Simulasi Keamanan Jaringan Komputer Penerapan Internet Positif

Abid Ariq Athallah[1], Agus Prihanto[2]

[1,2] Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya
[1]abid.ariq.athallah18@gmail.com
[2]agusprihanto@unesa.ac.id

***Abstrak*— Perkembangan *digital*, *internet* telah menjadi bagian *integral* dari kehidupan sehari-hari, namun juga membawa berbagai risiko keamanan. Penelitian ini mengeksplorasi penerapan *filtering internet* positif menggunakan pfSense sebagai sistem operasi *router* untuk meningkatkan keamanan jaringan. pfSense, yang berbasis *FreeBSD*, menyediakan berbagai fitur seperti *firewall, NAT, VPN,* dan *IDS/IPS*. Penelitian ini bertujuan untuk menentukan konfigurasi optimal pfSense dalam menyaring konten berbahaya dan tidak pantas, serta mengevaluasi dampaknya terhadap kinerja jaringan dan produktivitas dengan menggunakan pfSense dan fitur seperti *pfBlocker-NG*. Penelitian ini mensimulasikan penerapan *filtering* di lingkungan *virtual*, fokus pada kategori pornografi, judi online, dan *phishing*.**

Hasil penelitian menunjukkan bahwa bandwith sedikit lebih meningkat daripada sebelum penerapan *filtering firewall* ini. Penelitian ini memberikan panduan praktis untuk implementasi *filtering internet* positif, yang diharapkan dapat membantu institusi pendidikan, perusahaan, dan rumah tangga dalam menjaga keamanan jaringan mereka.

Kata Kunci*— *pfSense, FreeBSD, Filtering, Firewall, pfBlockerNG, Pornografi.

I. PENDAHULUAN

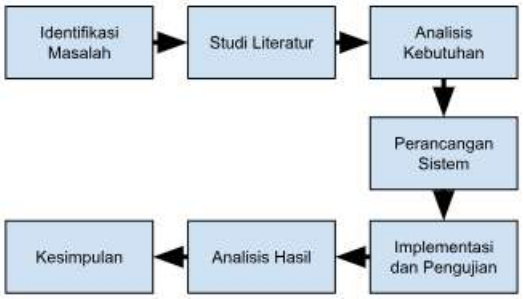
Di era *digital* saat ini, internet telah menjadi bagian penting dari kehidupan sehari-hari, menyediakan akses luas terhadap informasi dan layanan untuk keperluan pribadi, pendidikan, dan bisnis. Meski memberikan banyak manfaat, internet juga membawa risiko dan ancaman keamanan yang signifikan, yang dapat berdampak negatif jika tidak ada kontrol yang memadai. Salah satu solusi untuk mengatasi ancaman ini adalah melalui penerapan *filtering* internet positif, yang menyaring konten berbahaya dan tidak pantas [2].

Keamanan jaringan komputer sangat penting untuk menjaga integritas, kerahasiaan, dan ketersediaan data serta layanan di internet. Tanpa langkah-langkah keamanan yang tepat, jaringan komputer rentan terhadap berbagai serangan seperti *malware* dan *phishing*, yang bisa mencuri data sensitif atau mengganggu operasional. *Filtering* internet positif tidak hanya memblokir akses ke situs berbahaya tetapi juga meningkatkan produktivitas dengan membatasi akses ke situs yang tidak relevan dengan pekerjaan atau pendidikan. Ini juga melindungi anak-anak dan remaja dari konten yang tidak sesuai [4].

pfSense, sistem operasi *open-source* berbasis *FreeBSD*, menawarkan solusi fleksibel untuk mengelola dan mengamankan jaringan. Dengan fitur seperti *firewall*, *NAT*, *VPN, IDS/IPS*, dan *filtering* konten, pfSense sangat cocok untuk implementasi internet positif di berbagai lingkungan, termasuk institusi pendidikan, perusahaan, dan rumah tangga. Penelitian ini bertujuan menyediakan panduan praktis untuk implementasi *filtering* internet positif, dengan manfaat seperti peningkatan keamanan, produktivitas, dan perlindungan anak dari konten tidak sesuai [7].

II. METODOLOGI PENELITIAN

A. Tahapan Penelitian



Gbr. 1 Tahapan Penelitian

Pada gambar 1 dapat diketahui tahapan penelitian yang akan diterapkan pada penelitian ini, yaitu perlu dilakukan identifikasi masalah yang mendasari kebutuhan akan pengimplementasian *filtering* internet positif menggunakan pfSense. Masalah kebutuhan untuk melindungi pengguna jaringan dari akses ke konten berbahaya atau tidak pantas, serta keinginan untuk meningkatkan keamanan dan performa jaringan.

Langkah Selanjutnya adalah melakukan studi literatur untuk memahami konsep, teknologi, dan praktik mengenai filtering internet positif dan penggunaan pfSense sebagai solusi untuk keamanan jaringan. Literatur meliputi artikel penelitian, dokumen spesifikasi tentang pengaturan *firewall, filtering* konten dan penggunaan pfSense dalam konteks keamanan jaringan.

Langkah Berikutnya melakukan Analisis Kebutuhan fungsional dan non fungsional seperti fitur yang diperlukan, kinerja yang diharapkan dan integerasi dengan infrastruktur jaringan yang ada.

Langkah Berikutnya adalah merancang sistem secara rinci. Melibatkan pemilihan pemilihan komponen, Konfigurasi pfSense Perancangan Topologi Jaringan dan pengembangan

keamanan jaringan. Perancangan ini harus mempertimbangkan keamanan, kinerja, dan ketahanan jaringan.

Setelah merancang sistem jaringan lalu sistem akan di implementasikan sesuai dengan rencana yang dibuat proses ini meliputi instalasi perangkat keras dan perangkat lunak yang di gunakan, konfigurasi pfSense dan komponen lainya.

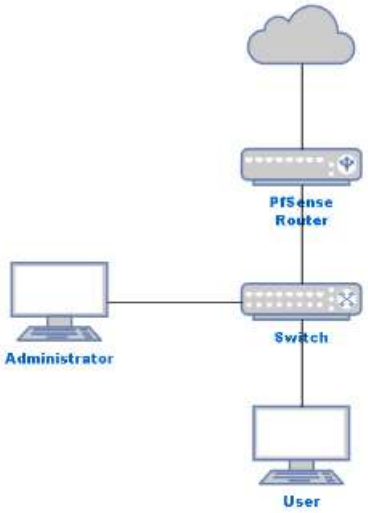
Setelah implementasi selesai, sistem akan diuji untuk memastikan bahwa itu memenuhi persyaratan dan berfungsi dengan baik.

Setelah pengujian selesai, kesimpulan hasil akan dianalisis untuk mengetahui keberhasilan sistem dalam memenuhi kebutuhan internet positif. Ini melibatkan hasil efektivitas *filtering* internet positif, performa jaringan, penyesuaian *filtering* dengan perkembangan internet, ketahanan *filtering* jika *load* berlebih. Berdasarkan analisis hasil, kesimpulan akan ditarik untuk mengevaluasi hasil penelitian, manfaat dan keterbatasan dari solusi serta memberikan kelemahan untuk pengembangan dimasa depan. Kesimpulan ini merangkum temuan utama implikasi dari penelitian yang dilakukan.

