfsense* ini tidak

adanya peningkatan dalam mengamankan jaringan dikarenakan tidak membuat inovasi baru atau peningkatan keamanan yang baru, perkembangannya lebih lambat ini menyebabkan tidak meningkatnya keamanan jaringan karena keamanan jaringan harus di tingkatkan seiring berkembangnya jaman maka diperlukannya *firewall* yang mumpuni dan lebih baik.

Oleh karena itu, dengan masalah tersebut maka dilakukan perancangan menggunakan firewall opnsense. OPNsense merupakan sistem operasi yang berbasis FreeBSD yang digunakan sebagai firewall yang bersifat open source dapat di unduh secara gratis dan perkembangan dan kebijakan pembaruannya cepat serta memberikan layanan extra terhadap penggunanya dan untuk keamanan jaringan. Dengan begitu diperlukannya perancangan *firewall router* menggunakan *Opnsense* untuk meningkatkan keamanan jaringan di PT. Pertamina Asset 2 Prabumulih dengan fitur *firewall* yang ada di *Opnsense*. Dengan permasalahan tersebut tujuan dari perancangan ini untuk sebagai *prototype* menggunakan *firewall opnsense* dalam meningkatkan keamanan jaringan di PT. Pertamina Asset 2 Prabumulih.

2. Tinjauan Pustaka

2.1 Jaringan Komputer

Jaringan komputer merupakan sebuah jaringan telekomunikasi yang membolehkan node-node untuk saling berbagi sumber daya (resources) [1]. Jaringan komputer merupakan kumpulan dari sejumlah perangkat berupa computer, hub, switch, router, atau perangkat jaringan lainnya yang terhubung dengan menggunakan media komunikasi tertentu [2]. Jaringan Komputer adalah suatu sistem yang terdiri atas computer dan perangkat jaringan lainnya yang bekerja sama untuk mencapai tujuan tertentu. Komputer, printer atau perangkat keras lainnya yang terhubung dengan jaringan disebut dengan istilah node [3].

Dari pengertian di atas penulis dapat menyimpulkan jaringan komputer merupakan koneksi antara dua atau lebih computer terhubungkan ke media transmisi berkabel atau nirkabel (nirkabel). Apabila dari dua unit komputer dapat bertukar data atau informasi dan berbagi perangkat keras dalam suatu jaringan maka keduanya dikatakan terhubung. Data-data yang seperti teks, audio atau video ditransmisikan melalui media kabel atau nirkabel, sehingga pengguna komputer di jaringan komputer dapat saling bertukar file atau data, printer yang sama digunakan untuk mencetak, dan menggunakan perangkat keras atau perangkat lunak yang terhubung dalam jaringan secara bersama-sama.

2.2 *Firewall*

Umumnya *firewall* dibuat untuk melindungi *Network internal* (LAN) terhadap berbagai gangguan atau serangan yang berasal dari luar (internet)". Karena mengingat dunia luar adalah dunia bebas sehingga potensi serangan dari dunia luar sangat besar. Dengan begitu *firewall* dapat digunakan sebagai alat untuk meningkatkan keamanan dan untuk melindungan data yang berada di dalam jaringan tersebut [1].

Sebuah firewall adalah pendekatan keamanan yang membantu mengimplementasikan kebijakan keamanan yang lebih besar, yang mendefinisikan servis dan akses yang diizinkan. Dalam hal ini Firewall menerapkan kebijakan ini dalam suatu bentuk konfigurasi jaringan, beberapa router dan host di jaringan, dan tindakan keamanan lainnya seperti mekanisme dalam autentikasi yang sangat kompleks dengan menggantikan password static [4].

2.3 Router

Router yang memungkinkan berbagai *LAN* yang terdiri dari switch atau hub untuk saling berkomunikasi Router umumnya dilengkapi firewall juga dapat dikonfigurasi untuk memfilter traffic berdasarkan kriteria yang di tentukan [5]. Pada hal ini contohnya hanya traffic web port 80 yang di izinkan melewati firewall [4].

Dari pengertian di atas dapat disimpulkan bahwa router merupakan perangkat yang sangat di perlukan dalam sebuah jaringan karena sebagai media penghubung komunikasi antar pengguna dengan pengguna lainnya dan juga router terdapat firewall yang sudah ada sendiri tetapi kurang baik jika di gunakan dalam jaringan skala besar dibutuhkan firewall lain bukan dari router tersebut.

