Jurnal Review Pendidikan dan Pengajaran
http://journal.universitaspahlawan.ac.id/index.php/jrpp
Volume 8 Nomor 2, 2025
P-2655-710X e-ISSN 2655-6022

Submitted : 29/04/2025
Reviewed : 08/05/2025
Accepted : 10/05/2025
Published : 29/05/2025

La Ode Muhammad Azlan[1]
Muhammad Arif Sulaiman[2]
Didik Sulistyo[3]

PEMODELAN IMPLEMENTASI FIREWALL SECURITY PORT DAN ACCESS CONTROL LIST UNTUK PENINGKATAN KEAMANAN JARINGAN INTRANET AUTOMATIC TERMINAL INFORMATION SERVICE

Abstrak
Keamanan jaringan merupakan aspek penting dalam sistem informasi, khususnya pada infrastruktur vital seperti Automatic Terminal Information Service (ATIS). Sistem ini menyampaikan informasi navigasi dan komunikasi penerbangan yang bersifat sensitif dan kritikal. Penelitian ini bertujuan untuk memodelkan dan mengimplementasikan fitur firewall security port pada switch manageable serta Access Control List (ACL) pada router untuk meningkatkan keamanan jaringan intranet ATIS. Metode penelitian yang digunakan adalah eksperimen dengan simulasi jaringan melalui Cisco Packet Tracer. Pengujian dilakukan dalam dua skenario: sebelum dan sesudah penerapan fitur keamanan. Hasil penelitian menunjukkan bahwa firewall security port efektif dalam membatasi akses tidak sah dengan mengatur port switch, sedangkan ACL mampu menyaring lalu lintas berdasarkan aturan tertentu. Kombinasi kedua fitur ini terbukti meningkatkan keamanan jaringan, mengurangi risiko penyusupan, serta menjaga integritas dan kerahasiaan data.
Kata Kunci : Keamanan Jaringan, Firewall Security Port, Access Control List, ATIS, Cisco Packet Tracer.

Abstract
Network security is a critical aspect of information systems, particularly in vital infrastructure such as the Automatic Terminal Information Service (ATIS). This system delivers sensitive and critical navigation and communication information for aviation operations. This study aims to model and implement firewall security port features on manageable switches and Access Control Lists (ACLs) on routers to enhance the security of the ATIS intranet network. The research uses an experimental method with network simulation through Cisco Packet Tracer. Testing is conducted in two scenarios: before and after the implementation of security features. The results show that firewall security ports effectively limit unauthorized access by configuring switch ports, while ACLs filter traffic based on defined rules. The combination of these two features significantly improves network security, reduces intrusion risks, and preserves data integrity and confidentiality.
Keywords : Network Security, Firewall Security Port, Access Control List, ATIS, Cisco Packet Tracer.

PENDAHULUAN

Automatic Terminal Information Service (ATIS) adalah sistem otomatis yang menyediakan informasi penting seperti kondisi cuaca, runway aktif, dan informasi penerbangan lainnya kepada pilot [1]. Sistem ini sangat bergantung pada integritas dan keamanan jaringan intranet untuk memastikan informasi yang disampaikan tetap valid dan tidak mengalami gangguan dari pihak yang tidak bertanggung jawab. Ancaman siber yang semakin kompleks menuntut penguatan sistem keamanan, salah satunya melalui penerapan firewall dan Access Control List (ACL) sebagai bentuk pengendalian akses pada perangkat jaringan [2].

ATIS terhubung dengan sistem lainnya seperti Automatic Weather Observation System (AWOS), AFTN, dan layanan data penerbangan lainnya, sehingga diperlukan sistem jaringan intranet yang terintegrasi dan aman dari intersepsi. Potensi ancaman dari perangkat asing atau

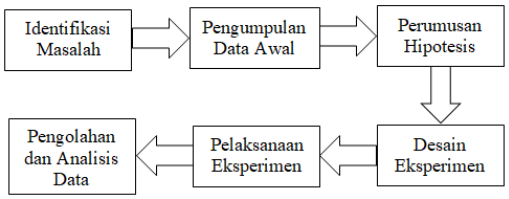
[1,2,3]Politeknik Penerbangan Indonesia Curug, Indonesia
email: laodemuhammadazlan20@gmail.com, arif.sulaiman@ppicurug.ac.id, di2k.sk80@gmail.com.

koneksi tidak sah yang masuk ke dalam jaringan harus dicegah melalui penerapan kebijakan keamanan berlapis [3].