B. Perancangan Sistem Jaringan

Perancangan jaringan itu penting dalam membangun infrastruktur jaringan yang aman. Tujuan dari perancangan ini adalah untuk memungkinkan pembangunan infrastruktur jaringan yang kuat, aman, dan baik.

Dalam arsitektur ini Pertama, terdapat koneksi langsung ke internet, yang merupakan sumber utama akses bagi pengguna jaringan. Di antara internet dan jaringan lokal, terdapat pfSense *Router* yang bertindak sebagai *gateway*. pfSense tidak hanya berfungsi sebagai *router*, tetapi juga berperan sebagai *firewall* yang dapat mengatur lalu lintas data masuk dan keluar, serta menerapkan kebijakan keamanan yang sesuai.



Gbr. 2 Topologi Jaringan yang Digunakan Dalam Penelitian ini

Pada Gambar 2 menjelaskan secara rinci Selain itu, ada sebuah *switch* yang menghubungkan berbagai perangkat dalam jaringan lokal, seperti komputer, laptop, dan perangkat *mobile*. Ini memungkinkan akses yang lancar antara perangkat-perangkat ini dan pengaturan jaringan yang fleksibel. Dalam skenario ini, terdapat dua *node* penting: *Node Administrator* dan *Node User*. *Node Administrator* digunakan oleh *administrator* jaringan untuk mengelola, mengkonfigurasi, dan memantau pfSense serta infrastruktur jaringan secara keseluruhan. Sementara itu, *Node User* adalah perangkat yang digunakan oleh pengguna jaringan untuk mengakses internet dan sumber daya jaringan lainnya.

Dalam aliran data, ketika pengguna di *Node User* mengajukan permintaan akses internet, permintaan tersebut akan diteruskan ke pfSense *Router*. Disinilah *filtering* internet positif dilakukan; pfSense memeriksa kebijakan keamanan yang telah ditetapkan dan memutuskan apakah permintaan tersebut diizinkan atau diblokir. Jika diizinkan, pfSense akan meneruskan permintaan tersebut ke internet melalui koneksi yang tersedia. Begitu ada respon dari internet, pfSense akan meneruskannya kembali ke *Node User* yang bersangkutan. Berikut manfaat skema jaringan ini:

1) itu memberikan kontrol penuh kepada *administrator* atas lalu lintas internet yang masuk dan keluar dari jaringan, memungkinkan penerapan kebijakan keamanan yang ketat.
2) dengan kehadiran *firewall* pada pfSense, jaringan dilindungi dari serangan luar dan risiko ancaman siber lainnya.
3) Terakhir, kemampuan manajemen dan pemantauan yang baik memungkinkan *administrator* untuk mengelola jaringan dengan efisien dan merespons dengan cepat terhadap perubahan kondisi atau ancaman yang mungkin muncul.

C. Analisis Kebutuhan

Kebutuhan yang diperlukan untuk melakukan penelitian dan pengujian ini adalah:

1) Kebutuhan perangkat keras (*Hardware*)
   Berikut merupakan spesifikasi dari perangkat keras yang digunakan untuk menunjang penelitian ini:
   a. CPU: Minimum Intel Core i5.
   b. RAM: Minimal 4 GB, direkomendasikan 8 GB atau lebih.
   c. Penyimpanan: SSD atau HDD dengan kapasitas cukup untuk sistem operasi dan aplikasi yaitu 40 GB.

2) Kebutuhan perangkat lunak (*Software*)
   Berikut merupakan spesifikasi dari perangkat lunak yang digunakan untuk menunjang penelitian ini:
   a. *Software* pfSense sebagai *router* OS untuk *filtering* internet positif dan memantau lalu lintas jaringan.
   b. *Software* Virtualisasi simulasi dilakukan dalam lingkungan virtual, seperti VMware atau *VirtualBox* diperlukan untuk menjalankan pfSense dan Apache Jmeter
   c. *Software Firewall* pfSense Untuk mengimplementasikan *filtering* internet positif

dengan lebih baik, beberapa paket tambahan seperti pfBlockerNG diperlukan untuk filtering konten.

d. *Software* Apache Jmeter untuk melakukan pengujian beban kinerja sistem *filtering* pfSense

Kemudian dilakukan pengujian sesuai dengan tujuan penelitian. Proses *Filtering* Internet Positif dilakukan dengan menggunakan pfSense pada VM yang telah diimplementasikan.

D. Skema Pengujian

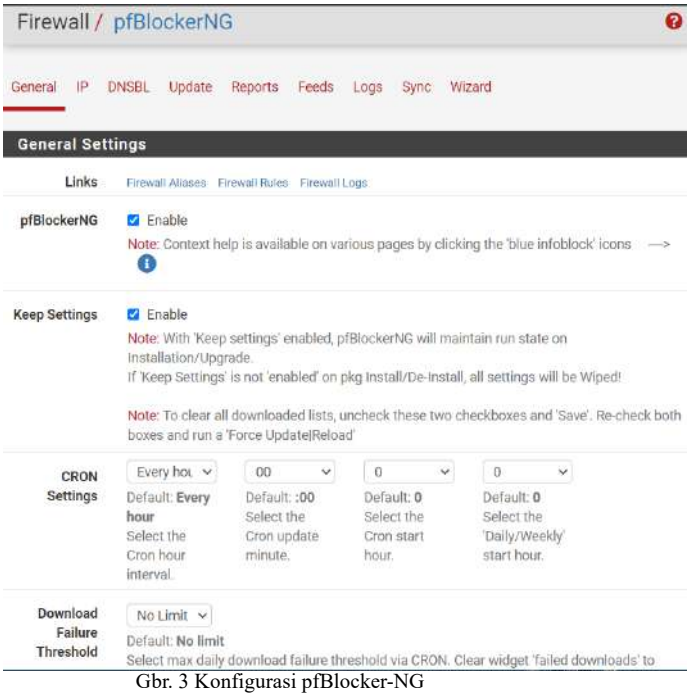
Pada Penelitian kali ini. Terdapat 3 Pengujian yang diterapkan:

1) Menguji Efektivitas *Filtering* Internet Positif pfSense harus mencegah akses ke situs web tersebut dan menampilkan pesan yang sesuai dengan kebijakan pfBlockerNG Sediakan.
2) Menguji Kinerja Jaringan Penggunaan *filtering* internet positif tidak boleh mengurangi kinerja jaringan secara signifikan, dan waktu respon yang diperlukan harus tetap dalam batas yang dapat diterima.
3) Menguji Ketahanan *Filtering Firewall* dari Beban Berlebih Jika Suatu Domain diberikan Beban 1000-3000 dalam waktu yang bersamaan apakah Filter Blokirnya Lolos atau Tidak.