2.4 *Pfsense*

Pfsense adalah firewall dan router jaringan open source yang berbasis sistem operasi FreeBSD. Pfsense dilengkapi dengan sebuah custom kernel dan third party software sebagai fungsi tambahan. Pfsense dilengkapi oleh web interface untuk mengkonfigurasikan firewall [6]. Pfsense adalah distribusi firewallnetwork yang bebas, berdasarkan pada sistem operasi FreeBSD dengan kernel khusus dan termasuk paket perangkat lunak bebas pihak ketiga untuk fungsionalitas tambahan. Perangkat lunak pfSense, dengan bantuan sistem paket, mampu menyediakan fungsionalitas yang sama dengan firewall komersial [7].

2.5 Opnsense

OPNsense merupakan suatu software firewall dan routing berbasis *FreeBSD* sifatnya *open source*, yang dimana mudah dipergunakan dan mudah dibangunnya atau di install. OPNsense mencakup sebagian fitur-fitur yang tersedia di firewall komersial yang berbayar dan mahal, atau mungkin lebih lengkap fiturnya pada banyak kasus [8]. Dan juga memberikan fitur yang banyak dari versi komersial atau berbayar dengan manfaat *open source* dan sudah terverifikasi.

Dengan tampilan yang bagus dan tampilan web gui *administrator* memudahkan kita dalam mengoprasikan OPNsense, meskipun orang yang baru belajar tentang routing dan firewall di jaringan local ataupun internet. dan ingat OPNsense adalah *open source* alias GPL GNU. *General Public License* (GPL) merupakan lisensi dari perangkat lunak bebas atau gratis, sedangkan GNU merupakan sistem perangkat lunak atau *software* yang terdiri dari perangkat lunak bebas (*Freeware*). Jadi OPNsense sebuah *software* yang sangat layak digunakan. Fitur-fitur yang disediakan OPNsense cukup lengkap, bahkan ada juga fitur yang hanya ada di perangkat *firewall* berbayar, dan masih banyak lagi fitur-fiturnya.

2.6 Keamanan Jaringan

Network Security merupakan sebuah topic dengana cakupan yang sangat luas dan sangat kompleks. *Network security* berkaitan dengan segala aktifitas yang dilakukan untuk mengamankan network, khususnya untuk melindungi *usability, availability, reliability, intergrity* dan *safety* dari *network* dan data. Target *network security* adalah bagaimana mencegah dan menghentikan berbagai *threats* (potensi serangan) agar tidak memasuki dan menyebar pada *network* kita. *Network security* mencakup komponen *hardware* dan *software* [1]. Pengertian keamanan jaringan komputer adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jarigan komputer. Diperlukannya langkah-langkah untuk pencegahan dan membantu menghentikan penyusup atau pengguna tidak sah untuk mengakses sistem jaringan komputer dan setiap bagiannya [9].

Berdasarkan pengertian di atas dapat di simpulkan bahwa keamanan jaringan merupakan suatu proses dalam melakukan pencegahan dan mengidentifikasi ataupun menghentikan berbagai ancaman supaya tidak masuk dan supaya penyusup tidak bisa masuk ke jaringan komputer dan sistem jaringan serta bagian lainnya [10].

2.7 VMWare

VMWare adalah salah satu *software* mesinvirtualisasi atau biasa yang dikenal dengan *Virtual-Machine, VMWare* dapat menjalankan *software* sistem operasi atau OS didalam sebuah sistem operasi. Contohnya ketika ingin menggunakan dual sistem operasi windows dan linux, jadi di windows dapat menginstall software VMWare dan di VMWare install OS linux [11]. VMware merupakan software virtualisasi yang bisa digunakan untuk membuat *virtual machine*.

Dengan Aplikasi Vmware ini bisa melakukan percobaan dengan menggunakan sistem OS apapun mulai dari windows, mac, linux, *install mikrotik di vmware* dan lain sebagainya. VMware dapat menjalankan banyak sistem operasi atau OS dalam satu PC atau laptop. Keuntungan melakukan percobaan dengan aplikasi Vmware yang lainnya adalah bisa bereksperimen tanpa harus takut kerusakan atau kehilangan pada OS utama [12].

3. Metodologi Penelitian

Metode yang digunakan dalam penelitian ini yaitu metode penelitian tindakan (Action Research) [13].

