PENERAPAN *PROXY SERVER* PADA MIKROTIK UNTUK *BLOCKING* SITUS NEGATIF DI JARINGAN KOMPUTER

(Studi Kasus: Laboratorium Fakultas Ilmu Komputer
Universitas Ichsan Gorontalo)

Oleh:

RAHMAT RAFLI SULEMAN

T3120032

SKRIPSI

Untuk Memenuhi Salah Satu Syarat

Guna Memperoleh Gelar Sarjana

PROGRAM SARJANA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS ICHSAN GORONTALO
GORONTALO
2024

PENGESAHAN SKRIPSI

PENERAPAN PROXY SERVER PADA MIKROTIK UNTUK BLOCKING SITUS NEGATIF DI JARINGAN KOMPUTER

(Studi Kasus: Laboratorium Fakultas Ilmu Komputer Universitas Ichsan Gorontalo)

Oleh:
Rahmat Rafli Suleman
T3120032

Diperiksa oleh panitia ujian strata satu(S1)
Universitas Ichsan Gorontalo
Gorontalo, Juni 2024

1 Ketua penguji
Sudirman S.Panna, M.Kom .....

2 Anggota
Sunarto Taliki, M.Kom .....

3 Anggota
Serwin, M.Kom .....

4 Anggota
Irvan Abraham Salihi, M.Kom .....

5 Anggota
Warid Yunus, M.Kom .....

Mengetahui,

Dekan Fakultas Ilmu Komputer	Ketua Program studi
Irvan Abraham Salihi, M.Kom	**Sudirman S.Panna, M.Kom**
NIDN. 0928028101	**NIDN. 0924038205**

PERSETUJUAN SKRIPSI

PENERAPAN *PROXY SERVER* PADA MIKROTIK UNTUK *BLOCKING* SITUS NEGATIF DI JARINGAN KOMPUTER

(Studi Kasus: Laboratorium Fakultas Ilmu Komputer Universitas Ichsan Gorontalo)

Oleh:

Rahmat Rafli Suleman

T3120032

SKRIPSI

Untuk memenuhi salah satu syarat ujian guna memperoleh gelar sarjana dan telah disetuji oleh pembimbing

Gorontalo, Juni 2024

Pembimbing Utama	Pembimbing Pendamping
Irvan Abraham Salihi, M.Kom	**Warid Yunus, M.Kom**
NIDN. 0928028101	**NIDN. 0914059001**

PERNYATAAN SKRIPSI

Dengan ini saya menyatakan bahwa :

1. Karya tulis saya (Skripsi) ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (Sarjana) baik di Universitas Ichsan Gorontalo maupun di Perguruan Tinggi lainnya.
2. Karya Tulis ini adalah murni gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan dari Tim Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah dipublikasikan orang lain, kecuali secara tertulis dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidak benaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya tulis ini, serta sanksi lainnya sesuai dengan norma-norma yang berlaku di Universitas Ichsan Gorontalo.

Gorontalo, Juni 2024

Yang membuat peryataan

RAHMAT RAFLI SULEMAN

ABSTRAK

RAHMAT RAFLI SULEMAN. T3120032. PENERAPAN *PROXY SERVER* PADA MIKROTIK UNTUK *BLOCKING* SITUS NEGATIF DI JARINGAN KOMPUTER

Penelitian ini bertujuan untuk mengatasi masalah akses terhadap situs negatif di Laboratorium Fakultas Ilmu Komputer Universitas Ichsan Gorontalo melalui penerapan *proxy server* pada Mikrotik. Masalah yang dihadapi adalah banyaknya mahasiswa yang membuka situs dengan konten negatif, seperti *pornografi* dan perjudian, yang dapat mengganggu proses pembelajaran dan suasana akademis. Metode yang digunakan dalam penelitian ini meliputi beberapa tahapan: analisis kebutuhan sistem, perancangan dan konfigurasi router Mikrotik, pembuatan *proxy server* menggunakan perangkat lunak Squid, serta pengujian sistem yang telah diimplementasikan. Dalam tahap analisis, dilakukan identifikasi terhadap situs-situs negatif yang sering diakses dan kebutuhan perangkat keras dan perangkat lunak yang diperlukan. Selanjutnya, tahap implementasi mencakup konfigurasi Mikrotik untuk memblokir akses VPN dan penetapan *proxy server* untuk menyaring konten negatif. Pengujian sistem dilakukan dengan membandingkan kondisi sebelum dan sesudah penerapan konfigurasi, serta pengamatan terhadap efektivitas pemblokiran situs dan akses VPN. Hasil penelitian menunjukkan bahwa kombinasi antara Mikrotik dan proxy server terbukti efektif dalam memblokir situs negatif dan mengurangi akses melalui VPN hingga 80%. Hal ini disebabkan oleh kemampuan Mikrotik dalam mengidentifikasi dan memblokir IP address VPN yang sering digunakan, serta efisiensi *proxy server* dalam menyaring lalu lintas internet. Kesimpulan dari penelitian ini adalah bahwa penerapan konfigurasi tersebut dapat meningkatkan keamanan dan kenyamanan penggunaan internet di lingkungan pendidikan, serta memberikan acuan untuk pengembangan sistem keamanan jaringan yang lebih efektif di masa mendatang. Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam upaya pengelolaan akses internet yang aman dan terkendali di institusi pendidikan.

Kata Kunci: Proxy Server, Mikrotik, Situs Negatif, Jaringan Komputer, Blokir VPN

ABSTRACT

RAHMAT RAFLI SULEMAN. T3120032. THE APPLICATION OF THE PROXY SERVER ON MIKROTIK FOR BLOCKING NEGATIVE SITES ON THE COMPUTER NETWORKS

This research aims to overcome the problem of accessing negative sites in the Laboratory of the Faculty of Computer Science, Universitas Ichsan Gorontalo by applying a proxy server on Mikrotik. The problem faced is that many students open sites with negative content, such as pornography and gambling, which can disrupt the learning process and academic atmosphere. The method used in this research includes several stages, namely the system needs analysis, Mikrotik router's design and configuration, development of a proxy server using Squid software, and testing the implemented system. The analysis stage includes the identification of negative sites often accessed and the hardware and software required to carry out. Furthermore, the implementation stage includes configuring Mikrotik to block VPN access and establishing a proxy server to filter the negative contents. System testing is done by comparing the conditions before and after the implementation of the configuration, as well as observing the effectiveness of site blocking and VPN access. The results show that the combination of Mikrotik and proxy servers is proven to be effective in blocking negative sites and reducing access via VPN by 80%. It is due to Mikrotik's ability to identify and block frequently used VPN IP addresses and the efficiency of proxy servers in filtering internet traffic. The conclusion of this research is that the application of these configurations can improve the security and comfort of internet use in an educational environment and provide a reference for a more effective network security system development in the future. This research is expected to make a significant contribution to efforts to manage secure and controlled internet access in educational institutions.

Keywords: *Proxy Server, Mikrotik, negative sites, computer network, VPN blocking*

KATA PENGANTAR

Alhamdulillah, penulis dapat menyelesaikan skripsi ini dengan judul "Penerapan *Proxy server* Pada Mikrotik Untuk *Blocking* Situs Negatif Di Jaringan Komputer (Studi Kasus: Laboratorium Fakultas Ilmu Komputer Universitas Ichsan Gorontalo" untuk memenuhi salah satu syarat mendapatkan gelar sarja Program studi Teknik Informatika Fakultas Ilmu Komputer Universitas Ichsan Gorontalo.

Penulis menyadari sepenuhnya bahwa skripsi ini tidak mungkin terwujud tanpa bantuan dan dorongan dari berbagai pihak, baik bantuan moril maupun materil. Untuk itu, dengan segala keikhlasan dan kerendahan hati, penulis mengucapkan banyak terima kasih dan penghargaan yang setinggi – tingginya kepada:

1. Ibu Dr. Dra. Juriko Abdusamad, M.Si, selaku Ketua Yayasan Pengembangan Ilmu Pengatahuan dan Teknologi (YPIPT) Ichsan Gorontalo.
2. Bapak Dr. Abdul. Gaffar Latjokke, M.Si, selaku Rektor Universitas Ichsan Gorontalo.
3. Bapak Irvan Abraham Salihi M.Kom, selaku Dekan Fakultas Ilmu Komputer Universitas Ichsan Gorontalo, Sekaligus selaku pembimbing I yang telah memberikan bimbingan dan arahan kepada penulis.
4. Bapak Sudirman Melangi M.Kom, selaku Wakil Dekan 1 Bidang Akademik Fakultas Ilmu Komputer Universitas Ichsan Gorontal.
5. Ibu Irma Surya Kumala Idris, M.Kom, selaku Wakil Dekan II Bidang Administrasi Umum dan Keuangan Fakultas Ilmu Komputer Universitas Ichsan Gorontalo.
6. Bapak Sudirman S. Panna, M.Kom, selaku Ketua Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Ichsan Gorontalo,
7. Bapak Warid Yunus, M.Kom, Selaku Pembimbing Pendamping yang telah Membimbing Penulis Selama Penyusunan Skripsi Ini,
8. Bapak dan Ibu Dosen Universitas Ichsan Gorontalo yang telah mendidik dan mengajarkan berbagai disIPlin ilmu kepada penulis,

9. Untuk panutan penulis, Bapak Suleman. Meskipun beliau hanya sempat menyelesaikan pendidikannya di Sekolah Dasar, beliau dengan penuh cinta dan ketulusan telah mendidik saya. Beliau selalu memberi semangat dan motivasi tanpa henti, hingga akhirnya saya dapat meraih gelar sarjana.
10. Ibu, pintu surgaku, terima kasih sebesar-besarnya penulis haturkan atas segala bentuk bantuan, semangat, dan doa yang telah Ibu berikan selama ini. Terima kasih atas nasihat yang selalu mengalir meskipun terkadang pikiran kita tidak selalu sejalan. Terima kasih atas kesabaran dan kebesaran hati Ibu dalam menghadapi penulis. Ibu adalah penguat dan pengingat paling hebat. Terima kasih telah menjadi tempatku untuk pulang, Ibu.
11. Teruntuk Kakak. Saya ingin menyampaikan rasa terima kasih yang sebesar-besarnya kepada kakak tercinta. Kakak adalah sosok yang selalu memberikan dukungan, dorongan, dan inspirasi dalam setiap langkah yang saya ambil. Terima kasih atas kesabaran, kasih sayang, dan bimbingan yang tak pernah putus. Kakak telah menjadi teladan bagi saya dalam mengejar impian dan menghadapi segala tantangan dengan hati yang kuat dan penuh semangat.
12. Adikku, Rasya. Terima kasih sudah ikut serta dalam proses penulis menempuh pendidikan sarjana selama ini, terima kasih atas semangat dan doa yang diberikan kepada penulis. Tumbuhlah menjadi versi paling hebat dari penulis.
13. Teruntuk seseorang yang belum dapat dituliskan namanya dengan jelas disini, namun sudah tertulis jelas di lauhul mahfudz untuk penulis, Terima kasih telah menjadi sumber motivasi penulis dalam menyelesaikan tulisan ini sebagai salah satu upaya memantaskan diri. Karena penulis percaya bahwa sesuatu yang ditakdirkan menjadi milik kita akan menuju pada kita bagaimanapun caranya.
14. Seluruh rekan-rekan seperjuangan yang berperan banyak memberikan pengalaman dan pembelajaran selama dibangku perkuliahan ini.
15. Almamater Universitas Ichsan Gorontalo, yang telah menjadi saksi penulis dalam berproses selama ini.
16. Dan yang terakhir, terima kasih kepada diri penulis. Kamu luar biasa karena masih bisa berdiri tegap menghadapi segala liku hidup, meskipun terkadang

rasa jenuh dan keinginan untuk berhenti datang menghampiri. Teruntuk diriku, kamu keren, kamu kuat, dan kamu hebat. Teruslah berjuang, Rafli.

Semoga Allah, SWT melimpahkan balasan atas jasa-jasa mereka kepada kamu. Penulis menyadari sepenuhnya bahwa apa yang telah dicapai ini masih jauh dari kesempurnaan dan masih banyak terdapat kekurangan. Oleh karena itu, penulis sangat mengharapkan adanya kritik dan saran yang konstruktif. Akhirnya penulis berharap semoga hasil yang telah dicapai ini dapat bermanfaat bagi kita semua, Aamiin.

Gorontalo, Juni 2024

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Kemajuan pesat dalam teknologi komunikasi saat ini sejalan dengan perkembangan zaman. Namun, di tengah peluang emas ini, terdapat oknum-oknum yang tidak bertanggung jawab yang memanfaatkannya untuk tujuan bisnis *ilegal*, seperti menyebarkan konten *pornografi*, melakukan penipuan, perdagangan narkoba, menjual senjata api, dan aktivitas negatif lainnya. Penggunaan terhadap konten semacam itu oleh anak-anak maupun orang dewasa berpotensi memberikan dampak merugikan pada masyarakat secara keseluruhan. Kehadiran informasi menjadi sangat penting untuk berbagai aspek dan salah satunya di bidang pendidikan [1].

Pemanfaatan internet dalam dunia pendidikan telah membawa dampak positif yang signifikan, namun juga tidak bisa diabaikan potensi dampak negatifnya. Internet, yang memberikan informasi dalam skala global, membuka pintu bagi kemungkinan akses terhadap konten yang merugikan seperti informasi yang tidak akurat, penyebaran berita palsu, pornografi, dan kekerasan. Terutama di kalangan pelajar yang belum memiliki keterampilan literasi digital yang memadai, mengidentifikasi konten yang bermanfaat dan yang sebaiknya dihindari dapat menjadi sulit. Dampak dari paparan konten negatif ini dapat meliputi penurunan nilai-nilai moral, gangguan emosional, dan gangguan pada proses belajar [1].

Dalam proses pembelajaran sehari-hari. Fakultas Ilmu Komputer di Universitas Ichsan Gorontalo menggunakan Laboratorium Komputer untuk mengakses informasi dari internet yang disediakan oleh Fakultas untuk proses pembelajaran. Dengan koneksi jaringan internet yang mudah diakses oleh mahasiswa, mereka dapat dengan bebas melakukan kegiatan browsing situs untuk pembelajaran, membuka situs pemutar audio dan video, serta mengakses situs-situs sosial. Namun, terdapat tantangan ketika beberapa mahasiswa cenderung membuka

situs terlarang atau situs dengan konten negatif, yang dapat membawa dampak negatif pada proses pembelajaran dan suasana akademis di laboratorium komputer tersebut.

Berdasarkan informasi yang tercatat dalam laporan Kementrian Komunikasi dan Informasi (KOMINFO), dari januari hingga oktober 2017, Konten berunsur *pornografi* menempati peringkat teratas dengan 16.902 kasus pemblokiran, diikuti oleh konten berisi SARA/Kebencian dengan jumlah 15.818 kasus. Selanjutnya, konten berita palsu (*hoax*) mencatatkan 7.633 kasus, diikuti oleh konten perjudian sebanyak 4.319 kasus, penipuan online sebanyak 2.457 kasus, dan kasus terkait *radikalisme/terorisme* juga sebanyak 2.457. Sementara itu, konten yang melanggar nilai-nilai sosial budaya menempati urutan terendah dengan 134 kasus, diikuti oleh konten yang memfasilitasi akses terhadap konten negatif sebanyak 54 kasus, dan konten kekerasan/*pornografi* anak hanya mencatatkan 36 kasus. Dan data pemblokiran terakhir di tahun 2022 menunjukan bahwa konten *pornografi* masih menempati peringkat teratas dengan jumlah 1.142.010 pemblokiran dan di ikuti oleh perjudian online dengan jumlah 540.410 pemblokiran [2].

Kementerian Komunikasi dan Informatika (KOMINFO) berdasarkan data diatas sebelumnya telah melakukan upaya untuk memerangi situs web yang dianggap merugikan di Indonesia. Namun, meskipun upaya tersebut telah dilakukan, masih belum sepenuhnya berhasil karena pengguna internet, terutama di Indonesia, masih dapat mengakses situs web tersebut melalui berbagai layanan VPN yang populer saat ini, seperti Browsec VPN. Untuk mengatasi masalah ini, tindakan tambahan akan dilakukan peneliti dengan berkonsentrasi pada pemblokiran IP address VPN, yang sering digunakan untuk permintaan *proxy*. Dengan demikian, tindakan ini memungkinkan berhasil membatasi sekitar 80% akses melalui VPN. Kombinasi kedua metode ini memungkinkan berhasil memblokir akses VPN pengguna.

Selain itu, untuk menyelesaikan masalah tersebut, peneliti di Laboratorium Fakultas Ilmu Komputer akan membuat peraturan untuk memblokir situs yang akan

meminimalkan akses ke situs yang tidak diinginkan. Untuk mengatasi masalah ini, peneliti akan melakukan konfigurasi pada perangkat router mikrotik dan membuat *proxy server*. Tindakan pengamanan yang kuat pada router mikrotik dan *proxy server* diperlukan untuk mencegah akses ke situs tersebut. Salah satu metode yang dapat digunakan adalah dengan menggunakan *proxy server* untuk memblokir situs.

Dengan menggabungkan penggunaan mikrotik dan *proxy server* ini dapat menciptakan lapisan keamanan yang efektif untuk mengelola akses internet. *Proxy server* berfungsi sebagai server yang dapat dikonfigurasi untuk memblokir lalu lintas, sedangkan mikrotik digunakan untuk memblokir akses VPN yang digunakan. Kombinasi ini memungkinkan penggunaan internet yang fleksibel sambil menghindari konten yang tidak diinginkan dan berbahaya.

Penelitian sebelumnya yang dilakukan oleh (Riski Nur Arrahman & Adhika Pramita Widyassri). Dengan judul "***Implementasi Proxy server* Sebagai *Content Filtering* Menggunakan Linux Debian Buster**". Bahwa sistem *proxy server* ini sangat membantu dalam memblokir website yang tidak berguna untuk digunakan di institusi pendidikan dan berisi konten negatif. Selain memblokir website, sistem *proxy server* ini juga dapat memfilter URL dan kata kunci (keyword) saat menggunakan browser untuk menemukan konten negatif. Hasil analisis deskripttif pengujian fungsional menunjukkan bahwa sistem *proxy server* dapat memblokir situs web dan memiliki tingkat kelayakan 100%. Dengan demikian, sistem *proxy server* dapat digunakan secara umum. Salah satu opsi untuk mendapatkan akses internet yang aman dan positif adalah sistem *proxy server* ini.[3].

Berdasarkan Latar Belakang diatas, maka peneliti tertarik untuk melakukan penelitian yang di beri judul **"PENERAPAN *PROXY SERVER* PADA MIKROTIK UNTUK *BLOCKING* SITUS NEGATIF DI JARINGAN KOMPUTER"**.

1.2. Identifikasi Masalah

Berdasarkan penjelasan tentang latar belakang permasalahan yang telah disebutkan, dapat disimpulkan bahwa permasalahannya terletak pada belum adanya

pembangunan sistem penghalang situs-situs negatif di Laboratorium Fakultas Ilmu Komputer Universitas Ichsan Gorontalo, Perlunya kebijakan jaringan yang efektif dan solusi teknologi seperti *proxy server* dan mikrotik untuk membatasi situs negatif.

1.3. Rumusan Masalah

Berdasarkan identifikasi masalah diatas, maka permasalahannya dapat disimpulkan sebagai berikut:

1. Bagaimana merancang sistem *Proxy server* Pada Mikrotik Untuk *Blocking* Situs Negatif di Laboratorium Fakultas Ilmu Komputer?
2. Bagaimana kinerja dari sistem *Proxy server* Pada Mikrotik Untuk *Blocking* Situs Negatif di Laboratorium Fakultas Ilmu Komputer?

1.4. Tujuan Penelitian

Berdasarkan Rumusan permasalahan diatas, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Merancang sistem *Proxy server* Pada Mikrotik Untuk *Blocking* Situs Negatif di Laboratorium Fakultas Ilmu Komputer.
2. Mengevaluasi kinerja dari sistem *Proxy server* Pada Mikrotik Untuk *Blocking* Situs Negatif di Laboratorium Fakultas Ilmu Komputer.

1.5. Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat, berupa:

1. Dalam konteks teoritis, memberikan kontribusi pada kemajuan ilmu pengetahuan dan teknologi, terutama di bidang ilmu komputer.
2. Dalam konteks praktis, kontribusi pemikiran, karya, serta bahan pertimbangan atau meningkatkan teknologi dan terutama dalam penggunaan perangkat mikrotik sebagai alat untuk mem*filter* situs negatif. Dengan mengImplementasikan solusi teknologi seperti *Proxy server* untuk mengendalikan dan membatasi akses ke situs-situs yang merugikan.

