DESAIN DAN IMPLEMENTASI *CI/CD* UNTUK MENGOTOMATISASI SISTEM PEMBLOKIRAN SITUS JUDI *ONLINE* BERBASIS *DNS FILTERING*

Ifani Wahidaturrahmi, Husain, Dadang Priyanto

Universitas Bumigora, Mataram, Indonesia

Correspondence : *e-mail*: ifaniwahidaturrahmi@gmail.com

Abstrak

Internet menjadi salah satu sarana penting untuk mencari informasi cepat sehingga tidak perlu waktu dan tenaga yang lebih banyak untuk bisa mendapatkan informasi yang dibutuhkan. Namun tidak sedikit juga kejahatan yang dilakukan pada jaringan internet seperti pencurian identitas, penipuan online, judi online, peretasan situs, konten illegal, Virtual Private Network (VPN) ilegal dan lain-lain. Indonesia saat ini menduduki peringkat pertama negara dengan jumlah pemain judi slot online terbanyak di Asia Tenggara. Data ini menunjukkan betapa seriusnya permasalahan perjudian online di Indonesia. Dimana judi online tidak hanya menyebabkan kerugian finansial yang besar, tetapi juga dapat menimbulkan dampak negatif lain seperti masalah sosial dan kesehatan mental. Penelitian ini bertujuan untuk membangun sistem pemblokiran situs judi online dalam keamanan jaringan berbasis Mikrotik dengan mengotomatisasi CI/CD pipeline dan konfigurasi DNS Filtering pada mikrotik sebagai solusi untuk mengurangi dampak negative yang terjadi akibat judi online. Penerapan DNS Filtering pada mikrotik mampu meningkatkan keamanan pada suatu jaringan. Penerapan CI/CD pipeline untuk melakukan otomatisasi konfigurasi DNS Filtering pada PNETLAB berhasil dilakukan sehingga dapat mempercepat proses perubahan pada konfigurasi yang dibuat dan dapat meminimalisir kesalahan. Hasil dari pengujian menunjukkan bahwa waktu diotomatisasi dengan CI/CD terbukti efektif dalam mengurangi waktu konfigurasi dan meningkatkan efisiensi serta konsistensi dalam memblokir situs-situs terlarang. Sistem ini dibangun dengan memanfaatkan Mikrotik sebagai router utama, Ubuntu Server sebagai controller otomatisasi, dan GitLab serta Ansible sebagai alat otomasi.

Kata kunci: *Judi Online, CI/CD, DNS Filtering, Ansible, Gitlab, PNETLab.*

Abstract

The internet is one of the important means to find information quickly so that it does not take more time and energy to get the information needed. However, there are also many crimes committed on the internet network such as identity theft, online fraud, online gambling, site hacking, illegal content, illegal Virtual Private Network (VPN) and others. Indonesia currently ranks first in the country with the largest number of online slot gambling players in Southeast Asia. This data shows how serious the problem of online gambling is in Indonesia. Where online gambling not only causes huge financial losses, but can also have other negative impacts such as social and mental health problems. This study aims to build an online gambling site blocking system in Mikrotik-based network security by automating the CI/CD pipeline and DNS Filtering configuration on Mikrotik as a solution to reduce the negative impacts caused by online gambling. The implementation of DNS Filtering on Mikrotik can improve security on a network. The implementation of the CI/CD pipeline to automate the DNS Filtering configuration on PNETLAB was successfully carried out so that it can speed up the process of changing the configuration made and can minimize errors. The results of the test show that the time automated with CI/CD has proven effective in reducing configuration time and increasing efficiency and consistency in blocking prohibited sites. This system is built by utilizing Mikrotik as the main router, Ubuntu Server as the automation controller, and GitLab and Ansible as automation tools.

