JURNAL ILMIAH KOMPUTER GRAFIS, Vol.16, No.1, JULI 2023, pp. 19 - 32

p-ISSN : 1979-0414(print), e-ISSN : 2621-6256 (online)

DOI : https://doi.org/10.51903/pixel.v16i1.1003

Analisis firewall sebagai bandwidth limiter dan network security menggunakan pfsense

Agung Wirjawan[1], Hilman Iskandar[2], Rahmad Hidayat[3], Dwiyanto[4], Ike Yuni Wulandari[5], Yudi Herdiana[6]

[1,2,3,4]Sekolah Tinggi Teknologi Mandala
Jalan Soekarno Hatta 597 Bandung, 022-7301738, e-mail: rhidayat4000@gmail.com
[5]Universitas Nurtanio
Jalan Pajajaran 219 Bandung, 022-6034484, e-mail: ikeyunipp@gmail.com
[6]Universitas Bale Bandung
Jalan RAA Wiranata Kusuma 7 Baleendah Kabupaten Bandung, 022-5940443, e-mail: fti@unibba.ac.id

ARTICLE INFO

Article history:

Received Februari 2023
Received in revised form April 2023
Accepted Mei 2023
Available online Juli 2023

ABSTRACT

Internet connections that are not always stable and data security is not maintained from various threats from outside attacks in the form of hackers, crackers, viruses, and so on are the main problems for every client. Using the pfSense analysis method, this study aims to address the above bandwidth management and network security issues. The pfSense analysis that the researchers carried out included an analysis of total bandwidth usage, data security, and information for each client on the P3DW Internet network (Center for Regional Revenue Management) Bandung III Soekarno-Hatta City. The results of the analysis concluded that pfSense can work as a firewall that functions as a bandwidth limiter and network security. The level of client satisfaction increases with the infrastructure designs being tested. With a web GUI that makes it easy for users to configure, the basic system used is FreeBSD which is open-source, making pfSense able to be an alternative choice for building a firewall that is reliable, flexible, and economical.

Keywords: Bandwidth Management, Firewall, pfSense, Network Security

Received Februari, 2021; Revised April, 2023; Accepted Juli, 2023

JURNAL ILMIAH KOMPUTER GRAFIS, Vol.16, No.1, JULI 2023, pp. 19 - 32
p-ISSN : 1979-0414(print), e-ISSN : 2621-6256 (online)
DOI : https://doi.org/10.51903/pixel.v16i1.1003

1. Pendahuluan

Seiring berkembangnya teknologi informasi saat ini, dan juga kebutuhan akan akses internet menjadikan internet suatu hal yang sangat penting, yang mungkin dapat dikategorikan sebagai kebutuhan pokok dimana hampir setiap orang, baik itu kalangan anak- anak, dewasa atau bahkan orang tua. Dengan berbagai maksud dan tujuannya pula seperti halnya untuk mencari informasi, membantu pekerjaan sehari-hari, untuk berkomunikasi satu sama lain atau mungkin hanya sebatas gaya hidup. Kaitannya dengan internet, baik dari segi penyediaan maupun pemakaian, manajemen *bandwidth* menjadi hal yang harus diperhatikan dan dipertimbangkan. Dalam hal ini lebih spesifik pada pembatasan *bandwidth* atau *bandwidth limiter*. Selain daripada itu ada hal lain yakni keamanan jaringan atau *network security* yang memiliki peranan penting, namun sering tidak diperhatikan oleh *client*. Kedua hal tersebut akan berdampak terhadap kelancaran dan keamanan pada jaringan Internet. *Bandwidth limiter* dan *network security* yang dilakukan secara keseluruhan ataupun pada setiap *client* adalah salah satu bagian yang penting untuk dilakukan bagi setiap Industri, Perusahaan atau Instansi Pemerintahan, baik itu skala besar seperti halnya Perusahaan Jasa Penyedia Internet atau *Internet Service Provider* maupun skala kecil seperti Perkantoran, Kampus dan Sekolah agar tewujud sebuah koneksi internet yang stabil, efektif, efisien dan optimal. Sering kita alami pada saat bekerja ataupun kuliah, pada saat sedang menggunakan internet terkadang sering terjadi gangguan, seperti halnya kecepatan koneksi menjadi lambat atau bahkan dapat sampai terputus. Selain daripada itu, keamanan data atau informasi juga terkadang dapat terancam oleh gangguan virus, *hacker*, *cracker*, atau kategori peretas lainnya yang mengintai untuk mencari celah agar dapat mengambil, memanfaatkan atau bahkan merusak data maupun informasi yang dimiliki oleh *client*. Demi terwujudnya Internet yang stabil, efektif, efisien dan optimal dan juga kemanan data atau informasi yang dimiliki oleh setiap *client* diperlukan sebuah alat ataupun sebuah sistem yang dapat bekerja sebagai *bandwidth limiter* dan juga sebagai *network security*. Sehingga untuk mengatasi permasalahan diatas, perlu dilakukan analisis pada ”*Firewall* sebagai *bandwidth limiter* dan *network security* menggunakan pfSense”. Hasil dari analisis ini diharapkan dapat memberikan sebuah informasi tentang bagaimana cara kerja pfSense sebagai objek utama penelitan yang dijadikan sebagai *bandwidth limiter* dan *network security*. Masalah yang dapat di ambil dari latar belakang di atas adalah Bagaimana cara kerja pfSense yang dibangun sebagai sebuah *firewall* yang berfungsi sebagai *bandwidth limiter*, dan *network security*; dan bagaimana cara melakukan konfigurasi *firewall* sebagai *bandwidth limiter* dan *network security* dengan menggunakan pfSense untuk memaksimalkan penggunaan akses internet di setiap *client* serta memberikan keamanan jaringan pada setiap *client*. Tujuan yang ingin dicapai dari penelitian ini adalah 1) Mewujudkan koneksi Internet yang lebih stabil, efektif, dan efisien; 2) Semua *client* dapat menggunakan Internet dengan lancar dan stabil walaupun *bandwidth* dalam kondisi padat (*full traffic)*; 3) Semua *client* mendapatkan *bandwidth* sesuai dengan kebutuhan; dan 4) Keamanan data/informasi setiap *client* menjadi lebih terjaga.