BAB II
LANDASAN TEORI

2.1. Tinjauan Studi

Berikut beberapa penelitian terdahulu yang berkaitan dengan *Proxy server*, yaitu:

Tabel 2. 1. Tinjauan Studi

NO	PENELITI	JUDUL	HASIL
1	Santoso & Setiawan Assegaff.[4]	Analisis Dan Rancang Bangun Sistem Layanan *Proxy server* Pada SMK Unggul Sakti Jambi. (2017)	Hasil penelitian menunjukkan bahwa Sistem layanan *proxy server* ini sangat membantu dalam memblokir situs web yang dianggap tidak sesuai untuk digunakan di bidang pendidikan.
2	Nana Suryana & Ddi Dwi Saputra [5]	Implementasi Penggunaan *Firewall*dan *Proxy server*untuk Membatasi Hak Akses Internet (2018)	Dengan kecepatan internet yang cepat, situs-situs yang tidak berguna dan berbahaya diblokir untuk mahasiswa dan guru. Ini meningkatkan keamanan jaringan.
3	Rosihan Aminuddin & Moch. Apriyadi HS [6]	*Implementasi Proxy server* Dengan Menggunakan Squid Di Cv. Nusantara Geotech Makassar	Konfigurasi yang dilakukan membantu CV. Nusantara Geotech, terutama dalam pembagian bandwidth, hak akses, dan melarang akses ke situs yang tidak diperlukan, seperti situs Facebook, pornografi, dan situs seks.2. *Cache* lokal Squid pada *proxy*

NO	PENELITI	JUDUL	HASIL
			server mempercepat akses halaman dengan menyimpan layanan data pada *proxy server*, sehingga mengurangi waktu akses user.

2.2. Tinjauan Pustaka

2.2.1. Jaringan Komputer

Menurut pengertian yang ada, jaringan komputer merujuk pada sekumpulan interkoneksi antara beberapa komputer. Dalam istilah yang lebih sederhana, jaringan komputer adalah gabungan beberapa komputer dan perangkat seperti router dan switch yang saling terhubung melalui berbagai jenis media, seperti media kabel atau nirkabel. Melalui media ini, informasi berupa data dapat mengalir dari satu komputer ke komputer lainnya atau bahkan dari satu komputer ke perangkat lain. Hasilnya, komputer-komputer yang saling terhubung ini dapat saling bertukar data dengan lancar. [7].

Jaringan Komputer mempunyai beberapa keunggulan dibandingkan dengan komputer yang berdiri sendiri (*stand-alone*) yaitu:

1. Jaringan memaksimalkan sumber daya manajemen yang lebih baik, seperti pengguna / *user* bisa saling berbagi layanan printer dengan kualitas tinggi, selain itu untuk penggunaan lisensi pada *software* jaringan lebih murah dari pada menggunakan lisensi tunggal dalam penggunaan jumlah yang sama.
2. Jaringan yang menggunakan internet membantu menjaga informasi agar tetap andal dan mutakhir, serta jika ada sistem penyimpanan terpusat yang dikelola dengan baik memungkinkan banyak pengguna yang bisa mengakses data dari banyak lokasi berbeda dan membatasi akses ke data saat sedang diproses.

3. Jaringan memudahkan dan mempercepat proses sharing data (berbagi file). Saat ini transfer data menggunakan jaringan dengan kecepatan tinggi lebih cepat dibanding dengan sarana tranfer data lainnya seperti menggunakan media flashdisk, disket, cd atau lainnya.
4. Jaringan membuat komunikasi antar kelompok dalam bekerja menjadi lebih efisien. Seperti pengiriman surat elektronik (*email*) merupakan kebutuhan dengan menggunakan sistem jaringan. Selain itu sebagian besar sistem jaringan digunakan untuk pemantauan proyek, *meeting online*, kerja *group* untuk membantu pekerja agar lebih produktif

Agar Sistem kerja jaringan komputer bisa mencapai tujuan, maka setiap bagian dari jaringan komputer akan melakukan permintaan (*request*) dan layanan (*service*). Adapun pihak yang melakukan permintaan disebut sebagai *client* dan pihak memberikan layanan disebut *server*. Pada jaringan komputer konsep ini disebut sebagai sistem *Client-Server*, dan digunakan pada hampir smua aplikasi jaringan komputer.

Berikut merupakan beberapa *type* jaringan berdasarkan skala areanya :.

1. PAN (*Personal Area Network*)

   PAN adalah jaringan komputer yang terdiri dari: Transmisi antara beberapa komputer atau antara komputer dan perangkat non-komputer seperti printer, mesin faks, telepon seluler, PDA, telepon seluler. Jangkauan PAN sangat terbatas, sekitar 9-10 meter. Semacam PAN dapat dibangun menggunakan teknologi kabel dan nirkabel Internet. Teknologi kawat PAN dapat terhubung melalui USB dan *FireWire*. *Wireless* PAN dapat dihubungkan melalui teknologi Bluetooth, WiFi dan inframerah.
2. LAN (*Local Area Network*)

   LAN adalah jaringan komputer yang hanya mencakup satu area kecil. seperti jaringan komputer kampus, gedung, kantor, rumah, sekolah atau kurang. Saat ini, sebagian besar jaringan area lokal didasarkan pada Teknologi IEEE 802.3 *Ethernet* menggunakan perangkat *switching* yang Kecepatan transfer data adalah 10, 100 atau 1000 Mbps.

3. MAN (*Metropolitan Area Network*)

   MAN Merupakan Jaringan dengan skala jarak jangkau antar kota, dengan teknologi yang digunakan oleh MAN mirip dengan LAN. itu hanya daerah lebih besar dan lebih banyak komputer yang terhubung ke jaringan MAN dibandingkan dengan jaringan area lokal. MAN adalah jaringan komputer Mencakup area berukuran kota atau kombinasi dari beberapa LAN yang terhubung menjadi jaringan yang besar. Jaringan metro dapat digabungkan Jaringan komputer beberapa sekolah atau beberapa kampus. MAN bisa di DiImplementasikan pada jaringan kabel dan nirkabel.

4. WAN (*Wide Area Network*)

   WAN adalah jaringan komputer yang mencakup area yang luas besar (lebar). Misalnya, jaringan komputer antar wilayah, kota atau kota bahkan sebuah negara, atau dapat didefinisikan sebagai jaringan komputer Diperlukan router dan saluran komunikasi umum. WAN digunakan untuk menghubungkan satu jaringan lokal ke jaringan lokal lainnya, sehingga pengguna atau komputer di lokasi yang sama dapat berkomunikasi dengan pengguna dan komputer di lokasi lain

2.2.2. Topologi Jaringan

Topologi mengacu pada susunan atau pola bagaimana perangkat seperti komputer, printer, dan lainnya dihubungkan dalam suatu jaringan. Ini mencakup aturan atau pola hubungan antara terminal-terminal dalam sistem jaringan komputer, yang berdampak pada kinerja jaringan. Ada beberapa jenis topologi, termasuk topologi bus, topologi ring, dan topologi star [8].

1. Topologi Bus

   Topologi bus adalah jenis di mana semua terminal terhubung ke satu jalur komunikasi yang memiliki ujung-ujungnya ditutup. Terdapat jalur utama yang menghubungkan komputer-komputer klien dengan jarak tertentu. Topologi ini termasuk pasif karena komputer hanya mendengarkan data melalui kartu antarmuka jaringan (NIC) mereka. Jika ada data untuk

mereka, maka akan diterima. Untuk mengirim data, komputer harus menunggu sampai jalur tidak sibuk.

2. Topologi Ring

Topologi ring memiliki komputer yang terhubung dalam lingkaran melalui kabel. Informasi mengalir dalam satu arah dari satu komputer ke komputer berikutnya dalam lingkaran. Setiap komputer meneruskan data ke komputer berikutnya.

3. Topologi star

Topologi star melibatkan komputer-komputer yang terhubung ke satu titik pusat seperti hub atau switch melalui kabel terpisah. Pusat ini mengatur komunikasi data dan mengalirkannya dari komputer ke stasiun tujuan. Kelebihannya adalah mudah untuk diperluas dengan menambahkan kabel baru antara komputer dan pusat.

2.2.3. Keamanan Jaringan

Keamanan jaringan merupakan salah satu Prinsip penting dalam melindungi sistem jaringan komputer dari penggunaan yang tidak sah. Tujuan utamanya adalah untuk menghindari akses sistem jaringan oleh orang yang tidak memiliki izin. Untuk menjaga keamanan ini, berbagai langkah pencegahan harus dilakukan untuk mencegah serangan, penyusupan, dan pemindaian. Dengan demikian, peneliti jaringan dapat menjaga kerahasiaan dan integritas data serta menjaga kinerja sistem jaringan tetap optimal. [9]

Tujuan utama dari keamanan jaringan komputer adalah untuk mengantisipasi risiko-risiko yang timbul dari ancaman fisik maupun logis terhadap jaringan komputer. Ancaman-ancaman tersebut dapat mengganggu kelancaran operasi di dalam jaringan komputer.

Beberapa aspek penting dalam menjaga keamanan jaringan adalah sebagai berikut:

1. Kerahasiaan (Confidentiality):

   Upaya untuk melindungi informasi dari akses oleh pihak yang tidak berhak. Ini mencakup melindungi data pribadi serta menjaga kerahasiaan informasi yang diberikan kepada pihak lain untuk tujuan tertentu. Contoh ancaman yang mengancam kerahasiaan termasuk pembacaan email oleh pihak yang tidak berwenang dan pelanggaran privasi data pelanggan. Solusi yang umum digunakan adalah kriptografi, yaitu teknik enkripsi dan dekripsi.

2. Integritas (Integrity):

   Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa izin dari pemilik informasi. Ancaman seperti Trojan, virus, dan perubahan konten email oleh pihak tidak berwenang dapat mengancam integritas data. Solusi yang umum digunakan adalah enkripsi dan tanda tangan digital.

3. Ketersediaan (Availability):

   Ketersediaan berkaitan dengan memastikan bahwa informasi dapat diakses sesuai kebutuhan. Ancaman seperti serangan Denial of Service (DoS) dapat mengakibatkan layanan menjadi tidak tersedia. Solusi untuk mengatasi masalah ini termasuk penggunaan spam blocker dan pembatasan koneksi.

4. Non-Repudiasi (Non-Repudiation):

   Prinsip ini mencegah individu untuk membantah transaksi atau tindakan yang telah dilakukan. Penggunaan tanda tangan digital dan teknologi enkripsi dapat mendukung Prinsip ini, tetapi juga memerlukan dukungan hukum agar sah secara hukum.

5. Autentikasi (Authentication):

   Autentikasi berkaitan dengan memastikan bahwa orang yang mengakses atau memberikan informasi adalah individu yang sah. Teknologi

seperti tanda air, tanda tangan digital, kata sandi, dan teknologi biometrik digunakan untuk memvalidasi autentikasi.

6. Kontrol Akses (Access Control):

   Aspek ini terkait dengan mengelola hak akses terhadap informasi. Sistem kontrol akses memastikan bahwa hanya individu yang memiliki otoritas yang dapat mengakses informasi tertentu. Ini sering melibatkan penggunaan kombinasi ID Pengguna dan kata sandi.

7. Akuntabilitas (Accountability):

   Akuntabilitas mengharuskan setiap aktivitas pengguna direkam dalam jaringan. Ini membantu dalam menentukan identitas dan aktivitas individu jika terjadi pelanggaran kebijakan. Akuntabilitas juga berperan dalam mencegah perilaku ilegal. Namun, sistem akuntabilitas harus memperhatikan risiko identitas palsu.

Dalam praktiknya, sistem keamanan jaringan sering menggabungkan beberapa aspek di atas untuk menciptakan lapisan perlindungan yang komprehensif."

2.3. Mikrotik

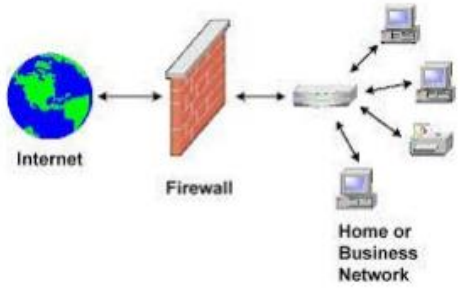
Mikrotik adalah router yang menggunakan proses perutean untuk mengirimkan paket data ke tujuannya melalui jaringan atau Internet. Router berfungsi untuk menghubungkan beberapa jaringan, mengirimkan data dari satu jaringan ke jaringan lain. Router Mikrotik adalah perangkat jaringan komputer yang berjalan pada sistem operasi Mikrotik RouterOS dan menggunakan kernel Linux. Router mikrotik memiliki banyak fitur, seperti manajemen bandwidth, *firewall* dengan access point untuk operasi dan akses, dan peneliti GUI Winbox untuk routing dan akses remote..

2.4. *Firewall*

Firewall juga dikenal sebagai "tembok api", adalah sebuah sistem yang melindungi keamanan jaringan dari orang yang tidak bertanggung jawab yang mencoba merusak, mengubah, atau mendistribusikan data, termasuk data sensitif

perusahaan, atau mencegah semua ancaman yang masuk ke jaringan. *Firewall* menggunakan aturan khusus untuk beroperasi. Rule ini nantinya yang akan menentukan tindakan yang dilakukan oleh router terhadap Paket yang melintasi router. Setiap peraturan memiliki kondisi dan prosedur yang harus diikuti.

Sebagian besar, penentuan kemampuan dan strategi peneliti jaringan akan menentukan seberapa mudah jaringan ditembus. Sementara kebijakan keamanan didasarkan pada keseimbangan antara fasilitas yang disediakan dan konsekuensi keamanan, *firewall* berfungsi sebagai alat untuk menerapkan kebijakan keamanan. Semakin ketat kebijakan keamanan, semakin kompleks konfigurasi layanan informasi atau semakin sedikit fasilitas yang tersedia di jaringan. Sebaliknya, dengan lebih banyak fasilitas yang dapat diakses atau Karena kebijakan keamanan sistem yang lemah, konfigurasi yang sederhana memungkinkan orang luar untuk masuk ke sistem.



Gambar 2. 1. Konsep Firewall Pada Jaringan [13]

Firewall sebenarnya adalah dinding yang dapat memisahkan ruang. Ini memastikan bahwa api di satu ruangan tidak menyebar ke ruangan lain. Namun, pada kenyataannya, *firewall* internet berfungsi sebagai benteng, melindungi terhadap serangan dari luar..

Fungsi dari *firewall* yaitu Membatasi paket yang memasuki jaringan *internal*, Membatasi paket yang meninggalkan jaringan *internal* serta Mencegah penyerang mendekati sistem pertahanan.

Firewall harus mengizinkan lalu lintas data keluar dan masuk dalam jaringan. *Firewall* dapat menjadi kombinasi yang tepat dari router, server, dan perangkat lunak pendamping. *Firewall* adalah suatu metode/sistem/mekanisme yang berlaku

pada perangkat keras, perangkat lunak, atau sistem itu sendiri, melindungi beberapa atau semua hubungan/aktivitas segmen dalam jaringan pribadi dengan jaringan *eksternal*, menyaring, membatasi, atau menyangkalnya. melakukan. Dalam jangkauan. Segmen dapat berupa workstation, server, router, atau jaringan area lokal (LAN).

2.4.1. Manfaat *Firewall*

Adapun Manfaat *firewall* pada jaringan komputer adalah sebagai berikut :

1. Perlindungan informasi sensitif dan berharga yang diabaikan. Misalnya, lalu lintas FTP (File Transfer Protocol) dari jaringan komputer dikendalikan oleh *firewall*. Ini dilakukan untuk mencegah pengguna di jaringan secara sengaja atau tidak sengaja mengirim file sensitif ke pengguna lain. digunakan sebagai *filter* untuk mencegah lalu lintas tertentu mengalir ke subnet jarin/gan Anda. Ini mencegah pengguna berbagi file atau bermain game melalui jaringan.
2. Manfaat *firewall* lainnya adalah untuk memodifikasi paket data yang datang di di *firewall*. Proses ini disebut *Network* Address Translation (NAT).

Adapun cara kerja dari sistem keamanan *firewall* yaitu :

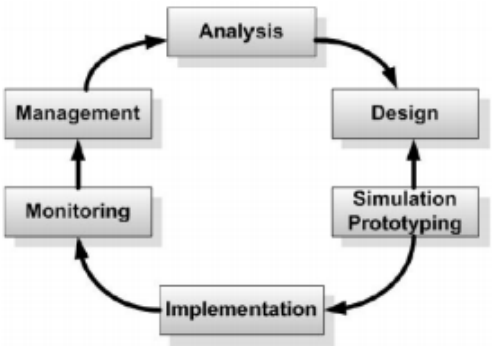
1. Mentutp port Kecuali untuk port tertentu yang harus tetap terbuka. *Firewall* komputer mencari port terbuka yang dapat diakses oleh peretas yang mencoba masuk ke jaringan komputer Anda, sehingga mereka bertindak sebagai pertahanan garis depan untuk mencegah segala macam peretasan ke jaringan Anda.
2. *Firewall* adalah perangkat keras atau perangkat lunak, tetapi *firewall* bekerja paling baik ketika kedua jenis perangkat ini digabungkan. *Firewall* tidak hanya membatasi akses ke jaringan komputer, tetapi juga memungkinkan akses jarak jauh ke jaringan pribadi melalui otentikasi dan sertifikat keamanan login.

3. *Firewall* merupaka perangkat keras dapat dibeli sebagai produk yang berdiri sendiri, tetapi biasanya ditemukan pada router broadband dan memerlukan pengaturan pada perangkat ini untuk mengakses jaringan komputer.

Cara kerja *firewall* lainnya adalah menyaring lalu lintas jaringan berdasarkan alamat IP, nomor port, dan protokol. *Firewall* dapat menyaring data dengan mengidentifikasi isi pesan itu sendiri.

2.4.2. *Network* Development Life Cycle (NDLC)

Network Development Life Cycle (NDLC) Sebuah model penting dari siklus hidup pengembangan jaringan (NDLC), proses desain jaringan komputer. NDLC sendiri merupakan siklus proses dari langkah-langkah mekanisme yang diperlukan untuk proses desain untuk mengembangkan atau mengembangkan sistem jaringan komputer [10].



Gambar 2. 2. Urutan Kerja NDLC [12]

Berikut adalah urutan kerja dari metode *Network* Developement Life Cycle.

1. Analisis

   Ini adalah langkah pertama dalam menganalisis yaitu kebutuhan yang dibutuhkan, masalah yang di hadapi, kebutuhan pengguna, dan topologi atau analisis jaringan yang ada.

2. Desain

   Pada tahap ini dilakukan Implementasi infrastruktur jaringan komputer dan semua lokasi di area produksi, gudang, dan ruang server yang menampung semua peralatan utama peralatan jaringan komputer

telah terhubung. Pada fase ini dibuat gambar topologi untuk memperkirakan kebutuhan yang ada.

3. Simulasi

Pada tahap ini, simulator dipilih untuk digunakan. Ini adalah model elemen jaringan skala besar dengan berbagai fungsi jaringan yang ditentukan dalam konfigurasinya. Ada beberapa simulasi yang memang juga menggunakan cara pengujian langsung.

4. Implementation

Pada tahapan ini akan memakan waktu lebih lama dari tahapan sebelumnya. Dalam Implementasi ini akan menerapkan semua yang telah direncanakan dan didesign sebelumnya. Implementasi merupakan tahapan yang sangat menentukan dari berhasil atau gagalnya project yang akan dibangun dan ditahap inilah Team Work akan diuji dilapangan untuk menyelesaikan masalah teknis dan non teknis..

5. Monitoring

Setelah Implementasi, fase pemantauan merupakan fase penting untuk memungkinkan komputer dan jaringan komunikasi berfungsi sesuai dengan kebutuhan dan tujuan desain awal.

6. Management

Pada tahap manajemen atau regulasi, salah satu perhatian khusus adalah masalah kebijakan. Kebijakan harus dibuat atau diatur oleh pihak-pihak terkait agar dapat menciptakan atau mengatur sistem yang dibangun dan dijalankan dengan baik oleh bisnis.

2.5. *Proxy server*

Proxy server berfungsi sebagai perantara antara komputer pengguna dan server tujuan di internet. Ketika pengguna menggunakan *proxy server* untuk mengakses internet, permintaan mereka akan diarahkan terlebih dahulu ke *proxy server*, yang kemudian meneruskannya ke server tujuan. Setelah menerima tanggapan dari server tujuan, *proxy server* akan meneruskannya kembali ke pengguna.

