JUNIF: Jurnal Nasional Informatika

p-ISSN: 2774-3497
e-ISSN: 2774-3500

Vol. 4 No. 2, 15 Oktober 2025, pp. 14-21

TEKNIK IMPLEMENTASI PENGIRIMAN DATA MENGGUNAKAN METODE FILE TRANSFER PROTOCOL (FTP) SERVER DENGAN LOGICAL FIREWALL DEFENSIVE LAYER

PENULIS

[1)]Julio Adi Putra, [2)]Filda Angellia

ABSTRAK

Pengiriman data secara aman merupakan salah satu aspek kritikal dalam infrastruktur jaringan perusahaan. Penelitian ini bertujuan untuk mengimplementasikan teknik pengiriman data menggunakan File Transfer Protocol (FTP) server yang dipadukan dengan logical firewall defensive layer di PT. Tunas Artha Gardatama. Logical firewall digunakan sebagai lapisan perlindungan tambahan untuk mengontrol dan memonitor lalu lintas data yang melalui server FTP, mencegah akses tidak sah dan serangan siber. Hasil penelitian menunjukkan bahwa implementasi FTP server dengan logical firewall defensive layer meningkatkan keamanan dan efisiensi pengiriman data dalam perusahaan. Sistem yang diterapkan mampu mengurangi risiko kebocoran data dan meningkatkan kepercayaan pengguna terhadap keamanan data.

Kata Kunci *FTP Server; Logical Firewal; Pengiriman Data; Keamanan Jaringan;*

AFILIASI

Prodi, Fakultas [1,2)] Program Studi Sistem Informasi, Fakultas Ilmu Komputer.
Nama Institusi [1,2)] Institut Bisnis dan Informatika Kosgoro 1957.
Alamat Institusi [1,2)] Jl. Moh Kahfi II, Srengseng Sawah, Jagakarsa, Jakarta Selatan, DKI Jakarta.

KORESPONDENSI

Penulis Julio Adi Putra
Email julio.adiputra.jap@gmail.com

DOI : https://doi.org/10.55122/junif.v4i2.1811

I. PENDAHULUAN

Di era digital, keamanan data merupakan prioritas utama bagi perusahaan yang terlibat dalam pengolahan dan transfer data dalam jumlah besar. PT. Tunas Artha Gardatama sebagai perusahaan yang bergerak dalam bidang jasa keuangan, memerlukan solusi pengiriman data yang tidak hanya cepat dan efisien, tetapi juga aman dari potensi ancaman siber. File Transfer Protocol (FTP) telah lama digunakan sebagai metode standar untuk pengiriman data, namun memiliki kelemahan dalam hal keamanan[1]. Oleh karena itu, penelitian ini mengusulkan penggunaan logical firewall defensive layer untuk memperkuat keamanan FTP server. Firewall ini berfungsi sebagai lapisan pelindung yang mengawasi dan mengontrol lalu lintas data masuk dan keluar dari server FTP. Tujuan utama dari penelitian ini adalah untuk menganalisis dan mengevaluasi efektivitas implementasi FTP server yang dilengkapi dengan logical firewall defensive layer dalam mengamankan pengiriman data di PT. Tunas Artha Gardatama. Seiring meningkatnya ancaman siber, kebutuhan akan mekanisme pertahanan yang lebih kuat menjadi semakin mendesak. Salah satu pendekatan yang dapat diimplementasikan adalah penggunaan logical firewall defensive layer, yaitu lapisan pertahanan tambahan yang dirancang untuk memonitor, menyaring, dan mengontrol lalu lintas data masuk maupun keluar dari FTP server [2]. Keberadaan logical firewall ini diharapkan mampu menambah tingkat keamanan dengan mencegah akses ilegal, meminimalisir risiko serangan brute force, serta memastikan bahwa hanya koneksi yang sah dan terverifikasi yang dapat mengakses server [3]. Selain itu, implementasi logical firewall defensive layer dapat memberikan fleksibilitas bagi administrator dalam mengatur aturan keamanan secara dinamis sesuai kebutuhan operasional Perusahaan [4]. Dengan adanya kemampuan untuk menyesuaikan konfigurasi pada firewall, perusahaan dapat merespons perubahan pola serangan siber dengan lebih cepat dan tepat. Hal ini menjadi penting mengingat ancaman siber tidak bersifat statis, melainkan berkembang sejalan dengan inovasi teknologi informasi yang terus berlanjut.

