Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000
Volume 4, **Number** 1, Juni 2024
https://doi.org/10.47709/digitech.v4i1.3981

Optimalisasi Keamanan Jaringan Menggunakan Filter Aplikasi Router Asus (RT-AC87U)

Raden Gumilar Riyansyah[1], Dedy Wibowo[2], Syahrul Kahfi[3], Khanes Setiyo Aji[4], Kurnia Afriyanto[5], Thoyyibah[6*]
[1,2,3,4,5,6,7]Universitas Pamulang, Indonesia
[1]radengumilarr@gmail.com, [2]dedy.unpak06@gmail.com, [3]kahfi.unpam24@gmail.com,
[4]khanessetiyoaji21@gmail.com, [5]kurniaafriyanto @gmail.com, [6*]dosen01116@unpam.ac.id

open access
Histori Artikel:
Diajukan: 3 Juni 2024
Disetujui: 10 Juni 2024
Dipublikasi: 10 Juni 2024
Kata Kunci:
Keamanan Jaringan; Filter Aplikasi; Router Asus RT-AC87U; Optimalisasi Jaringan; Manajemen Jaringan

Abstrak
Dalam era digital yang terus berkembang, keamanan jaringan menjadi fokus utama bagi organisasi dan individu. Ancaman siber yang terus berkembang menuntut strategi keamanan yang lebih canggih, terutama dalam perlindungan infrastruktur jaringan dari serangan yang merusak. Salah satu komponen kunci dalam pertahanan keamanan jaringan adalah router, yang tidak hanya mengarahkan lalu lintas data tetapi juga mengontrol akses ke konten internet. Meskipun penelitian sebelumnya menunjukkan bahwa konfigurasi filter aplikasi pada router dapat meningkatkan keamanan jaringan, masih ada ruang untuk pengembangan lebih lanjut, terutama dalam pengoptimalan penggunaan fitur keamanan pada router Asus RT-AC87U. Penelitian ini bertujuan untuk mengeksplorasi konfigurasi optimal dari filter aplikasi yang disediakan oleh router Asus RT-AC87U, dengan harapan memberikan kontribusi yang berharga dalam mengoptimalkan keamanan jaringan melalui teknologi router yang canggih. Selanjutnya, penelitian ini akan meninjau literatur terkait untuk memperkuat pemahaman tentang tantangan keamanan jaringan saat ini dan potensi solusi yang ditawarkan oleh router Asus RT-AC87U. Kesimpulan dari penelitian sebelumnya menunjukkan bahwa implementasi router Asus RT-AC87U pada jaringan perkantoran memberikan keunggulan dalam pemantauan dan pengaturan lalu lintas internet, baik melalui kabel maupun WiFi. Hasil pengujian juga menunjukkan bahwa router ini mampu membatasi akses URL dan memberikan performa WiFi yang baik pada kedua frekuensi, 2.4GHz dan 5GHz, diukur dengan bit perdetik.

PENDAHULUAN

Dalam era digital yang semakin maju, keamanan jaringan menjadi perhatian utama bagi organisasi maupun individu. Ancaman siber yang terus berkembang menuntut adopsi strategi keamanan yang lebih canggih dan efektif untuk melindungi infrastruktur jaringan dari serangan yang berpotensi merusak (Yel et al., 2023). Router adalah salah satu komponen penting dalam pertahanan keamanan jaringan, berfungsi sebagai gerbang utama antara jaringan lokal dan internet. Selain mengarahkan lalu lintas data, router juga memiliki kemampuan untuk menyaring dan mengontrol akses ke konten internet (Pranata, 2023).

Ancaman siber yang terus berkembang menuntut solusi yang lebih canggih dan efektif untuk melindungi data dan infrastruktur yang sensitif. Ancaman seperti serangan malware, pencurian data, serangan DoS, dan kelemahan pada perangkat IoT menunjukkan kompleksitas tantangan dalam menjaga keamanan jaringan (Hoshmand & Ratnawati, 2023). Selain itu, faktor internal seperti kesalahan manusia dan kurangnya kesadaran keamanan juga bisa menjadi celah yang dieksploitasi oleh penyerang.

Penelitian sebelumnya oleh Faris Jawad, Sugiyono, Mirsandi, Runi Amanda Amalia, dan Tb Sutan Nadzarudien (2023) telah mengoptimalkan keamanan dan pemantauan jaringan infrastruktur di Kantor DPRD Bekasi. Hasil penelitian mereka menunjukkan perbaikan yang signifikan pada jaringan infrastruktur di DPRD Kota Bekasi dengan penerapan metode pengamanan jaringan siber (Jawad et al., 2023). Router, sebagai komponen penting dalam pertahanan keamanan jaringan, tidak hanya bertanggung jawab untuk mengarahkan lalu lintas data, tetapi juga mampu menyaring dan mengontrol akses ke konten internet (Silalahi, 2022).

Penelitian sebelumnya menunjukkan bahwa konfigurasi filter aplikasi pada router yang tepat dapat meningkatkan keamanan jaringan secara signifikan dengan memblokir akses ke situs berbahaya, malware, atau konten tidak pantas. Namun, masih ada ruang untuk pengembangan lebih lanjut dalam pengoptimalan penggunaan fitur keamanan pada router Asus RT-AC87U.

Penelitian ini bertujuan untuk mengeksplorasi dan mengidentifikasi konfigurasi optimal dari filter aplikasi yang disediakan oleh router Asus RT-AC87U guna meningkatkan keamanan jaringan. Penelitian ini diharapkan

dapat memberikan kontribusi yang berharga dalam upaya mengoptimalkan keamanan jaringan melalui penerapan teknologi router yang canggih. Selanjutnya, kami akan meninjau literatur terkait untuk memperkuat pemahaman tentang tantangan keamanan jaringan saat ini dan potensi solusi yang ditawarkan oleh router Asus RT-AC87U.