Beberapa fungsi dan keuntungan utama *proxy server* adalah sebagai berikut:

1. Keamanan:

   Sebagai cara untuk meningkatkan keamanan dan privasi pengguna, *proxy server* dapat menyembunyikan alamat IP pengguna. Ini dapat digunakan untuk menghentikan seseorang dari mengakses situs web yang berpotensi berbahaya atau tidak diinginkan.
2. Kontrol akses:

   Administrasi jaringan memiliki kemampuan untuk mengawasi dan mengontrol aktivitas internet pengguna; mereka dapat membatasi akses ke konten tertentu, atau mengizinkan akses hanya ke situs yang disetujui.
3. Cachhing:

   Proxy server memiliki kemampuan untuk menyimpan salinan sementara, juga dikenal sebagai *cache*, dari halaman web yang sering diakses. Ini dapat mempercepat akses dan mengurangi penggunaan bandwidth.
4. Transparansi:

   Karena *proxy server* menyembunyikan alamat IP asli pengguna, pengguna dapat mengakses internet secara anonim.
5. *Filtering* konten:

   Ada kemampuan untuk memfilter konten menggunakan URL atau kata kunci untuk mencegah pengguna mengakses konten yang tidak pantas atau ilegal.

Organisasi dan lembaga pendidikan dapat menggunakan *proxy server* untuk melindungi jaringan mereka, mengontrol akses internet, dan memastikan penggunaan yang lebih aman dan sesuai dengan peraturan.[12]

2.6. Software Terkait

2.6.1. Ubuntu

Ubuntu adalah sistem operasi turunan dari distro Linux jenis Debian yang tidak stabil (sid). Tujuan dari proyek ini adalah untuk menciptakan sistem operasi dan paket aplikasinya yang gratis dan open source. Prinsip utama Ubuntu adalah

untuk tetap gratis (gratis selamanya) dan tidak ada tambahan untuk versi enterprise edition.

Berbagai kelebihan Ubuntu dibandingkan dengan distribusi Debian termasuk:

1. Pemaketan (Packaging)
2. Pemilihan aplikasi yang luas (Application choice)
3. Siklus pembaharuan yang rutin (Updates)
4. Dikenal karena stabilitas dan kualitasnya, terutama di sisi server (Stability and quality).

2.6.2. Putty

PuTTY, yang disebut sebagai "Transkripsi Suara", adalah aplikasi terminal emulator yang sangat berguna untuk berbagai kegiatan komunikasi dan transfer data. Aplikasi ini, yang dibuat oleh Simon Tatham pada tahun 1999, hanya dirancang untuk platform Microsoft. Namun, seiring dengan kemajuan teknologi dan popularitas yang terus meningkat, PuTTY telah berkembang menjadi salah satu alat utama dalam bidang komputasi dan jaringan. PuTTY tidak hanya dapat berfungsi sebagai terminal emulator, tetapi juga dapat digunakan sebagai konsol serial dan alat untuk mentransfer file melalui jaringan. PuTTY memiliki banyak keuntungan, salah satunya adalah statusnya sebagai perangkat lunak open source, yang memungkinkan pengguna mengakses dan mengubah kode sumber sesuai kebutuhan.

2.6.3. WinBox

Winbox adalah program yang dikembangkan oleh MikroTik untuk membantu pengguna mengelola perangkat jaringan mereka yang berbasis RouterOS. RouterOS sendiri adalah sistem operasi yang digunakan pada router dan perangkat jaringan MikroTik lainnya.

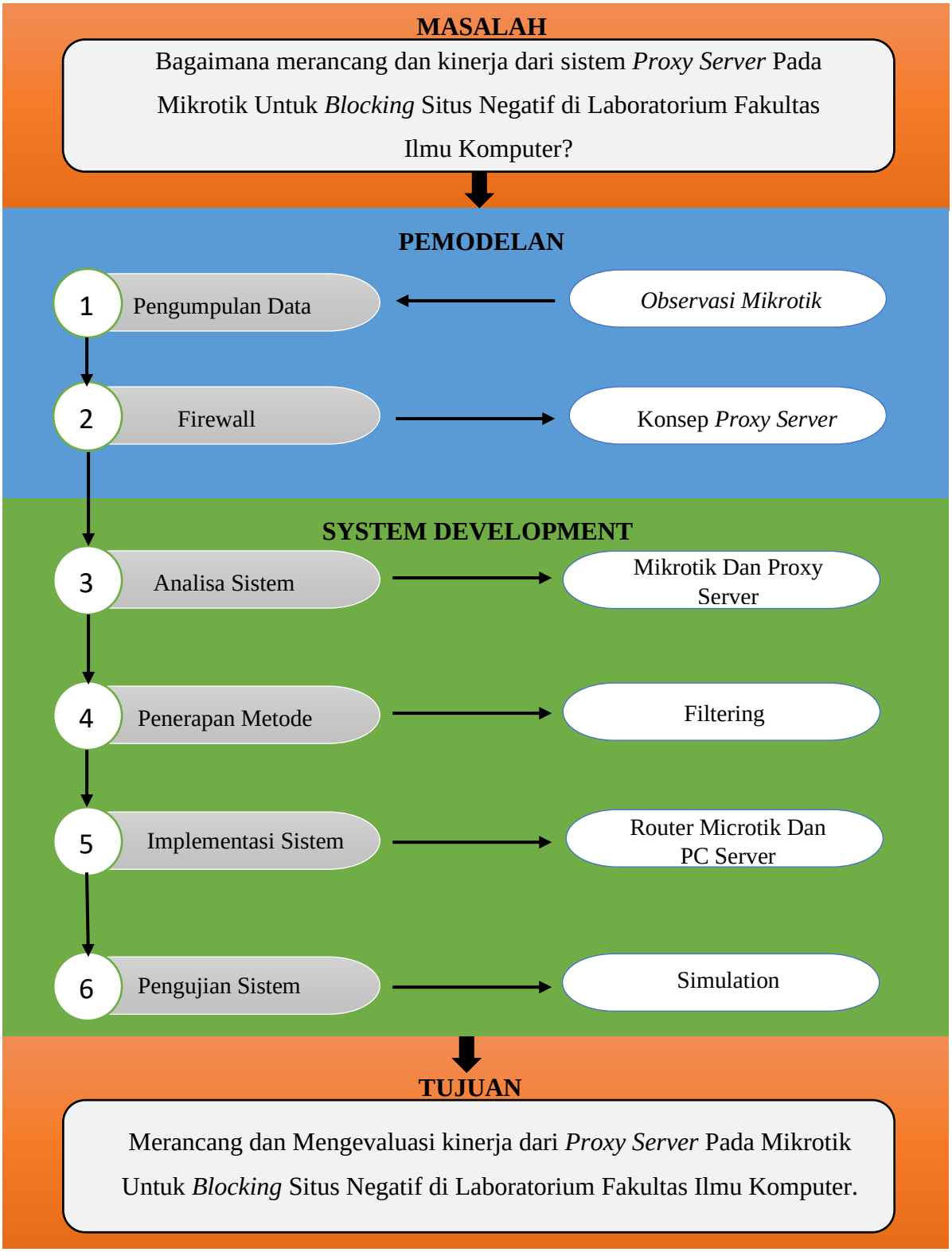
Beberapa fitur utama Winbox adalah sebagai berikut:

1. Antarmuka Pengguna Grafis (GUI): Winbox menawarkan antarmuka pengguna grafis yang sederhana dan mudah digunakan yang

memungkinkan pengguna mengubah perangkat MikroTik tanpa perlu mempelajari baris perintah.

2. Manajemen Konfigurasi: Pengguna dapat dengan mudah mengatur konfigurasi perangkat jaringan seperti manajemen pengguna, routing, *firewall*, dan antarmuka jaringan dengan Winbox.
3. Manajemen Pengguna: Winbox memungkinkan pengaturan keamanan yang lebih baik dengan mengatur pengguna, grup pengguna, hak akses, dan banyak lagi.
4. Monitoring Jaringan: Pengguna dapat melihat kinerja jaringan

2.7. Kerangka Pemikiran



Gambar 2. 3. Kerangka Pikir

BAB III
METODE PENELITIAN

3. 1 Jenis, Metode, Subjek, Objek, Waktu, dan Lokasi Penelitian

Penelitian ini menggunakan metode penelitian studi kasus. Berdasarkan konteks dan landasan konseptual yang telah diuraikan sebelumnya, fokus penelitian ini ditujukan pada Penerapan *Filtering* dengan *Proxy server* dan perangkat router mikrotik. Rentang penyusunan skripsi ini mencakup periode mulai dari 1 april 2023 hingga 12 Juni 2024, dan pelaksanaannya direalisasikan di lingkungan Laboratorium Fakultas Ilmu Komputer Universitas Ichsan Gorontalo. Dalam lingkup waktu dan lokasi tersebut, penelitian ini akan secara mendalam mengeksplorasi Implementasi serta efektivitas mekanisme *Filtering* dengan *Proxy server* yang diaplikasikan pada infrastruktur jaringan menggunakan PC komputer.

3. 2 Pengumpulan Data

3.2.1. Data Primer

Data Primer berasal dari informasi yang dikumpulkan melalui observasi langsung pada router Mikrotik di Laboratorium Fakultas Ilmu Komputer Universitas Ichsan Gorontalo dan wawancara dengan karyawan di bagian jaringan. Metode ini memungkinkan pengumpulan data secara langsung dari sumbernya, yaitu staf yang berpengalaman dalam manajemen jaringan dan perangkat Mikrotik. Wawancara mendalam tentang aspek-aspek teknis dan konfigurasi jaringan, dan melihat perangkat router Mikrotik secara langsung memberikan pemahaman praktis tentang bagaimana jaringan laboratorium diatur dan dikelola. Oleh karena itu, data awal ini berfungsi sebagai landasan utama yang asli untuk dianalisis dalam penelitian yang dilakukan.

3.2.2. Data Sekunder

Data Sekunder yaitu Data diperoleh dengan cara mengumpulkan data atau keterangan melalui berbagai macam referensi seperti hasil penelitian terdahulu, buku, jurnal yang terkait dari internet yang berhubungan dengan *Proxy server*.

3. 3 Desain Sistem

Untuk melindungi jaringan komputer dari situs web negatif, sistem yang direncanakan menggabungkan MikroTik Router dan *proxy server*. Komputer klien terhubung ke router MikroTik sebagai gateway, yang kemudian mengarahkan lalu lintas HTTP dan HTTPS ke *proxy server*. mikrotik berfungsi sebagai perantara antara klien dan internet, dan konfigurasi dilakukan untuk memastikan bahwa lalu lintas HTTP dan HTTPS diblokir dengan benar. Untuk memastikan kinerja dan keamanan sistem, uji coba dan pemeliharaan dilakukan, yang mencakup pemantauan kinerja jaringan dan pembaruan berkala terhadap daftar situs yang dilarang. Akibatnya, sistem ini menjaga pengguna dari konten yang tidak diinginkan atau berbahaya sambil mengontrol lalu lintas internet di jaringan.

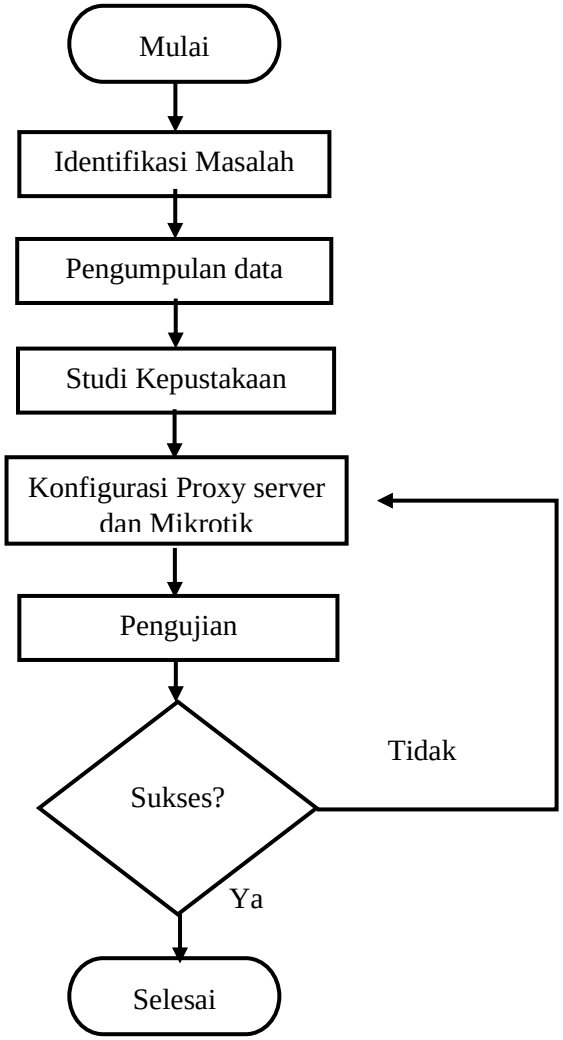
3. 4 Analisis sistem

3.4.1. *Proxy server*

Proxy server berfungsi sebagai perantara antara pengguna internet dan sumber daya online. Dalam pengendalian akses terhadap situs-situs negatif, penggunaan *proxy server* diterapkan dalam lingkup jaringan komputer. *Proxy server* memantau dan mengontrol lalu lintas internet dengan menerapkan daftar hitam (*blacklist*) untuk situs-situs yang diblokir. Selain itu, *proxy server* dilengkapi dengan fitur filter konten untuk deteksi dan pemblokiran situs berbahaya, pornografi, atau kekerasan. sementara enkripsi lalu lintas dan autentikasi pengguna meningkatkan keamanan dan privasi. Peneliti *proxy server* sebagai kontrol akses terhadap situs negatif menjadi topik penting dalam penelitian keamanan jaringan dan manajemen akses internet.

.

3. 5 Pemodelan



Gambar 3. 1. Alir Penelitian

3. 6 Pengujian Sistem

Pengujian sistem dalam penelitian ini difokuskan pada evaluasi efisiensi penerapan *proxy server* dan router MikroTik. Proses pengujian melibatkan pemantauan kinerja *proxy server* dalam memblokir situs web berbahaya, serta melakukan filtrasi terhadap lalu lintas internet. Evaluasi juga mencakup penilaian kemampuan *Proxy server* dan MikroTik dalam mengatur akses internet di lingkungan Fakultas Ilmu Komputer, Universitas Ichsan Gorontalo. Aspek yang di uji tingkat keberhasilan pemblokiran situs web yang telah diidentifikasi sebagai potensial merugikan. Selain itu, pengujian ini juga mengevaluasi sejauh mana kombinasi kedua *proxy* tersebut dapat mengurangi penggunaan VPN yang

umumnya digunakan untuk mengakses konten terlarang. Dengan harapan bahwa hasil pengujian dapat memberikan pemahaman mendalam terkait performa dan keamanan sistem *proxy server* yang diImplementasikan.

BAB IV
HASIL PENELITIAN

4.1. Pengumpulan Data

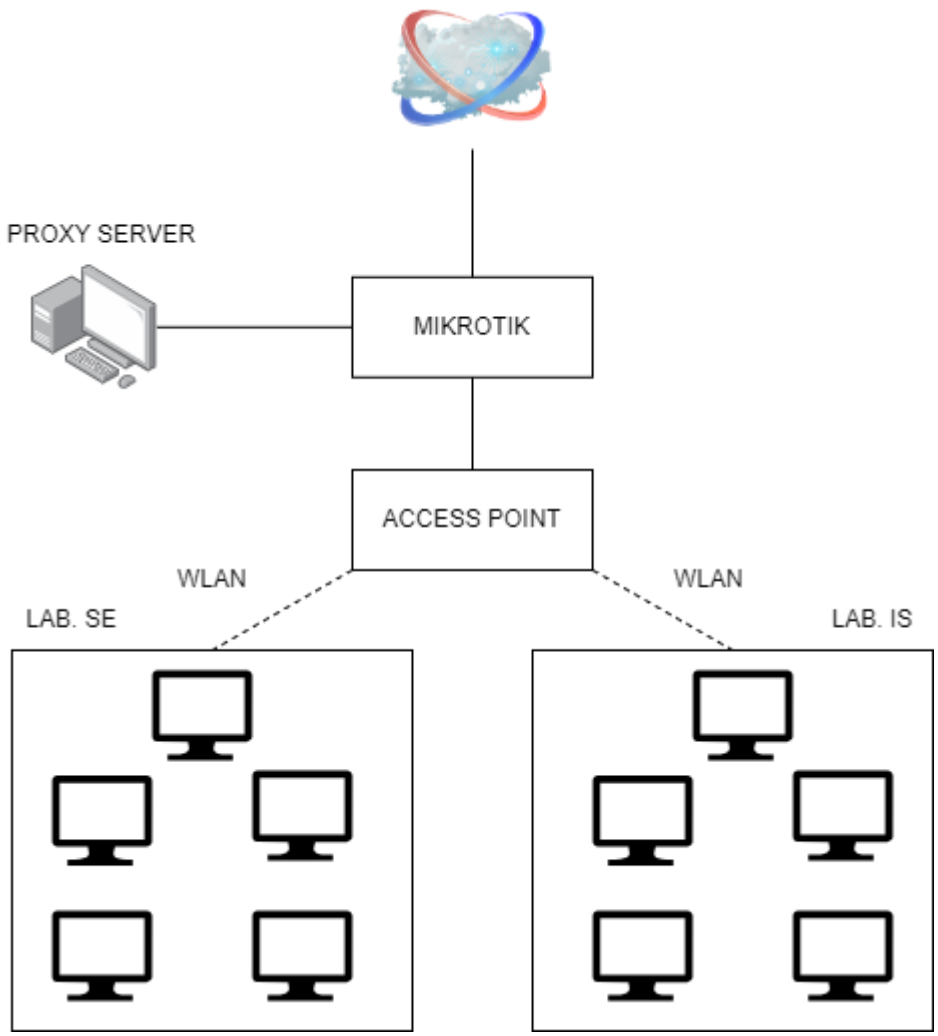
Dalam proses pengumpulan data, peneliti membuat daftar situs web yang dianggap negatif berdasarkan klasifikasi yang diberikan oleh lembaga yang berwenang, seperti Kementerian Komunikasi dan Informatika, serta literatur yang relevan. Daftar ini mencakup situs web berbahaya dan situs web dengan konten tidak pantas. Seperti yang dapat dilihat pada tabel dibawah ini.

Tabel 4. 1. Daftar Situs Negatif

NO	NAMA SITUS	KATEGORI
1	xn*x.com	Situs Dewasa
2	xh**mster.com	Situs Dewasa
3	x.com	Social Media
4	Porn*ub.com	Situs Dewasa
5	win*tarenyala.com	Judi Online
6	*lsoporn.com	Situs Dewasa
7	Maha168he*a.com	Judi Online

Untuk memblokir daftar situs negatif yang telah disusun, peneliti menggunakan MikroTik RouterOS dan *Squid Proxy*.Ada pun gambar yang tertera di bawah, tergambar sebuah konfigurasi topologi jaringan laboratorium. Tahap awalnya akan melibatkan penggunaan Internet sebagai sarana uji coba untuk *proxy server* setelah sistem telah sepenuhnya siap. Proses ini kemudian akan terhubung melalui router MikroTik yang berfungsi sebagai pengatur *proxy server*. Selanjutnya, router MikroTik akan terhubung dengan sebuah access point yang bertugas sebagai pemancar sinyal. Di sisi lain, terdapat pengguna yang akan terkoneksi ke hotspot yang telah dikonfigurasi sebelumnya. Dengan demikian, melalui rangkaian ini, terbentuklah sebuah infrastruktur jaringan yang

memungkinkan akses Internet yang diatur melalui *proxy server* untuk beberapa pengguna secara bersamaan. Adapun topologi yang di rencanakan sebagai berikut.



Gambar 4. 1. Rancangan Topologi Jaringan

4.2. Analisa dan Implementasi Sistem

4.2.1. Analisa Kebutuhan Sistem

Sebelum langkah konfigurasi dan penerapan metode penyaringan situs web, langkah awal yang dilakukan adalah menganalisis kebutuhan terkait perangkat keras dan perangkat lunak yang akan digunakan dalam penelitian. Dalam tahap ini, fokus diberikan pada pemahaman yang mendalam tentang spesifikasi perangkat keras yang diperlukan, seperti komputer atau server, serta perangkat lunak yang

dibutuhkan untuk mengImplementasikan metode penyaringan. Analisis ini bertujuan untuk memastikan bahwa semua aspek teknis yang diperlukan tersedia dan dapat mendukung efektifitas dari proses konfigurasi dan penerapan metode yang akan dilakukan.:

Tabel 4. 2. Kebutuhan Sistem

Hardware	Jumlah Unit	Keterangan
Leptop	1	Konfigurasi Mikrotik
Router Mikrotik	1	*Firewall*
Pc	1	Server Proxy
Access Point	1	Pemancar Sinyal
Software	**Versi**	**Keterangan**
Ubuntu	20.04.6	OS Server
Putty	0.80	Remote Server
Winbox	-	Tools Konfigurasi Mikrotik

4.2.2. Analisa Sistem Kerja Server Proxy

Sebagai server proxy, Squid akan digunakan yang akan berfungsi sebagai penyaring permintaan klien sebelum meneruskannya ke server tujuan. Penggunaan Daftar Kontrol Akses (ACL) merupakan suatu konfigurasi yang dapat diatur oleh peneliti guna mengatur lalu lintas situs web. ACL memungkinkan penerapan daftar hitam untuk menentukan situs web mana yang diizinkan atau diblokir. Melalui pendekatan ini, Squid menjadi sebuah alat yang sangat efektif dalam menghambat akses ke situs web yang tidak diinginkan atau berpotensi negatif.

