NARATIF : Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika
Vol. 08 No. 01 Juni 2026
P-ISSN: 2656-7377 || E-ISSN: 2714-8467

PERANCANGAN KEAMANAN JARINGAN DAN MANAJEMEN BANDWIDTH BERBASIS HTB UNTUK MENINGKATKAN QoS MENGGUNAKAN METODE NDLC

Hena Sulaeman[1], Ahsani Takwim[2]
Teknik Informatika[1, 2]
Universitas Teknologi Bandung[1, 2]
henasulaeman@utb-univ.ac.id[1] ahsanitakwim10@gmail.com[2]

Abstrak

Berdasarkan data yang telah di kumpulkan Universitas Teknologi Bandung pernah mengalami insiden keamanan jaringan berupa serangan *Brute Force* yang berhasil memperoleh kredensial pengguna serta serangan *Distributed Denial of Service* (DDoS) yang terdeteksi pada router jaringan. Selain itu, pengguna juga mengeluhkan lambatnya akses internet akibat belum optimalnya pengelolaan bandwidth. Penelitian ini bertujuan merancang dan mengimplementasikan sistem keamanan jaringan serta manajemen bandwidth untuk meningkatkan kualitas layanan jaringan (*Quality of Service atau QoS*) menggunakan metode *Network Development Life Cycle* (NDLC). Tahapan penelitian meliputi analysis, design, simulation, implementation, monitoring, dan management. Implementasi keamanan jaringan dilakukan melalui konfigurasi *Firewall Filter Rules, Firewall Mangle*, serta mekanisme proteksi terhadap serangan *Brute Force* dan DDoS. Sementara itu, optimasi bandwidth dilakukan menggunakan *Queue Tree* berbasis *Hierarchical Token Bucket* (HTB). Hasil penelitian menunjukkan bahwa konfigurasi Firewall Filter Rules berhasil mendeteksi dan memblokir alamat IP yang melakukan percobaan login berulang (Brute Force), sedangkan mekanisme proteksi DDoS mampu memfilter lalu lintas jaringan yang terindikasi sebagai serangan sehingga tidak mengganggu layanan jaringan. Selain itu, implementasi Queue Tree berbasis HTB berhasil mengalokasikan bandwidth sesuai dengan prioritas pengguna sehingga distribusi bandwidth menjadi lebih merata dan penggunaan jaringan lebih efisien. Penerapan metode NDLC juga terbukti memberikan tahapan yang sistematis dalam proses perancangan, implementasi, dan evaluasi infrastruktur jaringan. Dengan demikian, penelitian ini menghasilkan rancangan jaringan yang lebih aman, mampu mengoptimalkan penggunaan bandwidth, serta mendukung peningkatan kualitas layanan jaringan.
Kata kunci : Keamanan jaringan, manajemen *bandwidht, Network Development Life Cycle* (NDLC), *firewall filter rules*

Abstract

Based on the collected data, Universitas Teknologi Bandung has experienced network security incidents, including a Brute Force attack that successfully obtained user credentials and a Distributed Denial of Service (DDoS) attack detected on the network router. In addition, users reported slow internet access due to suboptimal bandwidth management. This study aims to design and implement a network security and bandwidth management system to improve network service quality (Quality of Service/QoS) using the Network Development Life Cycle (NDLC) method. The research stages consist of analysis, design, simulation, implementation, monitoring, and management. The network security implementation was carried out through the configuration of Firewall Filter Rules, Firewall Mangle, and protection mechanisms against Brute Force and DDoS attacks. Meanwhile, bandwidth optimization was implemented using Queue Tree based on the Hierarchical Token Bucket (HTB) method. The results show that the configured Firewall Filter Rules successfully detected and blocked IP addresses performing repeated login attempts (Brute Force), while the DDoS protection mechanism effectively filtered malicious network traffic, preventing disruptions to network services. Furthermore, the HTB-based Queue Tree successfully allocated bandwidth according to user priorities, resulting in a more balanced bandwidth distribution and more efficient network utilization. The implementation of the NDLC method also proved to provide a systematic approach for the design, implementation, and evaluation of network infrastructure. Therefore, this study produced a more secure network architecture, optimized bandwidth utilization, and contributed to improving the overall quality of network services
Keywords : Network security, bandwidth management, Network Development Life Cycle (NDLC), firewall filter rules

I. PENDAHULUAN

Perkembangan penetrasi pengguna internet di Indonesia menunjukkan tren peningkatan yang signifikan pada tahun 2026. Berdasarkan data, dari total populasi Indonesia yang mencapai 287.886.782 jiwa, sebanyak 235.261.078 jiwa telah terhubung dengan jaringan internet, atau setara dengan 81,72% dari total populasi. Selanjutnya, apabila ditinjau berdasarkan tingkat pendidikan, tingkat penetrasi penggunaan internet menunjukkan variasi yang cukup tinggi, yaitu pada kelompok pendidikan SMP/sederajat sebesar 82,48%, SMA/SMK/sederajat sebesar 90,44%, dan perguruan tinggi mencapai 92,49%. Temuan ini mengindikasikan bahwa tingkat pendidikan berpotensi memiliki keterkaitan dengan tingkat adopsi dan pemanfaatan internet di Indonesia." [1] .

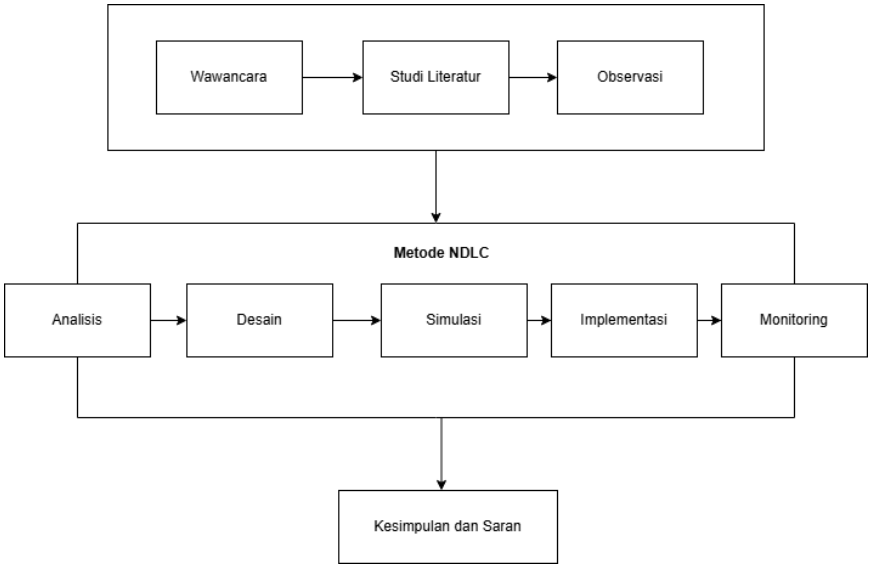
Berdasarkan data tersebut dapat disimpulkan bahwa penggunaan internet memiliki pengaruh yang signifikan terhadap berbagai aktivitas dan kebiasaan masyarakat, yang semakin banyak beralih dari ruang fisik (*physical space*) ke ruang siber (*cyber space*), terutama pada kelompok pendidikan di perguruan tinggi. Namun demikian, peningkatan tersebut juga menghadirkan tantangan yang besar terhadap aspek keamanan sistem jaringan. Berdasarkan hasil survei yang dikelola oleh AwanPintar.id, rata-rata serangan siber yang terjadi mencapai 15 serangan per jam, 890 serangan per menit, dan apabila dihitung dalam satu hari dapat mencapai 1.281.575 serangan.