Pembatasan penggunaan *bandwidth* pada setiap *client* atau disebut dengan istilah *bandwidth limiter* secara langsung akan berdampak terhadap kestabilan dan kecepatan koneksi, karena besaran *bandwidth* selalu berbanding lurus dengan kualitas koneksi, semakin besar *bandwidth* maka semakin bagus pula kualitas koneksi, begitupula sebaliknya. Akan tetapi besaran *bandwidth* yang dapat dikatakan sudah besar atau cukup, adakalanya tetap tidak dapat menciptakan sebuah koneksi yang

Received Februari, 2021; Revised April, 2023; Accepted Juli, 2023

optimal dikarenakan manajemen *bandwidth* yang kurang maksimal. Keamanan data dan informasi setiap *client* terkadang menjadi dikesampingan oleh setiap *client*, hal ini akibat faktor-faktor seperti halnya karena faktor ketidaktahuan dan ketidakmampuan setiap *Client* atau bahkan karena sifat acuh dari setiap *client* itu sendiri [1].

Bila kita berbicara tentang keamanan di dalam jaringan komputer, maka kita perlu mengetahui aspek-aspek apa saja yang berkaitan dengan keamanan di dalam jaringan komputer. Terdapat tiga aspek utama pada keamanan jaringan komputer yaitu 1) Aspek sistem, yang mencakup secara keseluruhan, baik itu *hardware* maupun *software*, kemudian 2) Aspek kebijakan, aspek yang memegang peranan penting sebelum proses implementasi sebuah sistem diberlakukan, dan yang terakhir 3) Aspek Pengguna, mecakup semua pengguna yang terlibat di dalam sistem pada jaringan komputer [2] [3].

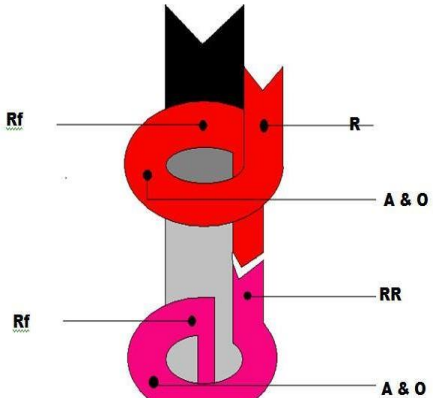
Berdasarkan rumusan masalah dan kerangka pemikiran yang telah diuraikan sebelumnya, maka hipotesis yang akan diuji dalam penelitian ini adalah 1) Pembatasan penggunaan *bandwidth* di setiap *client* dapat mengoptimalkan koneksi internet pada P3DW Kota Bandung III Soekarno-Hatta menjadi stabil, efektif, efisien dan optimal ; dan 2) Keamanan data dan informasi di P3DW Kota Bandung III Soekarno-Hatta menjadi lebih terjaga.

Pada penelitian yang dilakukan sebelumnya oleh [4] di Universitas Surakarta yang berjudul "Penerapan router PFSense berbasis *Free BSD* di Warnet EMAX Sragen" disimpulkan bahwa penerapan *router* pfsense berbasis free-BSD pada warnet emax Sragen memliki kelebihan gratis; dapat menghubungkan beberapa koneksi WAN dan *load balancing*; stabil; dan fitur yang banyak. Sedangkan apabila dilihat dari segi kekurangan yaitu diperlukan kapasitas RAM (Random Access Memory) untuk dapat menerapkan router pfsense tersebut. Lalu pada [5] dilakukan pendeteksian gangguan keamanan menggunakan aplikasi snort pada pfsense. Untuk metode penelitian digunakan PPDIOO sebagai metode pengembangan dalam implementasi. Hasilnya sistem snort mampu mengetahui sebagai alert dan menyimpannya di dalam log seperti serangan ping of death dan slowloris. Berdasarkan log snort pfsense mampu melakukan pemblokiran otomatis dalam durasi tertentu. Pfsense juga digunakan sebagai firewall dan router. Pfsense memiliki tampilan sederhana dengan web gui administrator memudahkan pengoperasiannya [6]. Pfsesnse bersama suricata digunakan untuk mengidentifikasi sering munculnya captcha pengganggu pada jaringan [7].