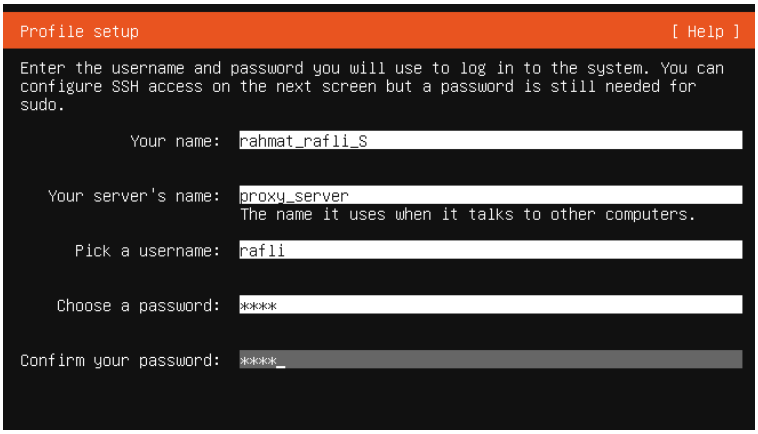
4.2.3. Implementasi Sistem Kerja *Proxy server*

1. Penginstalan Ubuntu

Implementasi sistem kerja *proxy server* dimulai dengan langkah pertama yakni pemasangan sistem operasi Ubuntu. Proses ini melibatkan penggunaan media penyimpanan berupa flashdisk yang telah dimuat dengan file sistem operasi Ubuntu

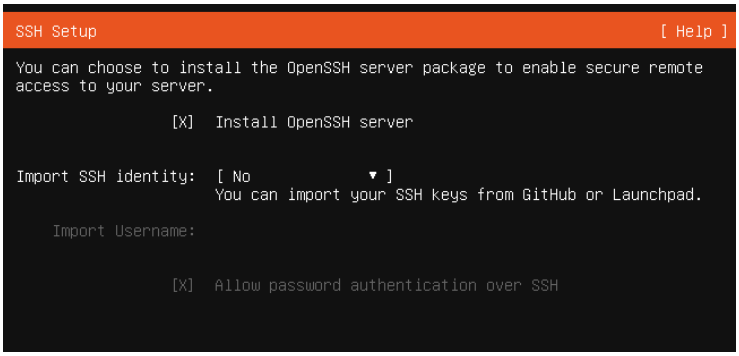
yang diperlukan, serta komputer yang ditujukan untuk penggunaan sebagai server, pada tahap pengistallan perlu dIPerhatikan beberapa tahap penting seperti berikut.

Perlu dIPerhatikan pada tahap ini dilakukan pembuatan akun peneliti untuk server proxy. Proses ini adalah langkah krusial dalam pengelolaan dan pengaturan server proxy, yang berfungsi sebagai perantara antara peneliti dan sumber daya jaringan. Peneliti memiliki hak istimewa untuk mengkonfigurasi, memonitor, dan memelihara fungsi-fungsi server proxy guna memastikan operasional yang optimal serta keamanan jaringan. Sebagaimana ditunjukkan dalam gambar berikut.



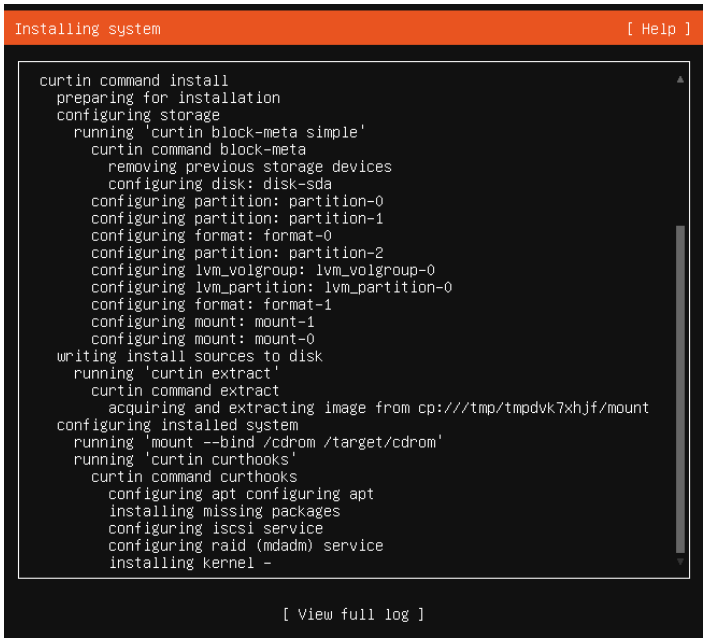
Gambar 4. 2. Konfigurasi Akun Peneliti

Selanjutnya, Dengan peneliti menginstal OpenSSH Server, peneliti dapat mengontrol dan mengelola server dari jarak jauh secara aman. Implementasi SSH juga memungkinkan akses yang lebih fleksibel dan efisien terhadap sumber daya server, mendukung operasi pemeliharaan, konfigurasi, dan pemecahan masalah yang dapat dilakukan tanpa kehadiran fisik di lokasi server.



Gambar 4. 3. Penginstallan Open SSH Server

Dan pada tahap akhir dari proses instalasi, peneliti melakukan langkah penting yaitu reboot sistem. Tindakan ini bertujuan untuk memuat ulang semua konfigurasi dan pengaturan yang telah diimplementasikan selama instalasi. Setelah sistem dihidupkan kembali, komputer akan beroperasi dengan konfigurasi terbaru, memastikan bahwa semua perubahan dan penyesuaian telah diterapkan dengan benar. Pada titik ini, sistem operasi Linux server sudah sepenuhnya siap untuk digunakan. Peneliti dapat mengakses server secara langsung melalui antarmuka lokal atau, lebih sering, melalui koneksi jarak jauh menggunakan Secure Shell (SSH).

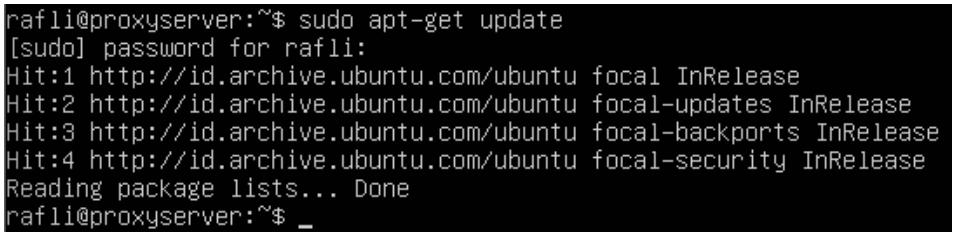


Gambar 4. 4. Reboot Sistem

2. Penginstalan Squid

Pertama-tama, peneliti melakukan proses peningkatan sistem operasi Ubuntu dengan pelaksanaan perintah "sudo apt-get update". Hal ini bertujuan untuk melakukan pembaruan terhadap daftar paket yang tersedia dalam repositori yang telah diinstal pada sistem. Repositori tersebut merupakan sumber paket perangkat lunak yang dikelola secara terpusat oleh Ubuntu. Dengan melakukan pembaruan ini, informasi terkini mengenai paket-paket perangkat lunak yang tersedia dapat diakses. Dalam konteks ini, pembaruan tersebut sangat penting untuk memastikan

bahwa sistem mendapatkan versi terbaru dari perangkat lunak yang diperlukan serta memperbaiki kerentanan keamanan yang mungkin ada.



Gambar 4. 5. Update Sistem

Tahapan ini juga bertujuan untuk memastikan kehandalan sistem operasi dengan memperbarui daftar paket yang sesuai dengan konfigurasi dan preferensi peneliti. Proses ini merupakan langkah awal yang krusial dalam menjaga kinerja dan keamanan sistem operasi Ubuntu.

Untuk melanjutkan proses penginstalan, peneliti mengetikan perintah yang tertera di bawah ini. Perintah tersebut akan mengarahkan sistem untuk melakukan instalasi paket perangkat lunak yang dibutuhkan untuk menjalankan program *proxy server* Squid. Perintah yang dimaksud adalah sebagai berikut:

Gambar 4. 6. Penginstallan Squid

Dengan mengetikkan perintah di atas, sistem akan secara otomatis menginisiasi proses pengunduhan dan pemasangan paket yang diperlukan untuk konfigurasi dan pengoperasian Squid. Prosedur ini mempertimbangkan kerangka kerja manajemen paket yang telah diimplementasikan dalam distribusi Ubuntu, memungkinkan pengguna untuk dengan mudah mengelola dan memperbarui perangkat lunak yang terinstal.

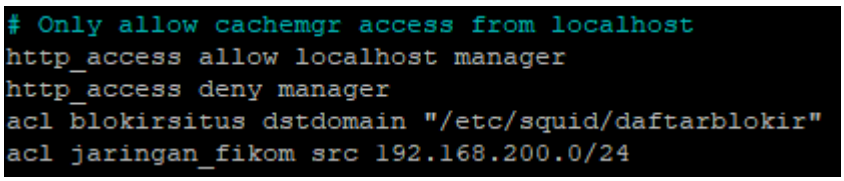
3. Konfigurasi Squid

Setelah proses instalasi squid selesai dilakukan pada server, langkah berikutnya yang dilakukan peneliti melakukan konfigurasi. Hal ini dilakukan dengan membuka file konfigurasi squid yang terletak pada direktori

"/etc/squid/squid.conf". Untuk membuka dan mengubah file konfigurasi tersebut, perintah yang digunakan adalah "sudo nano /etc/squid/squid.conf":

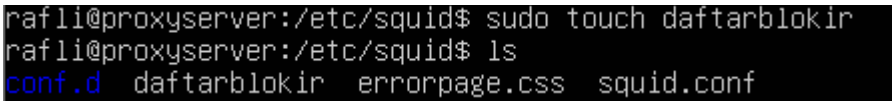
Gambar 4. 7. Membuka File Konfigurasi Squid

Selanjutnya, peneliti menambahkan ACL (Access Control List) dengan nama "blokirsitus", yang diarahkan ke direktori "/etc/squid/daftarblokir", memiliki peran dalam regulasi akses terhadap situs web tertentu. ACL ini difungsikan untuk mengendalikan akses terhadap *domain* yang telah peneliti cantumkan dalam daftar blokir. Implementasi ACL ini mengarah pada pemblokiran setiap permintaan klien yang menuju *domain-domain* yang tercantum dalam daftar blokir, sejalan dengan kebijakan yang telah ditetapkan oleh peneliti. Selanjutnya, penambahan ACL dengan nama "jaringan_fikom" dan alamat jaringan 192.168.200.0/24 memiliki fungsi spesifik dalam manajemen lalu lintas jaringan. Tujuan dari ACL ini adalah untuk mengatur akses ke server proxy dari jaringan_fikom, sebagaimana ditunjukkan dalam gambar berikut:



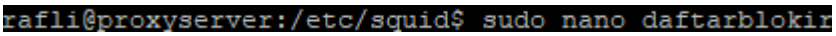
Gambar 4. 8. Konfigurasi Access Control List(ACL)

Setelah peneliti mengaktifan Access Control List (ACL), langkah pertama yang dilakukan oleh penelti menginisiasi pembuatan sebuah direktori yang akan berperan sebagai wadah penyimpanan daftar blokir. Dengan perintah (*sudo touch* daftar blokir) Selanjutnya, peneliti memvalidasi dengan memeriksa keberadaan direktori yang baru saja dibuat menggunakan perintah (ls), sebuah langkah praktis yang memastikan integritas dan konsistensi dalam proses tersebut, sebagaimana yang didemonstrasikan dalam ilustrasi gambar yang ada dibawah ini.



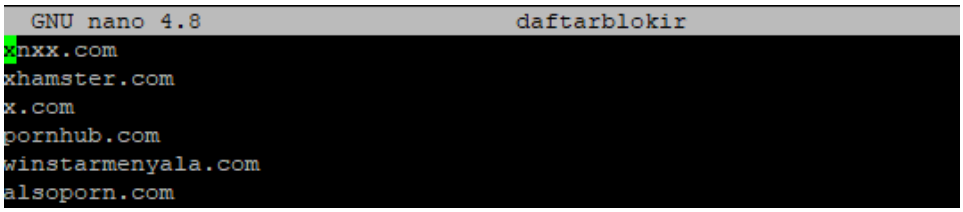
Gambar 4. 9. Membuat Direktori daftar blokir

Langkah selanjutnya dalam proses pengelolaan pengaturan blokir akses internet adalah dengan mengimplementasikan perintah "sudo nano daftarblokir" pada terminal. Perintah ini dapat membuat peneliti bisa mengakses mode pengeditan teks menggunakan editor nano yang berbasis terminal. Dalam proses ini, peneliti dapat menambahkan entri-entri yang merepresentasikan situs-situs yang akan diblokir dari akses internet.



Gambar 4. 10. Mengakses Directori Daftar Blokir

Langkah berikutnya dalam proses ini peneliti menetapkan daftar situs yang akan diblokir berdasarkan kriteria *domain* situs. Hal ini dilakukan dengan menggunakan algoritma yang mengidentifikasi kata kunci yang terkait dengan *domain* situs yang ingin diblokir. Dalam menentukan daftar blokir, aspek-aspek seperti relevansi konten, potensi risiko, dan kepentingan pengguna jaringan diambil sebagai pertimbangan utama. Metode ini memberikan landasan ilmiah yang kuat untuk memastikan bahwa pembatasan akses terhadap konten yang tidak diinginkan dilakukan secara tepat dan efisien, sesuai dengan kebutuhan dan kebijakan yang telah ditetapkan.



Gambar 4. 11. Penetapan Situs Blokir

Setelah menyelesaikan proses pengisian daftar situs yang akan diblokir, langkah selanjutnya peneliti melakukan reboot layanan Squid agar perubahan yang telah diimplementasikan dapat diterapkan dengan efektif. Dengan melakukan reboot, sistem akan melakukan proses restart yang menyeluruh, sehingga memungkinkan konfigurasi baru yang telah diterapkan dapat berjalan secara optimal. Selain itu, rebooting juga dapat membantu dalam memperbarui *cache* dan memastikan konsistensi penggunaan sumber daya jaringan yang efisien. Dengan

demikian ini dapat memperkuat kontrol terhadap akses ke situs yang diblokir dan memastikan kelancaran operasionalitas sistem jaringan secara keseluruhan.

```
rafli@proxyserver:/etc/squid$ /etc/init.d/squid3 restart
```

Gambar 4. 12. Restart *Squid Proxy*

Penyempurnaan infrastruktur jaringan peneliti membuat pengaturan izin akses pada *proxy server*, seperti yang dilakukan pada squid dengan menambahkan fitur (http_access deny blockirsitus). Tindakan ini memungkinkan server untuk secara otomatis memblokir akses ke situs-situs yang telah ditentukan peneliti sebelumnya dalam daftar blokir, mencegah akses yang tidak diinginkan atau berpotensi membahayakan dari pengguna internet. Di samping itu, pemberian izin server untuk beroperasi dalam jaringan yang telah peneliti tetapkan, seperti (jaringan_fikom), untuk memastikan keamanan dan fungsionalitas yang optimal. Seperti yang ada pada gambar di bawah ini.

```
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost
http_access deny blokirsitus
http_access allow jaringan_fikom
```

Gambar 4. 13. Konfigurasi access proxy

Langkah terakhir dalam proses ini peneliti melakukan reload dengan perintah "sudo systemctl reload squid.service". Perintah ini bertujuan untuk proses reload pada layanan *proxy server* Squid. Tindakan ini memungkinkan untuk pembaruan konfigurasi tanpa mengganggu ketersediaan layanan tersebut. Dengan menerapkan perintah tersebut, Squid secara efektif memuat ulang konfigurasi yang baru tanpa harus menghentikan dan memulai kembali layanan, yang dapat menyebabkan gangguan pada ketersediaan layanan.

```
rafli@proxyserver:~$ sudo systemctl reload squid.service
```

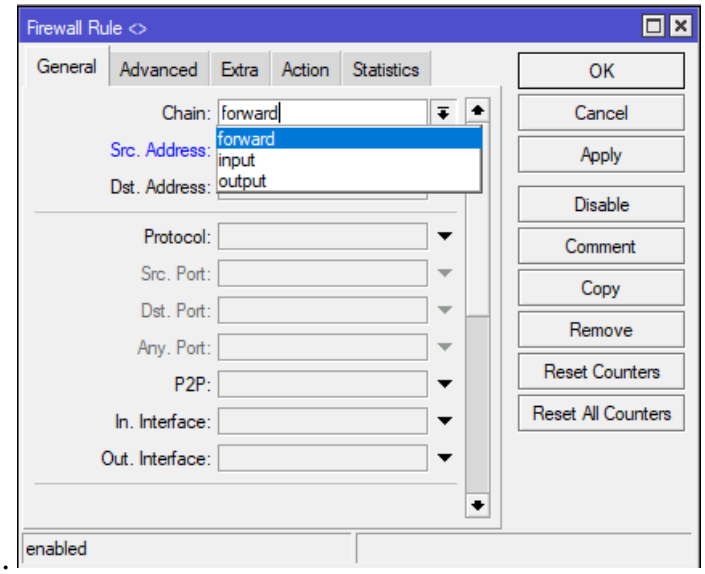
Gambar 4. 14. Reload *Squid Proxy*

4.2.4. Implementasi Sistem Kerja Mikrotik

Setelah melakukan konfigurasi pada *proxy server*, dampaknya terlihat pada aksesibilitas situs-situs yang terdaftar dalam daftar blokir, dimana mereka tidak dapat diakses. Namun, tantangan muncul ketika pengguna internet menggunakan layanan *Virtual Private Network* (VPN), yang memungkinkan akses terhadap situs-situs yang sebelumnya terhalang oleh pengaturan proxy. Untuk menangani permasalahan ini, langkah tambahan diperlukan dalam bentuk konfigurasi pada perangkat jaringan, seperti router MikroTik, yang melibatkan penerapan aturan *firewall* yang tepat. Aturan *firewall* ini dirancang untuk memblokir akses VPN. Dengan pendekatan ini, jaringan dapat mengoptimalkan kontrol akses dengan memperhitungkan perangkat lunak dan layanan tambahan yang dapat digunakan oleh pengguna untuk mengelabui pembatasan akses yang ada.

1. Implementasi Filter Rules

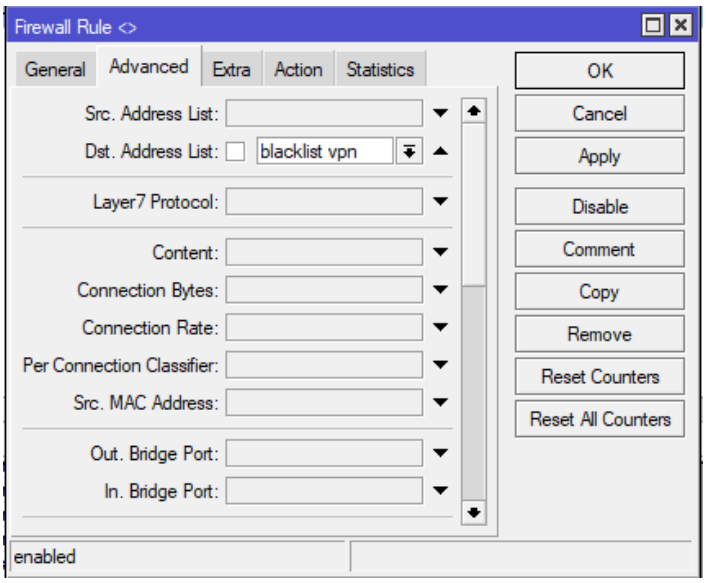
Implementasi sistem pemblokiran dengan filter rules adalah suatu proses yang diperlukan dalam rangka memastikan keamanan dan keteraturan akses jaringan internet. Langkah awal dalam implementasi ini melibatkan penandaan port masuk yang akan difilter untuk mengatur akses jaringan internet melalui aturan *firewall*. Melalui proses ini, sistem Mikrotik dapat mengidentifikasi secara tepat IP mana yang harus diblokir, sebagaimana ditunjukkan dalam gambar yang terlampir dibawah ini



Gambar 4. 15. Konfigurasi Port

Gambar di atas menunjukan pada parameter chain peneliti memilih forward karena untuk memproses trafik paket data yang hanya melewati router. Ini termasuk trafik dari jaringan public ke *local* atau sebaliknya dari jaringan *local* ke public, seperti yang terjadi saat kita browsing di internet melalui laptop. *Firewall* dapat mengatur trafik dari laptop ke internet melalui chain forward.