Dengan menyusun skema pengujian ini, dapat dilakukan secara sistematis untuk mengevaluasi keamanan performa pengaturan pfSense dalam penerapan *filtering* internet positif

III. HASIL DAN PEMBAHASAN

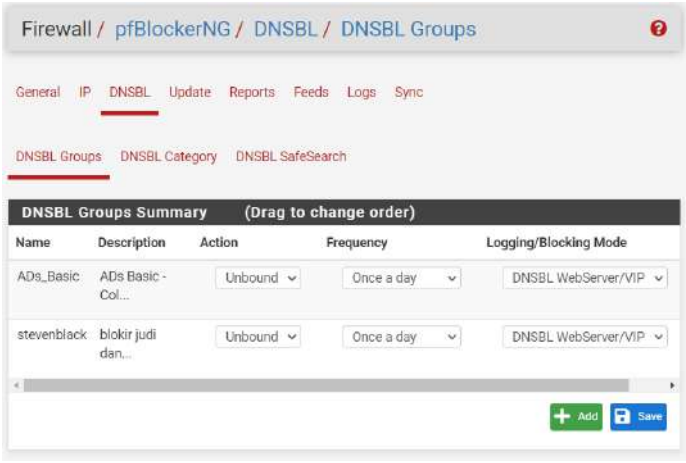
A. Konfigurasi pfBlocker-NG, DNSBL



Gbr. 3 Konfigurasi pfBlocker-NG

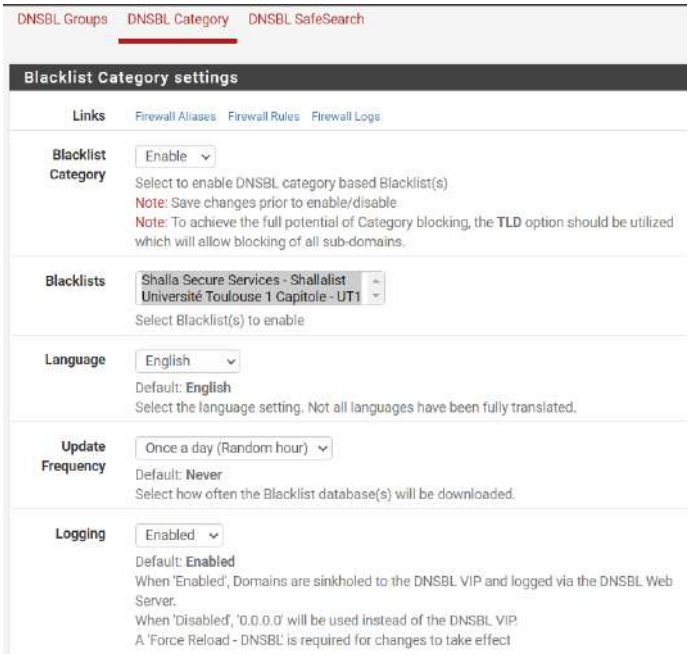
Pada Gambar 3 pfSense terdapat Paket Instalasi bernama pfBlocker-NG yang dimana berguna untuk Pemasangan *Firewall* dalam sistem keamanan jaringan untuk blokir situs dan *domain* konten negatif. Dan dialam pfBlocker-NG terdapat DNSBL. DNSBL memblokir akses ke domain yang masuk dalam daftar hitam dengan mengarahkan permintaan DNS untuk domain tersebut ke "*blackhole*", sehingga pengguna tidak dapat mengakses situs tersebut.

DNSBL diaktifkan dan mengkonfigurasi pengaturan dasar seperti antarmuka yang digunakan dan opsi *Safe Search*.



Gbr. 4 Konfigurasi pfBlocker-NG Sumber DNSBL

Pada Gambar 4 StevenBlack merupakan salah satu sumber *blocklist* yang populer digunakan untuk memblokir iklan, pelacak, dan konten berbahaya. untuk mengkonfigurasi StevenBlack pada pfBlocker-NG di pfSense dengan memasukkan *URL Blocklist*.



Gbr. 5 Konfigurasi pfBlocker-NG Blacklist Kategori

Gbr. 5 Konfigurasi pfBlocker-NG Blacklist Kategori Service

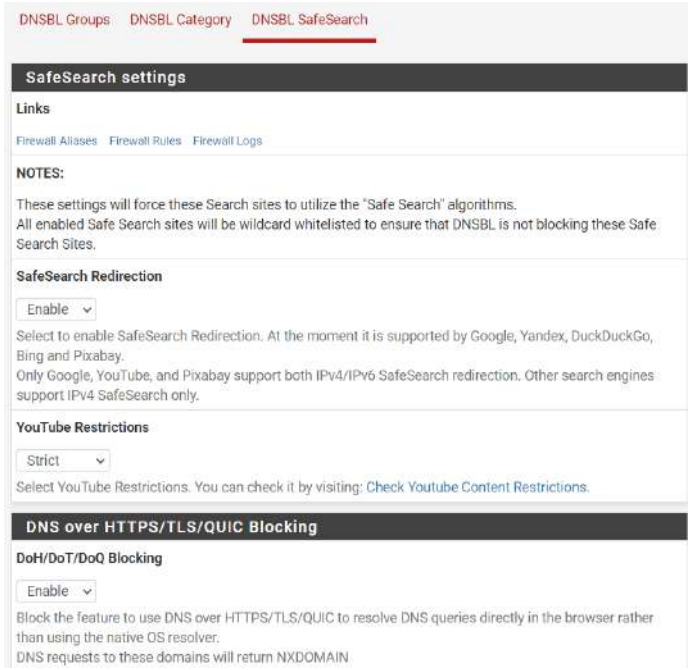
Pada Gambar 5 Masukkan blacklist service yg akan dipilih seperti *Shallalist* dan UT 1. Lalu klik save.

Kategori Pemblokiran: DNSBL memungkinkan pengaturan pemblokiran berdasarkan kategori seperti *malware*, iklan, jejaring sosial, konten dewasa, dan lain-lain, yang memudahkan dalam mengelompokkan dan mengelola domain yang diblokir.

A. *Konfigurasi DNSBL Safe Search*

Lalu pada DNSBL Terdapat *Safe Search* yang dimana Penerapan *SafeSearch* membawa manfaat dalam mengelola keamanan dalam mesin penelusur seperti *Google, Bing*, atau *Yahoo* dan juga Platform Video Seperti *Youtube*. Dalam *Safe Search* Mesin Penelusur tersebut disaring untuk konten yang tidak pantas atau tidak sesuai. Hal ini menjadi sangat penting terutama dalam lingkungan di mana anak-anak atau remaja dapat terpapar dengan konten yang tidak layak secara tidak sengaja.

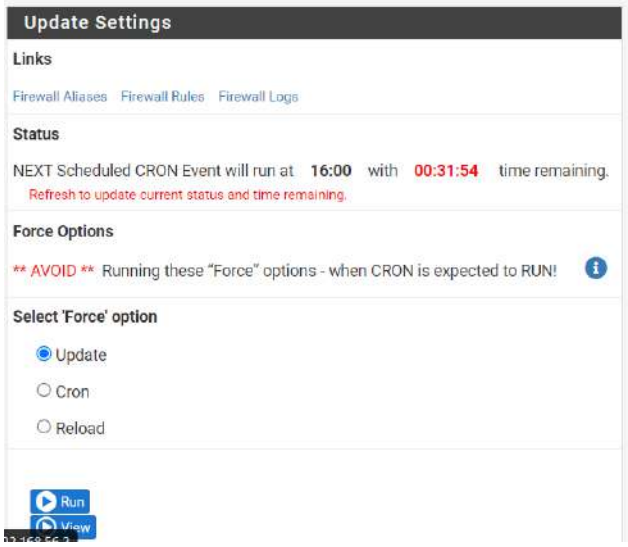
pfBlocker-NG memungkinkan *administrator* jaringan untuk mengontrol akses internet dengan memblokir situs-situs yang tidak diinginkan berdasarkan kriteria yang telah ditentukan.