Ancaman keamanan jaringan seperti *Distributed Denial of Service* (DDoS), *Man-in-the-Middle* (MITM) *attack*, serta brute force diperkirakan akan terus meningkat seiring perkembangan teknologi. Sistem deteksi konvensional semakin

kurang mampu dalam melakukan pertahanan maupun deteksi dini terhadap berbagai bentuk serangan, terutama serangan baru yang telah terintegrasi dengan teknologi kecerdasan buatan (*Artificial Intelligence/AI*) yang memiliki tingkat kompleksitas tinggi sehingga sulit untuk dideteksi. Salah satu mekanisme deteksi dan pengendalian pada jaringan yang umumnya terdapat pada perangkat router adalah firewall, yang berfungsi untuk menerapkan aturan (*rules*) kebijakan keamanan jaringan atau security policy. Firewall melakukan proses penyaringan (*filtering*) terhadap lalu lintas data masuk dan keluar, termasuk pengaturan akses port sesuai dengan kebijakan yang telah ditetapkan, dengan tujuan untuk meminimalkan risiko ancaman dari luar jaringan. [1].

Dalam penelitian ini, peneliti membahas jaringan komputer pada Universitas Teknologi Bandung. Berdasarkan hasil wawancara dengan salah satu staf pengelola jaringan di Universitas Teknologi Bandung, pernah terjadi insiden serangan brute force yang terdeteksi melalui jaringan internal kampus. Serangan tersebut bertujuan untuk mencari kombinasi username dan password yang valid, dalam kejadian tersebut, penyerang berhasil memperoleh kredensial yang valid sehingga dapat melakukan proses login menggunakan akun yang telah diperoleh. Selain itu pernah mendapatkan serangan brupa DDoS *Attack* yang terdeteksi oleh router pada jaringan, serta terdapat keluhan dari pengguna jaringan terkait kecepatan akses internet di lingkungan kampus yang relatif lambat.

Berdasarkan permasalahan tersebut, diperlukan upaya peningkatan keamanan jaringan sekaligus pengeloalaan bandwidth agar kualitas jaringan menjadi lebih optimal. Solusi yang diusulkan dalam penelitian ini adalah menerapkan metode *Network Development Life Cycle* (NDLC) sebagai kerangka kerja dalam perancangan dan implementasi serta evaluasi pada infrastruktur jaringan. Pada aspek keamanan jaringan perlu dilakukan kombinasi keamanan firewall dan *Intrusion Detection System* atau Intrusion *Prevention System* (IPS) serta konfigurasi anti *Brute Force* dan anti DDoS yang bisa di kombinasikan dengan firewall mangle agar bisa menandai packet yang dicurigai melakukan serangan secara dini. Pada aspek bandwidth perlu di terapkan Teknik *Quality of Service* (QoS) melalui pengaturan *Quee Tree* atau *Hierarchical Token Bucket* (HTB) yang bertujuan mengalokasikan bandwidth secara rasional dan sesuai dengan kebutuhan pengguna. Berdasarkan persoalan dan studi literasi, peneliti membuat kerangka penelitian sebagai berikut:



Gambar 1. Kerangka Penelitian

Pada kerangka penelitian di atas, tahapan pertama adalah mengumpulkan data awal melalui wawancara, studi literatur, dan observasi secara langsung di lingkungan Universitas Teknologi Bandung. Tahap ini bertujuan untuk mengidentifikasi kondisi jaringan yang sedang berjalan, permasalahan yang dihadapi, serta kebutuhan pengguna terhadap layanan jaringan. Selanjutnya, penulis melakukan analisis menggunakan metode *Network Development Life Cycle* (NDLC) sebagai dasar dalam merancang pengembangan infrastruktur jaringan.

Penelitian ini diharapkan menghasilkan rancangan infrastruktur jaringan yang lebih aman dan optimal melalui penerapan metode *Network Development Life Cycle* (NDLC). Rancangan tersebut diharapkan mampu meningkatkan keamanan jaringan dengan meminimalkan risiko serangan, seperti *brute force* dan *Distributed Denial of Service* (DDoS), melalui implementasi mekanisme keamanan yang sesuai. Selain itu, penelitian ini diharapkan dapat menghasilkan skema manajemen bandwidth yang lebih efektif melalui konfigurasi *Queue Tree* berbasis *Hierarchical Token Bucket* (HTB), sehingga alokasi bandwidth dapat dilakukan secara proporsional sesuai dengan kebutuhan pengguna. Dengan demikian, kualitas layanan jaringan *Quality of Service* (QoS) di lingkungan Universitas Teknologi Bandung diharapkan mengalami peningkatan.