Regulasi nasional seperti Peraturan Menteri Perhubungan No. PM 77 Tahun 2011 dan Keputusan Dirjen Perhubungan Udara No. KP 8 Tahun 2018 telah menggarisbawahi pentingnya pengamanan sistem komunikasi dan informasi di sektor penerbangan. Regulasi ini sejalan dengan standar internasional seperti ICAO Annex 17 yang menekankan perlindungan sistem informasi dalam layanan navigasi udara [4].

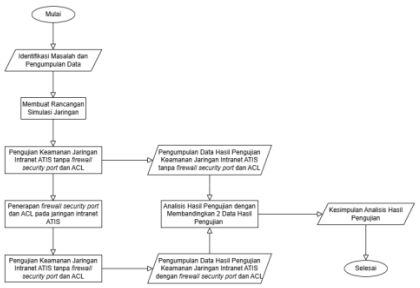
Penelitian ini mengangkat isu-isu keamanan jaringan dengan fokus pada implementasi firewall security port dan ACL di lingkungan ATIS yang telah disimulasikan untuk mengidentifikasi efektivitas strategi pertahanan jaringan terhadap ancaman umum seperti spoofing, scanning, dan unauthorized access.

METODE



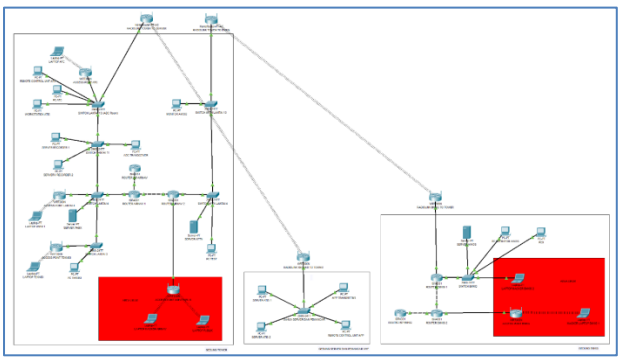
Gambar 1. Alur Metode Penelitian Eksperimen

Penelitian ini menggunakan metode eksperimen melalui simulasi topologi jaringan menggunakan Cisco Packet Tracer [5]. Simulasi ini bertujuan untuk merepresentasikan arsitektur jaringan ATIS yang umum ditemukan di lapangan.[6]



Gambar 2. Flowchart Pelaksaan Eksperimen

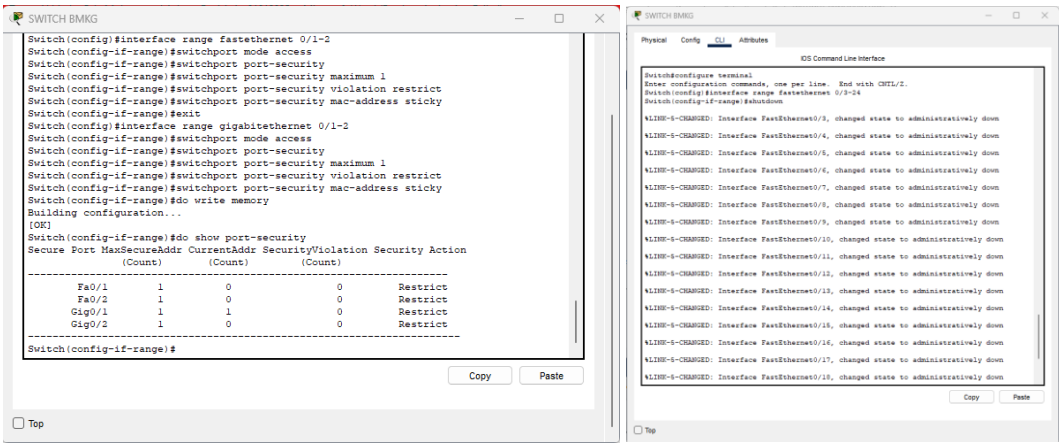
Topologi jaringan yang dirancang mencakup tiga gedung utama yang dimana dua gedung mewakili Perum LPPNPI AirNav (Gedung Tower dan Gedung Server atau Pemancat VHF) dan satu gedung BMKG, serta konektivitas ke berbagai server penting seperti ATIS, AWOS, dan AFTN. Dalam skenario ini, perangkat hacker juga dimasukkan untuk mensimulasikan ancaman eksternal terhadap jaringan [7].