2. Metode Penelitian

Pada penelitian ini dipilih metode *Action Research* yang tergolong dalam metode analisis secara kualitatif dimana pendekatan analisis dilakukan dengan cara menginterpretasi tabel-tabel, grafik-grafik, atau angka-angka yang ada kemudian dilakukan uraian dan penafsiran, yang berbeda dengan metode analisis secara kuantitatif yang menggunakan alat statistik sebagai bentuk pendekatan analisis. Pada penelitian ini, kami mendeskripsikan, mengaplikasikan dan menjelaskan situasi atau kondisi pada waktu yang bersamaan dengan melakukan perubahan untuk tujuan melakukan perubahan atau perbaikan dengan menghubungkan antara teori dengan praktek.

p-ISSN : 1979-0414 e-ISSN : 2621-6256



Gambar 1. Desain penelitian tindakan

Keterangan Gambar :
R = rencana tindakan
A&O = aplikasi tindakan dan observasi
Rf = refleksi
RR = revisi rencana.

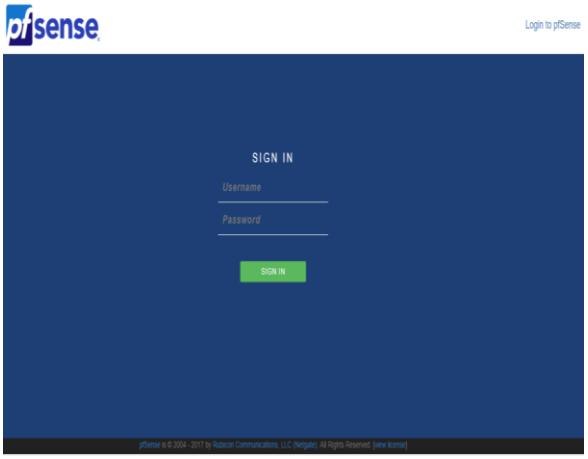
Sehubungan dengan perlunya optimalisasi pada jaringan internet, maka populasi penelitian ini merujuk pada Kantor P3DW Kota Bandung III Soekarno-Hatta, dimana sering terjadi pemakaian internet yang terkadang menjadi lambat karena beban internet yang tinggi, sehingga mengakibatkan *bandwidth* menjadi *full traffic* yang berdampak pada efektifitas dan efisiensi kinerja para pegawai kantor P3DW Wilayah Kota, sehingga permasalah ini harus diteliti lebih dalam agar kejadian tersebut dapat diminimalisir. Peneliti mendalami tentang bagaiamana cara kerja *firewall* sebagai sebuah *bandwidth limiter* dan juga sebagai *network security* yang dibangun menggunakan sistem operasi pfSense.

Pengambilan sampel didapat melalui pengamatan langsung pada kantor PPPD Wilayah Kota Bandung III Soekarno-Hatta pada saat aktifitas kerja selama jam kerja berlangsung, peneliti mencoba menggali informasi dari pegawai PPPD Wilayah Kota Bandung III Soekarno-Hatta sehingga data yang didapat menjadi lebih valid dan informasi menjadi lebih relevan. Data yang didapat dari penjelasan pegawai dan pengamatan langsung, sehingga hasil ini selanjutkan akan diteliti lebih dalam mengenai apa penyebab yang berdampak pada pemakaian internet yang sering *full traffic* yang menyebabkan menjadi kurangnya efektifitas dan efisiensi kinerja para pegawai.

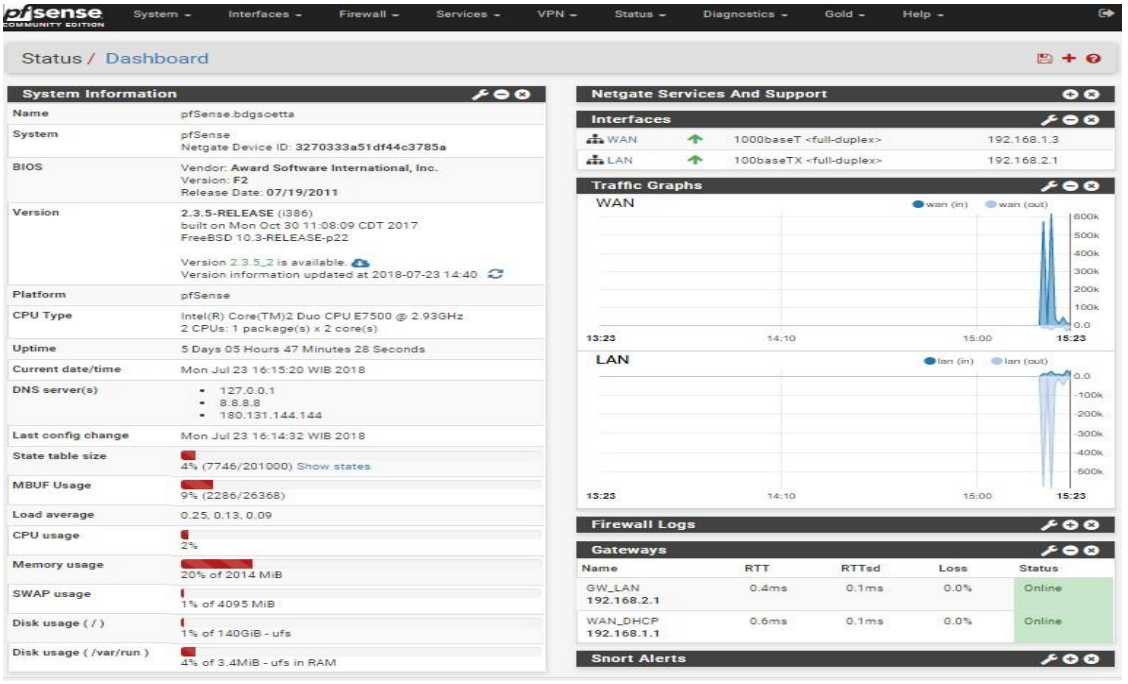
Pengumpulan data dalam penelitian ini berupa pengumpulan informasi dan pengamatan langsung di lapangan sehingga data dapat diperoleh dari hasil tersebut. Adapun hardware dan software yang digunakan sebagai alat penelitian sebagai berupa Personal Computer/Laptop, Switch/Hub/Access Point, Sistem Operasi Windows, Sistem Operasi pfSense, Browser Mozilla Firefox / Google Chrome.