Gbr. 6 Konfigurasi pfBlocker-NG DNSBL Safe Search

Pada Gambar 6 Dengan memanfaatkan fitur Kategori dan *filtering safe search*, *administrator* dapat dengan mudah mengelola dan menyesuaikan pengaturan blokir sesuai dengan kebutuhan spesifik jaringan mereka. Selain itu, kemampuan untuk memantau aktivitas dan log secara teratur memungkinkan deteksi dini terhadap akses yang tidak sah atau tidak diinginkan. Secara keseluruhan, penerapan *SafeSearch* dengan pfBlockerNG memberikan lapisan perlindungan tambahan yang penting dalam memastikan pengalaman online yang lebih aman dan terkendali.

B. *Konfigurasi DNSBL Update*



Gbr. 6 pfBlocker-NG DNSBL Update

Pada Gambar 6 pada pfBlocker-NG Terdapat Fitur Perbarui secara otomatis memperbarui daftar alamat IP dan nama domain yang digunakan untuk pemblokiran sesuai dengan jadwal yang telah ditentukan oleh *Administrator*. Fitur ini memastikan bahwa daftar blokir selalu *up-to-date* dengan informasi terbaru, yang penting untuk menjaga efektivitas dan keamanan jaringan. *Administrator* dapat menentukan seberapa sering pembaruan dilakukan, seperti setiap jam, harian, mingguan, atau bulanan. Ini memberikan keinginan untuk menyesuaikan pembaruan sesuai dengan kebutuhan spesifik jaringan. Dan pada Settingan Perbarui Otomatis Ini terdapat 3 pilihan *Force Update* yaitu "Update", "Corn", "Reload":

1) *Update*

pfBlocker-NG akan langsung memperbarui daftar pemblokiran atau daftar erat sesuai dengan konfigurasi yang telah diatur, tanpa mempertimbangkan jadwal yang telah ditetapkan sebelumnya. Ini berguna jika ingin memperbarui daftar secara manual di luar jadwal yang telah ditentukan.

2) *Corn*

Cron adalah utilitas di sistem operasi *Unix* yang digunakan untuk menjadwalkan tugas-tugas tertentu untuk mengeksekusi secara otomatis pada waktu yang ditentukan. Dengan memilih opsi ini, pembaruan akan dilakukan sesuai dengan jadwal *cron* yang telah dikonfigurasi sebelumnya.

3) *Reload*

Ini akan memuat ulang aturan-aturan *firewall* setelah pembaruan selesai. Ketika memperbarui daftar pemblokiran atau daftar erat, perlu memuat ulang aturan *firewall* agar perubahan dapat diterapkan secara efektif. Opsi ini akan secara otomatis

memuat ulang aturan-aturan *firewall* setelah pembaruan selesai, sehingga tidak perlu melakukannya secara manual.

```
[ UT1_gambling ]                exists.
[ UT1_lingerie ]                exists.
[ UT1_malware ]                 exists.
[ UT1_mixed_adult ]             exists.
[ UT1_phishing ]                exists.
[ UT1_redirector ]              exists.
[ UT1_sexual_education ]        exists.
[ UT1_strict_redirector ]       exists.
[ UT1_strong_redirector ]       exists.
[ StevenBlack_ADs ]             exists. [ 06/12/24 21:04:56 ]
[ judidanporno ]                exists.
[ kontenporno ]                 exists.
Saving DNSBL statistics... completed
--------------------------------------------------------------------------------
Assembling DNSBL database..... completed [ 06/12/24 21:04:58 ]
Stopping Unbound Resolver
Unbound stopped in 1 sec.
Starting Unbound Resolver... completed [ 06/12/24 21:05:04 ]
DNSBL update [ 405378 | PASSED  ]... completed [ 06/12/24 21:05:07 ]
--------------------------------------------------------------------------------

===[  GeoIP Process  ]=========================================


===[  IPv4 Process  ]==========================================

[ Abuse_Feodo_C2_v4 ]           Downloading update .. 200 OK. completed .
  ------------------------------
```

Gbr. 7 Konfigurasi pfBlocker-NG DNSBL Logs

Pada Gambar 7 adalah proses update Konfigurasi DNSBL dalam pfBlocker-NG.

Dengan demikian, instalasi pfSense di *VirtualBox* memerlukan pengaturan khusus untuk virtualisasi, namun langkah-langkahnya secara umum mirip dengan instalasi di lingkungan fisik.

C. *Hasil Pengujian Filtering Internet Positif*

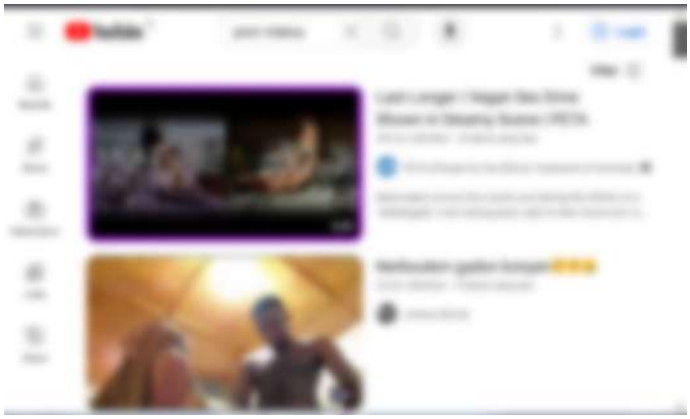
Pengujian *filtering* internet positif bertujuan untuk memastikan bahwa akses ke situs-situs Negatif, Berbahaya dan judi *online* berhasil diblokir. Menggunakan daftar situs yang termasuk dalam kategori Negatif, Berbahaya dan Judi, konten gambar yang dicari di google juga di filter sesuai dengan internet positif percobaan akses dilakukan. Hasil dari pengujian menunjukkan bahwa semua situs dalam daftar berhasil diblokir oleh sistem pfSense. Setiap percobaan akses diarahkan ke halaman peringatan yang menginformasikan bahwa situs tersebut tidak dapat diakses.

Selain itu, *log* di pfSense mencatat setiap upaya akses ke situs yang diblokir, memberikan visibilitas terhadap percobaan akses yang dicegah. Ini menunjukkan bahwa fitur *filtering* bekerja dengan baik dan efektif dalam menghalangi akses ke konten yang tidak diinginkan.