3.1 Melakukan Diagnosa

Pada tahapan ini penulis mengindentifikasi suatu permasalahan yang terjadi di jaringan PT. Pertamina Asset 2 prabumulih yang dimana di perusahaan PT. Pertamina Asset 2 ini menggunakan dua ISP yaitu Icon+ dan Astinet Telkom yang memiliki bandwidth masing-masing icon+ 40MB dan Astinet Telkom 20MB dan menggunakan firewall dari pfsense. Yang dimana saat ini pfsense belum melakukan pembaharuan sistem yang terakhir kali pembaruan pada tahun 2014. Sehingga ini menyebabkan tidak update dalam keamanan jaringan karena seiring perkembangan jaman dibutuhkannya firewall yang terbaru. Fitur firewall di pfsense sendiri yaitu stateful firewall , networdk address translation, penyaringan jaringan, rute fleksibel dan lain-lain. Tetapi dengan menggunakan pfsense ini tidak adanya peningkatan dalam mengamankan jaringan dikarenakan pfsense peningkatan keamanannya sangat lambat dan tidak ada inovasi terbaru seiring dengan perkembangan jaman, Ini menyebabkan kurangnya mengantisipasi ancaman-ancaman yang dapat merugikan jaringan dan memberikan resiko di jaringan tersebut seperti serangan Dos, penyebaran virus di jaringan.

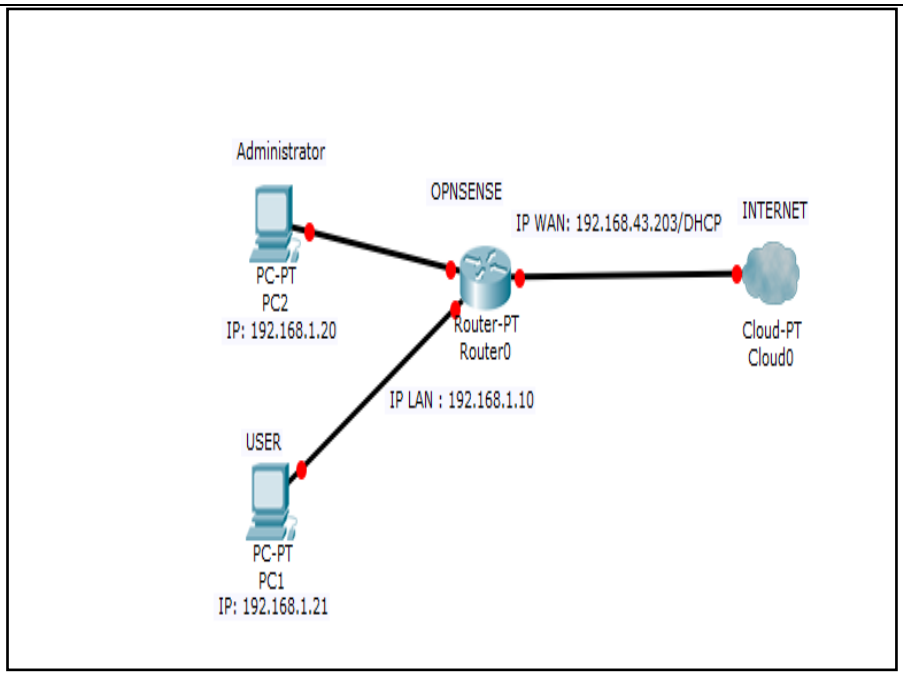
3.2 Membuat Rencana Tindakan

Setelah peneliti melakukan mengidentifikasi masalah yang ditemukan, selanjutnya dalam hal ini peneliti menyusun suatu rencana tindakan untuk menyelesaikan masalah dalam jaringan tersebut. Peneliti membuat rancangan jaringan lab kecil dengan menggunakan vmware workstation supaya memudahkan peneliti merancang tanpa harus menggunakan perangkat keras lain guna merancang tindakan tersebut. Setelah membuat lab kecil di vmware workstation tersebut selanjutnya peneliti mengatur IP address WAN dan LAN router tersebut dalam hal ini IP address WAN menggunakan DHCP dengan begitu ketika router terkoneksi internet maka dia akan mendapatkan ip address otomatis.

Dan pada IP address LAN menggunakan IP address static yang berarti kita sendiri yang memasukan IP address dan mengaturnya tidak otomatis seperti DHCP. Pada LAN juga ditambahkan pengaturan DHCP server yang diamana ketika ada user atau pengguna koneksi melalui LAN di router maka ip address user akan mengikuti aturan yang telah di setting di router LAN dan user tidak perlu setting IP addressnya lagi. Pada rencana tindakan ini peneliti menggunakan 2 buah pengguna yang mana 1 sebagai admin dan 1 sebagai user yang terhubung ke router melalui jaringan LAN. Selanjutnya peneliti melakukan konfigurasi pada firewall di opnsense. Dengan begitu di harapkan dapat meningkatkan keamanan jaringan dari ancaman luar yang dapat membahayakan di jaringan dan memudahkan admin dalam memanajemen karena tampilannya yang modern.