Pada tampilan utama server, pfSense menerapkan CLI (*Command Line Interface*) guna meminimalisir penggunaan *resource hardware* seperti *CPU Load* dan *RAM* yang digunakan.

JURNAL ILMIAH KOMPUTER GRAFIS p-ISSN : 1979-0414 e-ISSN : 2621-6256.



Gambar 2. Menu login pfSense



Gambar 3. Dashboard pfSense

Jenis data yang digunakan dalam penelitian ini adalah data internal yaitu data yang diperoleh langsung dari pihak instansi pemerintahan, sehingga informasi tidak melalui pihak perantara.

a) Sumber Data Primer

Data yang diperoleh melalui wawancara langsung dengan pegawai kantor P3DW Wilayah Kota Bandung III Soekarno-Hatta.

b) Sumber Data Sekunder

Data yang dikumpulkan dari pihak lain sebagai sarana untuk kepentingan mereka sendiri, data yang sudah ada atau tersedia yang kemudian diolah kembali untuk tujuan tertentu,data ini berupa literature, artikel, tulisan ilmiah yang dianggap relevan dengan topik yang sedang diteliti [8].

Pengumpulan data dilakukan dengan studi pustaka, penelitian lapangan berupa observasi, wawancara, dokumentasi, internet, kuesioner. Metode Kuesioner yang digunakan menggunakan dua metode perhitungan, yaitu skala *Guttman* dan skala *Likert*. Pada skala *Guttman* digunakan apabila ingin mendapatkan jawaban yang jelas terhadap suatu permasalahan yang ditanyakan. Variabel yang akan diukur dijabarkan menjadi indikator variabel. Kemudian indikator tersebut dijadikan sebagai titik tolak untuk menyusun item-item instrumen yang dapat berupa pertanyaan atau pernyataan. Skala *Likert* merupakan metode pengukuran yang digunakan untuk mengukur sikap, pendapat dan persepsi seseorang atau kelompok orang tentang fenomena sosial. Penentuan Skor jawaban merupakan nilai jawaban yang akan diberikan oleh responden. Hal pertama yang dilakukan adalah menentukan skor dari tiap jawaban yang akan diberikan. Contohnya, sikap yang akan kita pakai yaitu "setuju". Selanjutnya kita menentukan banyaknyajawaban pada tiap pertanyaan yang akan kita berikan. Misalnya 5 skala, berarti sangat tidak setuju, kurang setuju, cukup. Jika pertanyaan yang diberikan bersifat susah untuk diberikan jawaban, otomatis responden cenderung statik oleh karena itu kita dapat memberikan pilihan jawaban yang banyak, misal 7 atau 9 jawaban dari tiap pertanyaan. Hal ini bertujuan agar responden dapat memberikan penilaian sesuai dengan kriteria mereka berdasarkan pilihan yang ada.

Dalam penelitian ini, peneliti menggunakan pfSense sebagai server*firewall* yang digunakan sebagai bandwidth managemen dan network security. Selain itu, peneliti membuat sebuah simulasi berupa virtualisasi dari server tersebut sehingga proses penelitian ini dapat berjalan lebih baik.

Tabel 1. Definisi variabel

Variabel	Definisi variabel
Firewall	*Firewall* adalah sebuah aturan yang dapat diterapkan pada komponen *hardware*, *software* maupun sistem itu sendiri yang bertujuan untuk melindungi, melindungi dalam hal ini dapat dilakukan dengan teknik filterisasi, membatasi, juga dengan menolak sebuah permintaan koneksi
Network security	Keamanan komputer adalah tindakan pencegahan dari serangan pengguna komputer atau pengakses jaringan yang tidak bertanggung jawab
Bandwidth management	*Bandwidth management (Traffic Control/Shaping)* adalah istilah yang ditujukan pada suatu subsistem antrian packet dalam

	suatu jaringan. Secara singkat *traffic control/shaping* adalah suatu usaha mengontrol *traffic* jaringan jaringan sehingga sehingga *bandwidth* lebih optimal dan performa network lebih terjamin
Bandwidth limiter	*Bandwidth limiter* adalah *software* ataupun tools yang dapat kita gunakan untuk membatasi *bandwidth* koneksi untuk *client* pada suatu LAN atau WAN, dimaksudkan supaya setiap user memperoleh *bandwidth* yang sama dengan aplikasi *bandwidth limiter* ini

3. Hasil dan Pembahasan

3.1. Infrastruktur dan sistem awal

Diperlukan penelitian awal berupa pengumpulan data primer dan data sekunder berdasarkan rumusan masalah, identifikasi masalah dan metode penelitian yang telah diuraikan sebelumnya.

a) Data primer

Pengumpulan data primer dilakukan dengan metode kuesioner yang didistribusikan kepada seluruh *client* berjumlah 53 orang. Seluruhnya merupakan *client* yang memanfaatkan jaringan Internet di kantor P3DW Kota Bandung III Soekarno-Hatta, meliputi 29 Orang Aparatur Sipil Negara (ASN), 14 Orang Tenaga Kontrak Dinas, dan 10 Orang Mahasiswa / Siswa-Siswi Prakerin.