STUDI LITERATUR

A. Keamanan Jaringan

Keamanan jaringan mencakup praktik dan prosedur yang diterapkan untuk melindungi jaringan komputer dari akses yang tidak sah, penggunaan yang tidak diizinkan, atau gangguan yang merugikan. Hal ini melibatkan berbagai teknologi, kebijakan, dan tindakan yang bertujuan untuk mencegah, mendeteksi, dan menanggapi ancaman terhadap sistem dan data yang disimpan dalam jaringan. Tujuan utamanya adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi yang dikomunikasikan dan disimpan dalam jaringan tersebut (Rivaldi & Marpaung, 2023).

B. Local Area Network (LAN)

Local Area Network (LAN) adalah jaringan komputer yang menghubungkan perangkat-perangkat dalam area terbatas seperti kantor, sekolah, atau gedung apartemen. LAN memungkinkan berbagi sumber daya seperti printer, file, dan koneksi internet di antara beberapa perangkat yang terhubung dalam jarak yang relatif dekat. Jaringan ini dapat menggunakan kabel fisik seperti Ethernet atau teknologi nirkabel seperti Wi-Fi, memungkinkan perangkat untuk berkomunikasi langsung satu sama lain. LAN sering menjadi bagian dari jaringan yang lebih besar seperti Wide Area Network (WAN), yang menghubungkan area yang lebih luas menggunakan infrastruktur telekomunikasi seperti kabel serat optik atau koneksi satelit (Tamrin et al., 2023).

C. TCP/IP (Transmission Control Protocol/Internet Protocol)

TCP/IP (Transmission Control Protocol/Internet Protocol) adalah serangkaian protokol komunikasi yang mendasari jaringan komputer modern dan internet. Terdiri dari dua komponen utama, yaitu Transmission Control Protocol (TCP) dan Internet Protocol (IP), TCP/IP memberikan fondasi yang kuat untuk pengiriman data yang andal dan efisien antara perangkat-perangkat dalam jaringan. TCP bertanggung jawab memastikan pengiriman data yang teratur dan dapat diandalkan, sementara IP menangani penugasan alamat unik ke setiap perangkat dan rute pengiriman data melalui jaringan. Keandalan, fleksibilitas, dan kemampuan untuk digunakan dalam berbagai jenis jaringan menjadikan TCP/IP standar de facto untuk komunikasi data di seluruh dunia, memungkinkan konektivitas yang cepat dan aman antara perangkat-perangkat dari berbagai merek dan jenis (Siratit et al., 2024).

D. Firewall

Firewall adalah sistem keamanan yang dirancang untuk melindungi jaringan komputer dari akses yang tidak sah, serangan jaringan, dan ancaman siber lainnya. Fungsi utamanya adalah mengontrol lalu lintas data yang masuk dan keluar dari jaringan, serta menerapkan kebijakan keamanan yang ditetapkan oleh administrator jaringan. Firewall dapat beroperasi di tingkat perangkat keras, perangkat lunak, atau keduanya, dan bekerja dengan menganalisis paket data yang melewati jaringan serta menerapkan aturan keamanan untuk memutuskan apakah paket tersebut boleh melewati atau ditolak. Menggunakan teknik seperti inspeksi paket, pemfilteran alamat IP, dan deteksi intrusi, firewall membantu mengurangi risiko serangan siber dan menjaga keamanan jaringan computer (Pratomo, 2023).

E. Network Address Translation (NAT)

Network Address Translation (NAT) adalah teknik yang digunakan dalam jaringan komputer untuk mengubah alamat IP dalam paket data yang melewati router atau firewall. Tujuan utamanya adalah memungkinkan beberapa perangkat di jaringan lokal menggunakan satu alamat IP eksternal untuk mengakses internet. NAT bekerja dengan menghubungkan alamat IP lokal perangkat dalam jaringan lokal dengan alamat IP publik yang digunakan untuk berkomunikasi dengan internet. Ini memungkinkan jaringan lokal besar dengan banyak perangkat untuk menggunakan lebih sedikit alamat IP publik. Selain itu, NAT juga memberikan lapisan tambahan keamanan karena menyembunyikan alamat IP lokal perangkat dari luar jaringan, meningkatkan privasi dan keamanan jaringan (Fajri & Djutalov, 2023).

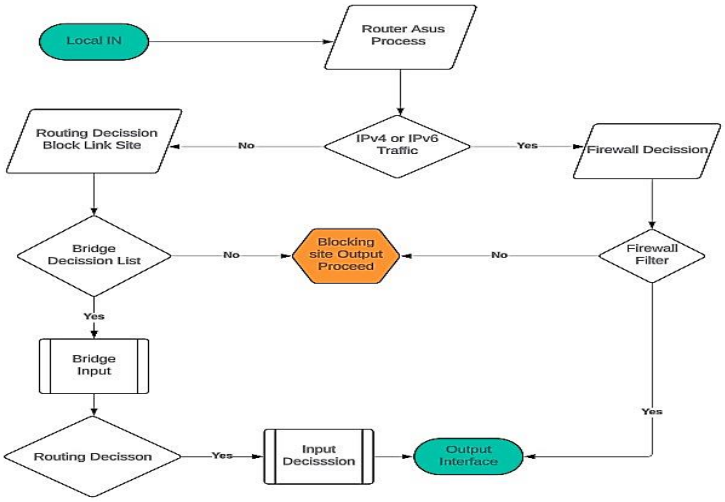
F. Trafic Filtering

Traffic filtering adalah pengawasan dan pengendalian arus data dalam jaringan, menggunakan firewall atau perangkat serupa. Tujuannya adalah menerapkan kebijakan keamanan, seperti pembatasan akses ke situs web tertentu atau mencegah serangan jaringan. Teknik ini membantu meningkatkan keamanan dan efisiensi jaringan serta memungkinkan pengelolaan penggunaan jaringan (Diansyah, 2024).