II. TINJAUAN PUSTAKA

1. Penelitian Terkait

Pada penelitian yang berjudul "Model Jaringan *Neural Network* untuk Deteksi Anomali pada Sistem Keamanan Siber: Rancangan, Implementasi, dan Analisis", peneliti menggunakan metode *Research* and *Development* (R&D) untuk mengembangkan model *Deep Learning* berbasis *Autoencoder* dan *Long Short-Term Memory* (LSTM) dalam mendeteksi anomali pada sistem keamanan siber. Hasil penelitian menunjukkan bahwa model yang dikembangkan memiliki tingkat efektivitas yang tinggi dalam mendeteksi intrusi secara real-time, sehingga terbukti efektif, efisien, dan inovatif dalam meningkatkan keamanan jaringan komputer[2]

Pada penelitian yang berjudul "Analisis Keamanan Jaringan dengan Metode *Security Life Cycle* di Universitas Ibn Khaldun Bogor", ditemukan beberapa permasalahan keamanan jaringan, di antaranya serangan *Denial of Service* (DoS) dan *Brute Force* yang menargetkan layanan hotspot serta Sistem Informasi Akademik (SIAK). Penelitian tersebut menerapkan metode *Security Life Cycle* (SLC) untuk merancang sistem keamanan jaringan dan menghasilkan sejumlah rekomendasi guna mengatasi kerentanan pada server SIAK maupun hotspot. Hasil penelitian menyimpulkan bahwa rekomendasi yang dihasilkan perlu diimplementasikan dan dievaluasi secara berkelanjutan agar celah keamanan dapat diminimalkan. Selain itu, penerapan SLC secara berkesinambungan direkomendasikan untuk menjaga keamanan jaringan dan sistem komputer di Universitas Ibn Khaldun Bogor [3].

Selanjutnya, pada penelitian yang berjudul "Efisiensi Bandwidth Melalui Pengembangan Model Jaringan Menggunakan Metode *Network Development Life Cycle* (NDLC)", permasalahan yang diangkat adalah ketidakstabilan jaringan internet yang berdampak pada penurunan kinerja perangkat operasional, keterlambatan penyelesaian laporan pelanggan, serta menurunnya pencapaian Key Performance Indicator (KPI). Penelitian tersebut menerapkan metode *Network Development Life Cycle* (NDLC) untuk mengoptimalkan penggunaan bandwidth berdasarkan prioritas pengguna. Hasil implementasi menunjukkan peningkatan efisiensi bandwidth yang signifikan, khususnya pada perangkat non-produktif, dengan penurunan penggunaan bandwidth dari 54 Mbps menjadi 2 Mbps atau lebih dari 90%. Selain itu, penerapan autentikasi pengguna yang terverifikasi juga meningkatkan keamanan jaringan sehingga mendukung kelancaran operasional dan pencapaian KPI organisasi [4].

Berdasarkan ketiga penelitian tersebut, dapat disimpulkan bahwa aspek keamanan jaringan dan manajemen bandwidth merupakan dua komponen penting dalam meningkatkan kualitas layanan jaringan. Penelitian pertama berfokus pada deteksi anomali menggunakan teknologi *Deep Learning*, penelitian kedua menitikberatkan pada pengelolaan keamanan jaringan melalui pendekatan *Security Life Cycle* (SLC), sedangkan penelitian ketiga berfokus pada optimasi bandwidth menggunakan metode *Network Development Life Cycle* (NDLC). Namun, belum terdapat penelitian yang mengintegrasikan penguatan keamanan jaringan dengan pengelolaan bandwidth dalam satu kerangka implementasi. Oleh karena itu, penelitian ini mengusulkan penerapan metode *Network Development Life Cycle* (NDLC) sebagai kerangka kerja untuk merancang dan mengimplementasikan sistem keamanan jaringan sekaligus manajemen bandwidth berbasis *Quality of Service* (QoS) dengan konsep *Hierarchical Token Bucket* (HTB). Pendekatan ini diharapkan tidak hanya mampu meningkatkan ketahanan jaringan terhadap ancaman seperti *Brute Force* dan *Distributed Denial of Service* (DDoS), tetapi juga mengoptimalkan distribusi bandwidth secara proporsional sesuai kebutuhan pengguna sehingga kualitas layanan jaringan (*Quality of Service*) menjadi lebih baik. [2], [3], [4].

2. Keamanan Jaringan.

Segala usaha atau tindakan yang bertujuan untuk melindungi kebijakan dan prosedur yang sudah dirancang pada infrastruktur jaringan, perangkat serta lingkungan atau environment yang disebut keamanan jaringan (*Netowork Security*). Berdasarkan hasil pemantauan dan analisis *Cyber Threat Intelligence* tahun 2023, BSSN juga melakukan penelusuran dugaan insiden siber dengan jumlah total 347 dugaan insiden siber dengan jumlah jenis dugaan insiden tertinggi yaitu *Data Breach*. Hasil penelusuran pada darknet, ditemukan adanya 1.674.185 temuan data exposure yang berdampak pada 429 stakeholder di Indonesia. Pada kasus web defacement ditemukan sebanyak 189 kasus yang telah dinotifikasi oleh BSSN dengan klasifikasi kasus paling banyak adalah web defacement pada halaman tersembunyi (hidden). Berdasarkan laporan yang diterima dari stakeholder pada layanan aduan siber, diperoleh sebanyak 1.417 aduan dengan kategori aduan terbanyak adalah *Cybercrime* sebanyak 86% [5].

Keamanan jaringan berkaitan dengan segala aktifitas yang dilakukan untuk mengamankan network, khususnya untuk melindungi *usability*, *reliability*, *integrity* dan *safety* dari *network* dan data. Target *network* security adalah bagaimana mencegah dan menghentikan berbagai threats (potensi serangan) agar tidak memasuki dan menyebarkan pada jaringan, keamanan jaringan mencangkup komponen hardware, software dan aturan-aturan atau kebijakan keamanan [6].

Berdasarkan uraian tersebut, dapat disimpulkan bahwa keamanan jaringan *(network security*) merupakan serangkaian kebijakan, mekanisme, dan teknologi yang diterapkan untuk melindungi infrastruktur jaringan, perangkat, serta data dari berbagai ancaman siber. Penerapan keamanan jaringan bertujuan untuk menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), serta keandalan (*reliability*) layanan jaringan. Meningkatnya jumlah insiden siber di Indonesia, seperti data breach, web defacement, dan cybercrime, menunjukkan bahwa penerapan sistem keamanan jaringan yang efektif menjadi kebutuhan yang

sangat penting. Oleh karena itu, diperlukan kombinasi perangkat keras, perangkat lunak, serta kebijakan keamanan yang terintegrasi untuk mencegah, mendeteksi, dan memitigasi berbagai ancaman siber sehingga kualitas dan kontinuitas layanan jaringan tetap terjaga.

3. DDoS

Serangan *Distributed Denial of Service* (DDoS) bertujuan untuk menggangu ketersediaan *availability* pada layanan server dengan cara membanjiri sumber daya target sehingga menyebabkan bandwidth pada jaringan atau kapasitas server habis yang menyebabkan penurunan kinerja atau bahkan penurunan layanan menjadi tidak tersedia, secara geografis serangan siber jenis ini menggunakan sejumalah besar computer atau perangkat yang terdistribusi untuk mengakses sumberdaya server secara bersamaan [7].