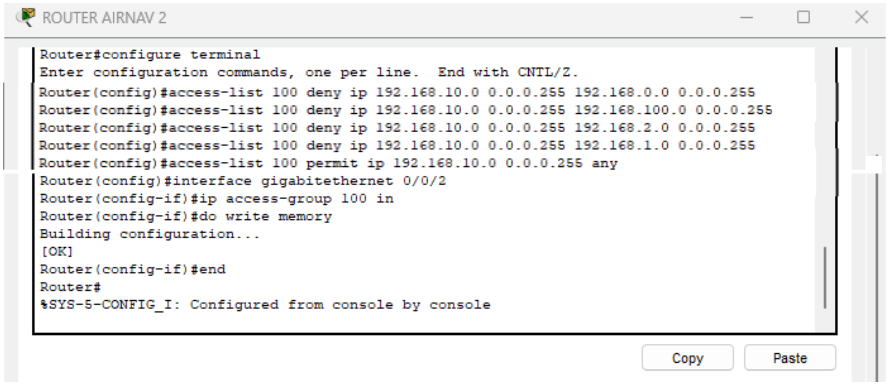
Gambar 3. Gedung dan Topologi Jaringan

Perancangan topologi dilakukan dengan membangun konektivitas antar-gedung yang mencerminkan koneksi dunia nyata melalui media wireless dan kabel. Dalam topologi ini,

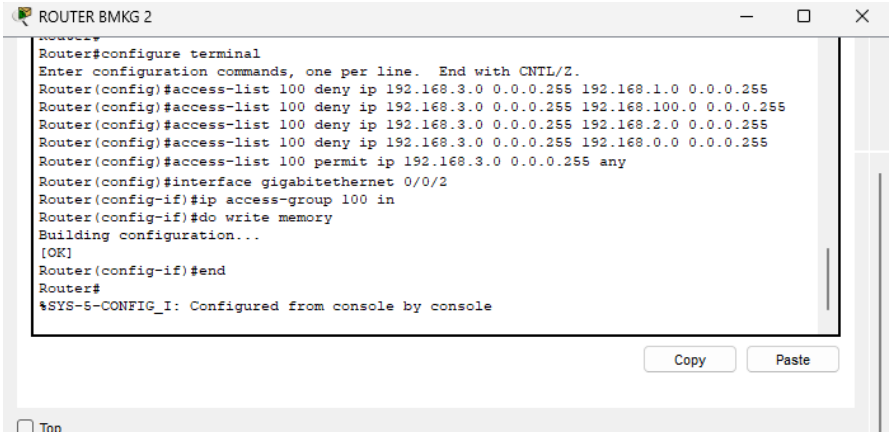
perangkat asing diasumsikan dapat terhubung melalui access point yang tersedia di area umum, maupun melalui port switch yang tidak dikendalikan dengan baik. Penggunaan switch manageable sangat penting dalam pengujian ini, karena memungkinkan pengaturan port secara selektif dan penerapan kebijakan keamanan port yang ketat [8].