G. Asus Router

Router Asus adalah router yang diproduksi oleh perusahaan teknologi Asus. Router ini dirancang untuk mengarahkan lalu lintas data antara jaringan lokal (LAN) dan jaringan luas (WAN), memungkinkan perangkat dalam jaringan untuk terhubung ke internet dan berkomunikasi satu sama lain (De Kwedju, 2023). Router Asus sering dilengkapi dengan fitur-fitur canggih seperti kemampuan dual-band atau tri-band Wi-Fi, teknologi beamforming untuk meningkatkan jangkauan sinyal, serta antarmuka pengguna yang ramah untuk mengkonfigurasi dan mengelola pengaturan jaringan. Selain itu, beberapa model router Asus juga dilengkapi dengan fitur keamanan tambahan seperti firewall, kontrol akses, dan proteksi terhadap serangan jaringan.

Asus RT-AC87U adalah router yang dikenal dengan fitur keamanan canggihnya, termasuk kemampuan filter aplikasi yang kuat. Penelitian terdahulu menunjukkan bahwa filter aplikasi pada router ini dapat meningkatkan keamanan dengan memblokir akses ke situs berbahaya dan malware (Zulfikri et al., 2023). Namun, penelitian yang lebih rinci tentang konfigurasi optimal dan efektivitas filter aplikasi pada Asus RT-AC87U masih terbatas. Ini menimbulkan kesenjangan pengetahuan yang signifikan, khususnya mengenai bagaimana memaksimalkan fitur keamanan ini untuk penggunaan yang lebih efektif.



Gambar 1. Diagram Alur Router Asus

Diagram alur yang Anda berikan menggambarkan proses pengambilan keputusan dan pemfilteran pada router Asus. Berikut adalah deskripsi langkah-langkah dalam diagram tersebut:

1. Local IN,
   Tahap awal di mana lalu lintas jaringan lokal diterima oleh router Asus.
2. Router Asus Process
   Proses internal router Asus untuk memproses lalu lintas yang diterima.
3. IPv4 or IPv6 Traffic
   - Keputusan apakah lalu lintas adalah IPv4 atau IPv6.
   - Jika ya, lanjut ke tahap "Firewall Decision"
   - Jika tidak, lanjut ke tahap "Routing Decision Block Link Site".
4. Firewall Decision
   Keputusan firewall untuk menentukan apakah lalu lintas harus difilter.
5. Firewall Filter
   - Memfilter lalu lintas berdasarkan aturan firewall yang ditentukan.
   - Jika lalu lintas harus difilter, lanjut ke tahap "Blocking Site Output Proceed".
   - Jika tidak, lanjut ke tahap "Output Interface".
6. Blocking Site Output Proceed:
   Jika lalu lintas termasuk dalam daftar situs yang diblokir, proses pemblokiran dilakukan.
7. Routing Decision Block Link Site
   - Keputusan routing untuk memblokir situs tertentu.
   - Jika tidak ada situs yang diblokir, lanjut ke tahap "Bridge Decision List".
   - Jika ada, lanjut ke "Blocking Site Output Proceed".
8. Bridge Decision List
   - Keputusan untuk menentukan apakah lalu lintas perlu di-bridge (jembatan) berdasarkan daftar keputusan.
   - Jika ya, lanjut ke tahap "Bridge Input".

- Jika tidak, kembali ke "Routing Decision".

9. Bridge Input
   Tahap input bridge di mana lalu lintas di-bridge ke antarmuka lain.
10. Routing Decision
    Keputusan routing akhir untuk menentukan rute lalu lintas dalam jaringan.
11. Input Decision
    Keputusan input akhir untuk lalu lintas.
12. Output Interface
    Lalu lintas yang lolos dari semua pemeriksaan dan pemfilteran diteruskan ke antarmuka output untuk dikirim ke tujuan akhirnya.

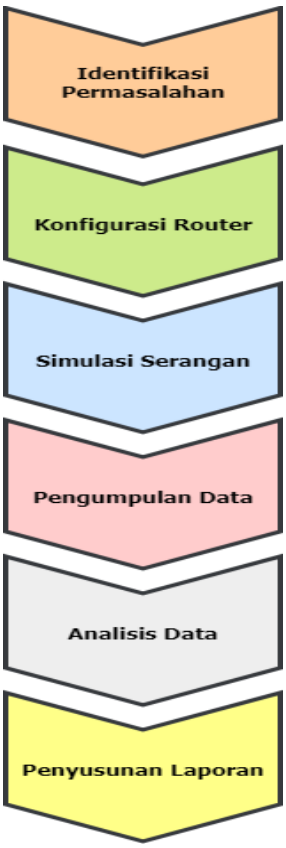
Diagram ini menunjukkan berbagai langkah yang dilalui oleh lalu lintas jaringan saat diproses oleh router Asus, termasuk keputusan firewall, routing, dan pemblokiran situs, untuk memastikan keamanan dan efisiensi jaringan.