Serangan *Distributed Denial of Service* (DDoS) adalah sekelompok serangan kolaboratif yang dilakukan oleh penyerang yang mengancam keamanan internet dan melanggar layanan. Dalam serangan ini, penyerang memanfaatkan sistem yang telah disusupi untuk mencegah pengguna sah mengakses sumber daya server dan menggunakannya untuk melakukan serangan ekstensif terhadap korban [8]

Serangan *Denial-of-Service* (DoS) dan *Distributed Denial-of-Service* (DDoS) merupakan ancaman serius terhadap ketersediaan layanan awan karena banyaknya kerentanan baru yang diperkenalkan oleh sifat awan, seperti multi-tenancy dan berbagi sumber daya. Tindakan yang mengarah ke DoS atau DDoS, yang tujuan utamanya adalah untuk mengganggu ketersediaan *Cloud*, dapat terjadi dari jarak jauh atau secara lokal dari layanan korban atau pengguna. Serangan ini umumnya menargetkan *bandwidth* komunikasi korban, sumber daya komputasi, *buffer* memori, protokol jaringan, atau logika pemrosesan aplikasi korban [9]

4. Brute Force

Brute Force adalah jenis serangan hacking yang dilakukan dengan mencoba mengumpulkan username dan password untuk di ujicoba atau di tebak baik secara otomatis (robot) atau manual yang dapat mengakibatkan jaringan menjadi tidak stabil dan semua perangkat yang tersambung kedalam router mikrotik akan terputus secara tiba-tiba dampak utama pada CIA triad adalah *Availability* (Ketersediaan) dan *Confidentiality* (Kerahasiaan) Dampak Jika serangan berhasil [10].

Serangan *brute force* umumnya menargetkan layanan autentikasi yang terbuka, seperti *Secure Shell* (SSH), *File Transfer Protocol* (FTP), dan sistem login berbasis web. Kelemahan dalam penerapan kebijakan kata sandi, seperti penggunaan password yang mudah ditebak atau tidak adanya pembatasan jumlah percobaan login, sering dimanfaatkan oleh penyerang untuk meningkatkan peluang k eberhasilan. Apabila serangan ini berhasil, dampaknya dapat berupa pengambilalihan sistem, pencurian data sensitif, serta gangguan terhadap ketersediaan layanan. Selain risiko keamanan, serangan brute force juga dapat memengaruhi kinerja server. Banyaknya percobaan login dalam waktu singkat dapat meningkatkan beban kerja sistem, yang pada akhirnya berdampak pada penurunan performa atau bahkan menyebabkan layanan tidak dapat diakses. Kondisi ini tentu merugikan organisasi yang bergantung pada ketersediaan layanan server secara terus-menerus [11].

Berdasarkan uraian tersebut, dapat disimpulkan bahwa brute force attack merupakan serangan yang dilakukadengan mencoba berbagai kombinasi username dan password secara berulang hingga memperoleh akses yang sah ke dalam sistem. Serangan ini umumnya menargetkan layanan autentikasi seperti SSH, FTP, dan web login, serta memanfaatkan kelemahan pada kebijakan kata sandi dan mekanisme autentikasi. Dampak utama brute force attack terhadap CIA Triad adalah terganggunya aspek *Availability* akibat meningkatnya beban sistem yang dapat menyebabkan penurunan kinerja atau terhentinya layanan. Selain itu, apabila serangan berhasil memperoleh akses tidak sah, aspek *Confidentiality* juga terancam karena penyerang dapat mengakses dan mencuri informasi sensitif. Oleh karena itu, penerapan mekanisme keamanan seperti kebijakan kata sandi yang kuat, pembatasan percobaan login, dan sistem deteksi intrusi menjadi langkah penting untuk mencegah serangan brute force.

5. QOS (*Quality of Service*)

QoS adalah sekumpulan teknologi dan kebijakan yang digunakan untuk mengelola lalu lintas jaringan. Tujuannya adalah untuk memastikan bahwa aplikasi penting mendapatkan bandwidth yang cukup dan latensi yang rendah. Jika jaringan tidak memiliki QoS, film tersebut bisa buffering, dan pengalaman menonton terganggu. Dengan QoS, dapat mengutamakan lalu lintas video dibandingkan dengan lalu lintas email [12] .

Menurut Houston dalam *Quality of Service* (QoS) merupakan metode pengukuran tentang seberapa baik jaringan dan merupakan suatu usaha untuk mendefinisikan karakteristik dan sifat suatu layanan. QoS digunakan untuk mengukur sekumpulan atribut kinerja yang telah di spesifikasikan dan diasosiasikan dengan suatu layanan. Berikut ini merupakan beberapa parameter QoS yang sering digunakan dalam mengukur performansi jaringan diantaranya adalah *Packet lost*, *Througput*, *Delay* dan *Jitter* [13].

Berdasarkan uraian tersebut, dapat disimpulkan bahwa *Quality of Service* (QoS) merupakan sekumpulan teknologi, mekanisme, dan kebijakan yang digunakan untuk mengelola lalu lintas jaringan agar layanan yang bersifat prioritas memperoleh alokasi bandwidth yang memadai, latensi yang rendah, dan kualitas komunikasi yang optimal. QoS juga berfungsi sebagai metode untuk mengukur tingkat kinerja suatu jaringan berdasarkan parameter-parameter tertentu, yaitu throughput, delay, jitter, dan packet loss. Pengukuran terhadap parameter

tersebut digunakan untuk mengevaluasi kualitas layanan jaringan serta memastikan bahwa jaringan mampu memberikan performa yang stabil, efisien, dan sesuai dengan kebutuhan pengguna.

