



Perancangan Dan Simulasi Jaringan Komputer Dengan Keamanan Firewall

Widian Dwi Putra¹, Munaldi^{2*}

^{1,2}Fakultas Ilmu Komputer, Program Studi Teknik Informatika, Universitas Pamulang, Kota Tangerang Selatan, Banten. Indonesia

Email: ¹widianputra06@gmail.com, ^{2*}dosen01573@unpam.ac.id

(* : coressponding author)

Abstrak - Perancangan keamanan jaringan merupakan aspek yang sangat penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data dalam suatu organisasi. Salah satu metode umum yang digunakan dalam desain keamanan jaringan adalah penerapan firewall dengan fokus pada pengamanan port. Tujuan dari penelitian ini adalah untuk mengembangkan sistem keamanan jaringan yang efektif dengan menggunakan metode firewall. Firewall memiliki kemampuan untuk mendeteksi dan merespons kemungkinan serangan. Penelitian ini akan mengeksplorasi konfigurasi firewall yang optimal, dengan mempertimbangkan kebutuhan spesifik organisasi dan karakteristik jaringan. Selain itu, penelitian ini akan mengevaluasi dampak penerapan firewall terhadap kinerja jaringan dan interkoneksi antar unit bisnis. Hasil penelitian ini diharapkan dapat memberikan pedoman praktis perancangan keamanan jaringan yang efisien dan efektif dengan memanfaatkan keamanan firewall. Kesimpulan dari penelitian ini diharapkan dapat menjadi dasar bagi organisasi dalam menerapkan langkah-langkah keamanan yang tepat dan proaktif dalam menghadapi ancaman yang terus berkembang di lingkungan jaringan.

Kata Kunci: Kemananan, Firewall, Jaringan Komputer

Abstract - Network security design is a very important aspect in maintaining the integrity, confidentiality and availability of data in an organization. One of the common methods used in network security design is the implementation of a firewall with a focus on port security. The aim of this research is to develop an effective network security system using the firewall method. Firewalls have the ability to detect and respond to possible attacks. This research will explore optimal firewall configurations, taking into account specific organizational needs and network characteristics. In addition, this research will evaluate the impact of firewall implementation on network performance and interconnection between business units. It is hoped that the results of this research can provide practical guidelines for designing efficient and effective network security by utilizing firewall security. It is hoped that the conclusions of this research can be a basis for organizations in implementing appropriate and proactive security measures in facing threats that continue to develop in the network environment.

Keywords: Security, Firewall, Computer Network

1. PENDAHULUAN

Keamanan jaringan merupakan fondasi yang krusial dalam menghadapi pesatnya perkembangan teknologi saat ini. Dalam era di mana konektivitas digital semakin mendalam, keamanan jaringan menjadi pilar utama untuk melindungi data sensitif, mencegah serangan cyber, dan memastikan integritas sistem. Tanpa keamanan jaringan yang kokoh, risiko ancaman keamanan seperti peretasan, pencurian data, dan serangan malware dapat mengancam kelangsungan operasional dan privasi informasi, menunjukkan bahwa keberlanjutan teknologi kita sangat tergantung pada ketangguhan sistem keamanan jaringan. Oleh karena itu, menggarisbawahi urgensi perlindungan jaringan bukan hanya sebagai prioritas, melainkan sebagai suatu keharusan esensial dalam menghadapi dinamika perkembangan teknologi yang terus berkembang.

Dalam era informasi yang semakin maju, di mana jaringan komputer menjadi elemen kritis dalam memfasilitasi komunikasi, pertukaran data, dan akses ke sumber daya digital, keamanan jaringan menjadi sebuah aspek yang tak terelakkan. Seiring dengan perkembangan teknologi, tantangan keamanan dalam lingkungan jaringan juga semakin kompleks dan beragam.

Ancaman-ancaman seperti serangan malware, peretasan, dan akses tidak sah terus meningkat, mengakibatkan dampak serius seperti pencurian data sensitif, kerugian finansial, dan kerusakan reputasi. Dalam menghadapi kompleksitas tantangan keamanan ini, keberadaan sistem keamanan jaringan menjadi sangat penting. Salah satu komponen utama dalam sistem keamanan

jaringan adalah firewall. Firewall berperan sebagai pencegah dan pengidentifikasi terhadap pengguna yang tidak sah yang berusaha memasuki jaringan komputer.