Ini merupakan topologi prototipe untuk peracangan jaringan menggunakan opnsense yang dimana meliputi 1 admin 1 user, opnsense sebagai firewall dan ISP digunakan sebagai internet. Pada perancangan ini menggunakan opnsense,

 ISSN: 2654-5438



Gambar 1. Topologi Prototipe Simulasi Opnsense

4. Hasil dan Pembahasan

4.1 Melakukan Tindakan

Dalam hal ini peneliti melakukan penerapan rencana tindakan tadi yaitu melakukan konfigurasi pada firewall router dengan rules dan aliases. Dengan mensetting firewall maka akses ke router selain ip address admin yang telah di input di router maka akan di tolak. Dan juga opnsense memanajemennya menggunakan website configure yang dimana berbentuk suatu website dan bisa mengakses dengan search engine dengan hanya memasukan ip address router ini sangat membantu admin dalam memanajemen.

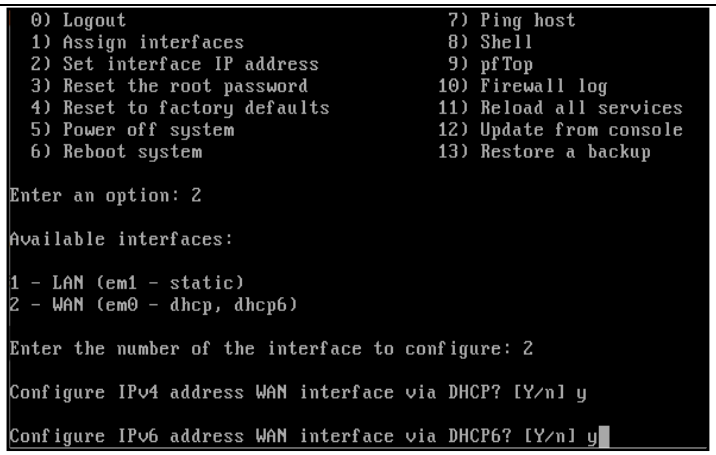
1) Konfigurasi *Ip Address Interface Opnsense*

Pada langkah ini peneliti melakukan konfigurasi ip address opnsense terlebih dahulu. Caranya sebagai berikut:

```
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):
> 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

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? [y/N] y

Enter the start address of the IPv4 client address range: 192.168.1.20
Enter the end address of the IPv4 client address range: 192.168.1.30
  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: 2

Available interfaces:

1 - LAN (em1 - static)
2 - WAN (em0 - dhcp, dhcp6)

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:
> 192.168.1.10
```

Gambar 2. Setting IP Address LAN

 ISSN: 2654-5438

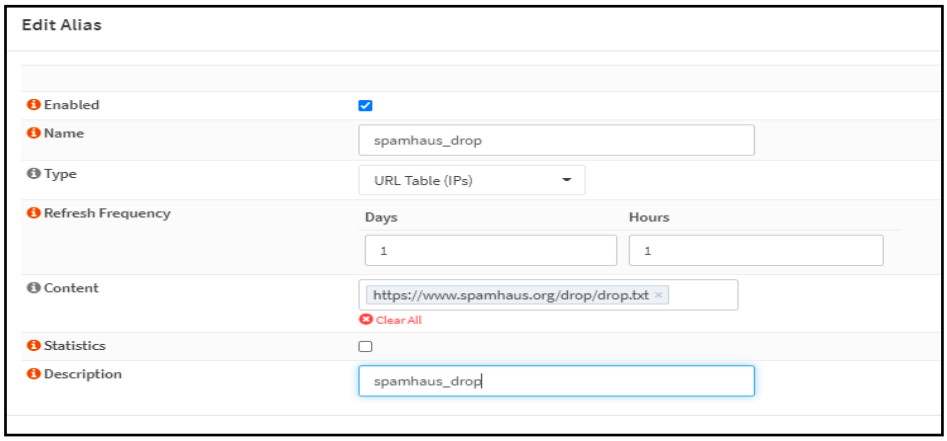


Gambar 3. Setting IP Address WAN

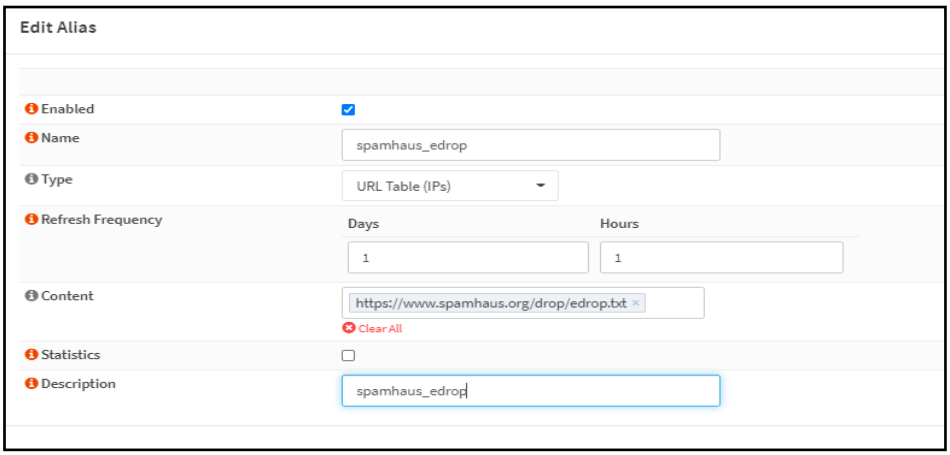
Pada Gambar 3 adalah *setting ip address wan* yang dimana menggunakan *DHCP* dengan begitu otomatis mendapatkan *ip address*.