Disini Saya Memberikan Contoh Situs Ilegal dan Negatif terpopuler di internet saat ini seperti:

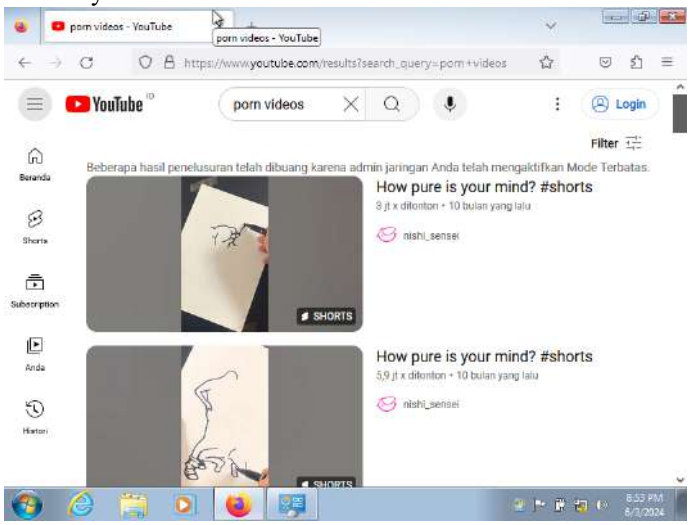
1) Betway.com
2) Sports.bwin.com
3) 009.casino
4) Bet365
5) Akses ke situs VPN Seperti vpnaffiliates.com
6) Oxbet.in
7) Safe Search Pornhub
8) Safe Search Videos XXX
9) Safe Search Youtube Porn Videos

Diatas adalah situs situs yang mewakili Penerapan *Filtering* Internet Positif, Kenapa Hanya 9 Situs Karena Keterbatasan Spesifikasi *Hardware* yang saya gunakan. Berikut Gambar Sebelum dan Sesudah Pengujian *Filtering* Internet Positif.



Gbr. 8 Safe Search Youtube Sebelum

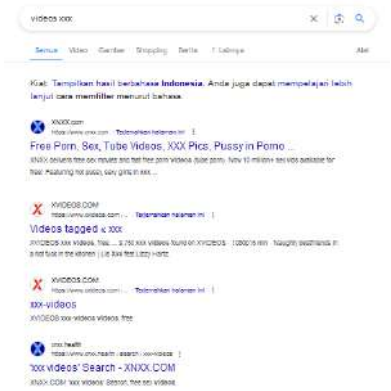
Pada Gambar 8 Penerapan Internet Positif *pada Safe Search Youtube* Sebelum ada Konfigurasi Ketika Mencari kata kunci "*Porn Videos*" akan muncul *video-video* yang tak pantas untuk pemuda dan anak di bawah umur hal ini sangat Berbahaya.



Gbr. 9 Safe Search Youtube Sesudah

Pada Gambar 9 Penerapan Internet Positif *pada Safe Search Youtube* Sesudah ada Konfigurasi Ketika Mencari kata kunci "*Porn Videos*" akan muncul *video-video* yang berbeda meskipun masih terdapat *Video* yang masih Negatif tapi hasilnya masih bisa diredam dan di filter sedikit lebih aman untuk usia dibawah umur.

Ini dikarenakan DNSBL pfBlocker Mem-Filter Konten *level* DNS ketika pengguna mencoba mengakses *youtube* dengan kata kunci "*Porn Videos*" permintaan DNS untuk konten tersebut akan diblokir.



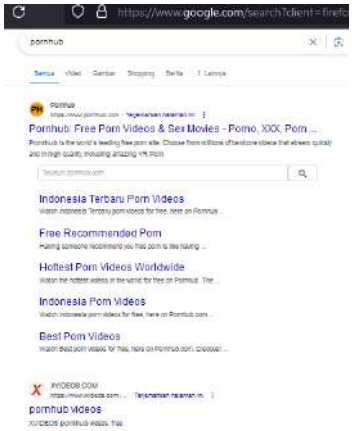
Gbr. 10 Safe Search Google Sebelum

Pada Gambar 10 Adalah Contoh Hasil Selanjutnya dari sebelum penerapan *filtering* internet positif tapi kali ini pengguna mencoba mengakses *google search bar* dengan kata kunci "*Videos XXX*" akan muncul situs yang negatif dan berbahaya untuk anak dibawah umur. Karena tidak ada halangan pada DNS-nya.

Gbr. 11 Safe Search Google Sesudah

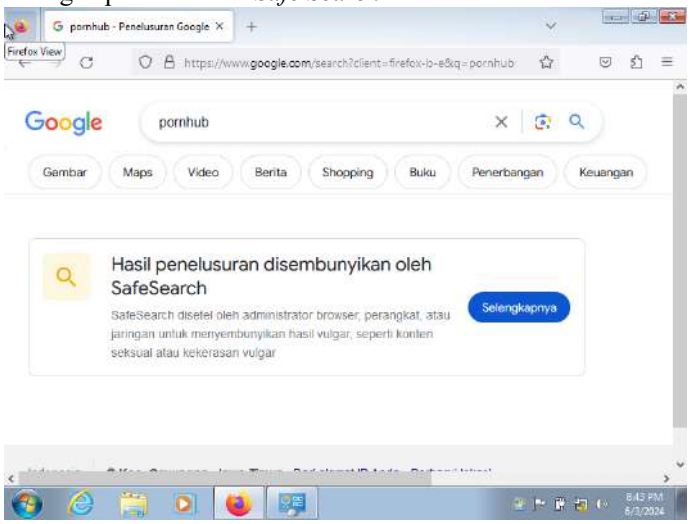
Pada Gambar 11 Penerapan Internet Positif pada *Safe Search Google* Sesudah ada Konfigurasi Ketika Mencari kata kunci "*Video XXX*" akan muncul *video-video* yang berbeda dan lebih aman untuk usia dibawah umur.

Ini dikarenakan DNSBL pfBlocker Mem-Filter Konten level DNS ketika pengguna mencoba mengakses *youtube* dengan kata kunci "*Porn Videos*" permintaan DNS untuk situs tersebut akan diblokir karena situs situs negatif sudah ada di DNSBL *Blacklist* yang sebelumnya di Konfigurasikan.



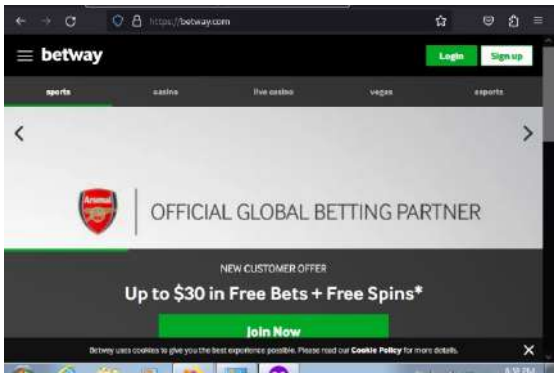
Gbr. 12 Safe Search Pornhub Sebelum

Pada Gambar 12 Adalah Contoh Hasil Selanjutnya dari sebelum penerapan *filtering* internet positif tapi kali ini pengguna mencoba mengakses *google search bar* dengan kata kunci "*Pornhub*" akan muncul situs pornografi yang negatif dan berbahaya untuk anak dibawah umur. Karena tidak ada halangan pada DNSBL *Safe Search*.