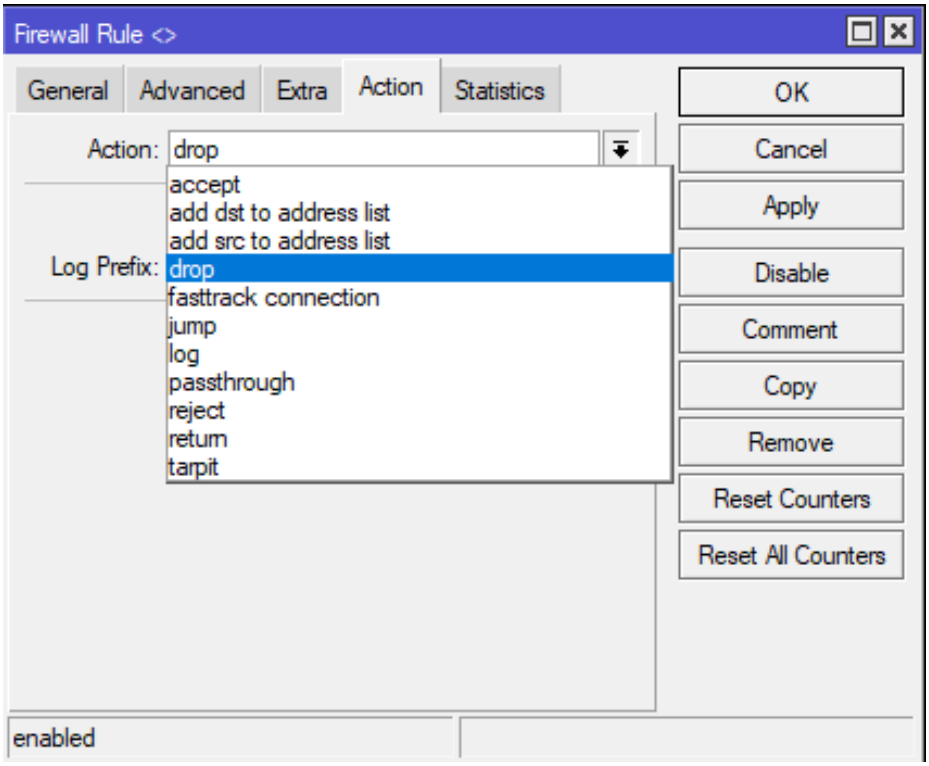
Langkah berikutnya adalah pemberian sebuah label oleh peneliti pada Daftar Alamat Tujuan dengan menggunakan istilah "*blacklist* VPN", sesuai dengan tampilan yang dijelaskan dalam ilustrasi di bawah ini.



Gambar 4. 16. Konfigurasi Dst. *Address list*

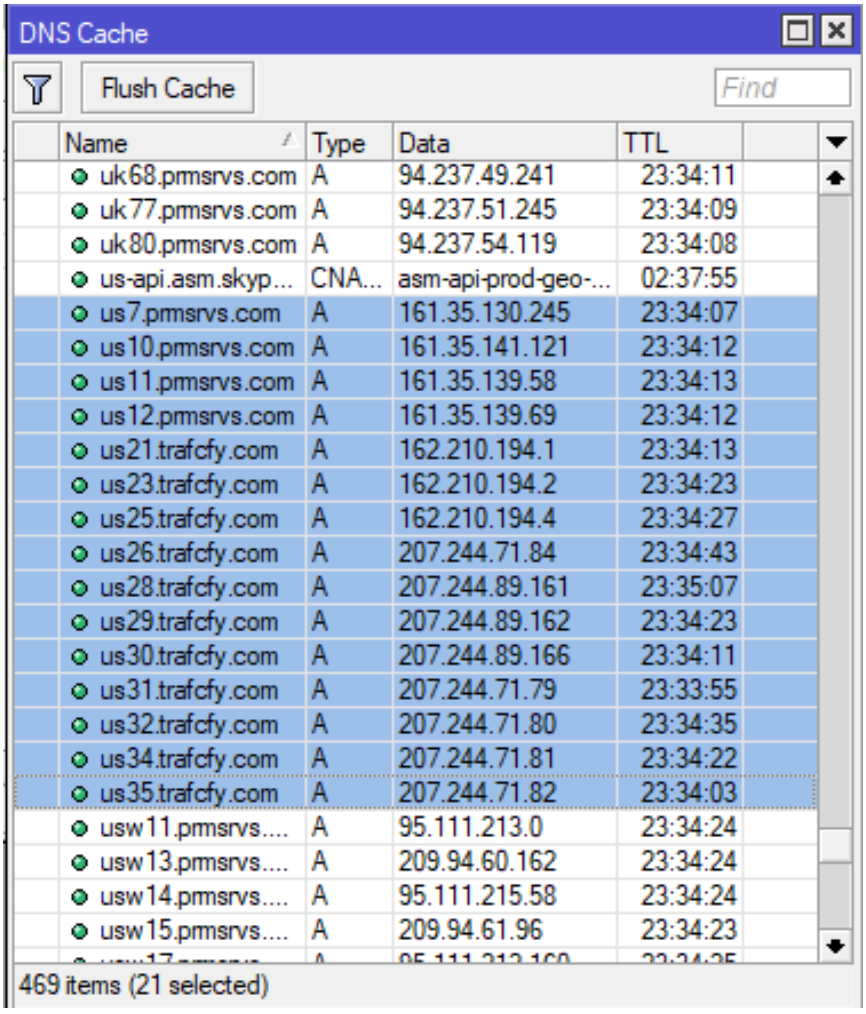
Penggunaan label yang sesuai dalam pengidentifikasian daftar ini memungkinkan peneliti untuk secara sistematis membedakannya dari entitas serupa serta mengelompokkannya dalam kategori yang relevan dengan infrastruktur VPN. Tindakan ini tidak hanya membantu dalam organisasi yang efisien tetapi juga memperkuat pengawasan dan pengendalian terhadap sumber daya yang terlibat.

Tahap berikutnya pada gambar di bawah ini peneliti mengimplementasi tindakan lanjutan yang disebut sebagai "*action drop*". Tujuan dari langkah ini adalah untuk memastikan bahwa ketika alamat IP VPN yang telah didaftarkan pada daftar alamat (*address list*) ditangkap oleh perangkat MikroTik, maka akan secara otomatis ditolak atau diblokir.



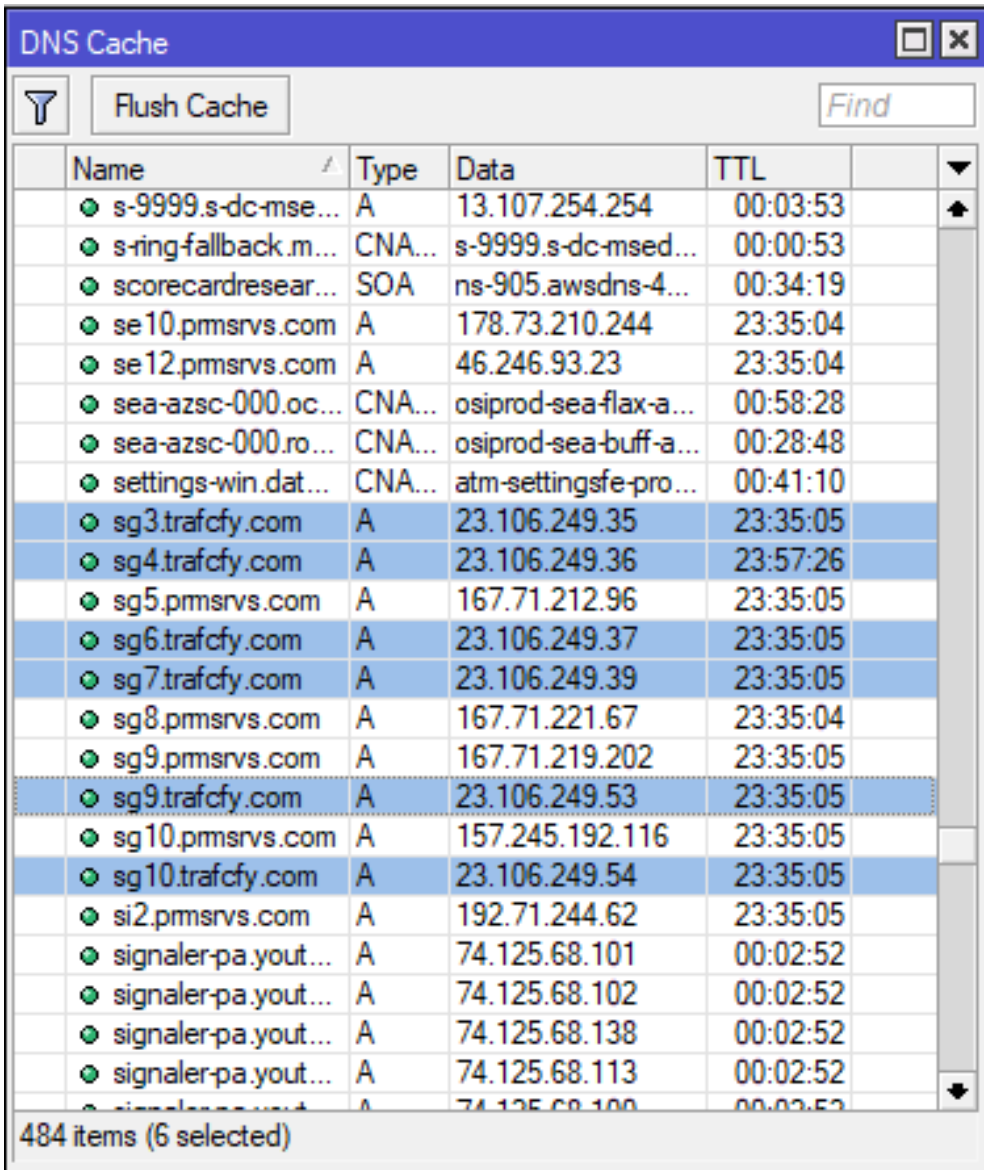
2. Pemantauan Akses Pada *DNS Cache*

Pemantauan akses pada *DNS Cache*. Dengan memantau akses pada *DNS Cache,* informasi yang dapat diperoleh terkait dengan alamat IP yang diminta oleh pengguna, serta sumber dan tujuan permintaan tersebut. Dengan demikian, pemantauan ini tidak hanya bertujuan untuk mengidentifikasi alamat IP, tetapi juga untuk menganalisis pola akses dan mengamati perilaku pengguna dalam menggunakan layanan jaringan. Hasil pemantauan ini kemudian dapat digunakan untuk pembuatan *address list* yang memungkinkan untuk pengelompokan atau pengaturan akses yang lebih terperinci dalam pengaturan keamanan jaringan.



Gambar 4. 17. Akses IP Address United State

Pada gambar di atas menyoroti hasil penggunaan layanan VPN Browsec yang telah diaktifkan dengan akses lokasi US (United Stated). Dalam gambar tersebut, terperlihat alamat IP dari VPN yang sedang berjalan pada perangkat MikroTik. Terdapat tiga alamat IP yang berbeda terdeteksi, yaitu (161.35.0.0), (162.210.0.0), dan (207.244.0.0), yang menunjukkan variasi alamat IP yang digunakan oleh sistem VPN. Fenomena ini merupakan strategi yang umum diterapkan dalam sistem VPN untuk menghindari deteksi oleh *firewall*, dengan menyediakan kumpulan alamat IP yang beragam.

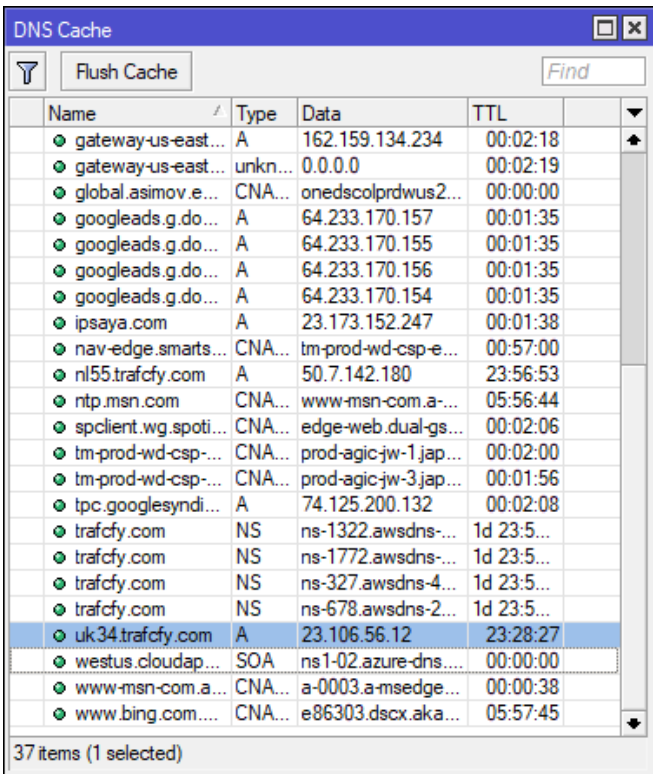


Gambar 4. 18. Akses IP Address Singapura

Pada gambar di atas, penggunaan *Virtual Private Network* (VPN) yang sama namun dengan lokasi yang berbeda, yaitu Singapura, menunjukkan bahwa terdapat hanya satu alamat IP VPN, yaitu (23.106.0.0), yang berfungsi pada perangkat Mikrotik. Kondisi ini memberikan beberapa keuntungan penting bagi peneliti. Pertama, adanya satu alamat IP VPN yang konsisten memudahkan proses identifikasi dan pelacakan lalu lintas data yang melewati jaringan. Kedua. risiko kesalahan dalam konfigurasi jaringan dan keamanan dapat diminimalkan, karena peneliti dapat fokus pada satu titik kontrol utama. Dengan demikian, penggunaan

satu alamat IP VPN pada lokasi yang sama melalui Mikrotik ini tidak hanya menyederhanakan proses administratif tetapi juga meningkatkan keakuratan dan efisiensi dalam penelitian dan manajemen jaringan.

Pada gambar di bawah ini, terlihat bahwa alamat IP yang berbeda digunakan di lokasi United Kingdom (UK) melalui penggunaan VPN Browsec untuk melewati sistem *firewall* yang telah dibangun. Alamat IP yang digunakan dalam skenario ini adalah (23.106.56.12). Penggunaan VPN, atau *Virtual Private Network*, memungkinkan pengguna untuk menyembunyikan alamat IP asli mereka dan menggantinya dengan alamat IP yang disediakan oleh layanan VPN. Ini berguna untuk mengakses konten yang dibatasi.



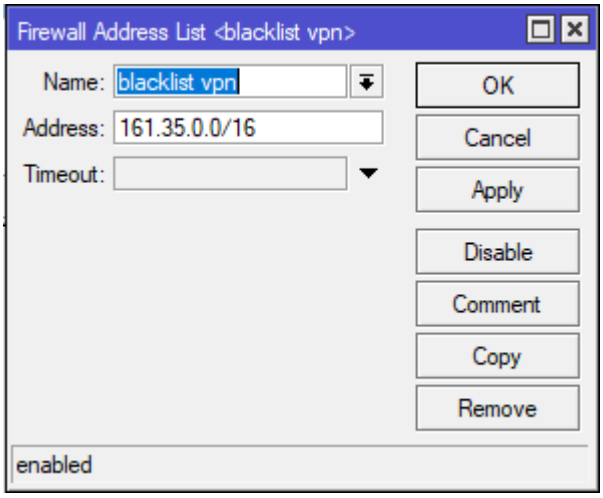
Gambar 4. 19. Akses IP Address United Kingdom

3. Implementasi *Address lists*

Dalam tahap berikutnya dari proses penetapan *Address list* pada perangkat MikroTik, peneliti secara sistematis menyusun daftar alamat IP yang digunakan

oleh layanan VPN setelah melalui fase pemantauan intensif. Pengamatan ini bertujuan untuk mengidentifikasi dan mencatat secara akurat semua alamat IP yang terkait dengan koneksi VPN yang telah diidentifikasi. Dengan menggunakan daftar alamat IP yang diperoleh, peneliti dapat mengintegrasikan *Address list* ini ke dalam konfigurasi *firewall* pada perangkat MikroTik. Proses ini bertujuan untuk mengimplementasikan kebijakan keamanan jaringan yang ketat, dengan cara memblokir akses ke alamat IP yang terkait dengan VPN yang tidak diizinkan, sehingga hanya koneksi yang sah dan diizinkan yang dapat melewati sistem keamanan jaringan.

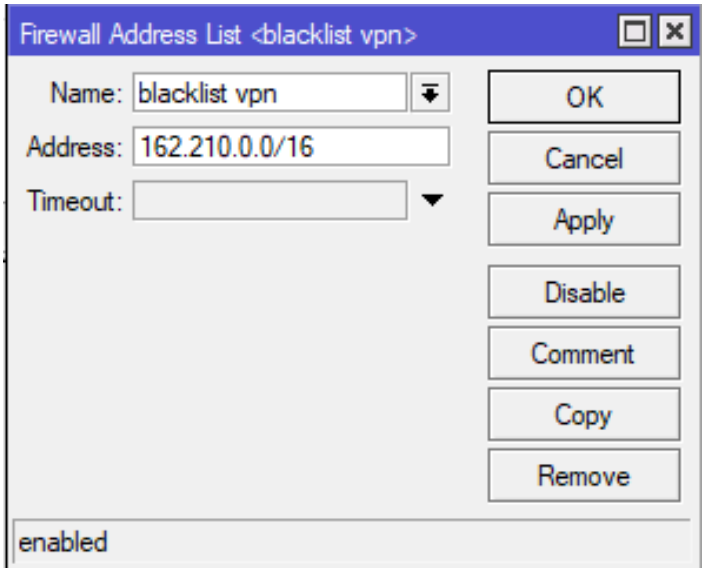
Untuk memblokir akses ke alamat IP yang terasosiasi dengan layanan VPN yang telah teridentifikasi, prosedur yang ditampilkan pada gambar di atas melibatkan pembuatan daftar alamat yang dinamakan "*blacklist* VPN". Dalam daftar ini, termasuk alamat IP spesifik yang akan diblokir, contohnya adalah VPN Browsec dengan lokasi di Amerika Serikat, menggunakan rentang IP 161.35.0.0/16.



Gambar 4. 20. Konfigurasi Addres List IP Unite state 161

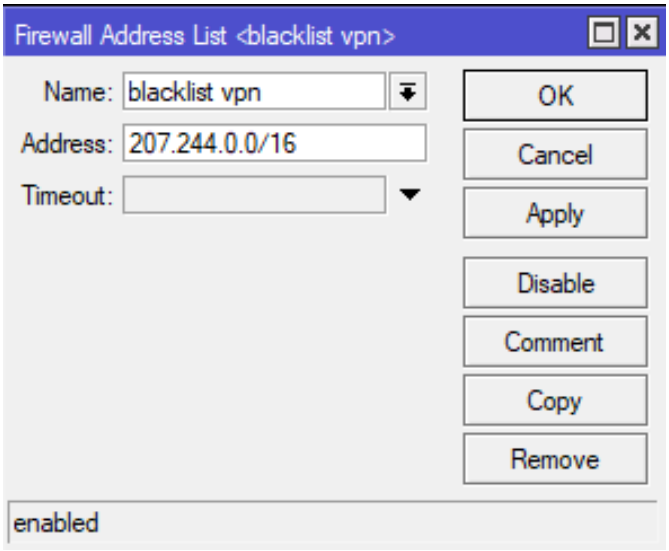
Mengingat bahwa Host ID dapat bervariasi untuk setiap pengguna VPN, angka 0 (nol) diberikan pada Host ID. Tujuan dari pemberian angka 0 ini adalah untuk memungkinkan sistem mendeteksi Host ID dengan syarat bahwa *Network* ID harus sesuai dengan hasil pemantauan sebelumnya. Strategi ini diimplementasikan untuk memastikan bahwa seluruh alamat IP dalam rentang yang sama dapat diidentifikasi dan diblokir secara efektif, meskipun Host ID berbeda-beda.

Pendekatan ini memungkinkan deteksi dan pemblokiran yang lebih efisien dan menyeluruh terhadap alamat IP yang digunakan oleh layanan VPN yang tidak diinginkan, sebagaimana juga ditunjukkan dalam gambar berikutnya.