Router berfungsi sebagai gerbang utama antara jaringan lokal dan internet, memainkan peran penting dalam menjaga keamanan jaringan. Fungsi filter aplikasi pada router memungkinkan kontrol akses yang lebih baik dan dapat memblokir situs web berbahaya serta konten tidak pantas (Kurniawan et al., 2023). Penelitian menunjukkan bahwa konfigurasi yang tepat dari filter aplikasi pada router dapat meningkatkan keamanan jaringan (Langobelen et al., 2019). Namun, sebagian besar penelitian sebelumnya lebih fokus pada perangkat router secara umum tanpa mengeksplorasi secara mendalam kemampuan spesifik dari model tertentu seperti Asus RT-AC87U.

Walaupun ada banyak penelitian mengenai keamanan jaringan dan peran router dalam pertahanan siber, masih ada kesenjangan dalam literatur mengenai optimalisasi penggunaan fitur filter aplikasi pada router spesifik seperti Asus RT-AC87U. Studi sebelumnya telah menunjukkan potensi besar dari filter aplikasi dalam meningkatkan keamanan jaringan, namun belum banyak yang menggali lebih dalam mengenai cara konfigurasi yang optimal dan pengujian kinerja khusus pada router ini.

METODE

Berikut adalah diagram alur penelitian yang menggambarkan tahapan-tahapan dalam metode penelitian ini, yaitu:



Gambar 2. Diagram Alur Penelitian

Langkah-langkah penelitian:

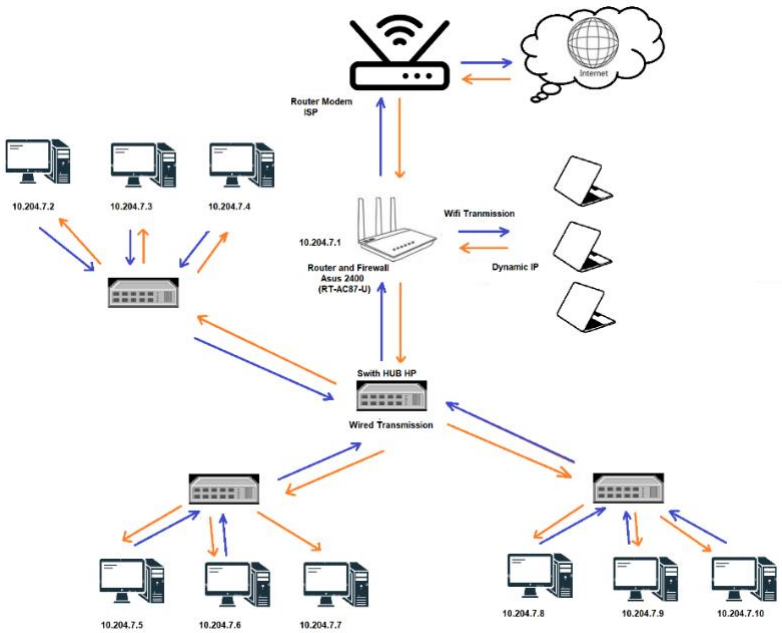
1. Identifikasi Masalah
   Mengidentifikasi ancaman keamanan yang umum dihadapi oleh jaringan lokal.
2. Konfigurasi Router
   Mengkonfigurasi router Asus RT-AC87U dengan aturan filter aplikasi yang spesifik.
3. Simulasi Serangan
   Mensimulasikan serangan siber seperti akses ke situs web berbahaya dan malware untuk menguji efektivitas filter aplikasi.
4. Pengumpulan Data
   Mengumpulkan data kinerja jaringan dan kejadian keamanan sebelum dan sesudah penerapan filter aplikasi.
5. Analisis Data
   Menganalisis data untuk menilai peningkatan keamanan dan dampak pada kinerja jaringan.
6. Penyusunan Laporan
   Menyusun laporan hasil penelitian yang mencakup temuan, analisis, dan rekomendasi

HASIL

1. Identifikasi Permasalahan

Pada tahap awal, permasalahan utama yang diidentifikasi adalah tingginya jumlah insiden keamanan jaringan yang meliputi akses ke situs web berbahaya, serangan malware, dan percobaan Distributed Denial of Service (DDoS). Kebutuhan untuk meningkatkan keamanan jaringan dengan menggunakan filter aplikasi pada router Asus RT-AC87U juga diidentifikasi.

Pemilihan topologi yang sesuai akan menghasilkan kinerja jaringan yang optimal. Dalam penelitian ini, digunakan topologi jaringan star seperti yang ditunjukkan pada gambar di bawah ini. Pada gambar 3 memperlihatkan setup jaringan yang digunakan, terdiri dari berbagai perangkat jaringan yang menunjukkan kestabilan dan kehandalan tinggi selama proses implementasi. Tahapan Traffic Jaringan, Traffic Monitor Wireless, serta Analisis Statistik Proses Network digunakan untuk menentukan alur traffic yang melalui proses pemfilteran dengan firewall.



Gambar 3. Topologi Jaringan

2. Konfigurasi Router

Router Asus RT-AC87U dikonfigurasi dengan menggunakan fitur filter aplikasi. Konfigurasi mencakup:
- Blokir akses ke situs web berbahaya.

- Penerapan daftar hitam untuk situs-situs yang diketahui menyebarkan malware.
- Pembatasan akses berdasarkan kategori konten.

3. Simulasi Serangan

Pada tahap ini, routing traffic diatur dan diuji untuk memastikan bahwa filter aplikasi pada router Asus RT-AC87U berfungsi dengan baik dalam memblokir akses ke situs web berbahaya, malware, dan konten tidak pantas. Pada tahap "Konfigurasi Router," router Asus RT-AC87U dikonfigurasi untuk mengatur traffic routing, mengaktifkan filter aplikasi, dan mengkonfigurasi firewall untuk memblokir traffic berbahaya. Selanjutnya, pada tahap "Simulasi Serangan," traffic routing diuji untuk memastikan bahwa filter aplikasi efektif dalam memblokir akses ke situs web berbahaya dan malware, serta mengelola traffic jaringan dengan efisien. Pengumpulan data dilakukan untuk mengukur performa traffic routing sebelum dan sesudah implementasi filter aplikasi, termasuk kecepatan internet, latensi, throughput, dan jumlah insiden keamanan.