Firewall adalah sebuah sistem atau perangkat yang berperan sebagai garis pertahanan pertama dalam perlindungan sistem. Keamanan jaringan adalah suatu sistem yang dirancang untuk melindungi integritas, kerahasiaan, dan ketersediaan data di dalam jaringan komputer. Dalam konteks ini, integritas merujuk pada keutuhan data, kerahasiaan berkaitan dengan privasi informasi, dan ketersediaan mengacu pada ketersediaan layanan dan sumber daya jaringan. Dengan meningkatnya serangan terhadap jaringan, penggunaan teknologi keamanan telah menjadi suatu keharusan. Keamanan jaringan tidak hanya melibatkan perangkat keras (hardware) dan perangkat lunak (software), tetapi juga melibatkan praktik-praktik keamanan yang efektif.

2. METODOLOGI

Metodologi merupakan sebuah cara yang di gunakan sebagai pedoman di dalam melakukan perancangan ataupun penelitian, sehingga perancangan dapat berjalan dari awal hingga selesai, Metodologi yang tepat diperlukan untuk merancang jaringan yang aman dengan mempertimbangkan berbagai faktor, seperti struktur topologi, pemilihan perangkat, serta penerapan aturan firewall yang ketat, ini bertujuan untuk memberikan panduan yang sistematis dalam merancang, menguji, dan mengimplementasikan jaringan komputer yang aman dengan menggunakan firewall. Berikut ini merupakan metodologi dari perancangan dan simulasi jaringan komputer dengan keamanan firewall.



Gambar 1. Metode Penelitian

2.1 Identifikasi Masalah

a. Ancaman Keamanan Jaringan

Jaringan komputer rentan terhadap serangan seperti hacking, malware, dan kebocoran data. Tanpa perlindungan yang memadai, risiko terhadap integritas dan kerahasiaan data semakin tinggi.

- Pengawasan Trafik yang Tidak Optimal Pengawasan trafik jaringan yang tidak memadai dapat membuka celah bagi akses tidak sah, seperti serangan DoS atau pemalsuan identitas, terutama pada jaringan besar.
- Kebijakan Keamanan yang Tidak Efektif Penyusunan kebijakan firewall yang kurang tepat dapat menyebabkan kesalahan dalam menyaring trafik yang berbahaya atau sah, mengancam keamanan jaringan.
- Pengaruh Terhadap Kinerja Jaringan Penerapan firewall dapat mengurangi kinerja jaringan, seperti peningkatan latency dan penurunan throughput, yang memerlukan desain yang optimal.
- Kesulitan dalam Pengujian Keamanan Perlu dilakukan simulasi serangan untuk menguji efektivitas firewall dalam menghadapi berbagai ancaman yang ada.

2.2. Studi Pustaka

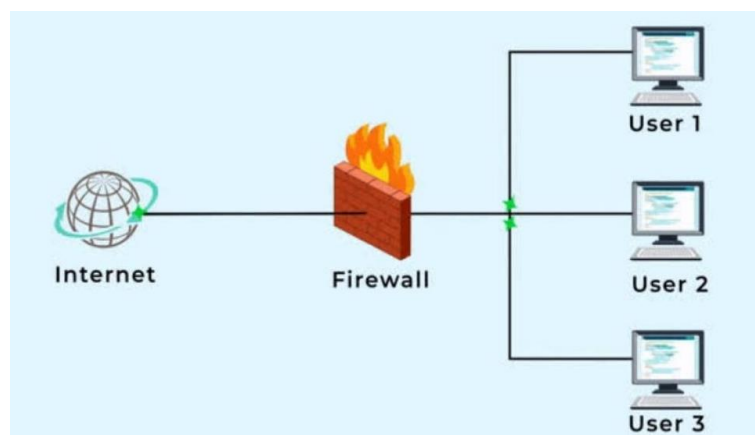
Studi pustaka adalah teknik pengumpulan data dan informasi yang dilakukan dengan membaca dan menganalisis berbagai literatur atau sumber tertulis. Studi pustaka juga dikenal dengan istilah lain, seperti kajian pustaka, tinjauan pustaka, kajian teoritis, landasan teori, dan telaah pustaka. Berikut adalah studi pustaka dari perancangan keamanan Jaringan Firewall.