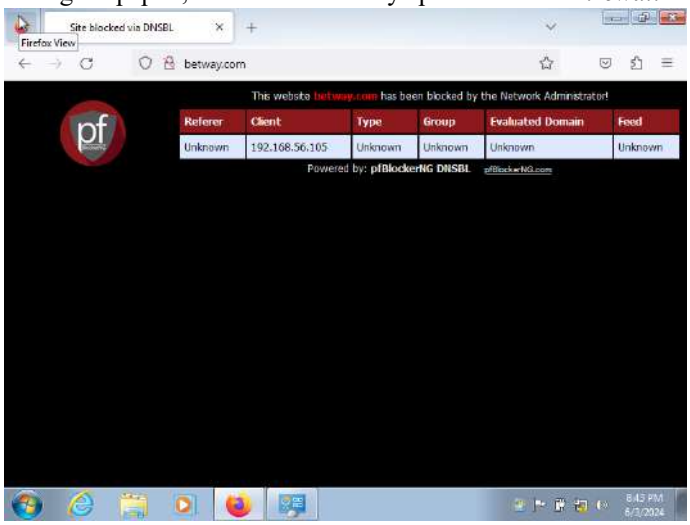
Gbr. 13 Safe Search Pornhub Sesudah

Pada Gambar 13 Merupakan Tampilan Blokir yang berbeda karena Penerapan Internet Positif pada *Safe Search Google* Sesudah ada Konfigurasi Ketika Mencari kata kunci "*Pornhub*"



Gbr. 14 Safe Search betway.com Sebelum

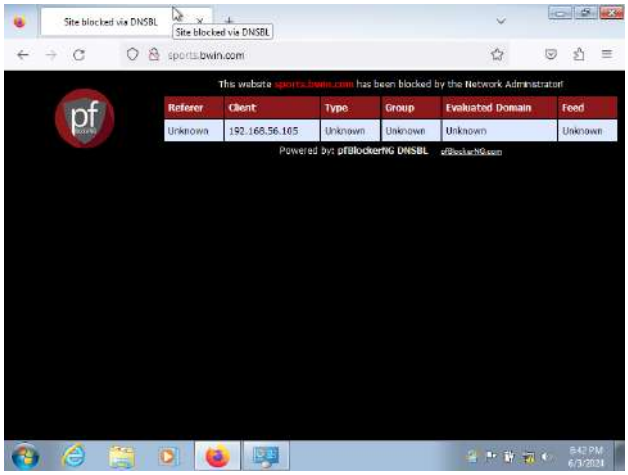
Pada Gambar 14 Adalah Contoh Hasil Selanjutnya dari sebelum penerapan *filtering* internet positif tapi kali ini pengguna mengakses situs judi *online* terbesar dan tidak ada halangan apapun, Karena tidak adanya pfBlockerNG *Firewall*.



Gbr. 15 Safe Search betway.com Sesudah

Pada Gambar 15 Merupakan Tampilan Blokir yang berbeda karena Penerapan Internet Positif pada *Domain* Judi *Online* "*betway.com*" pada Konfigurasi *Blocklist.*

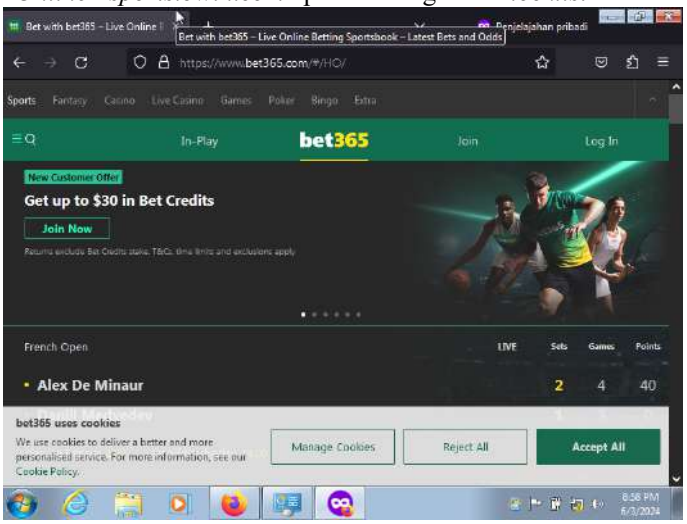
Gbr. 16 Safe Search sports.bwin.com Sebelum



Gbr. 17 Safe Search sports.bwin.com Sesudah

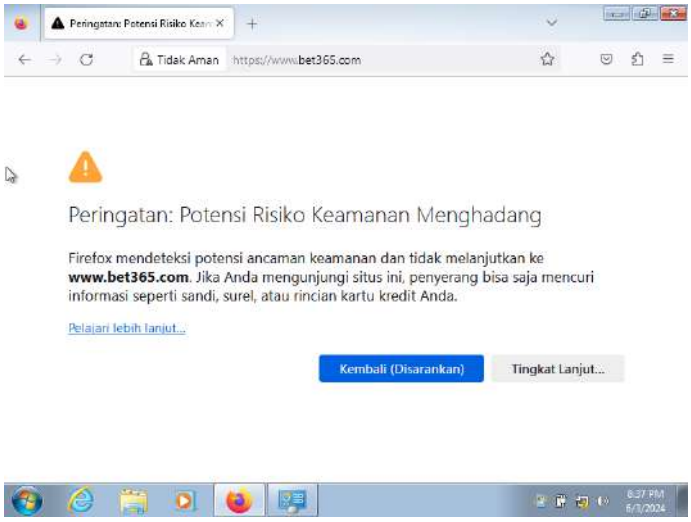
Pada Gambar 16 Adalah Contoh Hasil Selanjutnya dari sebelum penerapan *filtering* internet positif pengguna mengakses situs judi *online* lainya dan tidak ada halangan apapun, Karena tidak adanya pfBlockerNG *Firewall*.

Pada Gambar 17 Merupakan Tampilan Blokir yang berbeda karena Penerapan Internet Positif pada *Domain* Judi *Online "sports.bwin.com*" pada Konfigurasi *Blocklist*.



Gbr. 18 Safe Search bet365.com Sebelum

Pada Gambar 18 Adalah Contoh Hasil Selanjutnya dari sebelum penerapan *filtering* internet positif pengguna mengakses situs judi *online* lainya dan tidak ada halangan apapun, Karena tidak adanya pfBlockerNG *Firewall*.



Gbr. 19 Safe Search bet365.com Sesudah

Pada Gambar 19 Merupakan Tampilan Blokir yang berbeda karena Penerapan Internet Positif pada *Domain* Judi *Online "sports.bwin.com"* pada Konfigurasi *Blocklist*.

Selain *Domain* Diatas banyak sekali *domain* yang sudah masuk daftar hitam pada pfBlocker-NG. yang jika pengguna akses akan muncul notifikasi halaman yang sama seperti halnya contoh diatas.