2) Konfigurasi *Firewall Rules* dan *Aliases*

Pada tahapan ini yaitu mengkonfigurasi firewall di opnsense Dengan cara proteksi dari ip address spammer atau bots menggunakan spamhaus list drop dan edrop. Ini digunakan oleh firewall untuk menyaring lalu lintas yang berbahaya dari list IP address di drop dan edrop.

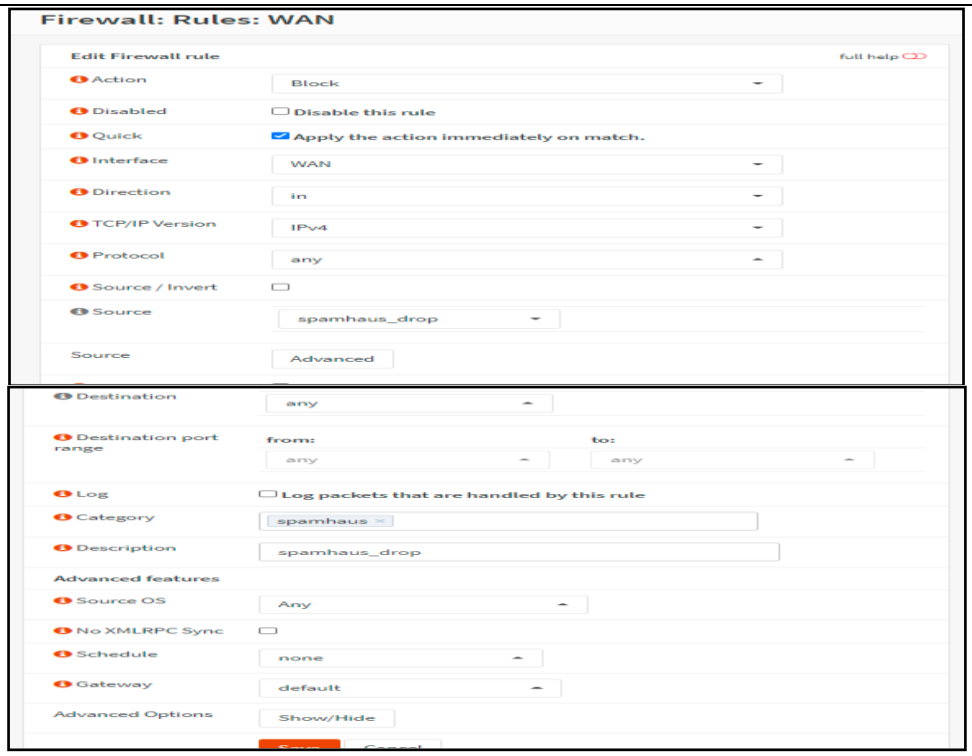