Gambar 4. Konfigurasi Firewall Security Port pada Switch Managable



Gambar 5. Konfigurasi ACL pada Router AirNav 2



Gambar 6. Konfigurasi ACL pada Router BMKG 2

Konfigurasi perangkat dilakukan secara bertahap. Pada switch manageable, semua port yang tidak digunakan dinonaktifkan, sedangkan port aktif dikonfigurasi dengan fitur port security. Port security ini membatasi jumlah perangkat yang dapat terkoneksi melalui satu port dan mengizinkan hanya MAC address tertentu untuk mengakses jaringan. Sementara itu, pada router dilakukan konfigurasi ACL untuk membatasi akses berdasarkan alamat IP sumber, tujuan, serta jenis protokol. ACL ini berfungsi sebagai filter lalu lintas data agar hanya perangkat dengan identitas yang sah yang diizinkan untuk mengakses layanan jaringan [9].

Perangkat *Hacker* pada Area Pengujian	Pengujian Konektivitas ke Perangkat	
	Sebelum Penerapan *firewall security port dan ACL*	Sesudah Penerapan *firewall security port dan ACL*
Area umum / publik AirNav	*Server* ATIS *Server* AWOS *Server* AFTN *Router* ISP / Internet	*Server* ATIS *Server* AWOS *Server* AFTN *Router* ISP / Internet
Area umum / publik BMKG	*Server* ATIS *Server* AWOS *Server* AFTN *Router* ISP / Internet	*Server* ATIS *Server* AWOS *Server* AFTN *Router* ISP / Internet
Switch BMKG	*Server* ATIS *Server* AWOS *Server* AFTN *Router* ISP / Internet	*Server* ATIS *Server* AWOS *Server* AFTN *Router* ISP / Internet

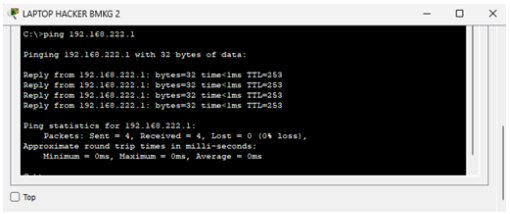
Tabel 1. Rencana Pengujian Simulasi Jaringan ATIS

Pengujian dilakukan dalam dua skenario utama, yaitu sebelum dan sesudah penerapan konfigurasi keamanan. Dalam skenario pertama, semua port switch dalam keadaan aktif dan router tidak memiliki filter ACL. Perangkat hacker diuji untuk mengakses server ATIS dan komponen lainnya. Pada skenario kedua, pengujian dilakukan setelah konfigurasi firewall port security dan ACL diterapkan. Pengujian dilakukan menggunakan metode ping, traceroute, serta pengamatan terhadap alur lalu lintas data untuk mengukur keberhasilan atau kegagalan perangkat asing dalam menembus sistem.

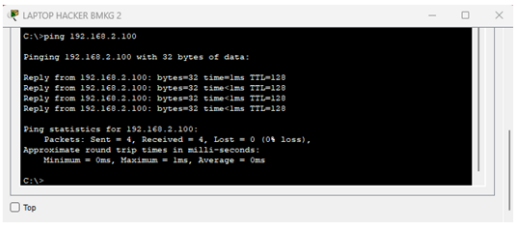
Analisis dilakukan secara kualitatif dan kuantitatif. Secara kualitatif, penulis mengamati pola lalu lintas jaringan dan respon sistem terhadap akses yang tidak sah. Secara kuantitatif, jumlah keberhasilan akses dari perangkat asing dibandingkan antara sebelum dan sesudah konfigurasi. Hasil dari eksperimen ini menjadi dasar penilaian efektivitas fitur firewall security port dan ACL dalam meningkatkan keamanan jaringan intranet ATIS [10].

HASIL DAN PEMBAHASAN

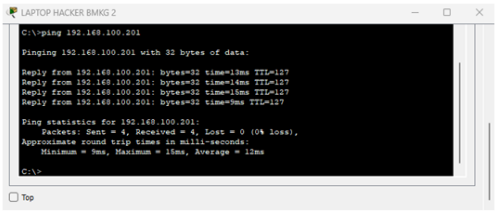
Skenario awal menunjukkan bahwa perangkat asing dapat dengan mudah mengakses server ATIS, AWOS, dan AFTN. Hal ini menunjukkan kelemahan signifikan dalam pengendalian akses dan ketiadaan mekanisme penyaringan trafik yang memadai. Tanpa adanya pengaturan pada port switch dan filter ACL di router, seluruh jaringan menjadi rentan terhadap berbagai jenis serangan seperti spoofing dan sniffing [11].