Keywords*: Judi Online, CI/CD, DNS Filtering, Ansible, Gitlab, PNETLab.*

1. Pendahuluan

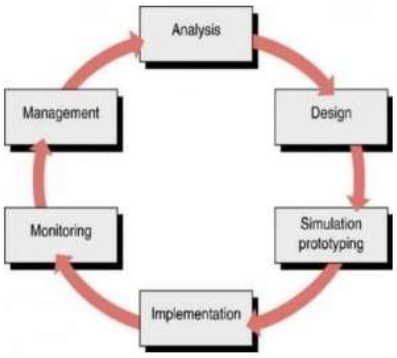
Perkembangan teknologi informasi yang pesat telah membawa dampak signifikan dalam berbagai aspek kehidupan, termasuk dalam bidang hiburan dan akses informasi. Namun, kemajuan ini juga membawa tantangan serius, salah satunya adalah maraknya akses ke situs-situs yang bersifat ilegal atau merugikan, seperti situs judi online. Judi online tidak hanya melanggar hukum di banyak negara, termasuk Indonesia, tetapi juga berdampak negatif terhadap kondisi sosial dan ekonomi masyarakat [1]. Internet menjadi salah satu sarana penting untuk mencari informasi cepat sehingga tidak perlu waktu dan tenaga yang lebih banyak untuk bisa mendapatkan informasi yang dibutuhkan [2]. Namun tidak sedikit juga kejahatan yang dilakukan pada jaringan internet seperti pencurian identitas, penipuan online, judi *online*, peretasan situs, konten illegal, *Virtual Private Network* (*VPN*) ilegal dan lainnya [3].

Pemerintah dan penyedia layanan internet (ISP) telah melakukan berbagai upaya untuk memblokir akses ke situs-situs tersebut. Salah satu metode yang umum digunakan adalah DNS Filtering, yaitu pemblokiran berdasarkan nama domain situs[4] Meskipun efektif, proses pemutakhiran daftar situs yang diblokir sering kali masih dilakukan secara manual atau setengah otomatis, sehingga menyulitkan dalam menghadapi banyaknya situs baru yang terus bermunculan [5] Keamanan jaringan dapat menjadi opsi pencegahan untuk mencegah terjadinya hal-hal yang tidak diinginkan. Keamanan jaringan merupakan salah satu kebutuhan mendasar bagi setiap jaringan komputer [6] Salah satu cara untuk mengamankan jaringan yang dapat diterapkan pada Mikrotik adalah dengan memanfaatkan fitur-fitur yang ada di dalamnya [7]. Indonesia saat ini menduduki peringkat pertama negara dengan jumlah pemain judi slot online terbanyak di Asia Tenggara. Data ini menunjukkan betapa seriusnya permasalahan perjudian online di Indonesia. Dimana judi *online* tidak hanya menyebabkan kerugian finansial yang besar, tetapi juga dapat menimbulkan dampak negatif lain seperti masalah sosial dan kesehatan mental [8]

Maka dari itu, dibutuhkan keamanan atau pemblokiran situs yang berkaitan dengan judi online agar dapat mengurangi akses masyarakat ke situs judi online atau mencegah terjadinya kejahatan di jaringan internet [9] *Firewall* merupakan salah satu fitur pada Mikrotik yang dapat diterapkan untuk mengamankan sebuah jaringan secara internal, sehingga memungkinkan melindungi jaringan dari berbagai serangan baik dari luar, dalam maupun dari router itu sendiri [10] *DNS filtering* juga dapat mencegah akses ke situs web yang tidak aman serta melindungi data dari serangan malware dan phishing. Fitur utama *DNS filtering* meliputi Keamanan *DNS, Anti-Spam,* dan *Filter URL* [11] Keamanan *DNS* melindungi sistem dari serangan seperti pembajakan *DNS* dan ancaman *cyber* lainnya, sementara pemfilteran *URL* memblokir akses ke situs web berbahaya [12] Dalam konteks ini, otomatisasi menjadi sangat penting untuk meningkatkan efisiensi dan konsistensi sistem pemblokiran. Salah satu solusi yang dapat diterapkan adalah metode *CI/CD (Continuous Integration / Continuous Deployment),* yang telah banyak digunakan dalam pengembangan perangkat lunak modern untuk mempercepat siklus pengembangan dan penerapan perubahan [13] Dengan menerapkan *CI/CD,* proses pemutakhiran daftar blokir dapat diotomatisasi mulai dari deteksi situs baru, validasi, hingga implementasi ke dalam sistem *DNS filtering* tanpa perlu intervensi manual secara terus-menerus [14] Dengan demikian, sistem pemblokiran dapat menjadi lebih responsif, akurat, dan mudah dikelola dalam skala besar [15]