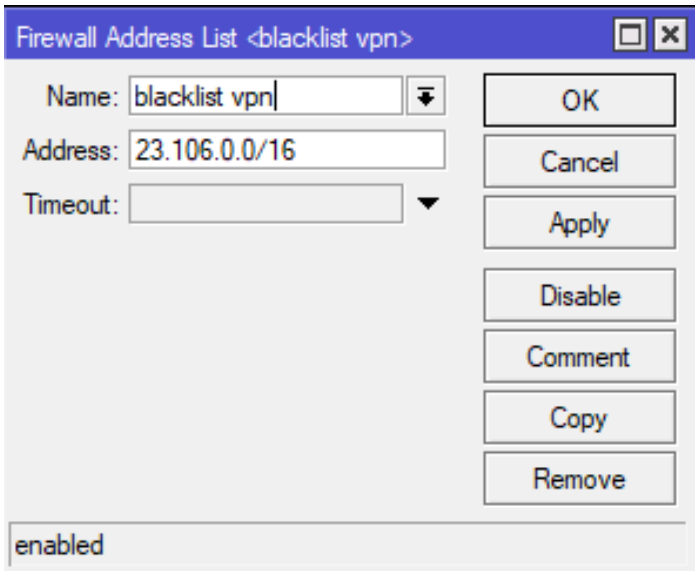
Gambar 4. 21. Konfigurasi Addres List United State 162

Gambar yang ditampilkan di atas memberikan ilustrasi mengenai alamat ip (*Internet Protocol*) yang diperoleh dari hasil pemantauan DNS (*Domain Name System*). Alamat IP tersebut kemudian diberi label sebagai "*blacklist* VPN," yang menandakan bahwa alamat-alamat IP tersebut masuk dalam daftar hitam dan akan diblokir. Salah satu subnet yang akan diblokir adalah 162.210.0.0/16, yang diketahui sebagai alamat IP yang digunakan oleh layanan Browsec VPN dengan akses lokasi US (United Stated).



Gambar 4. 22. Konfigurasi *Address list* United State 207

Gambar di atas peneliti membuat daftar alamat IP yang direncanakan untuk dimasukkan dalam "*blacklist* VPN" serta alamat IP yang akan diblokir dengan akses lokasi di Amerika Serikat (United States). Khususnya, alamat IP dengan rentang 207.244.0.0/16 yang diakses melalui Browsec VPN akan diblokir. Langkah ini diambil sebagai bagian dari upaya untuk mencegah akses ke alamat IP VPN yang telah teridentifikasi dan dikumpulkan. Selanjutnya membuat *address list* IP browsec VPN singapura dapat dilihat pada gambar di bawah.

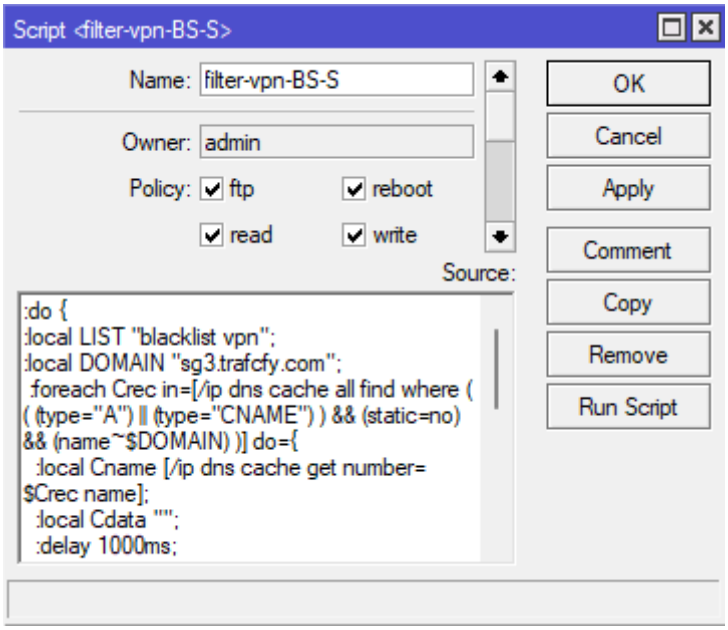


Gambar 4. 23. Konfigurasi *Address list* Singapure

Pada gambar di atas, disusun sebuah daftar alamat yang dinamakan "*blacklist* VPN" yang mencakup IP address yang akan diblokir. VPN Browsec yang berlokasi di Singapura dan United Kingdom memiliki *Network* ID yang identik, yaitu 23.106.0.0/16. Oleh karena itu, cukup dibuat satu daftar alamat saja untuk memblokir kedua lokasi tersebut.

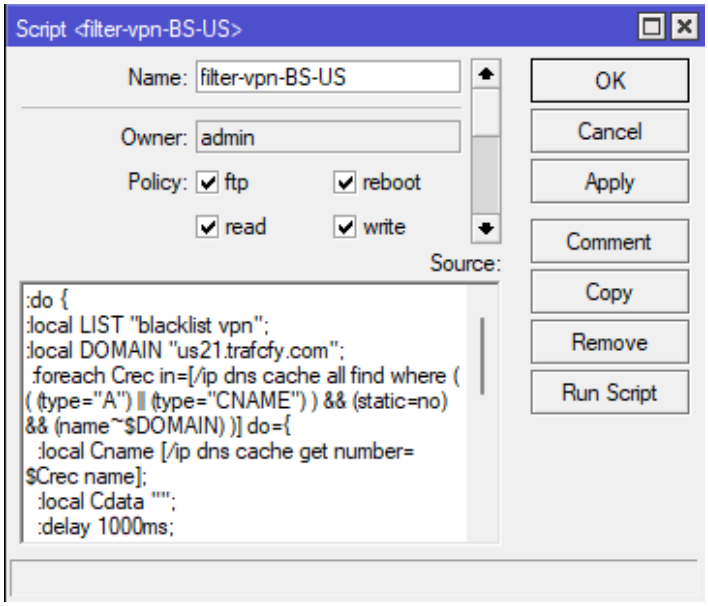
4. *Capture* DNS

Tujuan utama dari *capture* DNS adalah mamasukan skriptt, ini untuk mengambil seluruh entri DNS yang terkait dengan *domain* VPN dari *cache*, kemudian memasukkan alamat-alamat tersebut ke dalam daftar alamat *firewall* yang telah ditentukan sebelumnya, yaitu "*blacklist* vpn". Selain itu, skript ini juga menambahkan *domain* lokal VPN yang ditemukan “name DNS” ke dalam daftar tersebut. Ilustrasi proses ini dapat dilihat pada gambar di bawah ini.



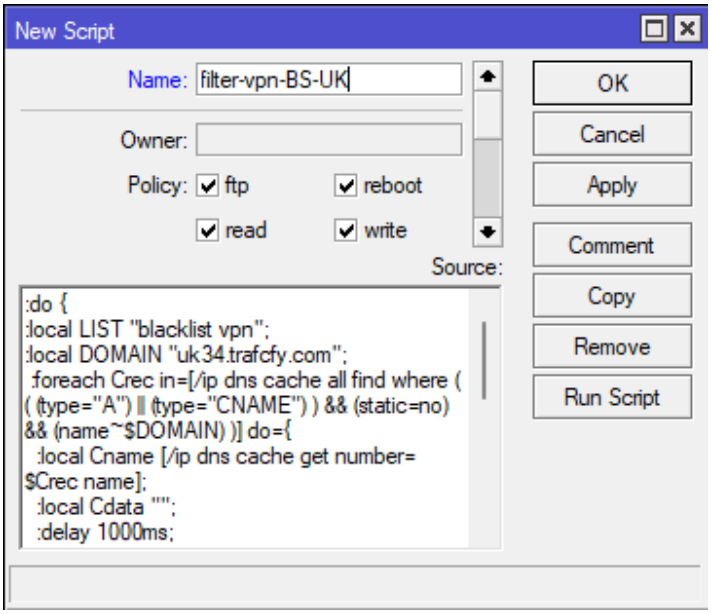
Gambar 4. 24. Konfigurasi *Capture* DNS

Pada gambar di atas, peneliti menggunakan *blacklist* vpn untuk mengambil *capture* DNS dari lokasi VPN Browsec di singapura. peneliti juga memasukkan *domain* lokal VPN yang peneliti peroleh, yaitu trafcfy.com, untuk mendapatkan semua entri DNS yang sesuai dengan *domain* VPN dari *cache*.



Gambar 4. 25. Konfigurasi *Capture* DNS United State

Gambar di atas menunjukan, peneliti menggunakan *blacklist* vpn untuk mengambil *capture* DNS dari lokasi United Stated di VPN Browsec. Selain itu, peneliti memasukkan *domain* lokal VPN peneliti, us21.trafcfy.com, untuk mendapatkan semua entri DNS yang sesuai dengan *domain* VPN dari *cache*.



Gambar 4. 26. Konfigurasi *Capture* DNS United Kingdom

Gambar di atas menunjukkan bahwa peneliti menggunakan *blacklist* VPN untuk mengambil *capture* DNS dari lokasi United Kingdom di VPN Browsec. Selain itu, peneliti memasukkan *domain* lokal VPN peneliti, uk34.trafcfy.com, untuk mendapatkan semua entri DNS yang sesuai dengan *domain* VPN dari *cache*.

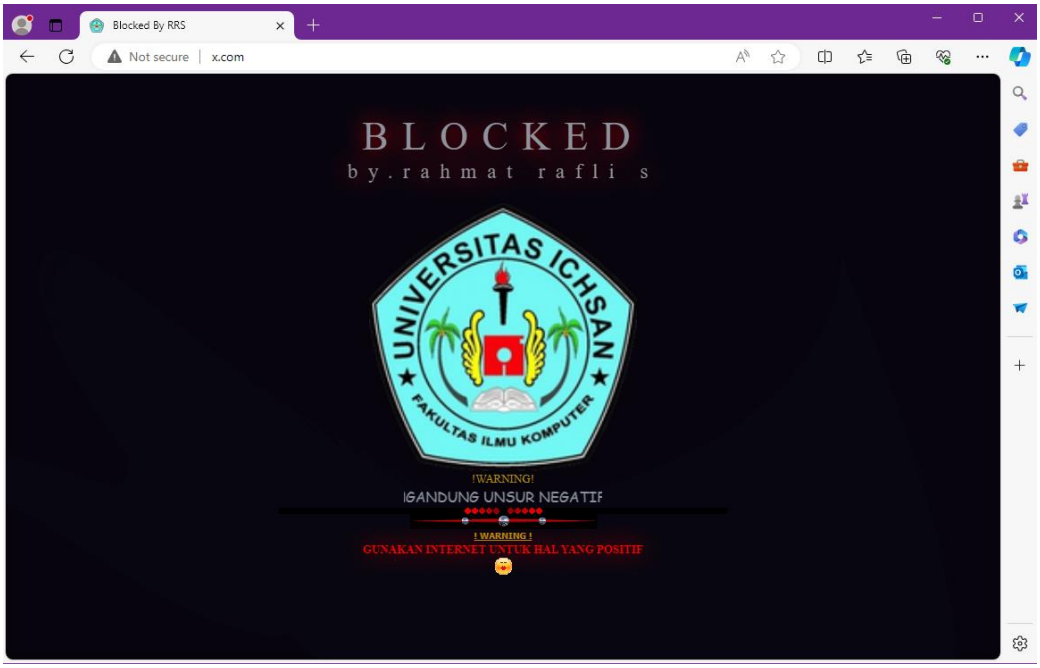
4.3. Pengujian Implemetasi Sistem

Pengujian sistem dilaksanakan oleh peneliti dengan menggunakan tiga peramban web, yaitu Microsoft Edge, Opera Browser, dan Google Chrome. Pengujian ini bertujuan untuk mengevaluasi efektivitas dan tingkat keberhasilan *proxy server* dalam memblokir situs web tertentu yang telah ditentukan sebelumnya. Pelaksanaan pengujian ini dilakukan dengan menggunakan sembilan unit komputer yang tersedia di laboratorium. Dalam proses pengujian, peneliti melakukan serangkaian uji coba yang terstruktur dan sistematis untuk mengamati bagaimana setiap peramban merespon pengaturan *proxy server*. Selain itu, peneliti juga mencatat dan menganalisis data terkait keberhasilan pemblokiran, dan konsistensi antara berbagai perangkat yang digunakan. Dengan demikian, hasil pengujian ini diharapkan dapat memberikan wawasan mendalam tentang kinerja dan reliabilitas *proxy server* dalam konteks penggunaan yang bervariasi, serta mengidentifikasi potensi kelemahan dan area yang memerlukan perbaikan lebih lanjut.

4.3.1. Pengujian Sesudah Menerapkan *Proxy server*

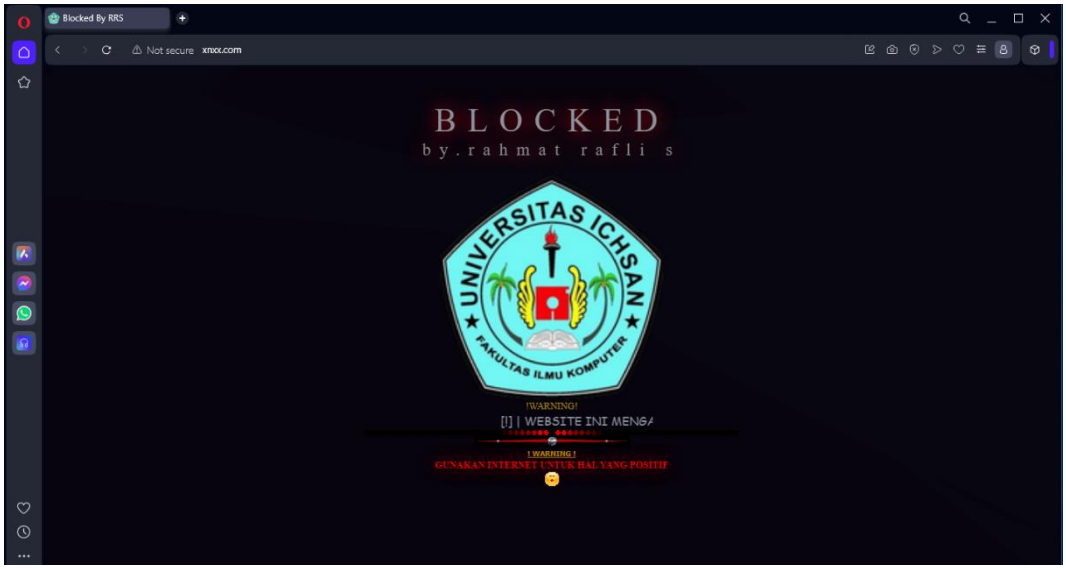
Berikut ini merupakan hasil pengujian dari situs yang berhasil diblokir menggunakan *Proxy server* pada lokasi penelitian.

Pada gambar di bawah salah satu unit komputer pada baris bagian depan memperlihat hasil pengujian pemblokiran situs menggunakan *proxy server*. Pengujian dilakukan dengan akses melaui Mikrosoft Edge menunjukkan bahwa pemblokiran bekerja dengan baik.



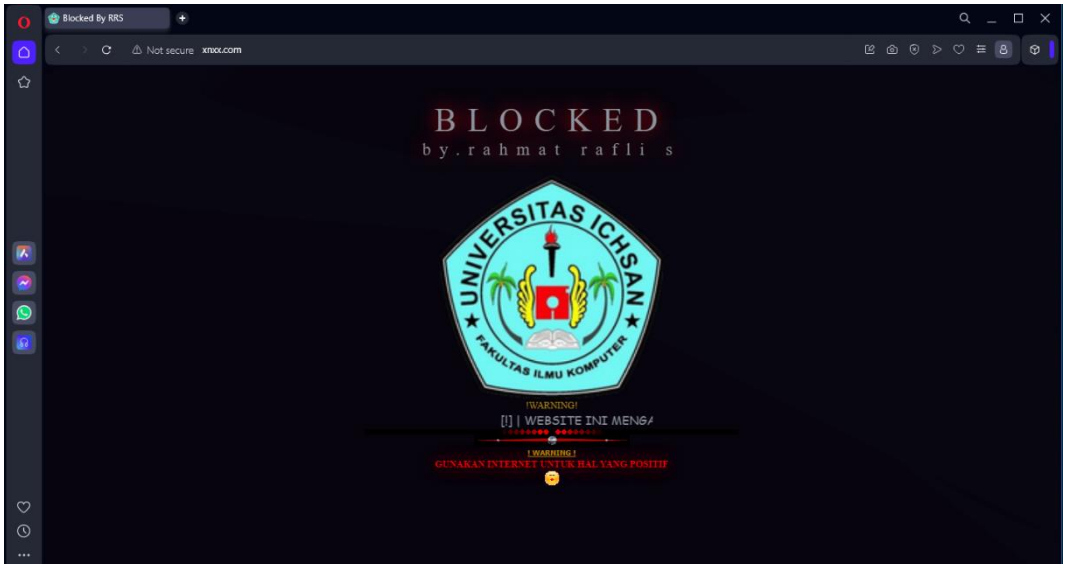
Gambar 4. 27. Pengujian *Proxy server* dengan Microsoft Edge

Selanjutnya, pada gambar di bawah ini salah satu unit komputer pada baris bagian tengah memperlihat tampilkan hasil pemblokiran yang diakses menggunakan Opera Browser. Gambar tersebut menunjukkan bahwa mekanisme pemblokiran berfungsi secara efektif, sebagaimana ditunjukkan oleh ketidakmampuan pengguna untuk mengakses konten yang dibatasi.



Gambar 4. 28. Pengujian *Proxy server* dengan Opera Browser

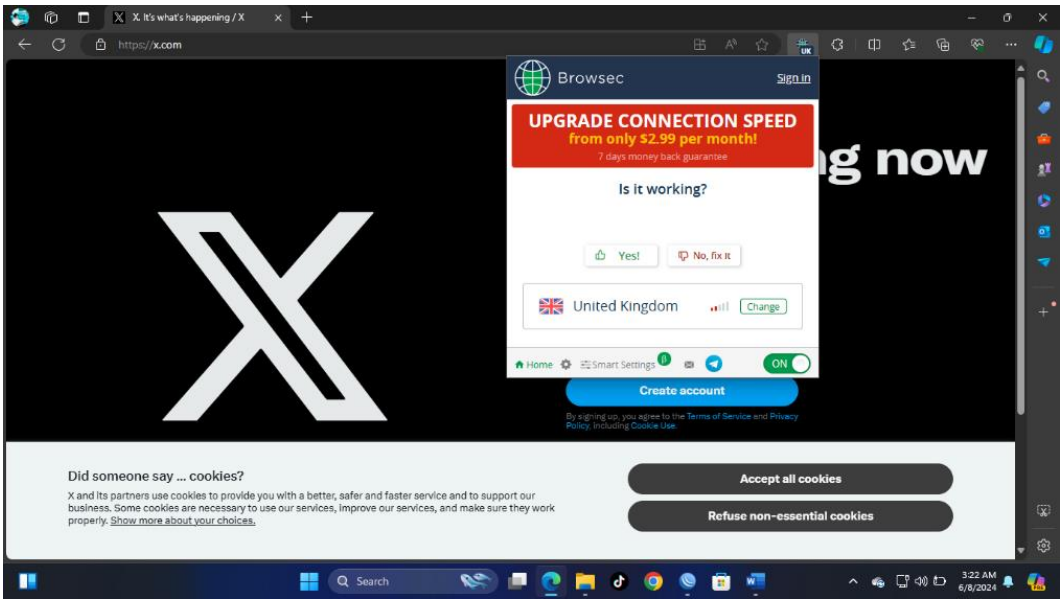
Gambar di bawah ini salah satu unit komputer pada baris bagian belakang memperlihat hasil pengujian akses situs web yang diblokir pada peramban Google Chrome dengan menggunakan *proxy server*. Hasil pengujian ini menunjukkan bahwa upaya untuk mengakses situs web yang diblokir melalui peramban Google Chrome berhasil dicegah, sesuai dengan ekspektasi pengujian.



Gambar 4. 29. Pengujian *Proxy server* dengan Google Chrome

4.3.2. Pengujian VPN Sebelum Menerapkan konfigurasi Mikrotik

Selanjutnya, peneliti melaksanakan pengujian akses terhadap situs x.com dengan menggunakan komputer laboratorium. Pengujian ini dilakukan sebelum mengkonfigurasi mikrotik, dengan tujuan untuk menguji efektivitas VPN dalam mengatasi aturan *proxy server* yang dikonfigurasi *firewall*. Hasil pengujian menunjukkan bahwa situs x.com berhasil diakses oleh salah satu komputer laboratorium bagian depan menggunakan microsoft edge. Hal ini diperlihatkan pada gambar di bawah, yang menunjukkan keberhasilan akses ke situs x.com saat VPN digunakan sebelum peneliti melakukan konfigurasi mikrotik untuk pemblokiran VPN.



Gambar 4. 30. Pengujian VPN Sebelum Konfigurasi Mikrotik dengan microsoft edge

Gambar di atas menampilkan pengujian di lokasi penelitian, akses situs web melalui penggunaan VPN. Hasil pengujian menunjukkan bahwa situs web dapat diakses dengan sukses menggunakan VPN yang diuji pada Microsoft Edge. Temuan ini mengindikasikan bahwa VPN dapat melewati *firewall* pada server proxy yang dibuat.