Dalam konteks perusahaan jasa keuangan yang menangani data sensitif dan bersifat rahasia, penerapan lapisan pengamanan tambahan seperti logical firewall defensive layer bukan hanya menjadi opsi, tetapi kebutuhan strategis[5]. Keamanan data yang terjamin dapat meningkatkan kepercayaan klien dan mitra bisnis, sekaligus mendukung kelancaran operasional internal [6]. Oleh karena itu, penelitian ini mengusulkan penggunaan logical firewall defensive layer untuk memperkuat keamanan FTP server di PT. Tunas Artha Gardatama. Tujuan utama dari penelitian ini adalah untuk menganalisis dan mengevaluasi efektivitas implementasi FTP server yang dilengkapi dengan logical firewall defensive layer dalam mengamankan proses pengiriman data, sehingga dapat memberikan rekomendasi sistem keamanan yang optimal bagi perusahaan. Penerapan solusi ini juga menjadi relevan karena semakin meningkatnya volume data yang dipertukarkan dalam operasional harian perusahaan. Pertumbuhan transaksi dan aktivitas digital secara langsung meningkatkan jumlah data yang harus diolah dan ditransfer, sehingga risiko kebocoran data pun semakin besar [7]. Dengan demikian, diperlukan sistem keamanan yang dapat menjaga integritas, kerahasiaan, dan ketersediaan data selama proses pertukaran.

Selain risiko serangan eksternal, ancaman internal seperti kesalahan konfigurasi atau akses yang tidak disengaja juga menjadi faktor yang perlu dipertimbangkan [8]. Logical firewall defensive layer dapat membantu meminimalisir risiko ini dengan menyediakan mekanisme kontrol akses yang lebih ketat dan terstruktur. Dengan adanya pengaturan berbasis aturan (rule-based filtering), administrator dapat mengatur siapa saja yang berhak mengakses server dan jenis aktivitas apa yang diperbolehkan, sehingga potensi terjadinya pelanggaran internal dapat ditekan. Dari perspektif regulasi, perusahaan jasa keuangan juga diharuskan mematuhi standar keamanan informasi untuk menjaga kerahasiaan dan keselamatan data nasabah [9]. Implementasi firewall pada FTP server dapat menjadi salah satu langkah pemenuhan standar tersebut. Dengan memiliki sistem keamanan berlapis, perusahaan dapat lebih mudah memenuhi audit keamanan, standar compliance, serta pedoman tata kelola keamanan informasi [10]. Dengan seluruh latar belakang tersebut, penelitian ini diharapkan dapat memberikan kontribusi nyata dalam pengembangan sistem keamanan data yang lebih kuat dan efisien di PT. Tunas Artha Gardatama. Selain menilai efektivitas logical firewall defensive layer

pada FTP server, penelitian ini juga bertujuan menghasilkan rekomendasi strategis bagi perusahaan dalam meningkatkan ketahanan sistem informasi terhadap berbagai ancaman siber yang terus berkembang.

II. METODE PENELITIAN

Penelitian ini dilakukan melalui beberapa tahapan utama yang meliputi analisa kebutuhan sistem, desain sistem, dan implementasi. Berikut adalah penjelasan lebih rinci untuk setiap tahapan tersebut :

2.1. Analisa Kebutuhan Sistem

Pada tahap ini, dilakukan identifikasi kebutuhan keamanan dan fungsionalitas yang diperlukan oleh PT. Tunas Artha Gardatama dalam pengiriman data. Langkah-langkah dalam analisa kebutuhan sistem meliputi :

- **Identifikasi Risiko Keamanan**
  Menganalisis potensi ancaman yang mungkin terjadi pada server FTP yang digunakan, seperti serangan brute force, sniffing, dan akses tidak sah. Analisis ini dilakukan dengan mengkaji rekam jejak serangan sebelumnya, pola lalu lintas data, serta kerentanan yang mungkin terdapat pada infrastruktur jaringan perusahaan.
- **Identifikasi Persyaratan Pengguna**
  Mengumpulkan informasi dari berbagai departemen yang menggunakan server FTP, untuk memahami kebutuhan spesifik terkait pengiriman data. Ini termasuk kecepatan pengiriman, ukuran file, frekuensi transfer, dan tingkat akses yang diperlukan.
- **Penentuan Standar Keamanan**
  Mengkaji kebijakan keamanan perusahaan dan standar industri yang relevan, seperti ISO/IEC 27001, untuk menentukan langkah-langkah keamanan yang harus diimplementasikan. Ini termasuk enkripsi data, otentikasi dua faktor, dan manajemen log.
- **Analisis Infrastruktur Saat Ini**
  Memeriksa infrastruktur jaringan yang ada, termasuk perangkat keras dan lunak yang mendukung server FTP, serta kemampuan firewall yang saat ini digunakan. Hal ini penting untuk memastikan kompatibilitas dengan sistem baru yang akan diimplementasikan.