Pelaksanaan pengumpulan data dilakukan pada saat jam kerja (07.30 – 16.00 WIB). Tujuan dilakukannya pengumpulan data adalah untuk memudahkan saat melakukan analisis, sehingga dalam pelaksanaan penelitian dapat menjadi lebih efektif. Pengumpulan data pada penelitian awal menggunakan metode pendekatan skala *guttman*. Pertanyaan yang diajukan berkaitan dengan kecepatan, kestabilan dan keamanan jaringan Internet, dengan maksud agar peneliti dapat lebih mendalami pada permasalah tersebut pada saat penelitian, sesuai dengan rumusan masalah. Tabel 2 memperlihatkan rekapitulasi kuesioner jaringan Internet Kantor P3DW Kota Bandung III Soekarno-Hatta.

b) Data sekunder

Selain data primer, diperlukan data sekunder sebagai data penunjang dalam penelitian. Data sekunder yang didapatkan adalah berupa informasi terkait infrastruktur jaringan pada kantor P3DW Kota Bandung III Soekarno-Hatta. Informasi ini mencakup *hardware* yang digunakan seperti halnya jumlah PC yang digunakan, *router*, *wifi*, dan *switch* yang digunakan dan sistem awal yang sedang berjalan.

Sebagai data penunjang atau data sekunder, penggunaan *speedtest* dapat dijadikan sebagai alat ukur untuk menguji kecepatan *bandwidth* pada jaringan yang digunakan. Pada *speedtest* terdapat 3

indikator yang dilakukan pengujian. Pertama adalah *Latency* atau dikenal dengan *ping*, adalah seberapa cepat transfer data (pergi dan kembali) antara komputer *client* dan server yang bersangkutan, biasanya dihitung dalam satuan *milisecond* atau milidetik. Berikutnya adalah *Download Speed* yang dihitung dengan satuan *megabits per second* (Mbps), yaitu seberapa cepat data ditarik dari server yang bersangkutan.. Dan yang ketiga adalah *Download Speed* yang dihitung dalam satuan *megabits per second* (Mbps), *yaitu s*eberapa cepat data dikirim ke server yang bersangkutan. Ketiga indikator diatas dapat mewakili *perfomance* Internet pada suatu jaringan, karena dalam melakukan aktifitas yang berkaitan dengan Internet ketiga indikator tersebut sangat berpengaruh terhadap kelancaran dan saling berhubungan.

Gambar 4. Hasil *speedtest* awal

Tabel 2 Rekapitulasi Kuesioner Jaringan Intenet

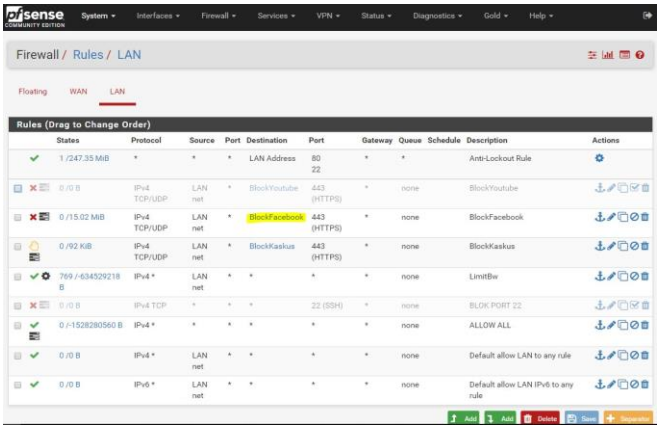
REKAPITULASI KUESIONER JARINGAN INTERNET P3DW KOTA BANDUNG III SOEKARNO-HATTA			
PERTANYAAN	JUMLAH RESPONDEN	SKOR	
		YA	TIDAK
Koneksi Internet menjadi melambat atau tidak stabil bilamana ada client atau pegawai lain yang melakukan downloading file besar.	53 Responden	48	5
Koneksi Internet menjadi melambat atau tidak stabil bilamana banyak client atau pegawai lain yang melakukan streaming film/youtube.	53 Responden	42	11
Koneksi Internet menjadi melambat atau tidak stabil pada saat jam sibuk (10.00 - 15.00)	53 Responden	48	5
Secara sengaja atau tidak dengan sengaja, browser komputer anda pernah membuka situs/website yang bermuatan konten negatif.	53 Responden	34	19
Komputer anda pernah terkena virus atau serangan lainnya (hacker,cracker,dll) ?	53 Responden	43	10
Bila salah satu atau lebih jawaban anda pada pertanyaan sebelumnya adalah "YA", Pekerjaan atau kinerja anda menjadi terganggu / kurang efektif ?	53 Responden	50	3
JUMLAH		265	53
RATA-RATA		44,2	8,8

3.2. Web filtering

Pembatasan akses terhadap situs-situs website yang dianggap dapat membuat penggunaan *bandwidth* menjadi tinggi seperti situs negatif, situs *online streaming*, situs penyedia aplikasi bajakan, situs penyedia film bajakan dan sebagainya, merupakan salah satu faktor yang apabila banyak *client* yang secara bersamaan banyak yang melakukan akses ke situs tersebut maka secara otomatis pemakaian *bandwidth* akan meningkat, bahkan dapat sampai pada titik maksimal bilamana setiap *client* melakukan akses yang tidak wajar. Perilaku tersebut secara tidak langsung akan merugikan *client* lain yang pada saat yang bersamaan memerlukan akses Internet untuk aplikasi penunjang kerjaan namun menjadi terhambat dikarenakan jumlah pemakaian *bandwidth* yang sudah maksimal. Dan juga selain dari itu, bilamana situs-situs yang bermuatan konten negatif dibiarkan begitu saja, tentu akan berdampak pada hal-hal lain pula, terutama dari segi keamanan data dan informasi, karena virus dan peretas banyak memanfaatkan konten-konten negatif sebagi salah satu celah agar dapat meretas data setiap *client*.