Gambar 4. 31. Pengujian VPN Sebelum Konfigurasi Mikrotik dengan Opera Browser

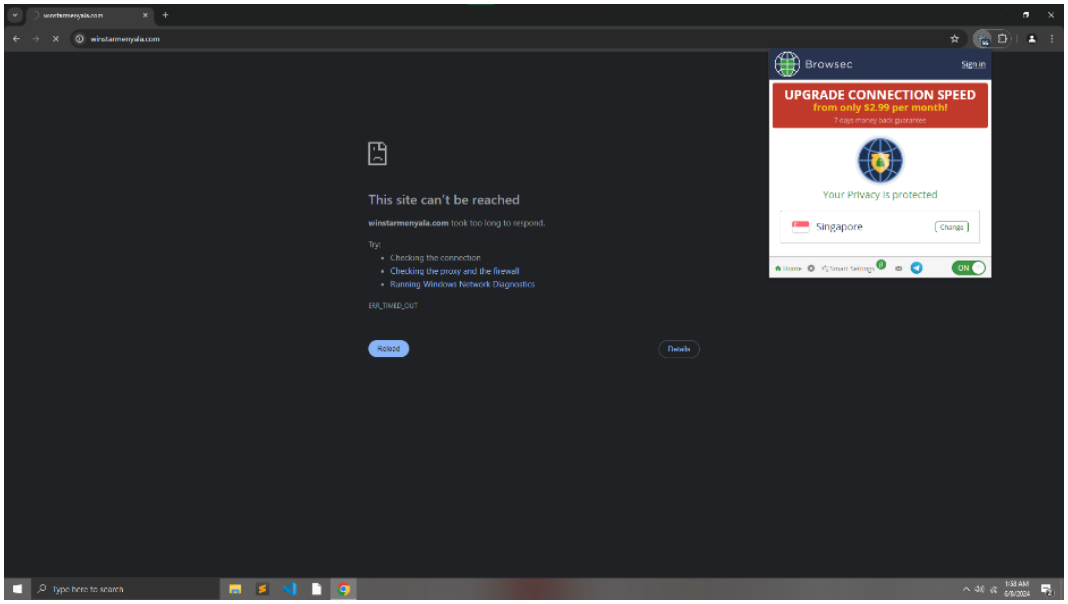
Gambar 5.5 menunjukkan pengujian akses situs web menggunakan VPN. Hasil pengujian menunjukkan bahwa situs x.com berhasil diakses oleh salah satu komputer laboratorium bagian tengah menggunakan browser Opera. Temuan ini menunjukkan bahwa VPN dapat melewati *firewall* pada server proxy di lokasi penelitian.

Gambar 4. 32. Pengujian VPN Sebelum Konfigurasi Mikrotik dengan Google Chrome

Gambar diatas menunjukkan pengujianl akses situs web menggunakan VPN. Hasil pengujian menunjukkan bahwa situs x.com berhasil diakses oleh salah satu komputer laboratorium bagian belakang menggunakan Google Chrome. Temuan ini menunjukkan bahwa VPN dapat melewati *firewall* pada server proxy.

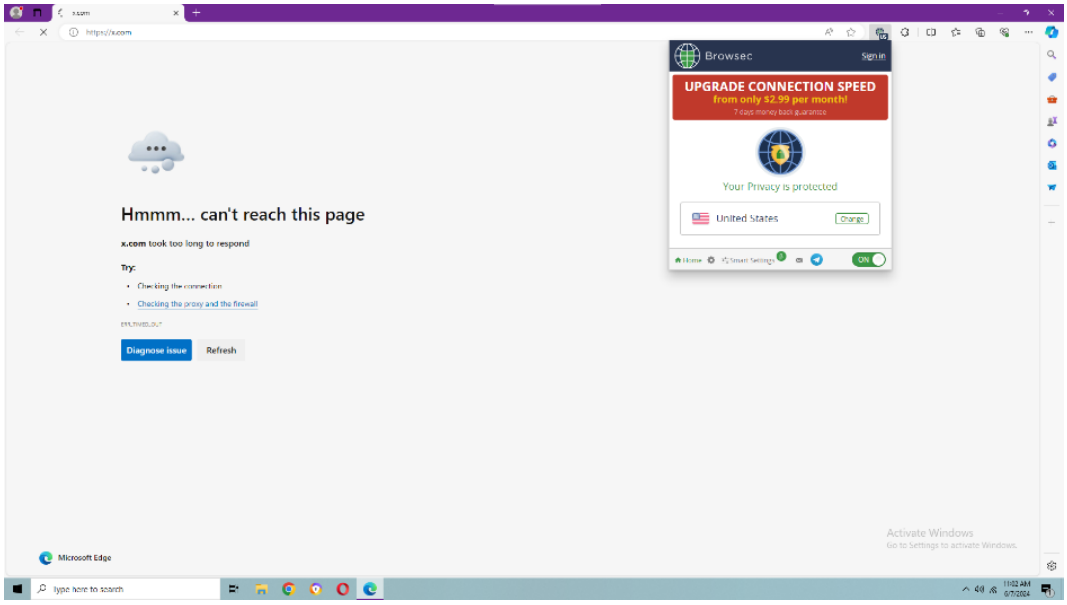
4.3.3. Pengujian VPN Sesudah Menerapkan Konfigurasi Mikrotik

Selanjutnya, peneliti melakukan uji akses terhadap VPN untuk mengakses situs x.com menggunakan salah satu komputer laboratorium bagian depan menggunakan google chrome. Setelah melakukan konfigurasi Mikrotik untuk memblokir VPN, hasil pengujian menunjukkan bahwa VPN berhasil diblokir pada komputer klien tersebut. Keberhasilan pemblokiran ini ditunjukkan pada gambar di bawah, yang mengilustrasikan efektivitas konfigurasi Mikrotik yang dilakukan oleh peneliti dalam menghalangi akses VPN.



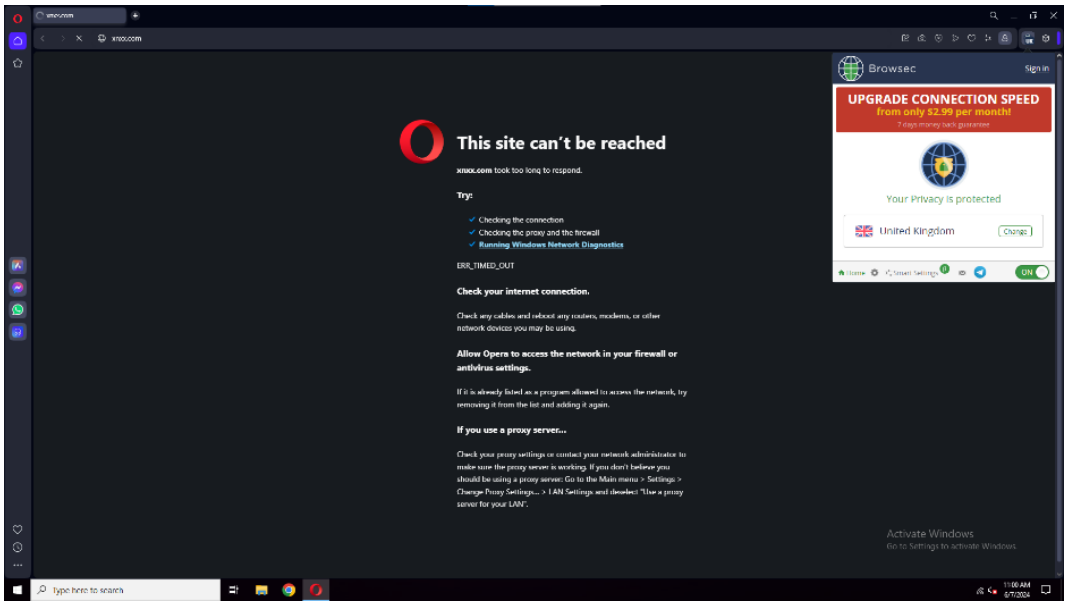
Gambar 4. 33. Pengujian VPN dengan Google Chrome
Setelah Konfigurasi Mikrotik

Gambar yang terlampir diatas menampilkan hasil dari upaya akses situs web yang menggunakan VPN. Berdasarkan hasil pengujian yang telah dilakukan, bahwa *proxy server* tidak mampu dilewati melalui VPN. Penemuan ini mengindikasikan bahwa konfigurasi terhadap perangkat Mikrotik telah berhasil dalam mencegah upaya VPN yang berusaha menembus server proxy.



Gambar 4. 34. Pengujian VPN dengan Microsoft Edge
Setelah Konfigurasi Mikrotik

Selanjutnya, gambar yang terlampir pada Gambar 5.8, menunjukkan hasil pengujian menggunakan Microsoft Edge, yang mengindikasikan bahwa server proxy tidak dapat diakses melalui VPN. Temuan ini menunjukkan bahwa konfigurasi pada perangkat Mikrotik berhasil mencegah upaya VPN untuk mengakses situs setelah konfigurasi mikrotik. Hasil ini memberikan bukti bahwa pengaturan keamanan yang diterapkan efektif dalam menjaga integritas dan keamanan jaringan dari upaya akses yang tidak sah.



Gambar 4. 35. Pengujian VPN dengan Opera Browser
Setelah Konfigurasi Mikrotik

BAB V
PEMBAHASAN PENELITIAN

5.1. Pembahasan Sistem

5.1.1. Tabel Penetapan *address list* VPN

Tabel yang tertera di bawah ini menyajikan hasil penetapan alamat Protokol Internet (IP) untuk *Virtual Private Network* (VPN) yang telah dikumpulkan melalui *cache* Sistem Nama *Domain* (DNS). Data tersebut merupakan hasil sementara yang belum dieksekusi atau divalidasi oleh prosedur *capture* DNS.

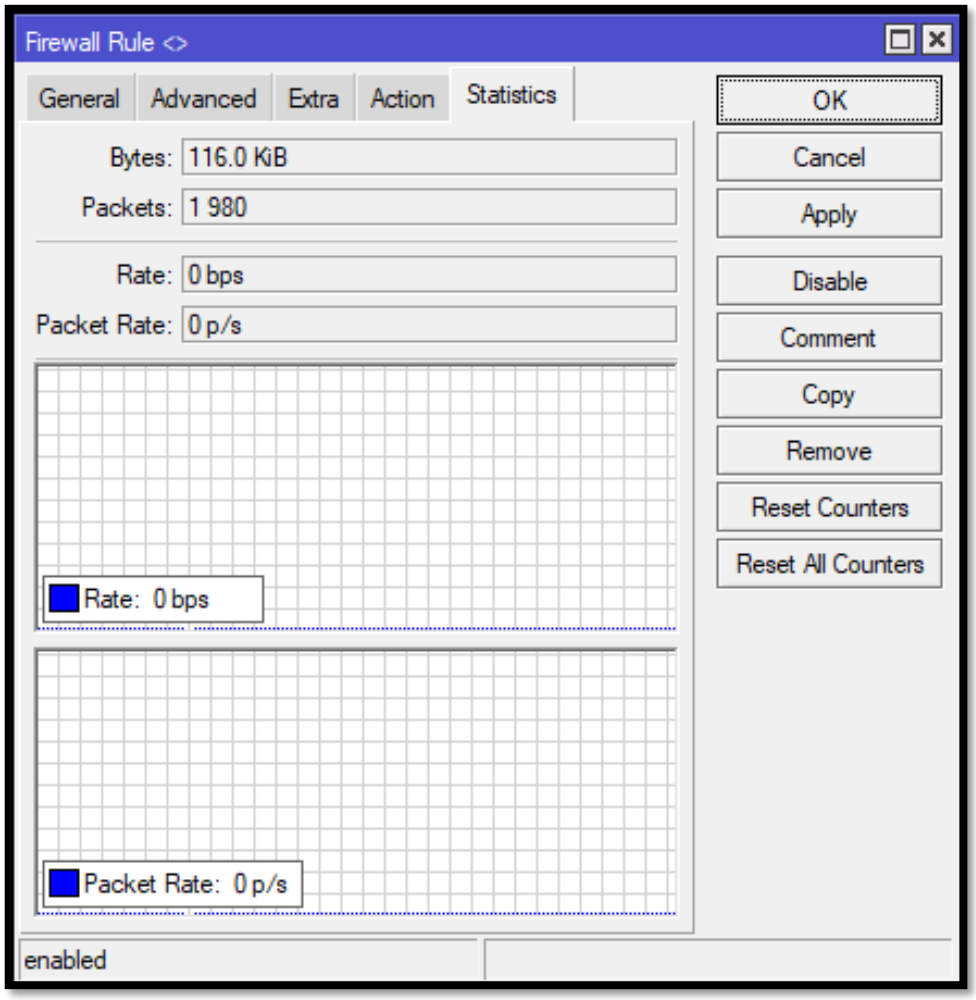
Tabel 5. 1. Penetapan *Address list* VPN

Nama List	IP Address	Status Akses
Blacklist VPN	162.210.0.0/16	Drop
Blacklist VPN	207.244.0.0/16	Drop
Blacklist VPN	161.35.0.0/16	Drop
Blacklist VPN	50.7.0.0/16	Drop
Blacklist VPN	23.106.0.0/16	Drop
Blacklist VPN	83.136.0.0/16	Drop
Blacklist VPN	94.237.0.0/16	Drop
Blacklist VPN	95.111.0.0/16	Drop
Blacklist VPN	209.94.0.0/16	Drop
Blacklist VPN	185.123.0.0/16	Drop
Blacklist VPN	167.71.0.0/16	Drop
Blacklist VPN	157.245.0.0/16	Drop
Blacklist VPN	178.128.0.0/16	Drop
Blacklist VPN	198.16.0.0/16	Drop

Proses pengumpulan ini penting dalam analisis jaringan karena *cache* DNS berfungsi sebagai mekanisme penyimpanan sementara untuk mempercepat akses data yang sering diminta. Oleh karena itu, hasil penetapan alamat IP VPN dari *cache* DNS mencerminkan data sementara yang berpotensi mengalami perubahan

setelah dilakukan eksekusi melalui *capture* DNS. *Capture* DNS, sebagai langkah lanjutan, bertujuan untuk memastikan validitas dan akurasi data alamat IP dengan cara menangkap dan memverifikasi permintaan DNS secara langsung saat terjadi. Dengan demikian, tabel ini memberikan gambaran awal mengenai alokasi alamat IP VPN yang akan diverifikasi lebih lanjut melalui *capture* DNS, sehingga dapat memberikan wawasan yang lebih akurat dan andal tentang konfigurasi jaringan dan kinerjanya.

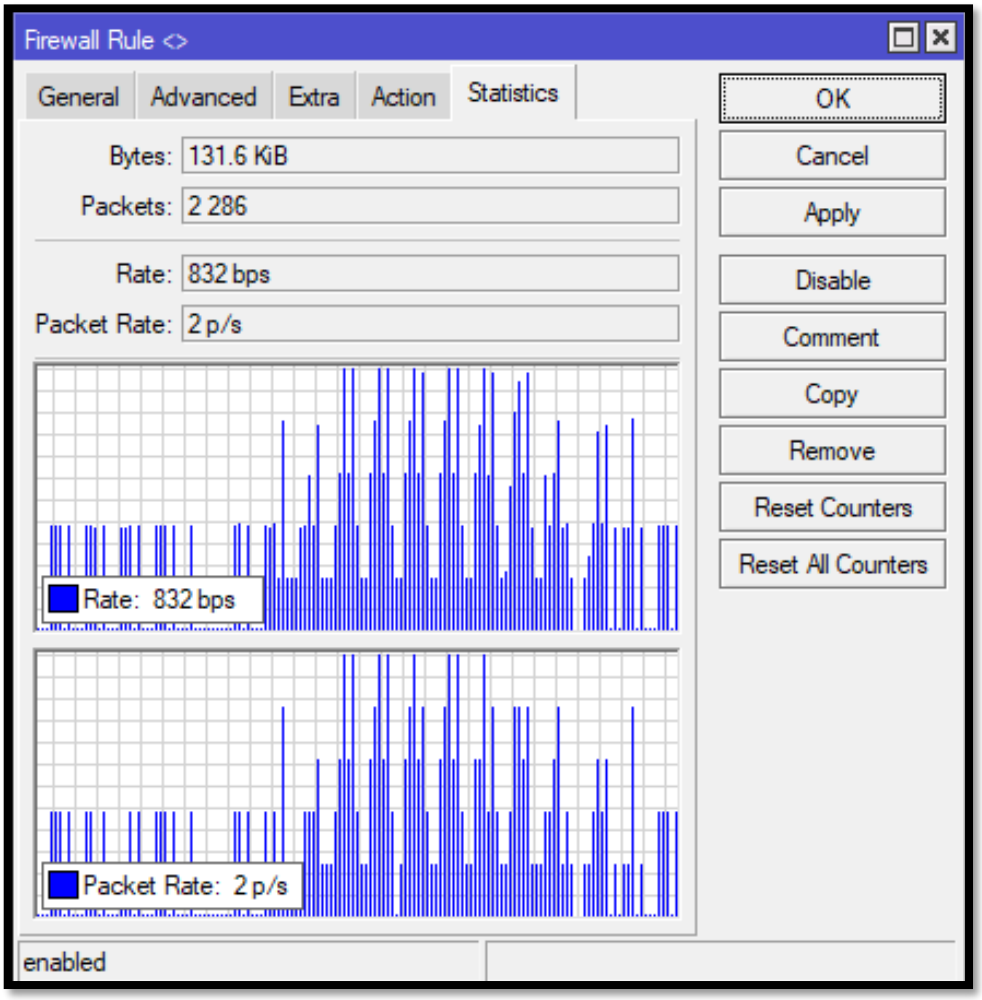
5.1.2. Hasil Tampilan Statistik Sebelum Akses VPN Masuk



Gambar 5. 1. Hasil Tampilan Statistik Sebelum Akses VPN Masuk

Pada gambar di atas, terlihat tampilan monitoring statistik data yang diminta oleh komputer yang mengakses sebelum menggunakan VPN. Dalam kondisi ini, tidak terdapat aktivitas trafik data yang terdeteksi sama sekali. Hal ini menunjukkan bahwa sebelum implementasi VPN, komputer tidak mengirim atau menerima data melalui *firewall* rule.

5.1.3. Hasil Tampilan Statistik Saat Akses VPN Masuk



Gambar 5. 2. Hasil Tampilan Statistik Saat Akses VPN Masuk

Gambar di atas menunjukkan tampilan pemantauan statistik data yang diminta oleh komputer yang mengakses jaringan menggunakan VPN. Dalam konteks ini, terlihat bahwa aturan *firewall* (*firewall* rule) berfungsi dengan efektif,

mempertahankan kebijakan yang telah ditetapkan untuk memblokir akses VPN ke internet melalui perangkat Mikrotik.

5.1.4. Tabel Hasil Log Akses Real-Time Pada Squid

Tabel 5. 2. Log Akses Real Time

Log akses		Status Akses	Keterangan
IP Address PC	**Situs web**		
192.168.200.241	x.com	Denied	Media Sosial
	youtube.com	Allow	Platform Vidio
192.168.200.244	xnxx.com	Denied	Situs Dewasa
	alsoporn.com		Situs Dewasa
	maha168heya.com		Judi Online
192.168.200.239	pornhub.com	Denied	Situs Dewasa
	winstarmenyala.com		Judi Online
192.168.200.235	tiktok.com	Allow	Platform vidio
192.168.200.252	x.com	Denied	Media Sosial
	youtube.com	Allow	Platform vidio
	alsoporn.com	Denied	Situs Dewasa
192.168.200.247	xnxx.com	Denied	Situs Dewasa
	alsoporn.com		Situs Dewasa
	maha168heya.com		Judi Online
192.168.200.246	pornhub.com	Denied	Situs Dewasa
	xnxx.com		Situs Dewasa
192.168.200.234	tiktok.com	Allow	Platform vidio
192.168.200.236	x.com	Denied	Media Sosial
	instagram.com	Allow	Media Sosial
	alsoporn.com	Denied	Situs Dewasa

Tabel yang disajikan di atas merupakan hasil dari pemantauan aktifitas dalam jaringan oleh para peneliti menggunakan mekanisme berbasis proxy server. Proses pemantauan ini memungkinkan pengidentifikasian situs yang telah diblokir sesuai dengan kebijakan yang ditetapkan, serta memungkinkan pengumpulan data yang komprehensif mengenai interaksi pengguna dan perangkat dalam jaringan. Dengan demikian, data yang terkumpul memfasilitasi analisis mendalam terkait pola penggunaan internet dan memungkinkan peneliti untuk mengambil langkah-langkah yang diperlukan dalam mengelola dan mengoptimalkan infrastruktur jaringan secara efektif. Metode ini memberikan gambaran yang akurat dan detail

mengenai aktivitas pengguna, sehingga mendukung dalam perumusan kebijakan yang tepat serta peningkatan keamanan jaringan secara keseluruhan.