2.2. Desain Sistem

Tahap desain sistem melibatkan perencanaan arsitektur server FTP yang dilengkapi dengan logical firewall defensive layer. Proses ini mencakup beberapa sub-tahapan berikut :

- **Desain Arsitektur Jaringan**
  Membuat blueprint arsitektur jaringan yang menunjukkan posisi server FTP, firewall, dan komponen lainnya dalam sistem. Arsitektur ini dirancang untuk memastikan data hanya mengalir melalui jalur yang aman dan dapat diawasi oleh firewall.
- **Konfigurasi FTP Server**
  Merancang konfigurasi server FTP yang mencakup pengaturan otentikasi pengguna, enkripsi SSL/TLS, dan manajemen izin akses. Konfigurasi ini disusun untuk meminimalkan risiko keamanan tanpa mengorbankan fungsionalitas sistem.
- **Pengaturan Logical Firewall**
  Merancang pengaturan firewall yang melibatkan pembuatan aturan dan kebijakan yang spesifik untuk memantau dan mengontrol lalu lintas data yang melalui server FTP. Firewall disetting untuk memfilter lalu lintas berdasarkan alamat IP, protokol, dan jenis data, serta mendeteksi pola perilaku yang mencurigakan.
- **Penentuan Skema Monitoring dan Logging**
  Desain juga meliputi pengaturan monitoring dan logging untuk memantau aktivitas server FTP dan firewall. Log yang dihasilkan akan digunakan untuk audit keamanan dan analisis insiden jika terjadi upaya akses tidak sah atau serangan.

2.3. Implementasi

Implementasi adalah tahap di mana desain sistem diterapkan pada lingkungan uji coba sebelum diimplementasikan secara penuh di infrastruktur PT. Tunas Artha Gardatama. Langkah- langkah implementasi meliputi:

- **Deploy FTP Server**
  Server FTP dipasang dan dikonfigurasi sesuai dengan desain yang telah dibuat. Implementasi ini meliputi pengaturan layanan FTP, pemasangan sertifikat SSL/TLS, dan integrasi dengan sistem otentikasi yang ada.
- **Instalasi dan Konfigurasi Firewall**
  Firewall diinstal dan dikonfigurasi untuk berfungsi sebagai lapisan defensif di depan server FTP. Aturan firewall yang telah dirancang diterapkan, dan dilakukan pengujian untuk memastikan bahwa firewall dapat mencegah akses tidak sah tanpa mengganggu transfer data yang sah.
- **Uji Coba Sistem**
  Dilakukan serangkaian uji coba untuk menguji efektivitas konfigurasi yang diterapkan. Uji coba ini melibatkan pengiriman data antara server FTP dan klien di bawah berbagai kondisi, termasuk simulasi serangan siber seperti brute force attack dan sniffing.
- **Evaluasi dan Penyesuaian**
  Berdasarkan hasil uji coba, dilakukan evaluasi untuk mengidentifikasi potensi kelemahan atau masalah yang muncul. Penyesuaian pada konfigurasi server FTP dan firewall dilakukan untuk mengoptimalkan performa dan keamanan sistem.
- **Dokumentasi**
  Semua konfigurasi dan hasil pengujian didokumentasikan secara rinci untuk referensi di masa mendatang dan untuk memastikan bahwa setiap langkah dapat diulang jika diperlukan. Implementasi ini diharapkan dapat menghasilkan sistem yang aman, andal, dan sesuai dengan kebutuhan PT. Tunas Artha Gardatama dalam pengiriman data.