6. HTB (*Hierarchical Token Bucket*)

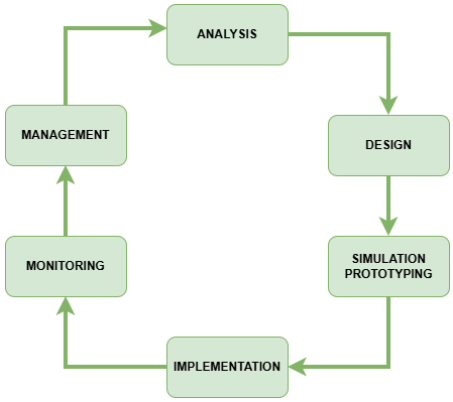
Hierarchical Token Bucket adalah suatu disiplin antrian classful yang berguna untuk menerapkan penanganan yang berbeda untuk berbagai jenis lalu lintas. Secara umum, kita bisamengatur hanya satu antrian untuk interface, tapi di RouterOS antrian yang melekat pada *Hierarchical Token Bucket* (HTB) Antrian dapat ditambahkan pada simple *Queue* / Queue Tree yang terdapat pada *Hierarchical Token Bucket* (HTB) *Hierarchical Token Bucket* (HTB) memungkinkan untuk membuat struktur antrian hirarki dan menentukan hubungan antar antrian, seperti "*parent-child*" atau "*child-child*". [14] .

Menurut citraweb HTB hanya bisa berjalan, apabila rule *queue client* berada di bawah setidaknya 1 level *parent*, setiap queue *client* memiliki parameter *limit-at* dan *max-limit*, dan parent queue harus memiliki besaran max-limit, jumlah seluruh *limit-at client* tidak boleh melebihi *max-limit parent*, *max-limit* setiap *client* harus lebih kecil atau sama dengan *max-limit parent*, untuk parent dengan level tertinggi, hanya membutuhkan *max-limit* (tidak membutuhkan parameter limit-at), untuk semua parent, maupun sub parent, paremeter priority tidak diperhitungkan. *Priority* hanya diperhitungkan pada child queue dan perhitungan *priority* baru akan dilakukan setelah semua *limit-at* (baik pada *child queue* maupun sub *parent*) telah terpenuhi.

Berdasarkan uraian di atas, dapat disimpulkan bahwa *Hierarchical Token Bucket* (HTB) merupakan metode manajemen *bandwidth* berbasis antrian (*queueing*) yang memungkinkan pembagian dan pengendalian lalulintas jaringan secara hierarkis melalui hubungan *parent-child.* HTB memberikan fleksibilitas dalam mengalokasikan bandwidth kepada setiap pengguna atau layanan berdasarkan parameter limit-at dan max-limit, sehingga distribusi bandwidth menjadi lebih adil, efesien, dan sesuai dengan prioritas yang telah ditentukan. Agar HTB dapat bekerja secara optimal, konfigurasi setiap queue harus mengikuti hierarki, dimana nilai limit -at dan max-limit pada child queue tidak boleh melebihi kapasitas parent queue. Dengan mekanisme tersebut, HTB mampu meningkatkan kualitas pengelolaan trafik jaringan dan mendukung tercapainya *Quality of Service* (QoS).

III. ANALISIS DAN PERANCANGAN

Setelah mendapatkan data awal melalui wawancara dengan staff IT yang mengelola jaringan kampus Universitas Teknologi Bandung, tahap penulis akan menggunakan metode *Network Development Life Cycle*(NDLC), untuk perancangan jaringan komputer. Metode tersebut terdiri dari analysis, design, simulation *prototype*, *implementation*, dan *monitoring*. Berikut merupakan tahapan dari metode NDLC sebagai berikut:



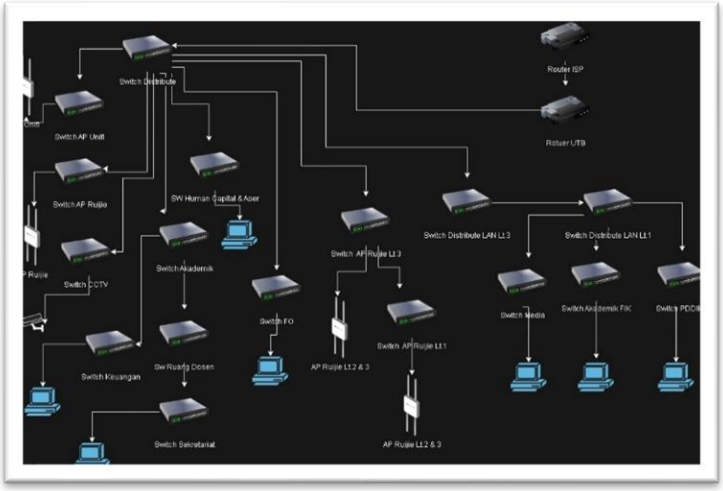
Gambar 2 . Metode Network Development Life Cycle

1. Tahapan analisis

Tahap Analysis merupakan tahap awal yang bertujuan untuk mengidentifikasi kebutuhan jaringan dan permasalahan yang dihadapi organisasi. Pada tahap ini dilakukan pengumpulan informasi melalui observasi, wawancara, dokumentasi, maupun studi literatur. Hasil analisis digunakan untuk mengetahui kondisi jaringan yang sedang berjalan, kebutuhan pengguna, spesifikasi perangkat yang diperlukan, serta potensi risiko yang dapat memengaruhi keamanan dan kinerja jaringan. Tahap analisis sudah di lakukan pada tahapan wawancara dengan narasumber.

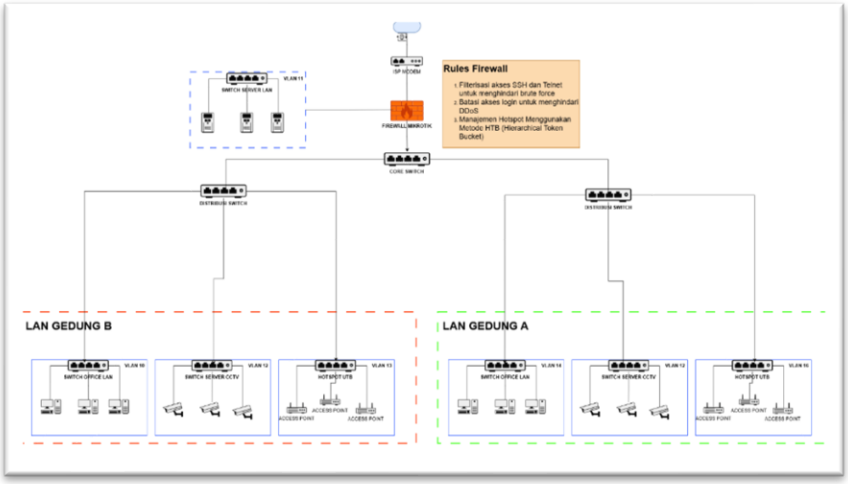
2. *Design*

Tahap *Design* bertujuan untuk menyusun rancangan jaringan berdasarkan hasil analisis. Perancangan meliputi penyusunan topologi jaringan, penentuan skema pengalamatan IP, segmentasi jaringan, pemilihan perangkat jaringan, serta perancangan sistem keamanan dan manajemen bandwidth. Tahap design meliputi perancangan topologi jaringan, perancangan aturan keamanan firewall, IDS/IPS dan proteksi *brute force* serta DDoS, Perancangan manajemen bandwidth berbasis HTB. Output : diagram topologi jaringan, dokumen desain system. Berikut diagram topologi jaringan yang sedang berjalan:



Gambar 3. Topologi yang sedang berjalan

Berdasarkan hasil analisis, penulis mengusulkan rancangan topologi jaringan yang akan diimplementasikan sebagai acuan dalam pengembangan infrastruktur jaringan menggunakan metode *Network Development Life Cycle* (NDLC). Rancangan ini bertujuan untuk meningkatkan keamanan jaringan melalui penerapan mekanisme pengamanan yang sesuai serta mengoptimalkan pengelolaan *bandwidth* agar kualitas layanan jaringan (*Quality of Service atau QoS*) menjadi lebih baik, stabil, dan efisien.



Gambar 4. Topologi Jaringan

3. Simulation prototyping

   Pada tahap ini dilakukan simulasi terhadap rancangan jaringan sebelum diterapkan pada lingkungan produksi. Simulasi bertujuan untuk memastikan bahwa desain yang dibuat telah sesuai dengan kebutuhan serta meminimalkan risiko kesalahan saat implementasi. Simulasi yang akan dilakukan menggunakan *tools* virtualisasi yaitu virtualbox. Output : hasil pengujian simulasi, revisi design apabila diperlukan. Akan di bahas pada Bab IV hasil dan pembahasan.

4. Implementation

   Tahap Implementation merupakan proses penerapan desain jaringan ke lingkungan nyata. Pada tahap ini dilakukan instalasi perangkat jaringan, konfigurasi router, switch, firewall, server, serta penerapan kebijakan keamanan dan manajemen bandwidth. Output : Infrastruktur jaringan yang telah dikonfigurasi dan siap digunakan. Akan di bahas pada Bab IV hasil dan pembahasan.

5. Monitoring

   Tahap Monitoring bertujuan untuk mengamati performa jaringan setelah implementasi. Pemantauan dilakukan untuk mengetahui efektivitas konfigurasi yang telah diterapkan serta mendeteksi gangguan maupun ancaman keamanan jaringan. Parameter yang diamati antara lain penggunaan bandwidth, trafik jaringan, upaya

serangan jaringan dan parameter QoS (*Quality of Service*). Output : Data performa Jaringan, hasil pengukuran QoS.

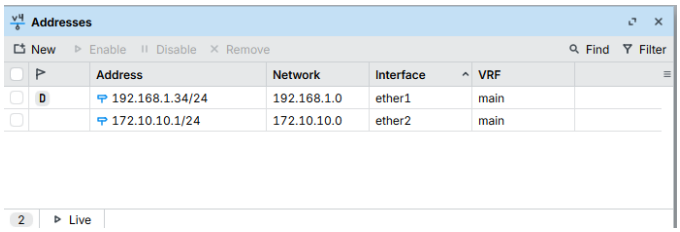
6. Management

Tahap terakhir adalah Management, yaitu proses pemeliharaan dan evaluasi jaringan secara berkelanjutan. Pada tahap ini dilakukan analisis terhadap hasil monitoring untuk menentukan tindakan perbaikan, pembaruan konfigurasi, pencadangan konfigurasi (*backup*), serta penyusunan dokumentasi jaringan. Dalam penelitian ini, tahap management menghasilkan rekomendasi pengembangan jaringan berdasarkan hasil evaluasi implementasi keamanan jaringan dan manajemen bandwidth. Output: rekomendasi perbaikan dan pengembangan jaringan serta strategi pemeliharaan jaringan secara berkelanjutan.

IV. HASIL DAN PEMBAHASAN

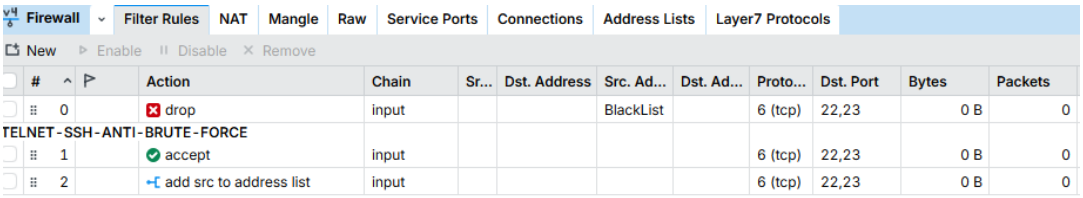
1. Implementasi

Pada tahap ini akan dijelaskan Hasill konfigurasi dan Rancangan pengembangan jaringan dengan metode NDLC dilakukan dengan perangkat simulasi Virtualbox dan *software* Winbox. Proses implementasi akan dilakukan sesuai dengan rancangan jaringan yang telah ditentukan.



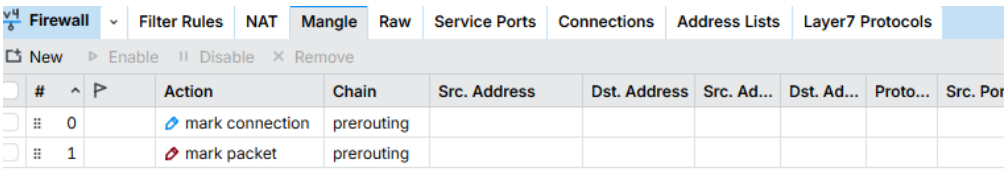
Gambar 5. Konfigurasi Ip address pada router mikrotik

Simulasi jaringan dilakukan menggunakan dua antarmuka (interface), yaitu ether1 dan ether2. Antarmuka ether1 dikonfigurasi sebagai jalur utama yang terhubung ke sumber koneksi internet (WAN), kemudian koneksi tersebut didistribusikan melalui router MikroTik. Selanjutnya, antarmuka ether2 dikonfigurasi sebagai jalur jaringan lokal (LAN) yang berfungsi mendistribusikan layanan jaringan kepada perangkat klien (*client*) atau *end user*. Konfigurasi ini digunakan sebagai dasar implementasi keamanan jaringan dan manajemen bandwidth pada proses pengujian.