2. Metode Penelitian

Metode peneltitian yang digunakan adalah Network Development Life Cycle (NDLC). Metode *NDLC* adalah pendekatan berstruktur untuk pengembangan jaringan yang melibatkan serangkaian langkah-langkah yang terorganisir, mulai dari perencanaan hingga pemeliharaan. Pendekatan ini mencakup proses secara menyeluruh, termasuk analisis kebutuhan, desain jaringan, implementasi, pengujian, serta pemeliharaan dan pemantauan berkelanjutan. Penelitian ini melalui tiga tahapan yaitu, mulai dari tahap analisis, desain kemudian simulasi prototype. Analisis merupakan tahap dimana penulis melakukan studi literatur dengan mengumpulkan jurnal ilmiah, skripsi, serta buku yang terkait dengan judul penelitian. Setelah melakukan studi literatur, selanjutnya dilakukan analisis. Desain merupakan tahap desain di mana dilakukan perancangan untuk memahami konsep kinematika yang abstrak melalui praktik langsung, kolaborasi, serta integrasi seni. Pendekatan ini relevan dengan perancangan sistem otomatisasi keamanan serta penerapan perangkat lunak yang diperlukan. Dan terakhir simulasi prototype pada tahap ini dilakukan simulasi percobaan pada mesin virtual yang dibuat untuk otomatisasi konfigurasi, baik sebelum maupun setelah penerapan CI/CD.



Gambar 1. Network Development Life Cycle (NDLC)

2.1 Pengumpulan Data

Sebelum melakukan perancangan sistem, dibutuhkan informasi yang jelas tentang bagaimana cara kerja dari sistem yang akan dibuat. Maka dari itu penulis melakukan proses Analisa dengan mengumpulkan data lalu kemudian menganalisis data tersebut. Pada pengumpulan data, penulis mempelajari beberapa artikel ilmiah serta buku-buku yang membahas tentang *CI/CD*, Otomatisasi, keamanan *firewall*. Serta mengupulkan beberapa situs judi online yang akan diblokir.pada tabel 1.

Tabel 1. Daftar situs judi online.

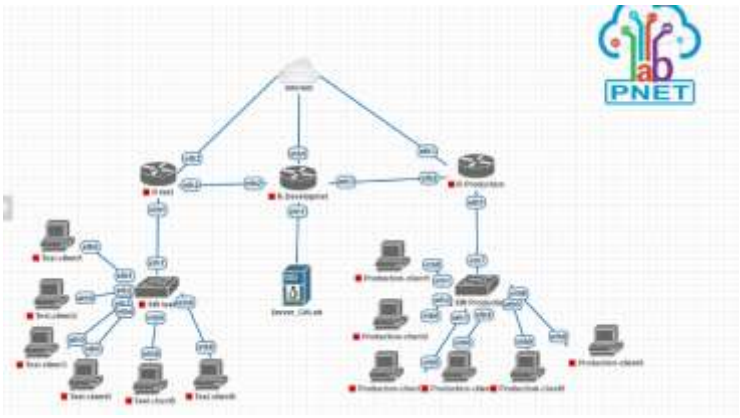
No	Situs judi online
1	Pokerstars
2	Sbobet
3	Zlink.fun