Gbr. 20 Safe Search 009.casino Sebelum

Pada Gambar 20 Adalah Contoh Hasil Selanjutnya dari sebelum penerapan *filtering* internet positif pengguna mengakses situs mengandung *malware* dan *phising* dan tidak ada halangan apapun, Karena tidak adanya pfBlockerNG *Firewall.*

Gbr. 21 Safe Search 009.casino Sesudah

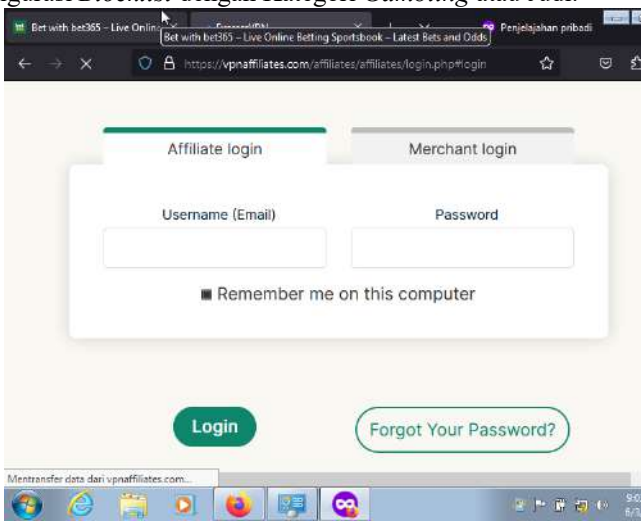
Pada Gambar 21 Merupakan Tampilan Blokir dari server pfSense karena Penerapan Internet Positif pada *Domain* mengandung *Malware* dan *Phishing* "*009.casino*" pada Konfigurasi *Blocklist.*

Gbr. 22 Safe Search oxbet.in Sebelum

Pada Gambar 22 Adalah Contoh Hasil Selanjutnya dari sebelum penerapan *filtering* internet positif pengguna mengakses situs mengandung *malware* dan *phising* dan tidak ada halangan apapun, Karena tidak adanya pfBlockerNG *Firewall.*

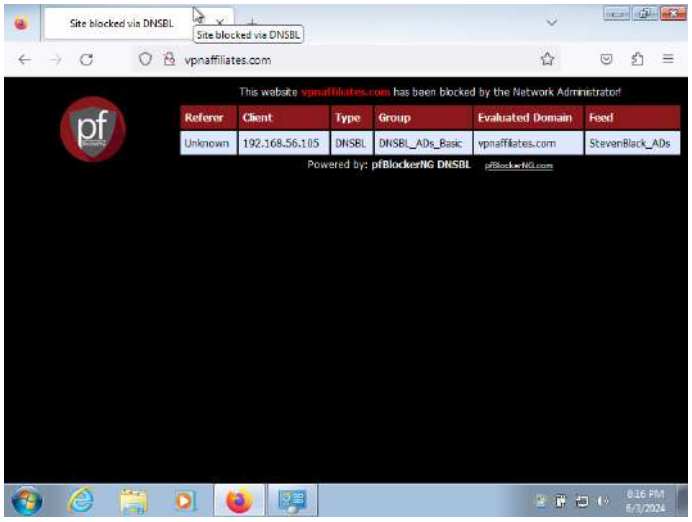
Gbr. 23 Safe Search oxbet.in Sesudah

Pada Gambar 23 Merupakan Tampilan Blokir dari server pfSense karena Penerapan Internet Positif pada *Domain* mengandung *Malware* dan *Phishing* "*oxbet.in*" pada Konfigurasi *Blocklist* dengan Kategori *Gambling* atau Judi.



Gbr. 24 Safe Search vpnaffiliates.com Sebelum

Pada Gambar 24 adalah Situs *VPN* karena itu cara ketika pengguna menggunakan *VPN* dan *PROXY* lain untuk membuka blokir dari *Blocklist* dari pfBlocker-NG jadi *Administrator* akan berusaha untuk memfilter akses ke situs VPN yang terpopuler yang ada di google saat ini.



Gbr. 25 Safe Search vpnaffiliates.com Sesudah

Pada Gambar 25 Merupakan Tampilan Blokir dari server pfSense karena Penerapan Internet Positif pada Akses Domain *VPN "vpnaffiliates.com"* pada Konfigurasi *Blocklist* dengan Kategori *VPN* dan *PROXY.*

Pengujian ini memperlihatkan bahwa pfSense mampu memberikan perlindungan yang diperlukan untuk menjaga keamanan dan kepatuhan dalam penggunaan internet di jaringan tersebut.

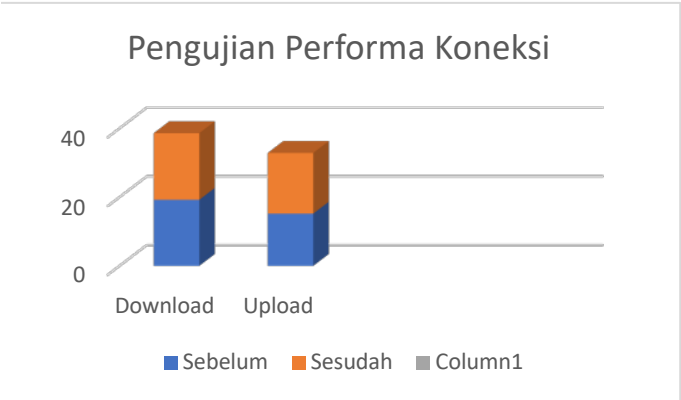
D. Pengujian Performa Bandwith Koneksi Sebelum dan Sesudah Filtering

Sebelum Penerapan *Filtering:*

Pada tahap awal pengujian, dilakukan pengukuran terhadap performa jaringan tanpa adanya filter yang diterapkan. Pengujian ini melibatkan beberapa metrik kunci seperti kecepatan *download*, dan kecepatan *upload*. dengan kecepatan *download* mencapai 19,221Mbps dan kecepatan *upload* sebesar 15,198Mbps.

Setelah penerapan *filtering* menggunakan pfSense

Pengujian ulang dilakukan untuk mengukur dampak pada performa jaringan. Hasilnya menunjukkan bahwa terdapat kecepatan *download* meningkat menjadi 19,373Mbps dan kecepatan *upload* menjadi 17,642 Mbps.



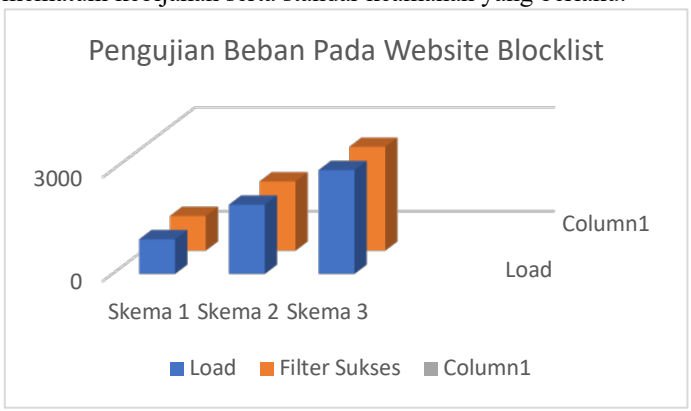
Gbr. 26 Safe Search vpnaffiliates.com Sesudah

Pada Gambar Grafik 26 Peningkatan Performa Ini dan perubahan ini karena banyak konten negatif yang disaring sehingga Data banyak yang tidak di proses dan diunduh lalu juga pfSense ini mendukung kompresi data, yang mengurangi ukuran data yang *ditransfer* antara server dan klien. Ini dapat mengurangi waktu yang dibutuhkan untuk mengunduh konten, terutama jika *bandwidth* jaringan terbatas dan juga banyak memblokir ancaman yang menghambat jaringan.