a. Jaringan Komputer dan Keamanannya

Jaringan komputer merupakan kumpulan perangkat yang saling terhubung untuk berbagi sumber daya dan informasi. Dalam sebuah jaringan komputer, komunikasi data dapat terjadi antara perangkat yang terhubung menggunakan berbagai protokol jaringan, seperti TCP/IP (Transmission Control Protocol/Internet Protocol). Keamanan jaringan adalah aspek penting yang harus dipertimbangkan untuk melindungi data dan informasi yang ada di dalamnya dari ancaman yang dapat merusak integritas, kerahasiaan, dan ketersediaannya. Keamanan jaringan dapat mencakup berbagai teknologi dan strategi, termasuk enkripsi data, autentikasi pengguna, dan perlindungan dari serangan eksternal.

b. Firewall dalam Keamanan Jaringan

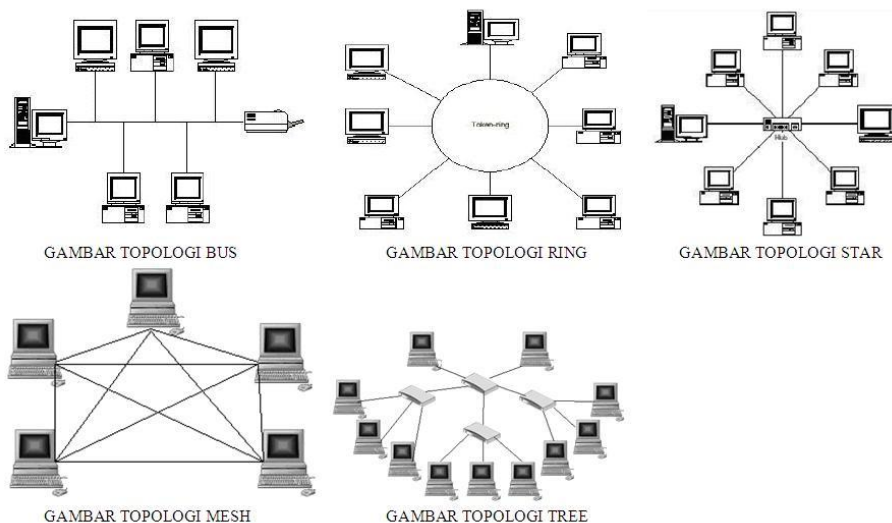
Firewall adalah sistem yang dirancang untuk memantau dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan. Fungsi utama firewall adalah untuk mencegah akses yang tidak sah ke dalam jaringan komputer serta menghalangi berbagai jenis serangan dari luar seperti peretasan dan malware.



Gambar 2. Firewall

2.3 Topologi Jaringan

Topologi jaringan adalah cara menghubungkan perangkat komputer dalam suatu jaringan, baik menggunakan kabel maupun tanpa kabel. Topologi jaringan menggambarkan hubungan geometris antara unsur-unsur dasar jaringan, seperti node, link, dan station.



Gambar 3. Topologi Jaringan



Berikut adalah beberapa jenis topologi diantaranya

- a. Topologi Ring
Topologi cincin menggunakan LAN card untuk membuat koneksi antara satu komputer dengan komputer yang lain dalam sebuah rangkaian yang berbentuk melingkar seperti cincin.
- b. Topologi Bus
Topologi ini digunakan pada jaringan berbasis kabel coaxial di sepanjang konektor dan node client. Konektor yang digunakan pada topologi bus yaitu terminator, BNC serta TNBC.
- c. Topologi Mesh
Topologi ini biasanya dimanfaatkan untuk instalasi dengan banyak jalur. Topologi ini juga menggunakan kabel tunggal sehingga pengiriman data bisa lebih cepat karena tidak melewati switch atau hub.
- d. Topologi Star
Topologi bintang menggunakan switch atau hub agar bisa terkoneksi dengan klien. Diantara berbagai jenis topologi, topologi star adalah yang paling sering digunakan.
- e. Topologi Tree
Topologi ini merupakan gabungan antara topologi star dan topologi bus. Jenis topologi ini digunakan untuk interkoneksi di antara hirarki yang berbeda-beda. Topologi tree ini memiliki rangkaian yang berbentuk struktur pohon.