Meskipun saat ini Pemerintah sudah banyak menutup akses terhadap situs-situs yang bermuatan konten negatif, namun masih terdapat situs-situs yang masih saja dapat lolos, maka perlu dilakukan *web filtering* pada tingkat bawah atau tingkat pemakai agar dapat tercipta koneksi internet menjadi lebih stabil, efektif, efisien dan optimal. Untuk melakukan filterisasi pada situs atau *website* yang akan dilakukan pembatasan akses, langkah pertama yang harus dilakukan adalah mencari tahu *IP address* situs atau *website* tersebut. Setiap situs atau *website* yang masih berskala kecil seperti halnya *website* sekolah, kampus, perusaahaan dsb, umumnya memiliki *single IP*. Berbeda halnya dengan *website* yang sudah berskala besar, seperti halnya *facebook*, *youtube*, *twitter* dsb, mereka memiliki IP yang banyak, karena memang server yang mereka miliki banyak dan tersebar di beberapa tempat. Sehingga untuk melakukan pembatasan akses pada *website* yang berskala besar memiliki kesulitan tersendiri karena agar dapat melakukan pembatasan secara keseluruhan maka kita harus secara keseluruhan pula mengumpulkan informasi *IP address* yang digunakan.

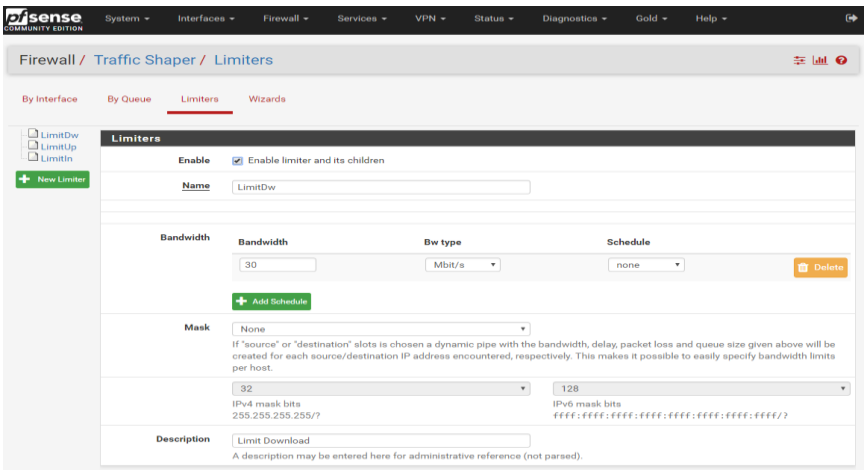
p-ISSN : 1979-0414 e-ISSN : 2621-6256



Gambar 5. Tampilan *Rules*

3.3. Pembatasan kecepatan download dan upload

Setiap *client* pasti menginginkan untuk mendapatkan kecepatan *download* yang tinggi, terutama bilamana *downloading file* dengan berukuran besar, namun hal ini perlu menjadi pertimbangan, jika semua *client* diberikan kecepatan *download* yang tinggi maka secara otomatis akan menyebabkan pemakaian *bandwidth* menjadi penuh. Sehingga bila kondisi *bandwidth* terus menerus dalam kondisi penuh maka perangkat yang berkerja sebagai *modem* atau *router* akan bekerja lebih keras, dan juga kestabilan koneksi internet menjadi terganggu. Satu hal lain mengenai *download* yang terkadang menjadi kurang tepat dalam memaknainya, banyak orang berasumsi bahwa *download* adalah pekerjaan mengambil data atau *file* dari Internet. Terdapat satu hal yang dilupakan, bahwasannya setiap kita mengakses suatu situs atau *website*, secara tidak langsung perangkat yang kita gunakan akan melakukan *downloading*, meskipun tidak nampak *file* atau data yang tertarik atau tersimpan kedalam perangkat yang digunakan.



Gambar 6. Konfigurasi Pembatas *Bandwidth* pada *Traffic Shaper*

Namun pada kenyataanya setiap kita melakukan akses kepada suatu situs atau *website*, secara otomatis perangkat melakukan *downloading* terhadap seluruh konten yang terdapat pada situs atau *website* yang dibuka. Setiap *file* atau data dari konten-konten tersebut tidak disimpan secara langsung, melainkan disimpan dalam sebuah bentuk atau tempat penyimpanan sementara pada *browser* yang digunakan atau dikenal dengan istilah *cache.*