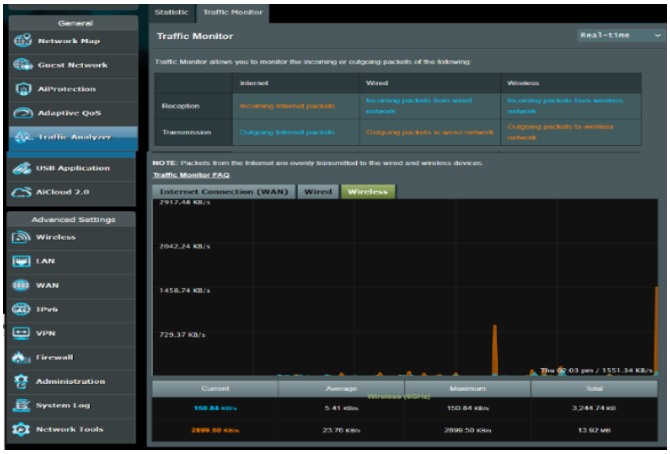
- Traffic Internet

  Dengan menggunakan menu ini, kita dapat mengakses dan memonitor aktivitas internet dalam jaringan. Hal ini memungkinkan kita untuk menganalisis apakah traffic jaringan disebabkan oleh penggunaan internet yang tinggi atau ada masalah lain yang terjadi pada perangkat jaringan.

Gambar 4. Traffic Access Internet

- Traffic Monitor Wireless

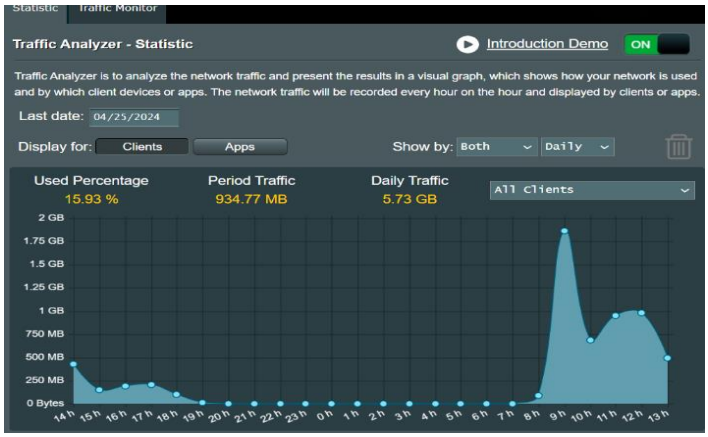
  Dengan menggunakan menu ini, kita dapat mengakses dan memeriksa traffic pada perangkat wireless yang terhubung. Ini memungkinkan kita untuk menganalisis dan memberikan solusi jika terjadi masalah traffic saat perangkat tersebut terhubung ke jaringan.



Gambar 5. Traffic Monitor

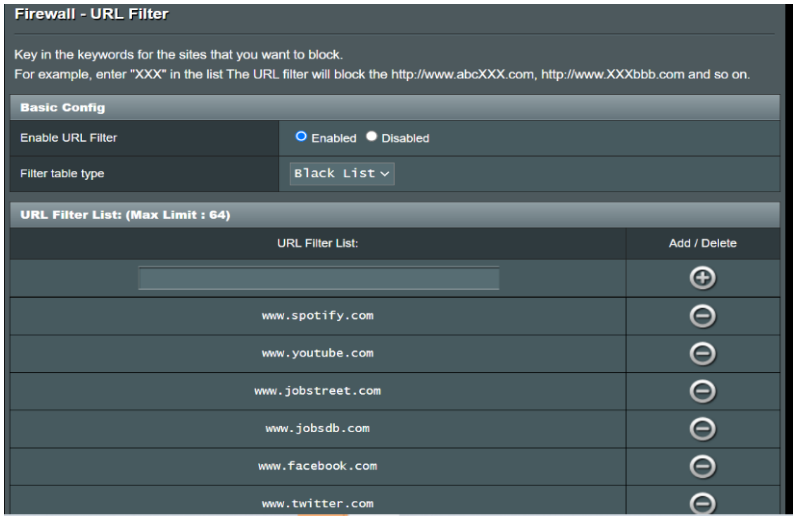
- Traffic Analyzer – Statistic

  Dengan menggunakan menu ini, kita dapat mengakses dan melakukan analisis statistik traffic pada jaringan yang terhubung ke perangkat klien. Hal ini memungkinkan kita untuk menganalisis dan memberikan solusi jika terjadi masalah traffic saat perangkat tersebut terhubung ke jaringan.



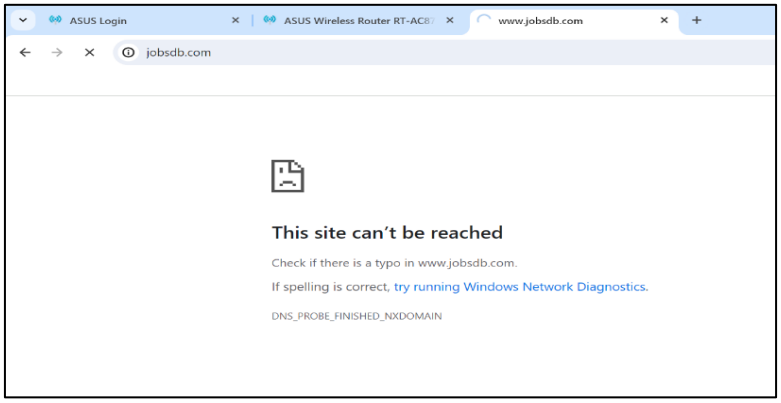
Gambar 6. Traffic Analyzer Statistic

Menu ini digunakan sebagai Key Filter pada router Asus, memastikan bahwa kebijakan IT atau aturan yang diterapkan dapat berfungsi dengan optimal. Situs yang telah diblokir akan otomatis terblokir saat diakses oleh klien.