2.4 Implementasi Metode Firewall

Firewall merupakan teknologi keamanan siber yang berfungsi untuk meningkatkan keamanan komputer yang terhubung ke jaringan. Firewall bekerja dengan cara:

- a. Menganalisis lalu lintas data yang masuk dan keluar jaringan
- b. Memfilter informasi yang masuk ke dalam jaringan
- c. Memantau dan mengontrol akses ke jaringan atau internet
- d. Mengidentifikasi dan mencegah serangan dari virus, malware, atau hacker

Dalam mengimplementasi metode firewall ada beberapa hal yang sisiapkan diantaranya :

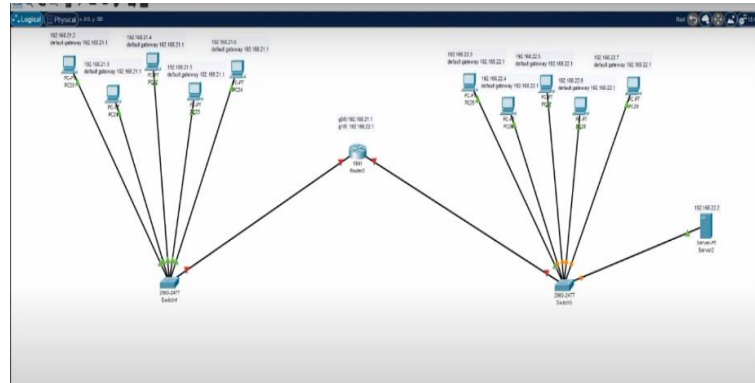
- a. Persiapkan Alat dan Software
- b. Menyusun Topologi Jaringan
- c. Mengonfigurasi Router dan Firewall
- d. Mengonfigurasi Komputer dan Server
- e. Pengujian Koneksi dan Keamanan
- f. Evaluasi dan Pemeliharaan

3. ANALISA DAN PEMBAHASAN

Pada perancangan jaringan ini, akan dibangun sebuah simulasi jaringan komputer dengan keamanan firewall yang menghubungkan berbagai perangkat seperti komputer klien (PC), server, router, dan firewall untuk menunjukkan bagaimana cara mengatur dan memanfaatkan firewall untuk menjaga jaringan dari potensi ancaman, serta untuk memastikan bahwa hanya lalu lintas yang sah yang dapat mengakses sumber daya dalam jaringan. Membuat topologi jaringan dan memanfaatkan area kerja dari cisco paket tracer yang dibutuhkan dan hubungkan dengan kabel diantaranya :

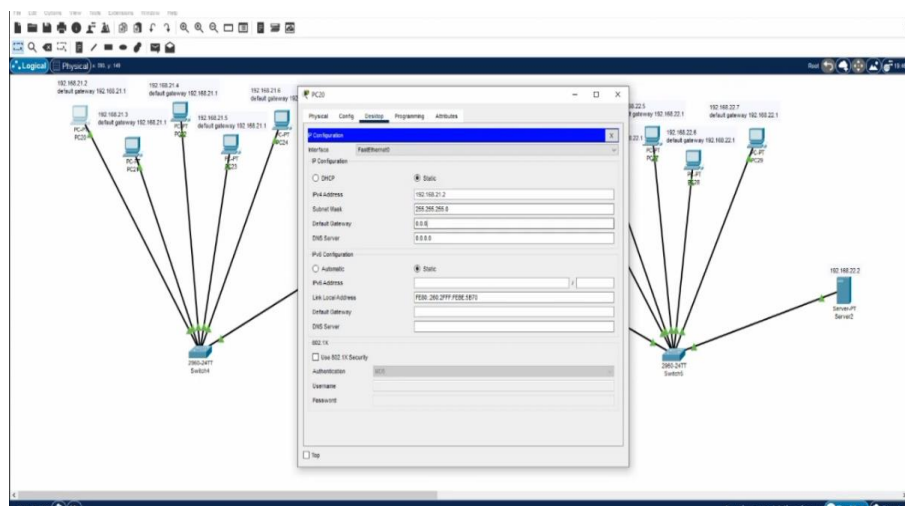
- a. Router

- b. 2 Buah Switch
- c. 10 Buah Pc/Komputer
- d. 1 Buah Server



Gambar 4. Analisa dan Pembahasan 1

Konfigurasi router lakukan konfigurasi untuk menentukan default gateway pada 10 pc dan 1 server, terdapat 2 default gateway yaitu yang pertama untuk gigabit Ethernet 0/0 192.168.21.1 yang kedua untuk gigabit Ethernet 1/0 192.168.22.1.