2.2 Analisa data

1. Artikel ilmiah pertama merupakan penelitian yang membahas tentang keamanan jaringan menggunakan *firewall* pada mikrotik untuk melakukan pembatasan akses dengan mengizikan beberapa *client* untuk mengakses internet dan membatasi akses *website* serta membatasi *download file* berdasarkan ekstensinya. Adapun fitur-fitur yang diterapkan yaitu *firewall NAT* yang berfungsi untuk mengubah alamat *ip* asal dan tujuan paket data yang melewati *router*.
2. Artikel ilmiah yang kedua membahas tentang perbandingan fitur layer 7 protokol dengan web proxy untuk melakukan blokir situs *http* dan *https* serta kebutuhan *resource* yang digunakan.
3. Artikel ilmiah yang ketiga membahas analisis dan implementasi *Domain Name Sistem* (*DNS*) pada mikrotik menggunakan metode *DNS Blocking* yaitu 36.86.63.185 dari *internetpositif.id*, hasil penelitian penulis telah berhasil memblokir 10 (Sepuluh) Situs besar Judi *Online.*
4. Artikel yang keempat bertujuan untuk mengetahui rancangan sistem blokir situs terlarang serta mengetahui hasil pengujian dan mengukur kinerja sistem blokir situs terlarang menggunakan *Pi - Hole* pada jaringan Lab TKJ Prodi Pendidikan Teknologi Informasi. Penelitian ini menggunakan metode *SDLC* (*Software Development Life Cycle*), meliputi tahapan analisis kebutuhan, desain topologi sistem, implementasi, pengujian, hingga pemeliharaan system.

2.3 Rancangan Jaringan Ujicoba

Rancangan jaringan ujicoba yang digunakan padasimulasi penerapan *DNS Filtering* sebagai keamanan jaringan yaitu menggunakan *PNETLab* dan *Gitlab* yang telas diinstal pada *VMWare Workstation* sesuai dengan skenario yang telah dibuat, seperti pada gambar 2



Gambar 2. Topologi Jaringan

Rencana jaringan uji coba menggunakan 1 unit laptop yang terhubung internet. Pada laptop tersebut akan diinstal VMware Workstation 16 Pro. Di dalam VMware akan diinstal PNETLab versi 4.2.10 sebagai simulator jaringan berbasis web, yang digunakan untuk mengimplementasikan rancangan jaringan. Di dalam VMware juga akan diinstal server GitLab, yang digunakan untuk uji coba simulasi secara otomatis dengan menggunakan Ansible dan implementasi CI/CD yang dihubungkan dengan satu router.

Setelah menginstal PNETLab, maka dibuat topologi jaringan melalui antarmuka web GUI dari PNETLab yang akan menerapkan keamanan sesuai dengan skenario, yaitu membuat server DHCP dengan lease, serta DNS Filtering untuk memblokir akses situs berdasarkan nama domain. Pada topologi tersebut dibuat 3 lingkungan, yaitu lingkungan router testing untuk menguji script yang dibuat pada lingkungan router development, kemudian jika sudah berhasil maka akan dilakukan deploy ke lingkungan router production.

2.4 Kebutuhan Perangkat Keras

Adapun kebutuhan yang diperlukan diantaranya perangkat keras dan perangkat lunak dalam penelitian ini adalah sebagai berikut :

A. Kebutuhan perangkat keras (Hardware)

Satu unit komputer yang diinstallkan vmware workstation dan didalamnya dibuatkan dua mesin virtual yaitu pnetlab da server gitlab dengan spesifikasi sebagai berikut :

1. Kebutuhan perangkat keras pada *PNETLab*
   a. Memory : 4 GB
   b. Processor : 4 Core
   c. Hardisk : 100 GB
2. Kebutuhan perangkat keras pada *server Gitlab*
   a. Memory : 3 GB
   b. Processor : 2 Core
   c. Hardisk : 30 GB

B. Kebutuhan perangkat lunak (Software)

Kebutuhan perangkat lunak yang diperlukan untuk melakukan otomatisasi *CI/CD pipeline* adalah sebagai berikut :