E. Pengujian dengan melakukan load secara bersamaan menggunakan Apache Jmeter

Pengujian beban secara bersamaan menggunakan Apache JMeter pada skema pfBlocker-NG sangat penting untuk memastikan kinerja dan keandalan sistem *firewall* dalam lingkungan jaringan yang sibuk. Dalam konteks ini, JMeter dapat digunakan untuk mensimulasikan lalu lintas jaringan yang berat dan beragam guna mengukur seberapa baik pfBlocker-NG menangani volume lalu lintas yang tinggi tanpa mengalami degradasi kinerja. Dengan melakukan pengujian seperti ini, administrator jaringan dapat mengidentifikasi batas kapasitas sistem dan titik-titik kegagalan potensial, sehingga bisa mengambil tindakan preventif untuk memperkuat infrastruktur keamanan. Selain itu, pengujian ini juga membantu dalam memastikan bahwa aturan blokir dan daftar hitam yang diterapkan oleh pfBlocker-NG bekerja dengan efektif, memblokir lalu lintas yang tidak diinginkan tanpa mengganggu lalu lintas yang sah.

Dalam skema pengujian ini, JMeter digunakan untuk mensimulasikan pengunjung yang mencoba mengakses situs *web* yang diblokir oleh pfBlocker-NG dengan mengirimkan permintaan *HTTP*. Analisis hasil pengujian ini memungkinkan optimasi konfigurasi pfBlocker-NG untuk mencapai keseimbangan optimal antara keamanan dan kinerja, serta memastikan bahwa sistem *firewall* tetap tangguh dan responsif terhadap berbagai jenis serangan dan kondisi lalu lintas yang ekstrem. Pengujian ini juga mendukung pemantauan berkelanjutan terhadap kesehatan dan kinerja sistem, yang sangat penting untuk menjaga keamanan jaringan dan mematuhi kebijakan serta standar keamanan yang berlaku.



Gbr. 27 Safe Search vpnaffiliates.com Sesudah

Pada Gambar Grafik 27 Pengujian Diatas dilakukan dengan beberapa skema *loop count* yang berbeda: 1000, 2000, dan 3000 kali. Skema *Load* 1000 dengan *Filtering* Suksesnya juga 1000. Skema *Load* 2000 dengan *Filtering* Suksesnya juga 2000, Skema *Load* 3000 dengan *Filtering* Suksesnya juga 3000 mewakili intensitas lalu lintas yang berbeda untuk melihat bagaimana pfBlocker-NG merespons terhadap berbagai tingkat beban.

IV. KESIMPULAN

Berikut Adalah Kesimpulan Dari penelitian Ini

1. Implementasi *firewall filtering* dengan pfSense untuk memblokir kategori-kategori tertentu seperti pornografi, judi *online*, dan *web phising* telah berhasil dilakukan. Dengan menggunakan paket pfBlocker-NG dapat mengkonfigurasi aturan-aturan yang memblokir dan memfilter akses ke situs-situs dalam kategori-kategori internet sehat.Kesimpulan dari pengujian Implementasi *firewall filtering* berhasil menerapkan pemblokiran terhadap konten-konten yang diinginkan sesuai dengan kategori yang telah ditentukan.
2. Penerapan Fitur *Update* Jadwal pada *Filtering GitHub Data Unified Hosts* Kesimpulan dari Penerapan fitur *schedule update* memastikan bahwa daftar pemblokiran dan Filter selalu diperbarui dengan data terbaru dari *GitHub Data Unified Hosts* secara otomatis, memungkinkan sistem untuk tetap *up-to-date* dalam memblokir konten-konten yang tidak diinginkan dalam Internet Sehat.
3. Perbandingan Performa Sebelum dan Sesudah Penerapan *Firewall Filtering* terhadap *Bandwidth Internet*. Sebelum penerapan *firewall filtering*, penggunaan *bandwidth internet* sedikit lebih tinggi karena banyak konten negatif yang disaring sehingga Data banyak yang tidak di proses dan diunduh lalu juga pfSense ini mendukung kompresi data, yang mengurangi ukuran data yang ditransfer antara server dan klien. Ini dapat mengurangi waktu yang dibutuhkan untuk mengunduh konten, terutama jika *bandwidth* jaringan terbatas dan juga banyak memblokir ancaman yang menghambat jaringan. Hal ini dapat menghasilkan efisiensi dalam penggunaan bandwidth dan meningkatkan kinerja jaringan secara keseluruhan.

REFERENSI

[1] S. Patton, D. Doss, and W. Yurcik, “Open source versus commercial firewalls: Functional comparison,” in Conference on Local Computer Networks, 2000, pp. 223–224, doi: 10.1109/LCN.2000.891032.

[2] M. Arunwan, T. Laong, and K. Atthayuwat, “Defensive performance comparison of firewall systems,” in 2016 Management and Innovation Technology International Conference, MITiCON 2016, 2017, pp. MIT221–MIT224, doi: 10.1109/MITICON.2016.8025212.

[3] D. Kumar and M. Gupta, “Implementation of Firewall & Intrusion Detection System Using pfSense To Enhance Network Security,” in International Journal of Electrical Electronics & Computer Science Engineering, 2018, pp. 131–137

[4] H. F. El-Sofany, S. A. El-Seoud, and I. A. T. F. Taj-Eddin, “A case study of the impact of denial of service attacks in cloud applications,” J. Commun., vol. 14, no. 2, pp. 153– 158, 2019, doi: 10.12720/jcm.14.2.153-158.

[5] G. A. Jaafar, S. M. Abdullah, and S. Ismail, “Review of Recent Detection Methods for HTTP DDoS Attack,” J. Comput. Networks Commun., vol. 2019, p. 10, 2019, doi: 10.1155/2019/1283472.

[6] H. Beitollahi and G. Deconinck, “Analyzing well-known countermeasures against distributed denial of service attacks,” Comput. Commun., vol. 35, no. 11, pp. 1312– 1332, 2012, doi: 10.1016/j.comcom.2012.04.008.

[7] A. Al Mugni, M. F. Herdiansah, M. G. Andhika and M. Ridwan, "DNSBL for Internet Content Filtering Utilizing pfSense as The Next Generation of Opensource Firewall," 2019 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Bandung, Indonesia, 2019, pp. 117-121, doi: 10.23919/EECSI48112.2019.8977017.

[8] Hakim, A. R. (2018). Penerapan load balancing pada router pfsense berbasis free bsd. Jurnal Edik Informatika Penelitian Bidang Komputer Sains dan Pendidikan Informatika, 4(1), 23-28.

[9] Ramadhan, M. S. F. (2023). PENERAPAN REDUNDANCY FIREWALL PFSENSE MENGGUNAKAN METODE CARP DENGAN PFSYNC DAN XMLRPC SYNC. Jurnal Indonesia: Manajemen Informatika dan Komunikasi, 4(3), 1704-1713.

[10] LAKSAMANA, A. R. (2021). IMPLEMENTASI DAN ANALISIS LOAD BALANCING PADA ROUTER PFSENSE. Universitas Sriwijaya, Palembang.

[11] Husufa, N., & Prihandi, I. (2022). Optimizing JMeter on performance testing using the bulk data method. Journal of Information Systems and Informatics, 4(2), 205-215.

[12] Permatasari, D. I. (2020). Pengujian aplikasi menggunakan metode load testing dengan apache jmeter pada sistem informasi pertanian. JUSTIN (Jurnal Sistem dan Teknologi Informasi), 8(1), 135-139.

[13] Huda, A. S., Prihantoro, C., & Pranata, M. (2023). Analisis Perbandingan QoS Pfsense dan Opnsense Menggunakan Metode Load Balancing. Media Informatika, 22(2), 87-95.