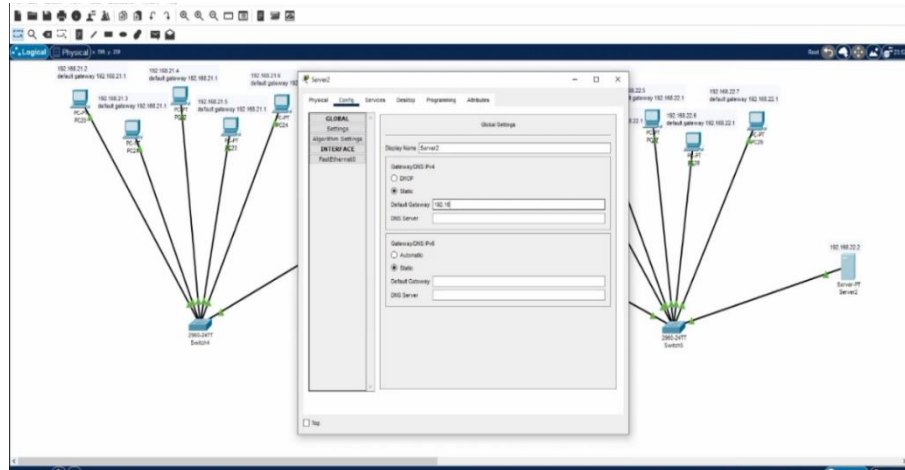
Gambar 5. Analisa dan Pembahasan 2

Menentukan alamat ip pc ip address merupakan bagian terpenting dalam menentukan sebuah koneksi jaringan dan merupakan identitas sebuah perangkat dalam jaringan yang tidak boleh dilupakan. Untuk konfigurasi ip address pada cisco paket tracer dapat dengan melakukan klik pada pc, kemudian masuk menu desktop dan pilih ip configuration.

Konfigurasi server Langkah Langkah :

- a. Klik pada device server
- b. Pilih menu config
- c. Input default gateway dengan 192.168.21.1
- d. Masih dalam menu config pilih menu fast Ethernet0
- e. Ceklis port status agar menjadi on
- f. Pindah ke menu services

- g. Pilih DNS server (on)
- h. Input nama domain pada kolom name
- i. Input address, sesuaikan dengan ip server saat dimenu config klik add

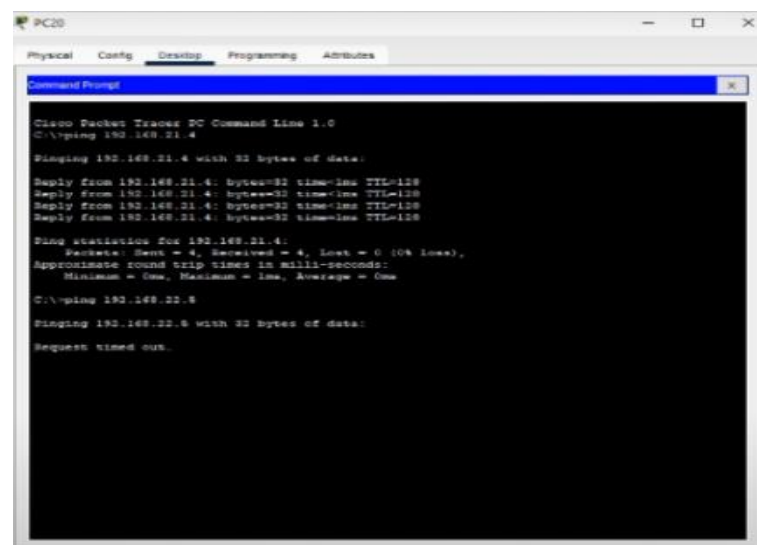


Gambar 6. Analisa dan Pembahasan 3

Mengaktifkan firewall konfigurasi firewall yang berbeda pada device server dengan Langkah sebagai berikut :

- a. Aktifkan service (on)
- b. Tentukan action
- c. Masukkan ip pada pc yang ingin diblokir aksesnya
- d. Mengubah protocol menjadi ip
- e. Memasukkan wildcard mask sesuai kebutuhan, dengan klik add config lalu memblokir akses terhadap pc1, pc2, pc3, pc4, pc5 dan memberikn akses pada pc6, pc7, pc8, pc9, pc10.

Setelah melakukan perancangan tersebut lakukan pengecekan atau test konfigurasi yang telah kita lakukan seperti gambar dibawah ini :



Gambar 7. Analisa dan Pembahasan 4



Dalam perancangan dan simulasi jaringan komputer dengan keamanan firewall ini, kami telah berhasil menunjukkan bagaimana firewall dapat berperan penting dalam melindungi jaringan dari ancaman eksternal maupun internal. Dengan menyusun topologi jaringan yang melibatkan perangkat seperti router, server, firewall, dan klien, serta mengonfigurasi firewall untuk memfilter lalu lintas yang tidak sah, kami dapat memastikan bahwa hanya akses yang sah yang diperbolehkan untuk mengakses sumber daya di dalam jaringan.