Gambar 4. *Spamhaus drop aliases*

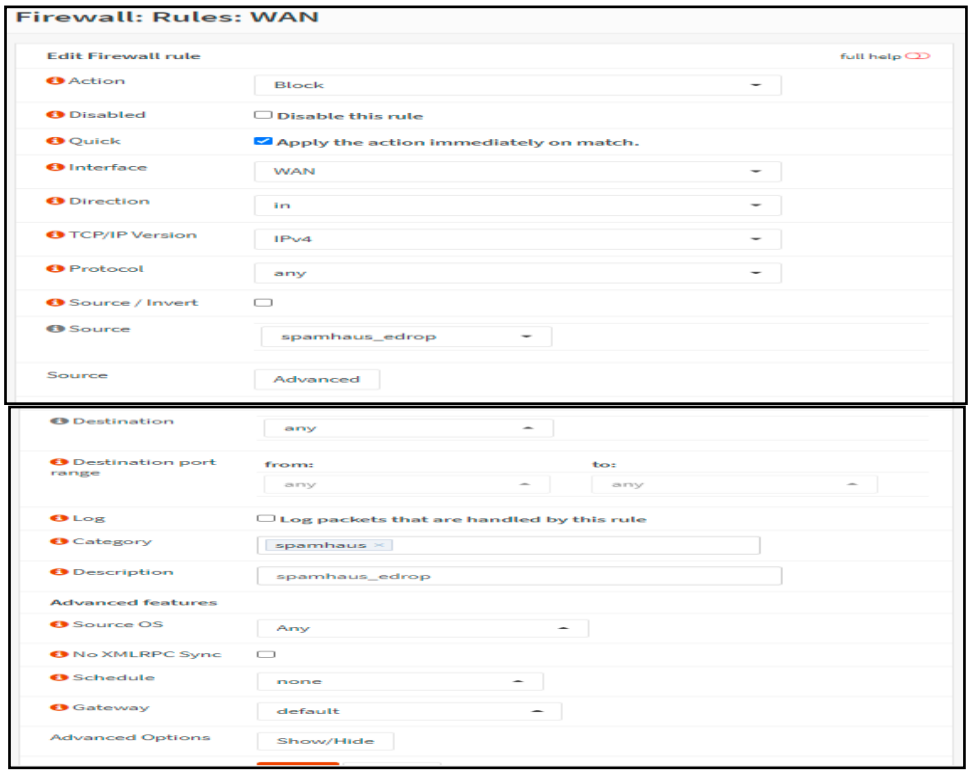


Gambar 5. *Spamhaus edrop aliases*

 ISSN: 2654-5438



Gambar 6. *Rules spamhaus drop*

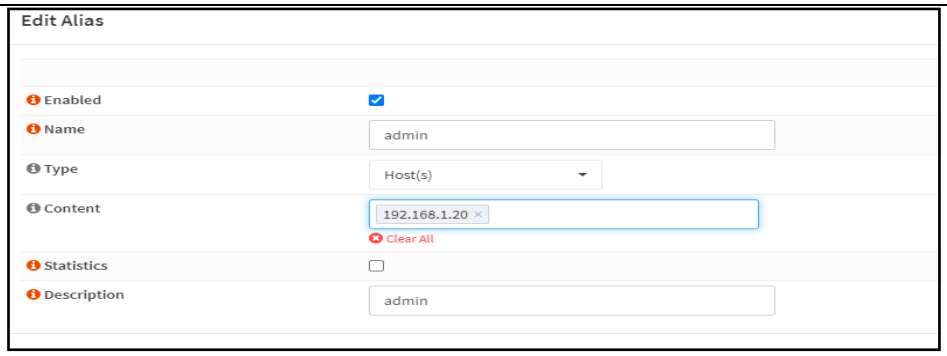


Gambar 7. *Rules spamhaus edrop*

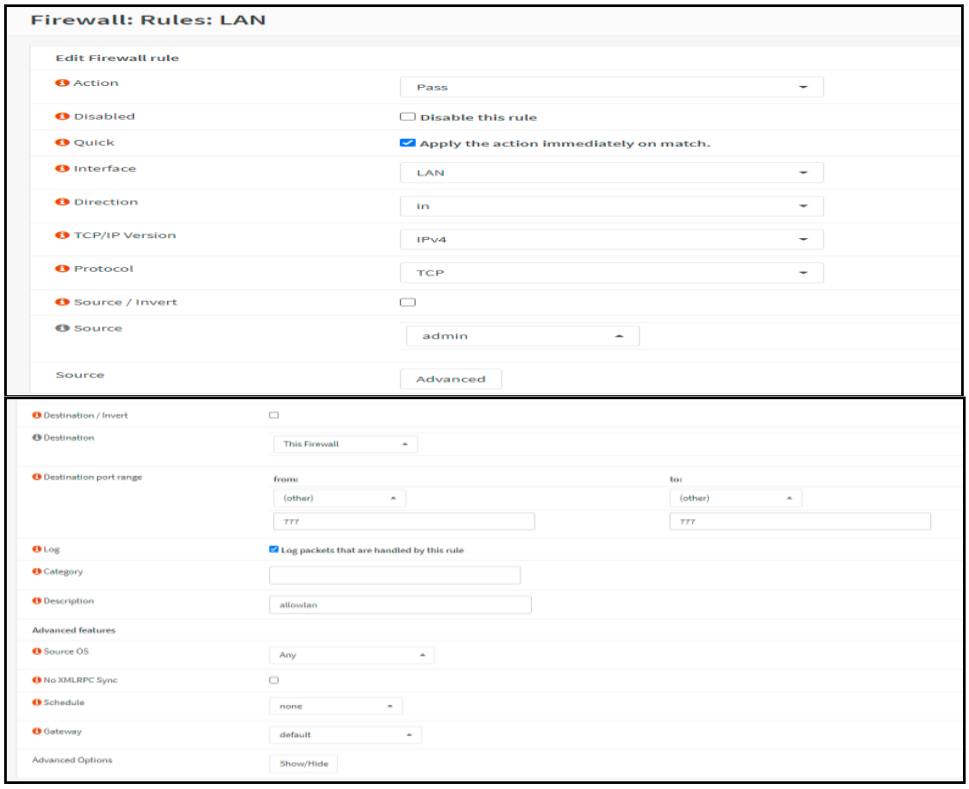
3) Konfigurasi firewall rules dan aliases akses ke router