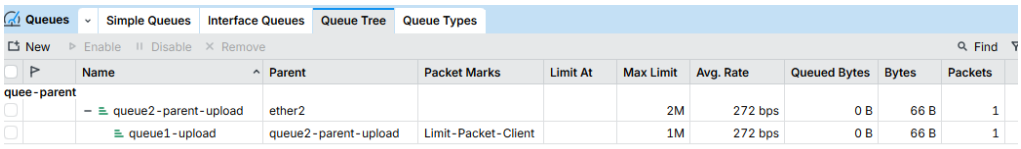
Gambar 5. *Filter Firewall Rules* Anti *Brute Force Attack*

Selanjutnya, dilakukan pengujian dengan mensimulasikan beberapa kali percobaan login menggunakan kredensial yang tidak valid. Hasil pengujian menunjukkan bahwa setelah jumlah percobaan login melebihi batas yang telah ditetapkan, alamat IP penyerang secara otomatis dimasukkan ke dalam *Address List* dan akses berikutnya diblokir oleh firewall. Dengan demikian, mekanisme *Firewall Filter Rules* berhasil mengurangi risiko keberhasilan serangan *Brute Force* terhadap router MikroTik dan meningkatkan keamanan jaringan.



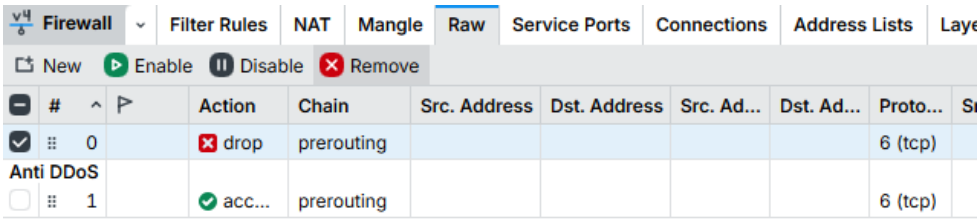
Gambar 6. Konfigurasi Mangle

Hasil konfigurasi menunjukkan bahwa setiap paket yang memenuhi kriteria aturan *Mangle* berhasil diberi tanda (mark packet) sesuai dengan kategori yang telah ditentukan. Penandaan tersebut menjadi acuan bagi *Queue Tree* dan menggunakan metode *Hierarchical Token Bucke* (HTB) dalam melakukan pembagian bandwidth secara proporsional, sehingga penggunaan bandwidth menjadi lebih terkontrol dan kualitas layanan jaringan (*Quality of Service* atau QoS) dapat ditingkatkan.



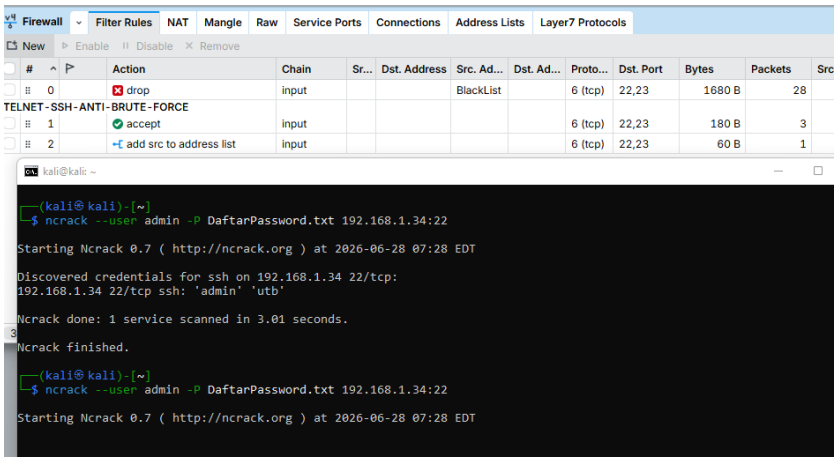
Gambar 7. Implementasi Queue Tree Dan HTB

Gambar 7 menunjukan konfigurasi *Queue Tree* berbasis HTB yang di terapkan pada router mikrotik untuk mengelola distribusi bandwidth berdasrkan packet marking yang telah di konfigurasi pada tahap sebelumnya.



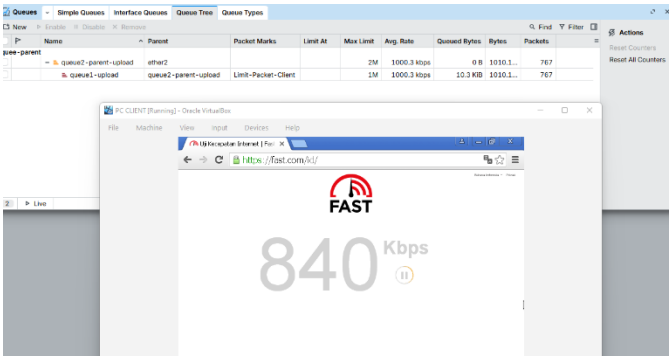
Gambar 8. Konfigurasi *Rules* RAW Firewall Anti DDoS

2. Pengujian



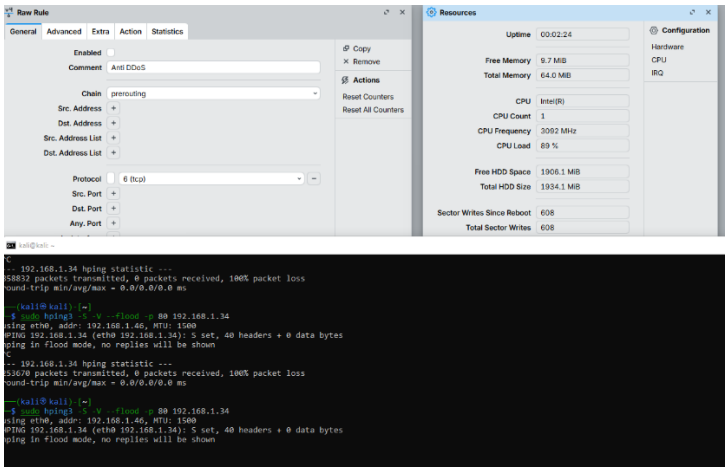
Gambar 9. Pengujian *Brute Force*

Hasil pengujian mekanisme proteksi terhadap serangan *Brute Force* pada router MikroTik. Pengujian dilakukan dengan mensimulasikan beberapa kali percobaan login menggunakan kredensial yang tidak *valid*. Berdasarkan hasil pengujian, Firewall Filter Rules berhasil mendeteksi aktivitas login yang mencurigakan dan secara otomatis memasukkan alamat IP penyerang ke dalam *Address List* untuk kemudian diblokir sesuai dengan aturan yang telah dikonfigurasi.