Implementasi sistem pengiriman data menggunakan FTP server yang dipadukan dengan logical firewall defensive layer dilakukan dengan pendekatan teknis yang terstruktur agar sistem dapat berfungsi optimal sekaligus memenuhi kebutuhan keamanan data perusahaan. Server yang digunakan berbasis **Ubuntu Server 22.04 LTS** sebagai sistem operasi utama, sedangkan perangkat lunak FTP yang dipilih adalah **vsftpd (Very Secure FTP Daemon)** karena memiliki tingkat stabilitas dan keamanan tinggi. Proses instalasi dilakukan dengan perintah dasar:

sudo apt install vsftpd

Setelah instalasi selesai, dilakukan konfigurasi pada berkas /etc/vsftpd.conf untuk mengaktifkan fitur keamanan, antara lain menonaktifkan akses anonim, mengaktifkan otentikasi pengguna lokal, serta mengaktifkan enkripsi SSL/TLS. Beberapa konfigurasi penting yang diterapkan antara lain:

anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES
ssl_enable=YES
rsa_cert_file=/etc/ssl/certs/vsftpd.pem

Pengaturan ini memastikan bahwa hanya pengguna yang terdaftar dan memiliki izin yang dapat mengakses server FTP, serta seluruh proses pengiriman data dilakukan dalam koneksi terenkripsi. Selanjutnya, logical firewall dikonfigurasikan menggunakan sistem pfSense 2.6.0 yang berfungsi sebagai lapisan pelindung antara jaringan internal dan eksternal. Firewall ini diatur untuk memfilter lalu lintas jaringan yang melalui port

FTP (port 20 dan 21), serta menerapkan mode passive FTP pada rentang port 40000–50000. Aturan firewall disusun agar hanya alamat IP internal perusahaan (misalnya 192.168.1.0/24) yang diizinkan mengakses server FTP, sedangkan koneksi lain akan ditolak secara otomatis. Selain itu, firewall juga dilengkapi modul Intrusion Detection and Prevention System (IDPS) menggunakan Snort untuk mendeteksi aktivitas mencurigakan seperti brute force attack, sniffing, atau upaya port scanning. Bila sistem mendeteksi serangan, firewall secara otomatis memblokir alamat IP penyerang dan mencatat log insiden untuk keperluan audit keamanan. Proses monitoring dan logging juga menjadi bagian penting dari sistem ini. Semua aktivitas FTP dicatat melalui syslog dan dapat dipantau secara real-time melalui antarmuka dashboard pfSense. Data log digunakan oleh tim IT untuk analisis keamanan dan identifikasi potensi ancaman di masa mendatang.

Tahap pengujian sistem dilakukan dengan beberapa skenario untuk mengukur keamanan, efisiensi, dan stabilitas sistem. Pengujian kecepatan transfer dilakukan menggunakan file uji berukuran 100 MB antar dua node jaringan, baik internal maupun eksternal. Hasilnya menunjukkan bahwa penambahan firewall tidak menurunkan kecepatan transfer secara signifikan. Selain itu, pengujian terhadap serangan brute force menggunakan alat Hydra Tool menunjukkan bahwa firewall mampu mendeteksi dan memblokir IP penyerang dalam waktu kurang dari lima detik. Hasil pengujian ini menunjukkan bahwa integrasi FTP server dengan logical firewall defensive layer mampu meningkatkan keamanan pengiriman data secara signifikan tanpa mengorbankan performa sistem. Sistem berjalan stabil dalam kondisi beban tinggi dan berhasil mengurangi risiko akses tidak sah serta kebocoran data pada jaringan perusahaan.

2.4. Pengujian

Pengujian dilakukan untuk memastikan bahwa implementasi server FTP dengan logical firewall defensive layer berfungsi sesuai harapan. Tahap pengujian meliputi :

- **Uji Keamanan**
  Simulasi serangan seperti brute force attack, sniffing, dan SQL injection untuk menguji efektivitas firewall dalam mencegah akses tidak sah.
- **Uji Kinerja**
  Pengukuran kecepatan transfer data dengan dan tanpa firewall untuk memastikan firewall tidak menyebabkan bottleneck.
- **Uji Fungsionalitas**
  Pengujian kelengkapan fitur FTP server, seperti otentikasi, enkripsi, dan izin akses, untuk memastikan semuanya berjalan dengan benar.
- **Uji Beban**
  Pengujian dengan volume data besar untuk melihat bagaimana sistem menangani beban tinggi dan memastikan kestabilan server..

2.5. Evaluasi

Hasil pengujian dievaluasi untuk mengidentifikasi keberhasilan dan area yang memerlukan perbaikan:

- **Keamanan**
  Firewall terbukti efektif memblokir serangan tanpa mengurangi kinerja sistem, menunjukkan bahwa sistem berhasil meningkatkan keamanan secara signifikan.
- **Kinerja**
  Tidak ada penurunan signifikan dalam kecepatan transfer data, menandakan firewall tidak menyebabkan hambatan berarti.
- **Kestabilan**
  Sistem tetap stabil di bawah beban tinggi, memastikan server mampu menangani operasi perusahaan secara efisien.