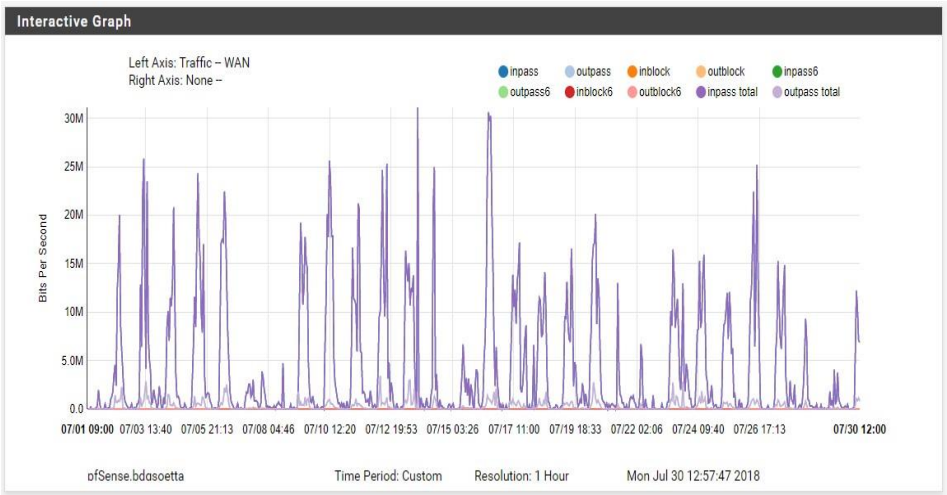
Selain daripada *download*, kecepatan *upload* terkadang menjadi salah satu bagian yang penting oleh sebagian orang terutama oleh para pegawai yang memiliki tugas yang lebih banyak dalam melakukan *upload*, seperti halnya *uploading* dokumen, lampiran, gambar, foto dan video yang berkaitan dengan tugasnya. Sama halnya dengan *download*, perlu dilakukan perhatian dan penanganan lebih agar *bandwidth upload* pun dapat optimal. PfSense memiliki fitur pembatasan kecepat *download* atau disebut dengan *download limiter*, penggunanaan fitur ini sebagai upaya agar kestabilan koneksi internet tetap terjaga.

3.4. AntiVirus ClamAV

Pencegahan terhadap virus umunya dilakukan dengan menggunakan program *Anti-Virus*, terdapat banyak program *Anti-Virus* yang berbayar dan tidak berbayar yang dapat di unduh di Internet, namun masih banyak orang yang belum terlalu memahami betul program *Anti- Virus* ini. Kalangan masyarakat yang sudah terbiasa dengan Informasi dan Teknologi (IT) saat ini mungkin sudah memahami seberapa pentingnya program *Anti-Virus*, namun dikalangan anak-anak dan lanjut usia yang masih belum terbiasa dengan Informasi dan Teknologi mungkin masih asing dengan yang namanya program *Anti-Virus.* Meskipun sering dianggap hal yang tidak begitu penting oleh sebagian orang, namun sebenarnya program *Anti-Virus* adalah salah satu upaya pencegahan dalam menjaga keamanan data dan informasi, maka dari itu perlu upaya agar keamanan data dan informasi setiap *client* tetap terjaga yaitu dengan menerapkan sistem atau program *Anti-Virus* yang dapat bekerja secara menyeluruh meskipun pada setiap *client* sudah terdapat program *Anti-Virus* yang berbeda.

Dalam pfSense, terdapat program *Anti-Virus* yang bernama ClamAV, *Anti-Virus* ini merupakan salah satu fitur untuk keamanan jaringan yang disediakan oleh pfSense dalam menjaga keamanan data dan informasi dari setiap *client*. Berikut adalah hasil analisis mengenai konfigurasi dan cara kerja ClamAV pada pfSense. Pada fitur ClamAV *Anti-Virus*, dapat kita lihat beberapa konfigurasi yang dapat kita sesuaikan seperti halnya *Redirect URL* jika kita ingin mengalihkan ke *URL* yang telah kita tentukan pada saat *client* membuka *website* atau situs yang bermuatan virus. Lalu ada pilihan *Clamav Database Update*, yang mana *user* diberikan pilihan waktu periode untuk melakukan pembaruan basis data virus secara otomatis yang dilakukan oleh pfSense.

3.5. Kinerja Bandwidth



Gambar 7. Grafik Total Bandwidth

Dapat kita perhatikan grafik di atas, dimana pada pekan ke dua, penerapan kebijakan *web filtering*, *Upload* dan *Download Limitation*, dan *Anti-Virus* belum sepenuhnya diterapkan, sehingga rata-rata pemakaian masih tinggi, sedangkan pada pekan ke tiga dan empat, setelah diterapkan kebijakan *web filtering*, *Upload* dan *Download Limitation*, dan *Anti-Virus* rata-rata jumlah pemakaian *bandwidth* terjadi penurunan.

Jika dilakukan pengujian kecepatan menggunakan *speedtest* yang dapat diakses melalui *browser*, dapat kita lihat hasil berupa *ping*, unduh (*download)* dan unggah (*upload)* yang didapatkan sangat baik, dalam artiandidapatkan pada *download dan Upload* sangat tinggi.

Berbeda dengan hasil yang didapatkan pada saat fungsi *bandwidth limiter* pada pfSense belum di aktifkan, kecepatan unduh dan kecepatan unggah yang didapatkan sesudah *bandwitdth limiter* dikatifkan terjadi penurunan. Namun perlu kita amati, *PING* secara angka menurun, itu menandakan bahwa waktu akses mengalami penurunan, dalam artian kecepatan akses menjadi lebih cepat. Jumlah kenaikan dan penurunan akan berubah bilamana jumlah pembatasan *bandwidth* pada pfSense terdapat perubahan, hal ini menunjukan bahwa fungsi *bandwidth limiter* pada pfSense berjalan dengan baik.