Pada konfigurasi ini yakni mengatur firewall rules dan aliases pada opnsense hanya IP address admin bisa akses ke web router. Konfigurasinya sebagai berikut:

 ISSN: 2654-5438



Gambar 8. *Setting aliases admin*



Gambar 9. *Setting rules admin*

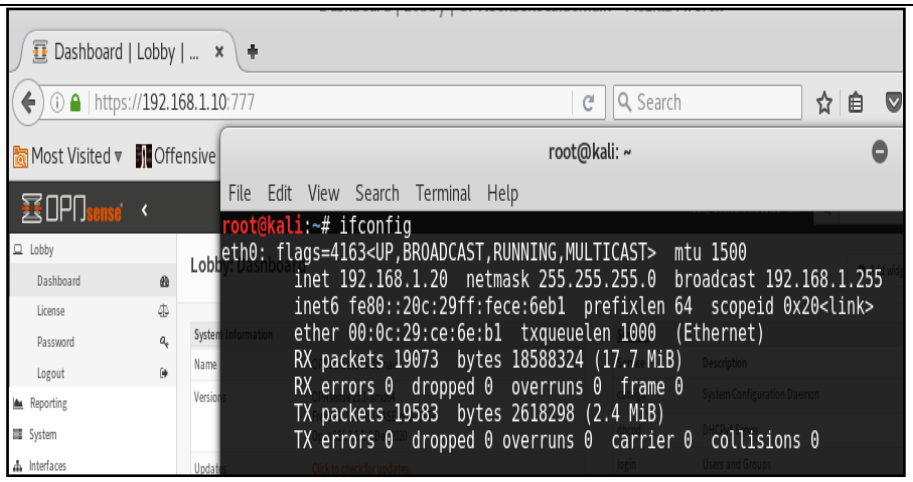
4.2 Melakukan Evaluasi

Hasil dari perancangan firewall router menggunakan Opnsense untuk meningkatkan keamanan jaringan di PT. Pertamina Asset 2 Prabumulih yaitu:

1) Hasil dari konfigurasi firewall menggunakan spamhaus drop dan edrop dapat mengantisipasi ancaman dari luar ke jaringan yang menggunakan IP address netblock dibajak atau disewa oleh spammer untuk operasi kejahatan cyber seperti penyebaran virus, pengunduh Trojan, serangan dos. Daftat list ip address drop digunakan untuk menyaring lalu lintas yang berbahaya dari netblock ini.

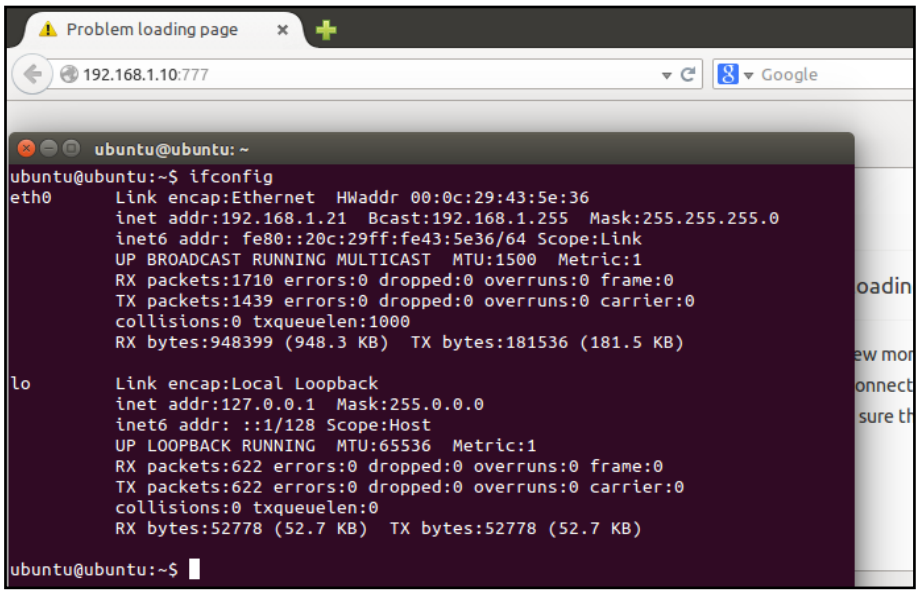
2) Hasil konfigurasi hanya IP address admin yang bisa akses ke router. Berikut ini merupakan contoh hasil dari konfigurasi hanya IP address admin yang bisa akses ke router. Dengan begitu router lebih aman dan tidak ada penyusup yang bisa masuk ke router.