Berdasarkan evaluasi ini, sistem dianggap berhasil memenuhi tujuan dan kebutuhan PT. Tunas Artha Gardatama.

III. HASIL DAN PEMBAHASAN

Setelah proses implementasi dan pengujian, sejumlah hasil diperoleh yang memberikan gambaran tentang efektivitas sistem yang telah diterapkan di PT. Tunas Artha Gardatama. Berikut adalah hasil dan pembahasan lebih rinci dari penelitian ini:

3.1. Keamanan Data yang Meningkat

Hasil pengujian menunjukkan bahwa penerapan logical firewall defensive layer pada FTP server secara signifikan meningkatkan keamanan pengiriman data. Beberapa poin utama yang menjadi temuan dalam aspek keamanan meliputi:

- **Deteksi dan Pencegahan Serangan**
  Firewall berhasil mendeteksi dan memblokir berbagai jenis serangan, termasuk brute force attack dan sniffing. Hal ini terbukti dari log yang menunjukkan upaya akses tidak sah yang dihalangi oleh firewall. Dengan konfigurasi yang tepat, firewall dapat membedakan antara lalu lintas data yang sah dan yang mencurigakan, sehingga mencegah serangan sebelum mencapai server FTP.
- **Otentikasi yang Lebih Ketat**
  Sistem otentikasi pada server FTP diperkuat dengan lapisan keamanan tambahan dari firewall, seperti pengaturan aturan berdasarkan alamat IP dan protokol tertentu. Hal ini membatasi akses hanya kepada pengguna yang berwenang dan meminimalkan risiko kebocoran data melalui akses yang tidak sah.
- **Enkripsi Data**
  Implementasi SSL/TLS pada server FTP memastikan bahwa data yang dikirim dan diterima terenkripsi dengan baik. Firewall juga berperan dalam memastikan bahwa hanya lalu lintas terenkripsi yang diizinkan melewati jaringan, menambah lapisan keamanan terhadap potensi penyadapan.

3.2. Efisiensi Pengiriman Data

Meskipun fokus utama adalah meningkatkan keamanan, hasil pengujian juga menunjukkan bahwa efisiensi pengiriman data tidak terpengaruh secara signifikan. Beberapa temuan utama dalam aspek ini meliputi:

- **Kecepatan Transfer Data**
  Pengujian terhadap kecepatan transfer data menunjukkan bahwa penambahan firewall tidak menyebabkan penurunan performa yang berarti. Kecepatan rata- rata pengiriman data tetap berada dalam batas yang dapat diterima oleh standar operasional perusahaan. Ini menunjukkan bahwa firewall telah dikonfigurasi dengan efisien tanpa menghambat lalu lintas jaringan.
- **Manajemen Beban**
  Saat diuji dengan volume data yang besar, sistem tetap mampu menjaga stabilitas dan kecepatan transfer. Firewall berhasil mengelola lalu lintas data dengan baik, bahkan di bawah beban tinggi, tanpa terjadi overloading atau penurunan performa server.

3.3. Pengaturan Akses yang Lebih Granular

Implementasi logical firewall defensive layer memungkinkan pengaturan akses yang lebih detail dan terkontrol. Hasil ini menunjukkan:

- **Kustomisasi Akses**
  Dengan firewall, perusahaan dapat mengatur izin akses berdasarkan peran pengguna, jenis data, dan lokasi geografis. Misalnya, akses ke server FTP dapat dibatasi hanya untuk pengguna dari lokasi tertentu atau yang menggunakan protokol tertentu. Ini meningkatkan keamanan sekaligus

memberikan fleksibilitas dalam manajemen akses.

- **Log dan Monitoring**
  Firewall menyediakan fitur log dan monitoring yang memadai untuk melacak aktivitas jaringan secara real-time. Ini memungkinkan tim IT untuk mendeteksi dan merespon ancaman dengan cepat, serta melakukan audit keamanan secara berkala. Data log ini sangat berguna dalam analisis pasca-insiden dan untuk meningkatkan kebijakan keamanan di masa mendatang.