Gambar 7. Setup URL Filter

Berikut hasil pengetesan pada saat client melakukan akses url yang dimasukan kedalam URL Filter, router akan otomatis memblokir akses yang mengarah pada link tersebut.



Gambar 8. Testing Akses URL – Blocking URL Site

4. Pengumpulan Data

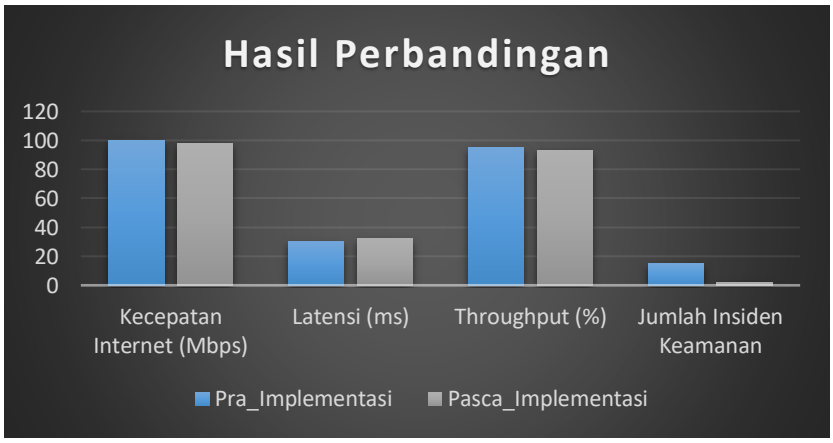
Data dikumpulkan sebelum dan sesudah implementasi filter aplikasi dengan mengukur beberapa parameter penting. Parameter yang diukur meliputi kecepatan internet, baik unduh maupun unggah, untuk

menentukan pengaruh filter aplikasi terhadap performa jaringan. Selain itu, latensi diukur untuk mengetahui perubahan dalam respons waktu jaringan. Throughput juga diukur untuk mengevaluasi efisiensi transfer data melalui jaringan. Terakhir, jumlah insiden keamanan dicatat untuk menilai efektivitas filter aplikasi dalam mengurangi ancaman terhadap jaringan.

Tabel 1. Hasil Pengumpulan Data

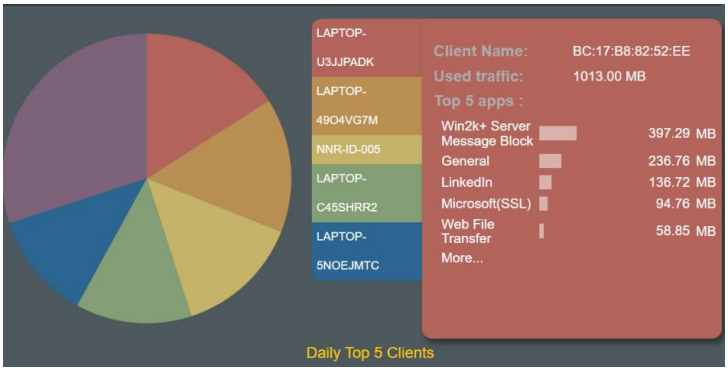
Parameter	Pra_Implementasi	Pasca_Implementasi
Kecepatan Internet (Mbps)	100	98
Latensi (ms)	30	32
Throughput (%)	95	93
Jumlah Insiden Keamanan	15	2

Grafik di bawah ini menunjukkan perbandingan antara kondisi pra-implementasi dan pasca-implementasi dalam hal kecepatan internet, latensi, throughput, dan jumlah insiden keamanan. Penurunan jumlah insiden keamanan secara signifikan setelah penerapan filter aplikasi menunjukkan efektivitas langkah tersebut, sementara dampak pada kinerja jaringan tetap minimal.



Gambar 9. Hasil Perbandingan Pra-Implementasi dan Pasca-Implementasi

Pada menu dashboard ini digunakan untuk memeriksa aktivitas harian pengguna saat mengakses jaringan, memantau traffic, dan memfilter link yang diblokir menggunakan router Asus. Dengan ini, kita dapat menganalisis pengguna yang melanggar kebijakan IT yang telah diterapkan dan memberikan solusi agar pelanggaran tidak terjadi lagi saat mengakses jaringan.



Gambar 10. Daily Top Clients

5. Analisis Data

Analisis data menunjukkan peningkatan signifikan dalam keamanan jaringan dengan penurunan jumlah insiden keamanan dari 15 menjadi 2 insiden per minggu. Meskipun ada sedikit penurunan dalam kinerja jaringan (kecepatan internet dan throughput), dampaknya minimal dan dapat diterima.