3.6. Pembatasan akses website

Penerapan kebijakan *Web Filtering* yang sudah dilakukan tentu akan berdampak langsung terhadap jumlah pemakaian *bandwidth* setiap harinya, hal ini terjadi karena bilamana kebijakan pembatasan akses terhadap website atau situs yang bermuatan konten negatif atau yang memuat konten sangat banyak. Seperti halnya situs porno, situs film bajakan, *youtube* dsb, bilamana dilakukan *blocking* terhadap situs-situs tersebut maka pemakaian *bandwidth* memungkinkan terjadi penurunan. Dapat dilihat pada pesan *error* yang dimunculkan bahwasannya *connection refused* atau koneksi ditolak, bukan karena tidak adanya koneksi yang mengakibatkan tidak dapat diaksesnya situs tersebut. Penerapan ClamAV *Anti-Virus* juga memberikan tambahan pengamanan terhadap keamanan data atau informasi setiap *client*, setelah dilakukan uji coba dengan melakukan *download virus-test file* dan *hacking.* Tercatat didalam *logs* bahwa telah terdeteksi virus dan tindakan *phising* (tindakan mencuri identitas / *password*).

Gambar 8. Speedtest sebelum dan sesudah

3.7. Indeks kepuasan layanan internet

Untuk memastikan hasil analisis pada penelitian yang dilakukan, perlu dilakukan pengumpulan data kepuasan layanan jaringan Internet yang didistribusikan kepada seluruh *client.* Metode yang digunakan untuk melakukan pengumpulan data menggunkan kuesioner dengan metode pendekatan skala likert. Berikut adalah hasil rekapitulasi dan perhitungan kuesioner kepuasan layanan Internet.

Dengan hasil perhitungan sebagai berikut :

Jumlah Pilihan : 5

Jumlah Pertanyaan : 5
Jumlah Responden : 53 Orang
(Y) Skor Tertinggi x Jumlah Responden : *n* X 53 Orang
(X) Skor Tertinggi x Jumlah Responden : *n* X 53 Orang

Rumus Interval

I = 100 / Jumlah Skor (Likert)
Maka (I) = 100 / 5 = 20 (jarak interval dari terendah 0% hingga tertinggi 100%)
Setelah dilakukan perhitungan terhadap kelima pertanyaan, didapat hasil interpretasi skornya berdasarkan interval :

- Angka 0% – 19,99% = Sangat (tidak setuju/buruk/kurang sekali)
- Angka 20% – 39,99% = Tidak setuju / Kurang baik)
- Angka 40% – 59,99% = Cukup / Netral
- Angka 60% – 79,99% = (Setuju/Baik/ suka)
- Angka 80% – 100% = Sangat (setuju/Baik/Suka)

Dari hasil perhitungan setiap pertanyaan bila dirata-ratakan maka diperoleh hasil berikut :
Jumlah skor Rata-Rata / Y x 100

$$= \frac{(191+218+218+179+183)}{5} / 265 \times 100$$

= 197.8 / 265 x 100
= 74.64 % (Setuju/Baik/suka)

4. Kesimpulan

PfSense merupakan sebuah sistem berbasis FreeBSD yang bersifat *open-source* (gratis), didukung dengan beberapa kelebihan lain seperti *Web Configuration* yang memudahkan pengguna dalam melakukan konfigurasi, dan flexibel. Penerapan fitur-fitur seperti pembatasan akses terhadap situs atau *website*, pembatasan kecepatan *download* dan *upload*, serta penerapan *Anti-Virus* yang terpusat, dapat berjalan dengan baik sehingga upaya untuk menciptakan koneksi internet yang stabil, efektif, efisien dan optimal. Selain daripada itu, keamanan data ataupun informasi dari setiap *client* menjadi lebih terjaga. PfSense dapat difungsikan sebagai *router* utama dan *firewall* secara bersamaan, sehingga dapat memungkinkan untuk dilakukan efisiensi biaya infrastruktur jaringan. Kemudian ClamAV yang terdapat pada pfSense, dapat dikembangkan lagi dengan melakukan konfigurasi lebih lanjut agar dapat pengamanan jaringan dapat lebih optimal.

Referensi

[1] Winarno S., Putri TD. Jaringan Komputer dengan TCP/IP. Edisi pertama. Bandung: Modula. 2015.
[2] Pratama IPAE. Handbook jaringan komputer: teori dan praktik berbasiskan open source. Edisi kedua. Bandung: Penerbit Informatika. 2015.
[3] Gingin Y., Rachman O. Router. Bandung: Informatika. 2012.
[4] Sarifin A., Astuti BRT. Penerapan router pfsense berbasis free bsd di warnet emax sragen. *IJNS*. 2012; 1(1): 61-66.
[5] Arman M., Rachmat N. Implementasi sistem keamanan web server menggunakan pfsense. *Jusikom*. 2020; 5(1): 13-23.
[6] Hakim AR. Penerapan load balancing pada router pfsense berbasis free bsd. *Edik Informatika*. 2017: 4(1): 23-28.
[7] Shofia, NH. 2019. Network traffic monitoring di jaringan internet ums menggunakan suricata dan pfsense. http://eprints.ums.ac.id/77047/2/L200150056-Nur-Hasna-Shofia-Naskah.pdf

[8] Hidayat, R. *Desain dan analisis patch sirkular untuk aplikasi antena tag rfid dengan algoritma propagasi balik jaringan syaraf tiruan*. SNaPP. Bandung. 2016.