1. *VMWare Workstation* 16 pro untuk membuat dan menjalankan jaringan *virtual* pada *PNETLab* dan *Gitlab.*
2. *Putty* digunakan untuk *remote access* sehingga dapat dilaukan konfigurasi pada setiap perangkat.
3. *Bitvise ssh client*
4. *Mikrotik chr* (*Cloud Hoster Router*) sebagai mesin *router virtual.*
5. *Gitlab server* layanan yang berupa *virtual machine* yang di dalamnya memuat sistem operasi yaitu ubuntu 22.04.3 lts yang sudah terinstall dan terkonfigurasi *Ansible* dan *Gitlab* yang telah berisi file-file *playbook.*

3. Hasil dan Pembahasan

3.1. Hasil Instalasi dan Konfiguasi

Pada sub bab ini akan dipaparkan langkah serta hasil dari instalasi dan konfigurasi pada *PNETLab*, *Ansible Automation Engine*, *GitLab server* dan konfigurasi yang terinstall pada *PNETLab* yang terdiri dari *router Testing*, *router Production*, dan *router Development* dimana diimplementasikan keamanan pada *LAN* menggunakan fitur-fitur pada *firewall* mikrotik yaitu menolak atau memblokir akses *website* pada *link* judi *online* berdasarkan *domain*.

A. Hasil Instalasi dan Konfigurasi PNETLab

Gambar 3. Hasil Instalasi PNETLab

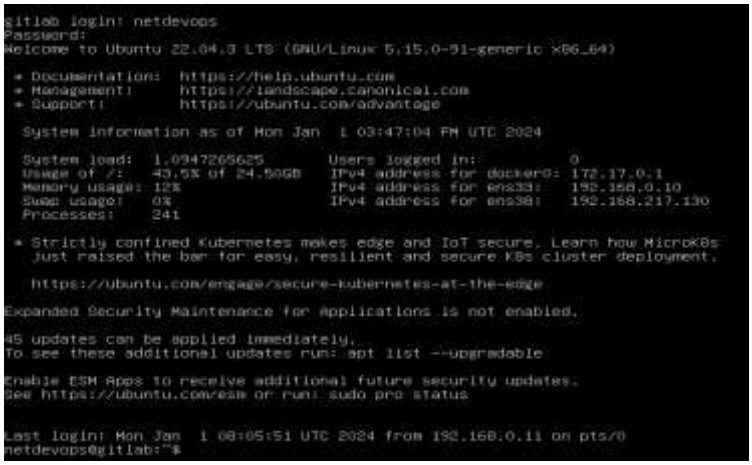
Untuk melakukan konfigurasi lebih lanjut dan membuat desain pada *PNETLab*, harus mengakses *Web Grapichal User Interface* (*GUI*) dari *PNETLab*. Dengan cara membuka browser pada windows kemudian memasukkan alamat akses yang telah diberikan dari *PNETLab*. Selanjutnya akan tampil antarmuka manajemen berbasis web dari *PNETLab*, seperti pada gambar berikut :

Gambar 4. Tampilan Web GUI PNETLab

Tahapan ini dilakukan dengan mengkaji beberapa referensi terkait pemblokiran situs menggunakan *firewall*, *DNS Filtering*, serta penerapan *CI/CD* dalam konfigurasi jaringan. Sehingga, dari analisis ini, disimpulkan bahwa :

- Mikrotik dapat dijadikan pusat pengendali lalu lintas internet berbasis *DNS Filtering*.
- *DNS Filtering* mampu memblokir domain berdasarkan basis data domain berbahaya.
- *CI/CD* diperlukan untuk menghindari konfigurasi manual berulang dan mendukung otomatisasi *deployment*.