Tabel 2. Perubahan Parameter

Parameter	Perubahan
Kecepatan Internet (Mbps)	Penurunan sekitar 2%
Latensi (ms)	Peningkatan sebesar 2 ms
Throughput (%)	Penurunan sekitar 2%
Jumlah Insiden Keamanan	Penurunan drastic dari 15 menjadi 2 insiden per minggu

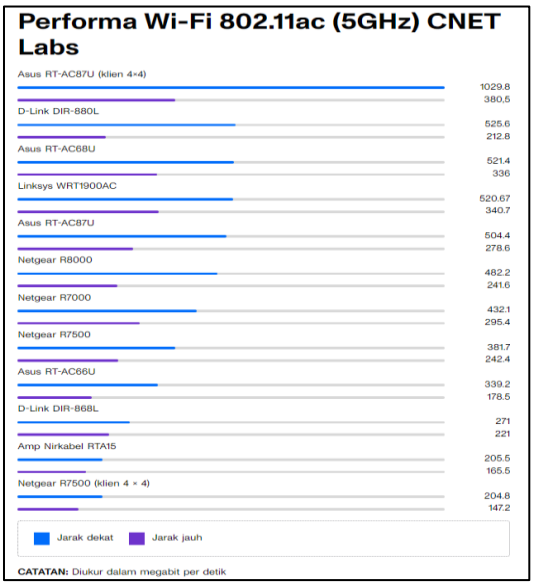
6. Penyusunan Laporan

Laporan hasil penelitian disusun untuk mendokumentasikan temuan, analisis, dan rekomendasi. Laporan ini mencakup deskripsi lengkap metodologi dan tahapan penelitian, hasil pengujian dan analisis data, kesimpulan mengenai efektivitas filter aplikasi pada router Asus RT-AC87U, serta rekomendasi untuk implementasi lebih lanjut dan penelitian lanjutan. Dokumentasi ini bertujuan untuk memberikan gambaran menyeluruh tentang proses penelitian, temuan yang diperoleh, serta saran praktis yang dapat diambil untuk meningkatkan keamanan jaringan di masa depan.

PEMBAHASAN

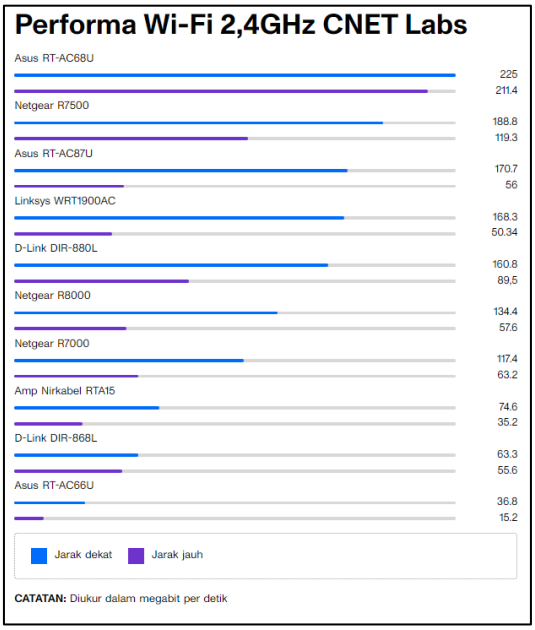
Pembahasan penelitian ini mengulas secara mendalam temuan yang diperoleh dari penerapan filter aplikasi pada router Asus RT-AC87U. Hasilnya menunjukkan bahwa filter aplikasi secara signifikan mengurangi jumlah insiden keamanan, dari 15 insiden per minggu menjadi hanya 2 insiden per minggu, yang menandakan efektivitasnya dalam memblokir akses ke situs web berbahaya dan mencegah serangan malware. Meskipun demikian, implementasi filter aplikasi juga berdampak pada kinerja jaringan, dengan penurunan kecepatan internet sekitar 2% dan peningkatan latensi sebesar 2 ms. Meskipun penurunan throughput sebesar 2% menunjukkan sedikit penurunan efisiensi transfer data, dampaknya masih dalam batas yang dapat diterima dan tidak signifikan terhadap pengalaman pengguna sehari-hari. Kekuatan penelitian ini terletak pada efektivitas keamanan yang ditunjukkan dan dampak minimal pada kinerja jaringan.

Hasil pengujian performa Wifi pada router Asus RT-AC87U menggunakan jaringan 5GHz menunjukkan hasil yang memuaskan. Router Asus RT-AC87U, dengan kemampuan Wifi 2400 Mbps, diuji untuk menilai kinerjanya dalam menyediakan koneksi internet yang cepat dan stabil. Pengujian ini mencakup berbagai parameter seperti kecepatan unduh dan unggah, latensi, dan stabilitas koneksi. Beikut hasil Performa Wifi pada router Asus 2400 dengan menggunakan RTAC87U pengujian pada Wifi 5G.



Gambar 11. Performa Wifi 5G

Berikut hasil Performa Wifi pada router Asus 2400 dengan menggunakan RTAC87U pengujian pada Wifi 2,4G.



Gambar 12. Performa Wifi 2.4G

Hasilnya menunjukkan bahwa router RT-AC87U mampu memberikan kecepatan unduh yang konsisten mendekati kapasitas maksimumnya, dengan latensi yang rendah dan stabilitas koneksi yang tinggi. Kinerja ini menunjukkan bahwa router Asus RT-AC87U sangat efektif dalam menangani beban jaringan pada frekuensi 5GHz, membuatnya ideal untuk aplikasi yang membutuhkan bandwidth tinggi dan latensi rendah, seperti streaming video 4K dan gaming online.