Keberhasilan dalam implementasi firewall pada jaringan ini menunjukkan bahwa firewall merupakan alat yang efektif untuk meningkatkan keamanan jaringan komputer, terutama dalam mengontrol aliran data yang masuk dan keluar. Melalui penerapan aturan akses berbasis IP, port, dan protokol yang tepat, firewall mampu menyaring serangan potensial seperti akses tidak sah atau eksploitasi terhadap celah keamanan.

Namun, perlu diingat bahwa firewall hanya satu lapisan dari sistem keamanan yang lebih besar. Agar sistem keamanan jaringan tetap efektif, perlu adanya pemantauan berkala, pembaruan perangkat dan kebijakan, serta penggunaan metode keamanan tambahan, seperti enkripsi dan deteksi intrusi. Sebagai langkah selanjutnya, pemeliharaan yang rutin dan evaluasi atas kebijakan keamanan yang diterapkan dalam firewall harus dilakukan untuk memastikan perlindungan yang optimal.

4. KESIMPULAN

Dalam perancangan dan simulasi jaringan komputer dengan keamanan firewall ini, dapat disimpulkan bahwa penerapan firewall sangat efektif untuk melindungi jaringan dari ancaman eksternal maupun internal. Dengan menggunakan firewall untuk mengontrol dan memfilter lalu lintas yang masuk dan keluar, hanya lalu lintas yang sah yang diizinkan, sementara akses yang tidak sah atau berpotensi berbahaya diblokir.

Simulasi ini membuktikan bahwa firewall berperan penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data dalam jaringan komputer. Konfigurasi firewall yang tepat, termasuk pengaturan aturan akses berbasis IP, port, dan protokol, dapat memberikan perlindungan yang kuat terhadap serangan dari luar seperti akses tidak sah, eksploitasi celah keamanan, serta serangan berbasis jaringan seperti DDoS. Namun, meskipun firewall sangat penting, perlu diingat bahwa keamanan jaringan tidak hanya bergantung pada firewall. Firewall harus dilengkapi dengan kebijakan keamanan yang lebih komprehensif dan dilengkapi dengan alat tambahan seperti sistem deteksi intrusi (IDS), enkripsi data, dan pemantauan terus-menerus untuk melindungi jaringan secara lebih efektif.

Secara keseluruhan, implementasi firewall dalam jaringan komputer merupakan langkah awal yang penting dalam menciptakan sistem keamanan yang solid. Pemeliharaan dan pembaruan secara berkala serta evaluasi kebijakan keamanan yang diterapkan adalah kunci untuk menjaga keamanan jaringan dalam menghadapi ancaman yang terus berkembang.

DAFTAR PUSTAKA

- Hasibuan, M. S. (2018). Keylogger pada Aspek Keamanan Komputer. *Jurnal Teknovasi: Jurnal Teknik dan Inovasi Mesin Otomotif, Komputer, Industri dan Elektronika*, 3(1), 8-15.
- Sinaga, Anita Sinder RM. *Keamanan Komputer*. CV INSAN CENDEKIA MANDIRI, 2020.
- Riduan, Ahmad, and Nanang Sadikin. "Perancangan Firewall Menggunakan Fortigate Di PT Swadharma Duta Data." *Jurnal Maklumatika* (2021): 90-98.
- Kusumaningsih, Rr Yuliana Rachmawati, Azhar Munif, and Erfanti Fatkhiah. "Simulasi Jaringan Komputer Lokal Berbasis Wireless dan Pengamanan Firewall Server Menggunakan Cisco Packet Tracer di PT. Time Excelindo." *Prosiding Seminar Nasional Teknologi Informasi dan Bisnis*. 2022.
- Wicaksono, Dwiki. *Sistem Keamanan Jaringan Menggunakan Firewall Dengan Metode Port Blocking Dan Firewall Filtering*. Diss. JATISI, 2022.
- Cahyawati, Relita Kurnia, et al. "Perancangan Keamanan Jaringan Menggunakan Metode Firewall Security Port." *Prosiding Seminar Nasional Amikom Surakarta*. 2023.
- Setiawan, E. D., & Raharjo, M. (2023). Perancangan Keamanan Jaringan Next-Generation Firewall menggunakan Router Fortinet pada PT. Alodokter Teknologi Solusi. *Jurnal Informatika Terpadu*, 9(1), 34-39.