Gambar 10. Pengujian Limitasi Bandwidth

Hasil pengujian limitasi bandwidth setelah penerapan *Queue Tree* berbasis *Hierarchical Token Bucket* (HTB) pada router MikroTik. Pengujian dilakukan untuk memastikan bahwa alokasi bandwidth pada setiap pengguna atau layanan telah sesuai dengan konfigurasi yang ditetapkan. Hasil pengujian menunjukkan bahwa mekanisme pembatasan bandwidth berjalan dengan baik, di mana setiap pengguna memperoleh kapasitas bandwidth sesuai dengan prioritas dan batas maksimum (*max-limit*) yang telah dikonfigurasi. Dengan demikian, penggunaan bandwidth menjadi lebih terkontrol, pembagian bandwidth lebih adil, serta kualitas layanan jaringan (*Quality of Service* atau QoS) dapat dipertahankan meskipun terjadi peningkatan trafik jaringan.



Gambar 10. Pengujian DDoS Attack

Hasil pengujian mekanisme proteksi terhadap serangan *Distributed Denial of Service* (DDoS) pada router MikroTik. Pengujian dilakukan dengan mensimulasikan trafik dalam jumlah besar menuju jaringan untuk menguji kemampuan *Firewall Filter Rules* dalam mendeteksi dan memitigasi serangan.

V. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa penerapan metode *Network Development Life Cycle* (NDLC) mampu menjadi kerangka kerja yang sistematis dalam proses analisis, perancangan, implementasi, dan evaluasi infrastruktur jaringan di Universitas Teknologi Bandung. Metode ini memberikan tahapan yang terstruktur sehingga proses pengembangan jaringan dapat dilakukan secara lebih efektif sesuai dengan kebutuhan organisasi.

Pada aspek keamanan jaringan, implementasi *Firewall Filter Rules*, *Firewall Mangle*, serta mekanisme proteksi terhadap serangan *Brute Force* dan *Distributed Denial of Service* (DDoS) berhasil meningkatkan keamanan infrastruktur jaringan. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi aktivitas yang mencurigakan, melakukan pemblokiran otomatis terhadap alamat IP yang terindikasi melakukan serangan, serta mengurangi risiko akses tidak sah ke perangkat jaringan.

Pada aspek manajemen bandwidth, penerapan *Queue Tree* berbasis *Hierarchical Token Bucket* (HTB) berhasil mengalokasikan *bandwidth* secara *proporsional* sesuai dengan prioritas pengguna dan layanan. Mekanisme ini mampu mengoptimalkan penggunaan bandwidth, mengurangi kemacetan (*congestion*), serta meningkatkan kualitas layanan jaringan (*Quality of Service* atau QoS) melalui distribusi bandwidth yang lebih stabil dan efisien.

REFERENSI

[1] M. Arif, T. Jonson, and A. Zulkarnaen, “SURVEI PENETRASI INTERNET DAN PERILAKU PENGGUNAAN INTERNET APJII,” 2026.
[2] Nursiaga Rahmat, Nana Mulyana, and Handika Sanjaya, “MODEL JARINGAN NEURALUNTUK DETEKSI ANOMALI PADA SISTEM KEAMANAN (SIBER): RANCANGAN, IMPLEMENTASI, DAN ANALISIS,” vol. 1, pp. 1–9, Jun. 2025.
[3] Ade Hendri Hendrawan, Foni Agus Setiawan, and Arif Sekto Mulyo, “ANALISIS KEAMANAN JARINGAN DENGAN METODE SECURITY LIFECYCLE DI UNIVERSITAS IBN KHALDUN BOGOR”.
[4] R. Fajarudin, “EFISIENSI BANDWIDTH MELALUI PENGEMBANGAN MODEL JARINGAN MENGGUNAKAN METODE NETWORK DEVELOPMENT LIFE CYCLE (NDLC): STUDI KASUS PT RUT,” 2026.
[5] Id-SIRTII/CC - BSSN, “LANSKAP KEAMANAN SIBER INDONESIA,” Jakarta, 2023.
[6] Rifkie Primartha, *BELAJAR SECURITY JARINGAN KOMPUTER BERBASIS CERTIFIED ETHICAL HACKER (CEH)*, 2nd ed. Bandung: INFORMATIKA, 2023.
[7] nidasyifan@telkomuniversity.ac.id, “DDoS : Definisi, Contoh, Cara Kerja, serta Penanganan,” *Telokom University Jakarta*, Jakarta, pp. 1–1, Feb. 05, 2024.
[8] Mousa Taghizadeh Manavi, “Defense mechanisms against Distributed Denial of Service attacks : A survey,” *Computers & Electrical Engineering*, pp. 1–3, Nov. 2018.
[9] A. Bonguet and M. Bellaiche, “A survey of Denial-of-Service and distributed Denial of Service attacks and defenses in cloud computing,” *Future Internet*, vol. 9, no. 3, Aug. 2017, doi: 10.3390/fi9030043.

[10] Yudi mulyanto, "ANALISIS KEAMANAN LOGIN ROUTER MIKROTIK DARI SERANGAN BRUTE FORCE MENGGUNAKAN METODE PENETRATION TESTING," *Jinteks (Hurnal Informatika Teknologi dan Sains)*, vol. 4, pp. 1–5, Aug. 2022.
[11] R. Rahman, M. A. Yunus, and Z. Yasin, "Analisis Dan Mitigasi Serangan Brute Force Pada Server Menggunakan Tools Keamanan Open Source," Online, 2026.
[12] ID-Networkers, "Mengoptimalkan Bandwidth dengan QoS: Panduan Lengkap untuk Administrator Jaringan."
[13] K. Gede, W. P. Putra, G. S. Santyadiputra, M. Windu, and A. Kesiman, "PENERAPAN MANAJEMEN BANDWIDTH MENGGUNAKAN METODE HIERARCHICAL TOKEN BUCKET PADA LAYANAN HOTSPOT MIKROTIK UNDIKSHA," 2020.
[14] T. Rahman, B. Ibrahim, H. Nurdin, and M. Qomaruddin, "HIERARCHICAL TOKEN BUCKET (HTB) PADA QUALITY OF SERVICE PT. EKA BOGAINTI," *Rabit : Jurnal Teknologi dan Sistem Informasi Univrab*, vol. 8, no. 1, pp. 82–91, Jan. 2023, doi: 10.36341/rabit.v8i1.2963.