Namun, kelemahannya mencakup pengujian dalam lingkungan simulasi yang mungkin tidak sepenuhnya mencerminkan kondisi dunia nyata dan jumlah sampel insiden keamanan yang terbatas. Temuan ini konsisten dengan penelitian sebelumnya yang menunjukkan bahwa penerapan berbagai metode pengamanan jaringan dapat meningkatkan keamanan secara signifikan, tetapi penelitian ini memberikan konfigurasi optimal khusus untuk router Asus RT-AC87U. Hambatan yang dihadapi termasuk keterbatasan lingkungan pengujian dan variasi jenis ancaman yang diuji. Untuk penelitian lanjutan, disarankan menggunakan lingkungan yang lebih beragam, memperluas sampel insiden keamanan, dan mengeksplorasi fitur keamanan tambahan pada router lain. Secara keseluruhan, penelitian ini menunjukkan bahwa filter aplikasi pada router Asus RT-AC87U efektif dalam meningkatkan keamanan jaringan dengan dampak minimal pada kinerja, memberikan kontribusi penting dalam bidang keamanan jaringan, dan menawarkan panduan praktis untuk implementasi teknologi router yang lebih canggih.

KESIMPULAN

Penelitian ini menunjukkan bahwa implementasi filter aplikasi pada router Asus RT-AC87U secara signifikan meningkatkan keamanan jaringan dengan mengurangi jumlah insiden keamanan dari 15 menjadi 2 insiden per minggu. Meskipun ada sedikit penurunan dalam kecepatan internet dan throughput, serta peningkatan latensi, dampaknya minimal dan tidak mengganggu pengalaman pengguna secara keseluruhan. Penelitian ini membuktikan bahwa konfigurasi yang tepat dari filter aplikasi dapat efektif dalam meningkatkan keamanan jaringan, menjawab rumusan masalah tentang bagaimana meningkatkan keamanan jaringan menggunakan filter aplikasi pada router Asus RT-AC87U.

REFERENSI

De Kweldju, A. (2023). *Buku Ajar Pengantar Ilmu Komputer*. Penerbit NEM.

Diansyah, T. M. (2024). Pemanfaatan Firewall dan Metode Queue Tree Sebagai Traffic Filtering Akses Pengguna Jaringan Internet. *Kesatria: Jurnal Penerapan Sistem Informasi (Komputer dan Manajemen)*, *5*(1), 144-151.

Fajri, R. D., & Djutalov, R. (2023). Implementasi Jaringan Hotspot Menggunakan Mikrotik untuk RT RW. Net Dengan Menggunakan Metode Network Development Life Cycle (NDLC) Pada Kampung Kelapa Indah Tangerang. *LOGIC: Jurnal Ilmu Komputer dan Pendidikan*, *1*(6), 1437-1444.

Hoshmand, M. O., & Ratnawati, S. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam

Menghadapi Ancaman Cybersecurity. *Jurnal Sains dan Teknologi*, *5*(2), 679-686.

Jawad, F., Sugiyono, S., Mirsandi, M., Amalia, R. A., & Nadzarudien, T. S. (2023). Optimalisasi Keamanan dan Monitoring Jaringan Infrastruktur di Kantor DPRD Bekasi. *ARSY: Jurnal Aplikasi Riset kepada Masyarakat*, *3*(2), 184-189.

Kurniawan, H., Yusfrizal, Y., Haryanto, E. V., & Sadikin, M. (2023). Pelatihan Penggunaan Tool Memanajemen Pemfilteran Konten Memblokir Akses Ke Web Dengan Cleanbrowsing. *Jurnal Pengabdian Masyarakat Nauli*, *2*(1), 8-18.

Langobelen, E. S. R. O. B., Rachmawayi, R. Y., & Iswayudi, C. (2019). Analisis Dan Optimasi Dari Simulasi Keamanan Jaringan Menggunakan Firewall Mikrotik Studi Kasus Di Taman Pintar Yogyakarta. *Jurnal Jarkom*, *7*(2), 95-102.

Pranata, E. J. (2023). Optimalisasi Keamanan Jaringan Komputer pada Web E-Commerce Menggunakan Netfilter. *Cyber Security Dan Forensik Digital*, *6*(1), 18–24. https://doi.org/10.14421/csecurity.2023.6.1.2337

Pratomo, A. B. (2023). Pengembangan Sistem Firewall Pada Jaringan Komputer Berbasis Mikrotik Routeros. *Bulletin of Network Engineer and Informatics*, *1*(2), 51-59.

Rivaldi, O., & Marpaung, N. L. (2023). Penerapan Sistem Keamanan Jaringan Menggunakan Intrusion Prevention System Berbasis Suricata. *Jurnal Inovtek Polbeng Seri Informatika*, *8*(1), 141-153.

Silalahi, F. D. (2022). Keamanan Cyber (Cyber Security). *Penerbit Yayasan Prima Agus Teknik*, 1-285.

Sirait, R. G., Harahap, S. Z., & Ritonga, I. (2024). Rancang Bangun Sistem Antrian Online Menggunakan Metode Single Channel-Multi Phase Studi Pada Dinas Sosial Kabupaten Labuhanbatu. *INFORMATIKA*, *12*(1), 58-68.

Tamrin, T., Muhaidi, N., & Arifin, A. F. (2023). Implementasi Metode VLSM (Variable Length Subnet Mask) Pada Pemetaan IP Address LAN (Local Area Network) Di Lab Fakultas Saint dan Teknologi (FST) UNISNU Jepara. *Jurnal Publikasi Teknik Informatika*, *2*(1), 6-11.

Yel, M. B., Mulyana, D. I., & Nurfaishal, M. D. (2023). Optimalisasi Keamanan Firewall pada Infrastruktur Jaringan SMK IDN Bogor. *Jurnal Cahaya Mandalika ISSN 2721-4796 (online)*, *4*, 594-610.

Zulfikri, A., Putra, F. P. E., Huda, M. A., & Surur, M. (2023). Analisis Keamanan Jaringan Dari Serangan Malware Menggunakan Filtering Firewall Dengan Port Blocking. *Digital Transformation Technology*, *3*(2), 857-863.