B. Hasil Insalasi dan Konfigurasi Gitlab Server



Gambar 5. Hasil Instalasi GitLab

Desain sistem dilakukan pada dua jaringan *virtual* yang dibuat menggunakan *PNETLab* dan dikendalikan melalui *GitLab CI/CD pipeline*. Adapun komponen utama yang dirancang :

- Topologi Jaringan : Dua jaringan *ISP virtual* yang disimulasikan pada *VMWare* menggunakan Mikrotik sebagai router utama.
- Server Otomasi : *Server Ubuntu* 22.04.3 LTS sebagai Ansible controller.
- Skrip Otomatisasi : *Playbook Ansible* dibuat untuk mengonfigurasi Mikrotik secara otomatis menggunakan *API RouterOS*.
- *DNS Filtering* : Menggunakan daftar *domain* situs judi online yang disusun berdasarkan hasil *crawling* publik *DNS blocklist*.

CI/CD Pipeline: *GitLab* digunakan untuk menjalankan *playbook* secara otomatis setiap kali terjadi *update* pada *file* konfigurasi *DNS Filtering*

3.2. Hasil Simulasi jaringan Uji Coba

Tahapan ini melakukan uji coba simulasi terhadap sistem. Pengujian dilakukan dalam dua scenario

Tabel 1. Hasil Pengujian Jaringan Uji Coba.

Parameter	Tanpa CI/CD	Dengan CI/CD
Waktu konfigurasi (rata-rata)	15 menit	< 2 menit
Jumlah situs terblokir	±20 domain	>100 domain
Ketesediaan Sistem	Manual restart	Otomatis & Stabil

Dari hasil ini dapat disimpulkan bahwa penggunaan *CI/CD* mampu mempercepat proses *deployment filter* dan meningkatkan skala serta konsistensi pemblokiran *domain* secara efisien.

4. Kesimpulan

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan menggunakan metode *Network Development Life Cycle* (*NDLC*) dengan tahapan *Analysis, Design*, dan *Simulation Prototyping*, maka dapat disimpulkan beberapa hal sebagai berikut:

Desain sistem pemblokiran situs judi online berbasis *DNS Filtering* yang diotomatisasi dengan *CI/CD* terbukti efektif dalam mengurangi waktu konfigurasi dan meningkatkan efisiensi serta konsistensi dalam memblokir situs-situs terlarang. Sistem ini dibangun dengan memanfaatkan Mikrotik sebagai *router* utama, *Ubuntu Server* sebagai *controller* otomatisasi, dan *GitLab* serta *Ansible* sebagai alat otomasi. Implementasi *CI/CD* memberikan kemudahan dalam pengelolaan konfigurasi jaringan

secara otomatis, sehingga mengurangi pekerjaan manual yang berulang dan meminimalkan potensi kesalahan manusia. Dengan sistem ini, pembaruan daftar domain yang diblokir dapat dilakukan hanya dengan satu kali *push* ke *repository GitLab*.

Penggunaan *DNS Filtering* secara terpusat memungkinkan pengelolaan keamanan jaringan yang lebih luas dan sistematis, terutama jika diterapkan pada institusi atau jaringan berskala besar seperti *ISP*, sekolah, atau instansi pemerintahan. Hasil simulasi menunjukkan peningkatan efektivitas sistem dalam memblokir lebih banyak situs judi online dibandingkan metode konfigurasi manual, serta mempercepat waktu deployment konfigurasi.

Daftar Pustaka

[1] Amrullah, J. D. R., Prasetya, F. B., Rahma, A. S., Setyorini, A. D., Salsabila, A. N., & Nuraisyah, V. (2024). Efektivitas Peran Kurikulum Merdeka terhadap Tantangan Revolusi Industri 4.0 bagi Generasi Alpha. *Jurnal Pendidikan Dan Pembelajaran Indonesia (JPPI)*, *4*(4), 1313–1328.

[2] Huraerah, A. J. A., Abdullah, A. W., & Rivai, A. (2024). Pengaruh teknologi informasi dan komunikasi terhadap pendidikan indonesia. *Journal of Islamic Education Policy*, *8*(2).