 ISSN: 2654-5438



Gambar 10. Hasil konfigurasi *ip address admin*

Ini merupakan hasil dari user akses ke website router dan tidak bisa mengaksesnya. Dengan tidak bisa akses ke router dengan ip address user lain atau selain admin maka router akan aman dari penyusup yang ingin masuk ke router.



Gambar 11. Hasil konfigurasi *ip address client*

5. Kesimpulan

Dari hasil penelitian yang telah penulis lakukan, dengan begitu kesimpulan dari penulis yaitu:

1. Dengan menggunakan Opnsense ini keamanan jaringan maka akan selalu update karena seiring perkembangan jaman opnsense sendiri akan ada pembaruan atau inovasi terbaru untuk meningkatkan keamanan jaringan tampilannya juga lebih modern ada tools navigasi pencarian. Sudah berkerjasama dengan HardenedBSD sehingga dapat dipastikan firewall ini terbuka dan terarah tujuannya.
2. Dengan memblokir akses ke website router yaitu website konfigurasi router, user maupun attacker tidak dapat mengaksesnya karena telah di atur ip address dari admin saja yang bisa mengaksesnya sehingga keamanan jaringan tidak bisa diretas.

Referensi

[1] Sofana, Iwan, *Jaringan Komputer Berbasis Mikrotik*. Bandung: Informatika Bandung, 2017.
[2] Harun S, Aqis M, ”Rancang Bangun Arsitektur Jaringan Komputer Teknologi Metropolitan Area Network (MAN) Dengan Menggunakan Metode Network Development Life Cycle (NDLC),” . *Jurnal J-Ensitec*, vol. 4, no. 1,pp. 142-146, 2017.
[3] D. Irawan and Fatoni, “Optimasi Network Berbasis Multi VLAN (Virtual Local Area Network*),” Jurnal Informatika*, vol. 7, no. 2, pp. 37-43, 2019.
[4] Purbo, Onno W, *internet – TCP/IP: Konsep & Implementasi*. Yogyakarta: ANDI, 2018.
[5] MADCOMS, *Manajemen Sistem Jaringan Komputer dengan Mikrotik RouterOS*. Yogyakarta: ANDI, 2016.
[6] Ahmad T, Rendy M, Ratna M, “Analisis Throughput dan High Availability Firewall sebagai Virtualized Network Function pada VMware ESXI,” *SENIATI*, vol. 1, no. 1, pp. 149-154, 2019.
[7] Molavi A, Nur R, “Implementasi Sistem Keamanan Web Server Menggunakan Pfsens,” *Jusikom : Jurnal Sistem Komputer Musirawas*, vol. 5, no. 1, pp. 13-23, 2020.
[8] Stephani, Elsa, Fitri Nova, Ervan Asri,” Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server,” *Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 1, no. 2, pp. 67-74, 2020.
[9] Supendar, H, "Penerapan Linux Zenytal Sebagai Filtering dan Bandwidth Management Pada Jaringan PT. Anta Citra Arges," *Jurnal Teknik Komputer Amik BSI*, vol. 2, no. 1, pp. 22-30, 2016.
[10] Munawar,Zen dan Novianti Indah P, “Keamanan Jaringan Komputer Pada Era Big Data,“ *Jurnal Sistem Informasi – J-SIKA*, vol. 02, no. 01, pp. 14-20, 2020.
[11] Pati, R.Aditya, Mia R, Mochammad F, “Pembuatan Sistem Monitoring untuk Pendeteksi Gangguan Komunikasi pada Jaringan Menggunakan Cacti,” *e-Proceeding of Applied Science*, vol. 4, no. 3, pp. 2076-2085, 2018.
[12] Hermawan,Rudi, “Analisa Cara Kerja dan Dampak dari Serangan Virus Spyware,” *Jurnal String*, vol. 1, no. 1, pp. 10-18, 2016.
[13] R. N. Dasmen and Rasmila, “Implementasi Raspberry Pi 3 pada Sistem Pengontrol Lampu berbasis Raspbian Jessie,” *JEPIN (Jurnal Edukasi dan Penelit. Inform.*, vol. 5, no. 1, pp. 46–53, 2019.