5.1.5. Tabel Hasil *Capture* DNS Oleh Script

Tabel 5. 3. Hasil *Capture* DNS

Browsec VPN		**Status Akses**		
IP Location	**IP Address**	**Chrome**	**Opera Browser**	**Microsoft Edge**
Singapure	23.106.249.35	Drop	Drop	Drop
	23.106.249.34	Drop	Drop	Drop
	23.106.249.39	Drop	Drop	Drop
	23.106.249.36	Drop	Drop	Drop
	23.106.249.53	Drop	Drop	Drop
	23.106.249.52	Drop	Drop	Drop
	23.106.249.44	Drop	Drop	Drop
	23.106.249.54	Drop	Drop	Drop
	23.106.249.37	Drop	Drop	Drop
United Kingdom	23.106.56.12	Drop	Drop	Drop
	23.106.56.54	Drop	Drop	Drop
	23.106.56.13	Drop	Drop	Drop
	23.106.56.52	Drop	Drop	Drop
	23.106.56.36	Drop	Drop	Drop
	23.106.56.14	Drop	Drop	Drop
	23.106.56.19	Drop	Drop	Drop
	23.106.56.11	Drop	Drop	Drop
	23.106.56.53	Drop	Drop	Drop
	23.106.56.43	Drop	Drop	Drop
	23.106.56.22	Drop	Drop	Drop
	23.106.56.35	Drop	Drop	Drop
	23.106.56.37	Drop	Drop	Drop
	23.106.56.51	Drop	Drop	Drop
United Stated	162.210.194.1	Drop	Drop	Drop
	207.244.71.82	Drop	Drop	Drop
	207.244.89.161	Drop	Drop	Drop
	207.244.71.80	Drop	Drop	Drop
	207.244.89.166	Drop	Drop	Drop
	162.210.194.4	Drop	Drop	Drop
	162.210.194.3	Drop	Drop	Drop
	162.210.194.2	Drop	Drop	Drop
	207.244.71.79	Drop	Drop	Drop
	207.244.71.84	Drop	Drop	Drop
	207.244.71.81	Drop	Drop	Drop

Pada penelitian ini, dilakukan serangkaian eksperimen untuk menguji akses jaringan menggunakan *Virtual Private Network* (VPN). Tujuan utama dari eksperimen ini adalah untuk mengevaluasi variasi alamat IP yang diperoleh melalui pencatatan *Domain Name System* (DNS) secara otomatis. Prosedur ini melibatkan pemanfaatan teknologi VPN untuk mengakses berbagai server dan layanan di internet, yang pada gilirannya memungkinkan peneliti mengamati perubahan dan distribusi alamat IP yang ditangkap selama periode pengujian. Hasil dari eksperimen ini diindikasikan dengan jelas dalam Tabel 5.3, yang menyajikan data komprehensif mengenai beragam alamat IP yang terdeteksi selama proses pencatatan DNS dan memblokirnya. Analisis data ini memungkinkan pemahaman yang lebih mendalam mengenai dinamika dan pola penggunaan alamat IP dalam konteks akses VPN, serta implikasinya terhadap privasi dan keamanan data pengguna. Studi ini memberikan wawasan kritis mengenai efektivitas VPN dalam melindungi identitas pengguna melalui rotasi alamat IP dan peran penting DNS dalam memfasilitasi deteksi tersebut.

BAB VI
PENUTUP

6.1. Kesimpulan

Penelitian ini membahas implementasi sistem *Blocking* situs negatif menggunakan *proxy server* dan filter rules pada Mikrotik di Laboratorium Fakultas Ilmu Komputer. Beberapa kesimpulan yang dapat diambil adalah sebagai berikut:

1. Sistem yang dirancang berhasil dan mampu memblokir akses ke situs web negatif secara efektif. Penggunaan *proxy server* berhasil memblokir situs-situs yang dianggap peneliti merugikan atau tidak pantas, seperti x.com dan porn*ub.com, sehingga tidak dapat diakses melalui jaringan laboratorium.
2. Sistem yang diterapkan juga menunjukkan kemampuan dalam mengurangi penggunaan VPN untuk mengakses konten terlarang. Analisis DNS *capture* menunjukkan bahwa filter rules yang diterapkan membuat penggunaan VPN untuk mengakses situs negatif menjadi kurang efektif

6.2. Saran

Berdasarkan temuan dan kesimpulan penelitian ini, beberapa saran untuk pengembangan dan penerapan lebih lanjut adalah:

1. Sistem yang diterapkan dalam penelitian ini tidak memiliki kemampuan untuk melakukan pemblokiran situs secara otomatis. Saat ini, semua situs yang dianggap negatif dipilih dan dimasukkan ke dalam daftar hitam (*blacklist*) secara manual oleh peneliti. Oleh karena itu, diharapkan penelitian selanjutnya dapat mengembangkan sistem yang mampu mendeteksi situs atau konten negatif dan memblokirnya secara otomatis. Hal ini akan meningkatkan efisiensi dan efektivitas dalam pengelolaan konten negatif di internet.
2. Konfigurasi Mikrotik yang diterapkan dalam penelitian ini belum mampu melakukan pemblokiran otomatis terhadap IP VPN dari luar negeri. Semua IP VPN luar negeri dipilih dan dimasukkan ke dalam daftar blacklist secara manual oleh peneliti. Oleh karena itu, diharapkan penelitian selanjutnya

dapat mengembangkan konfigurasi Mikrotik yang mampu mendeteksi dan memblokir IP VPN luar negeri secara otomatis.

Penelitian ini menunjukkan bahwa penggunaan *proxy server* dan filter rules pada Mikrotik dapat menjadi solusi efektif untuk memblokir akses ke situs negatif dan mengurangi penggunaan VPN untuk tujuan yang tidak diinginkan di jaringan komputer laboratorium.

DAFTAR PUSTAKA

[1] W, Y., Fitriana, Y. B., Susanto, A., Susanto, E. S., & Hamdani, F. (2022). Implemetasi *Filtering* Alamat Website Pada *Proxy server* Menggunakan Raspberry-Pi. *Jurnal Informatika: Jurnal pengembangan IT (JPIT), Vol.7, No.1*.

[2] Ferrissa, W. (2017, November 30). *Ini Konten Negatif yang Dominan di Indonesia*. Retrieved from Kementerian Komunikasi dan Informatika RI: https://www.kominfo.go.id/*Content*/detail/11711/ini-konten-negatif-yang-dominan-di-indonesia/0/sorotan_media

[3] Arrahman, R., & Pramita, A.W. (2013). *Implementasi Proxy server* Sebagai *Content Filtering* Menggunakan Linux Debian Buster. Jurnal Ilmiah Intech : Information Technology Journal of UMUS *Volume 4 Nomor 1*.

[4] Irawan, G. T., Djaohar, M., & Duskarnaen, M. F. (2018). IMPLEMENTASI DAN IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN *FIREWALL* DAN *PROXY SERVER* BERBASIS MIKROTIK DI SMA NEGERI 1 KOTA SUKABUMI. *Jurnal Pinter Vol 2. No.1*.

[5] Noviansyah, M., & Saiyar, H. (2020). PEMANFAATAN *PROXY SERVER* SEBAGAI PENGOPTIMAL KEAMANAN. *JURNAL KHATULISTIWA INFORMATIKA, VOL. VIII, NO.1*.

[6] Hambali. (2018). MEMBANGUN *BLOCKING* SITUS DENGAN MENGGUNAKAN *PROXY SERVER* MIKROTIK RB750 GUNA MENDUKUNG INTERNET SEHAT. *Seminar Nasional Royal (SENAR)*, 205-210.

[7] MADIUN, M. (2013). *Cepat dan Mudah membangun Sistem Jaringan Komputer*. Yogyakarta: C.V Andi OFFSET.

[8] Sofana, I. (2013). *Membangun Jaringan Komputer*. Bandung: Informatika Bandung.

[9] Purba, W. W., & Efendi, R. (Agustus 2020). Implementasi dan analisis sistem keamanan jaringan komputer menggunakan SNORT . *AITI: Jurnal Teknologi Informasi, Volume 17 No. 2, 143-158*, ISSN 1693-8348 E-ISSN 2615-7128.

[10] H, F. R., "ANALISIS DAN IMPLEMENTASI *FIREWALL* DENGAN METODE PORT ADDRESS TRANSLATION PADA MIKROTIK OS FIT," *Photosynthetica*, 2018.

[11] Mamuko, & Ardi, V. (2016, February 4). *IMPLEMENTASI PROXY SERVER UNTUK MENINGKATKAN KEMAMPUAN FILTER ACCESS CONTROL LIST PADA ROUTER*. Retrieved from Repository Politeknik Negeri Manado: http://repository.polimdo.ac.id/id/eprint/622

[12] Pelealu, R. A., Wonggo, D., & Kembuan, O. (Juni 2020). Implementasi dan Implementasi Jaringan Komputer SMK Negeri 1 Tahuna. *JOINTER, Vol. 1, No.1*.

[13] Daro, T. (2020, November 16). *How to block icmp requests to the WAN IP on your Mikrotik router*. Retrieved from https://timigate.com/: https://timigate.com/2017/12/mikrotik-security-how-to-block-icmp.html#comment-21368

LAMPIRAN

Lamiran 1

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS ICHSAN GORONTALO
FAKULTAS ILMU KOMPUTER
UPT. PERPUSTAKAAN FAKULTAS
SK. MENDIKNAS RI NO. 84/D/0/2001
Jl. Achmad Nadjamuddin No.17 Telp(0435) 829975 Fax. (0435) 829976 Gorontalo

SURAT KETERANGAN BEBAS PUSTAKA

No : 018/Perpustakaan-Fikom/VI/2024

Perpustakaan Fakultas Ilmu Komputer (FIKOM) Universitas Ichsan Gorontalo dengan ini menerangkan bahwa :

Nama Anggota	:	Rahmat Rafli Suleman
No. Induk	:	T3120032
No. Anggota	:	M202438

Terhitung mulai hari, tanggal : Senin, 10 Juni 2024, dinyatakan telah bebas pinjam buku dan koleksi perpustakaan lainnya.

Demikian keterangan ini di buat untuk di pergunakan sebagaimana mestinya.

Gorontalo, 10 Juni 2024
Mengetahui,
Kepala Perpustakaan

Apriyanto Alhamad, M.Kom
NIDN : 0924048601

Lampiran 2

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
UNIVERSITAS ICHSAN GORONTALO
FAKULTAS ILMU KOMPUTER
SURAT KEPUTUSAN MENDIKNAS RI NOMOR 84/D/O/2001
Jl. Achmad Najamuddin No. 17 Telp. (0435) 829975 Fax (0435) 829976 Gorontalo

SURAT REKOMENDASI BEBAS PLAGIASI
No. 145/FIKOM-UIG/R/VI/2024

Yang bertanda tangan di bawah ini :

Nama	: Irvan Abraham Salihi, M.Kom
NIDN	: 0928028101
Jabatan	: Dekan Fakultas Ilmu Komputer

Dengan ini menerangkan bahwa :

Nama Mahasiswa	:	Rahmat Rafli Suleman
NIM	:	T3120032
Program Studi	:	Teknik Informatika (S1)
Fakultas	:	Fakultas Ilmu Komputer
Judul Skripsi	:	Penerapan Proxy Server Pada Mikrotik Untuk Blocking Situs Negatif Di Jaringan Komputer

Sesuai hasil pengecekan tingkat kemiripan skripsi melalui aplikasi **Turnitin** untuk judul skripsi di atas diperoleh hasil *Similarity* sebesar **16%**, berdasarkan Peraturan Rektor No. 32 Tahun 2019 tentang Pendeteksian Plagiat pada Setiap Karya Ilmiah di Lingkungan Universitas Ichsan Gorontalo dan persyaratan pemberian surat rekomendasi verifikasi calon wisudawan dari LLDIKTI Wil. XVI, bahwa batas kemiripan skripsi maksimal 30%, untuk itu skripsi tersebut di atas dinyatakan **BEBAS PLAGIASI** dan layak untuk diujiankan.

Demikian surat rekomendasi ini dibuat untuk digunakan sebagaimana mestinya.

Mengetahui
Dekan,

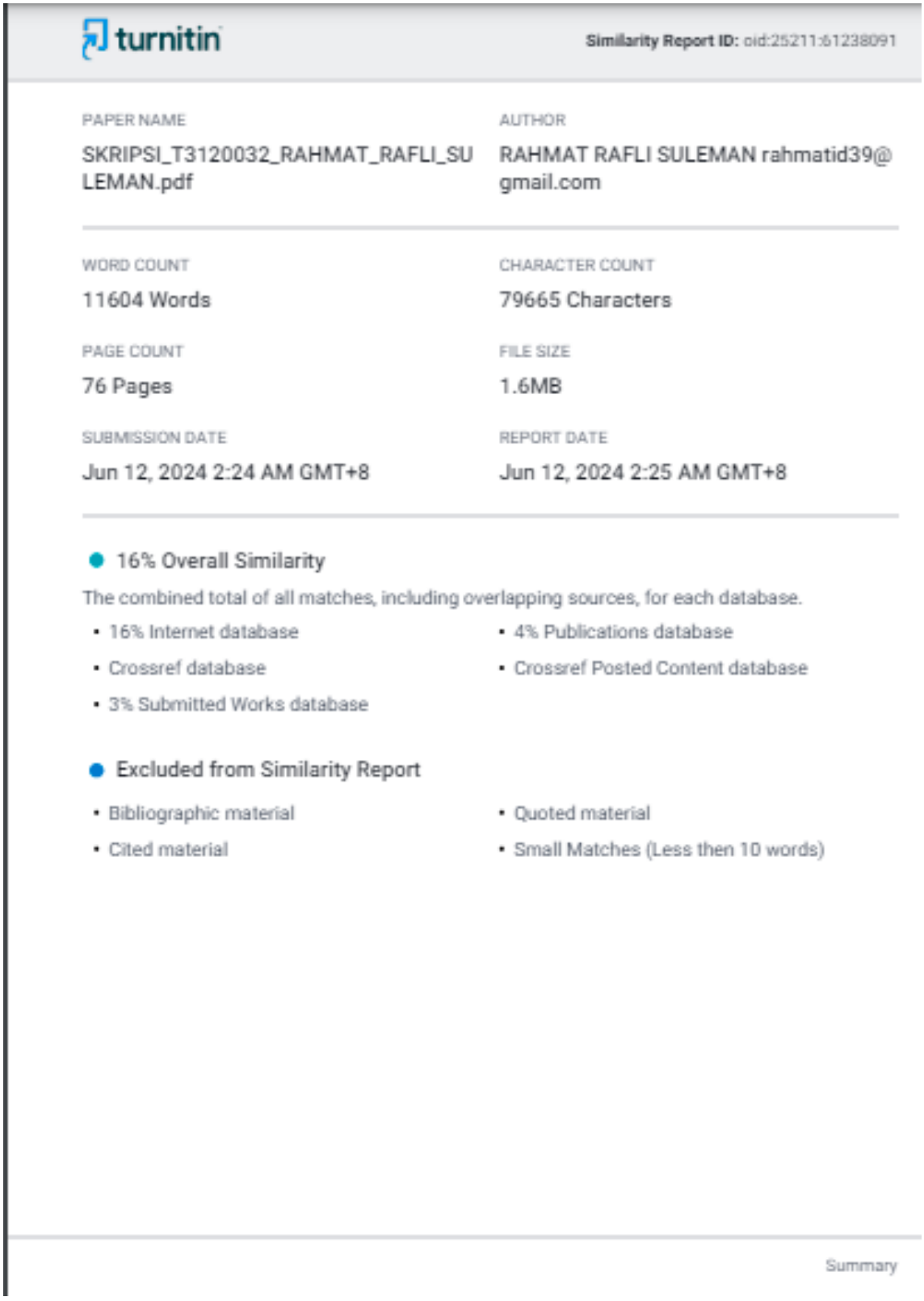
Irvan Abraham Salihi, M.Kom
NIDN. 0928028101

Gorontalo, 13 Juni 2024
Tim Verifikasi,

Zulfrianto Y. Lamasigi, M.Kom
NIDN. 0914089101

Terlampir :
Hasil Pengecekan Turnitin

Lampiran 3



turnitin

Similarity Report ID: oid:25211:61238091

PAPER NAME
SKRIPSI_T3120032_RAHMAT_RAFLI_SULEMAN.pdf

AUTHOR
RAHMAT RAFLI SULEMAN rahmatid39@gmail.com

WORD COUNT
11604 Words

CHARACTER COUNT
79665 Characters

PAGE COUNT
76 Pages

FILE SIZE
1.6MB

SUBMISSION DATE
Jun 12, 2024 2:24 AM GMT+8

REPORT DATE
Jun 12, 2024 2:25 AM GMT+8

● 16% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

- 16% Internet database
- 4% Publications database
- Crossref database
- Crossref Posted Content database
- 3% Submitted Works database

● Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less then 10 words)

Summary

turnitin

Similarity Report ID: oid:25211:61238091

16% Overall Similarity

Top sources found in the following databases:

- 16% Internet database
- Crossref database
- 3% Submitted Works database
- 4% Publications database
- Crossref Posted Content database

TOP SOURCES

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	coursehero.com Internet	1%
2	seminar.bsi.ac.id Internet	1%
3	docplayer.info Internet	1%
4	kc.umn.ac.id Internet	<1%
5	scribd.com Internet	<1%
6	LL Dikti IX Turnitin Consortium on 2019-07-16 Submitted works	<1%
7	media.neliti.com Internet	<1%
8	datadosen.com Internet	<1%

9	idmetafora.com Internet	<1%
10	id.scribd.com Internet	<1%
11	pradirwancell.blogspot.com Internet	<1%
12	123dok.com Internet	<1%
13	kelompok6offaa.wordpress.com Internet	<1%
14	repositori.uin-alauddin.ac.id Internet	<1%
15	es.scribd.com Internet	<1%
16	repository.bsi.ac.id Internet	<1%
17	anyflip.com Internet	<1%
18	erepo.unud.ac.id Internet	<1%
19	elearningsupport.org Internet	<1%
20	LL Dikti IX Turnitin Consortium on 2019-07-16 Submitted works	<1%

21	ecampus.pelitabangsa.ac.id Internet	<1%
22	repository.unja.ac.id Internet	<1%
23	repository.widyatama.ac.id Internet	<1%
24	sman15-bdl.sch.id Internet	<1%
25	eprints.unisbank.ac.id Internet	<1%
26	pdfcoffee.com Internet	<1%
27	ejurnal.unisan.ac.id Internet	<1%
28	goens89.blogspot.com Internet	<1%
29	id.123dok.com Internet	<1%
30	repository.unsri.ac.id Internet	<1%
31	repository.unwidha.ac.id Internet	<1%
32	adoc.pub Internet	<1%

33	dspace.uii.ac.id Internet	<1%
34	eprints.ums.ac.id Internet	<1%
35	text-id.123dok.com Internet	<1%
36	aryojuned.wordpress.com Internet	<1%
37	librepo.stikesnas.ac.id Internet	<1%
38	repository.stietribhakti.ac.id Internet	<1%
39	dewisofia03.wordpress.com Internet	<1%
40	dosen.upi-yai.ac.id Internet	<1%
41	eprints.uns.ac.id Internet	<1%
42	jurnalkonstitusi.mkri.id Internet	<1%
43	library.binus.ac.id Internet	<1%
44	pelayananpublik.id Internet	<1%

45	rinjani.unitri.ac.id Internet	<1%
46	Muhammad Fachry Altarik, Andriyan Dwi Putra. "Perancangan Keaman... Crossref	<1%
47	eprints.undip.ac.id Internet	<1%
48	eprints.untirta.ac.id Internet	<1%
49	irfanamir89.blogspot.com Internet	<1%
50	katalog.ukdw.ac.id Internet	<1%
51	publikasi.mercubuana.ac.id Internet	<1%
52	skp2manokwari-ppid.pertanian.go.id Internet	<1%
53	digilib.unpas.ac.id Internet	<1%
54	faizfaisal44.wordpress.com Internet	<1%
55	repository.ub.ac.id Internet	<1%
56	neliti.com Internet	<1%

Lampiran 4

DAFTAR RIWAYAT HIDUP

Nama : Rahmat Rafli Suleman

Tempat, Tgl Lahir : Buol, 06 Januari 2002

Alamat : Panilan Jaya, Buol, Sulawesi Tengah

Email : rahmatid39@gmail.com

Riwayat Pendidikan:

1. Tahun 2014 Menyelesaikan Pendidikan di SDN 9 Tiloan

2. Tahun 2017, Menyelesaikan Pendidikan di SMPN 2 Tiloan

3. Tahun 2020, Menyelesaikan Pendidikan di SMK Negeri 1 Biau.

4. Tahun 2020, Mendaftar dan Diterima Menjadi Mahasiswa di Universitas Ichsan Gorontalo

Riwayat Pekerjaan:

Tahun 2020 s/d saat ini menjadi bagian dari admin civitas akademik Universitas Ichsan Gorontalo.