3.4. Tantangan dan Pembelajaran

Selama implementasi, beberapa tantangan diidentifikasi dan diselesaikan, yang memberikan pembelajaran penting untuk pengembangan lebih lanjut:

- **Kompleksitas Konfigurasi**
  Salah satu tantangan utama adalah konfigurasi firewall yang memerlukan keahlian khusus untuk memastikan tidak mengganggu operasional normal FTP server. Tim IT harus memastikan bahwa aturan firewall yang diterapkan tidak terlalu ketat sehingga menghalangi lalu lintas data yang sah. Ini memerlukan pengujian berulang dan penyesuaian yang teliti.
- **Pemeliharaan Sistem**
  Sistem yang lebih kompleks ini memerlukan pemeliharaan yang lebih intensif, termasuk pembaruan aturan firewall dan monitoring log secara rutin. Tantangan ini dapat diatasi dengan pelatihan tambahan bagi tim IT dan penggunaan alat otomatisasi untuk mempermudah pemeliharaan.

3.5. Dampak Terhadap Operasional Perusahaan

Implementasi sistem ini memberikan dampak positif yang signifikan terhadap operasional PT. Tunas Artha Gardatama:

- **Kepercayaan Pengguna**
  Dengan peningkatan keamanan, kepercayaan pengguna internal terhadap sistem pengiriman data meningkat. Mereka merasa lebih aman dalam menjalankan operasional yang melibatkan transfer data penting, yang berdampak positif pada produktivitas keseluruhan.
- **Kepatuhan Terhadap Regulasi**
  Sistem baru ini membantu perusahaan mematuhi berbagai regulasi keamanan data yang berlaku, termasuk perlindungan data pribadi dan standar industri lainnya. Ini memberikan keunggulan kompetitif dan mengurangi risiko terkait dengan ketidakpatuhan hukum.

IV. SIMPULAN

Implementasi FTP server dengan logical firewall defensive layer di PT. Tunas Artha Gardatama berhasil mencapai tujuan utama penelitian, yaitu meningkatkan keamanan tanpa mengorbankan efisiensi pengiriman data. Firewall memberikan perlindungan tambahan yang diperlukan terhadap berbagai ancaman siber, sementara sistem tetap responsif dan stabil di bawah berbagai kondisi operasional. Tantangan yang dihadapi selama implementasi memberikan wawasan berharga untuk perbaikan berkelanjutan dan pengembangan sistem keamanan di masa depan.

REFERENSI

[1] J. Generic *et al.*, “Implementasi FTP Server dengan Metode Transfer Layer Security untuk Keamanan Transfer Data Menggunakan,” vol. 9, no. 2, pp. 348–355, 2014.

[2] R. W. Anwar, T. Abdullah, and F. Pastore, “applied sciences Firewall Best Practices for Securing Smart Healthcare Environment : A Review,” 2021.

[3] R. Satra and F. Fattah, “Keamanan Jaringan VLAN dan VoIP Menggunakan Firewall,” vol. 2, no. 1, pp. 27–35, 2021.

[4] E. Suteja, E. K. N, and S. Raharjo, “MENGURANGI KEJAHATAN CYBER MENGGUNAKAN TEKNIK DEMILITARIZED ZONE (DMZ) DAN FIREWALL RULES (Studi Kasus : Laboratorium Basis Data IST AKPRIND),” *J. JARKOM*, vol. 09, no. 01, pp. 71–80, 2021.

[5] P. P. Laskowski, “Internet security – Technology and social awareness of the dangers,” *Stud. Logic, Gramm. Rhetor.*, vol. 50, no. 1, pp. 239–252, 2017, doi: 10.1515/slgr-2017-0027.

[6] J. M. Kizza, *Computer Network Security Computer Network Security*, vol. 1. 2007.

[7] V. Bhavsar, A. Kadlak, and S. Sharma, “Study on Phishing Attacks,” *Int. J. Comput. Appl.*, vol. 182, no. 33, pp. 27–29, 2018, doi: 10.5120/ijca2018918286.

[8] J. Sistim, F. Prasetyo, E. Putra, A. Hamzah, W. Agel, and R. O. F. Kusuma, “Impelementasi Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking,” vol. 5, no. 4, pp. 82–87, 2024, doi: 10.60083/jsisfotek.v5i4.329.

[9] G. Abdumalikov, “Profound Importance of Cyber security in the Field of Business,” no. c, pp. 43–46, 2022, [Online]. Available: https://media.neliti.com/media/publications/408257-profound-importance-of-cyber-security-in-a2668cec.pdf.

[10] S. Kadry and W. Hassan, “Design and Implementation of System and Network Security for an Enterprise With Worldwide Branches.,” *J. Theor. Appl. Inf. Technol.*, vol. 4, no. 2, pp. 111–118, 2008, [Online]. Available: http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=32507429&site=ehost-live&scope=site.