[3] Kusumaningsih, R., & Suhardi, S. (2023). Penanggulangan Pemberantasan Judi Online Di Masyarakat. *ADMA: Jurnal Pengabdian Dan Pemberdayaan Masyarakat*, *4*(1), 1–10.

[4] Alpery, A., & Ridha, M. A. F. (2021). Implementasi CI/CD Dalam Pengembangan Aplikasi Web Menggunakan Docker dan Jenkins. *Applied Business and Engineering Conference*, 287–296.

[5] de Fretes, A. V. C., Aritonang, M. A. S., Thamrin, M., Masril, M. A., Jufri, J., Andaria, A. C., Ernawati, T., Naufal, A. R., Sugianto, C. A., & Ekawati, N. (2024). *Pengantar Ilmu Komputer*. Yayasan Tri Edukasi Ilmiah.

[6] Markhamah, R. M. (2023). *UPAYA DIREKTORAT TINDAK PIDANA SIBER BARESKRIM POLRI DALAM MENGEDUKASI MASYARAKAT TENTANG KEAMANAN SIBER DI MEDIA SOSIAL*. Universitas Nasional.

[7] Aditya, V. T. (2024). *Manajemen Ancaman dan Keamanan Jaringan melalui Penggunaan Firewall dengan Mikrotik pada PT Dinamika Mediakom*. Universitas Islam Indonesia.

[8] Satra, R., & Fattah, F. (2021). *Buletin Sistem Informasi dan Teknologi Islam Keamanan Jaringan VLAN dan VoIP Menggunakan Firewall Informasi Artikel Abstrak*. *2*(1), 27–35.

[9] SUSI, A. (2024). *PENGEMBANGAN SISTEM KEAMANAN JARINGAN WIFI BERBASIS MIKROTIK MENGGUNAKAN METODE NETWORK DEVELOPMENT LIFE CYCLE (NDLC)*. Universitas Dehasen Bengkulu.

[10] Ariadi, F., & Saputra, S. (2024). Pengenalan Model 7 Osi Layer Pada Siswa-Siswi Sma Islam Terpadu Insan Madani 8. *Praxis: Jurnal Pengabdian Kepada Masyarakat*, *4*(2), 30–36. https://www.pijarpemikiran.com/index.php/praxis/article/view/689

[11] Aziz, K., Zakir, S., Aprison, W., & Efriyanti, L. (2024). Implementasi Keamanan Jaringan Dengan Metode Firewall Filtering Menggunakan Mikrotik Di Smkn 3 Payakumbuh. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 3343–3352. https://doi.org/10.36040/jati.v8i3.9662

[12] Cahya, B., Rizki, F., Sutiyo, A., Saputra, Y. El, & Elfarizi, M. (2023). Implementasi Firewall Pada Mikrotik Untuk Keamanan Jaringan. *Jurnal JOCOTIS-Journal Science Informatica and Robotics E*, *1*(2), 63–80. https://jurnal.ittc.web.id/index.php/jct/

[13] Chandra, R. A., Murhaban, M., Suryadi, S., & Mukhlizar, M. (2024). Analisis Dan Perbandingan Kinerja Proxmox Virtual Envorment Dalam Virtualisasi Pada Os Debian Dan Ubuntu. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(3), 3687–3692. https://doi.org/10.36040/jati.v8i3.9795

[14] Elradi, M. D. (2023). Ansible: A Reliable Tool for Automation. *Electrical and Computer Engineering Studies*, *2*(1), 1–11. https://doi.org/10.58396/eces020104

[15] Farid, A., & Anugrah, I. G. (2021). Implementasi CI/CD Pipeline Pada Framework Androbase Dengan Menggunakan Jenkins (Studi Kasus: PT. Andromedia). *Jurnal Nasional Komputasi Dan Teknologi Informasi (JNKTI)*, *4*(6), 522–527. https://doi.org/10.32672/jnkti.v4i6.3703