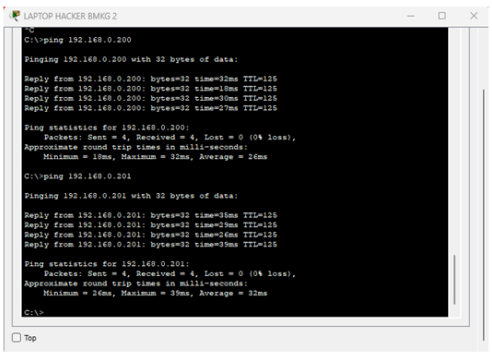
Hasil Ping ke Router ISP BMKG



Hasil Ping ke Server AWOS



Hasil Ping ke Server AFTN



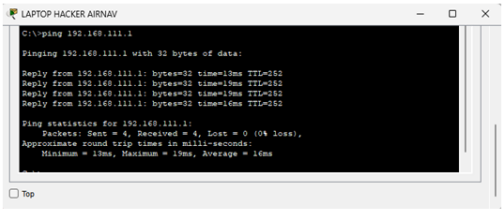
Hasil Ping ke Server ATIS

Gambar 7. Hasil Pengujian Pada Skenario awal

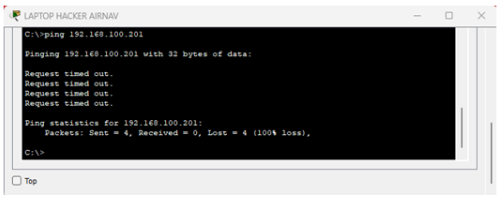
Setelah penerapan firewall security port, perubahan signifikan terjadi. Semua port yang

tidak digunakan berhasil dinonaktifkan, dan hanya perangkat dengan MAC address yang telah terdaftar dapat mengakses jaringan. Hal ini membatasi ruang gerak perangkat asing yang mencoba untuk mengakses jaringan melalui port tidak sah [12]. Switch manageable berperan penting dalam mengelola akses fisik ke jaringan dengan memastikan bahwa koneksi hanya diberikan kepada perangkat yang telah diverifikasi. Penerapan ACL memberikan lapisan perlindungan tambahan. Router hanya mengizinkan lalu lintas dari subnet dan alamat IP yang dikenali, serta menolak semua koneksi dari alamat asing atau tidak terdaftar. Aturan ACL yang digunakan sangat spesifik terhadap protokol dan jenis layanan, seperti mengizinkan hanya trafik TCP ke port tertentu atau membatasi akses hanya ke jaringan lokal, berikut hasil pengujian setelah penerapan yang meliputi:

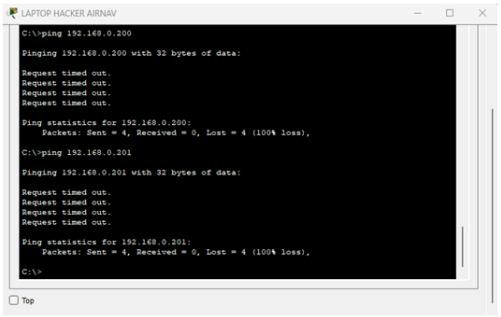
1. Perangkat hacker pada area umum AirNav.



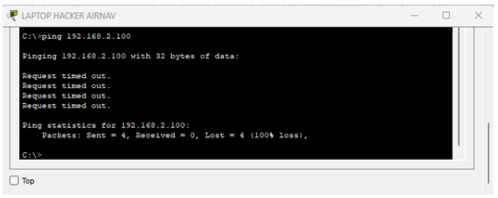
Hasil Ping dari Perangkat Hacker ke Router ISP AirNav



Hasil Ping dari Perangkat Hacker ke Server AFTN



Hasil Ping dari Perangkat Hacker ke Server ATIS

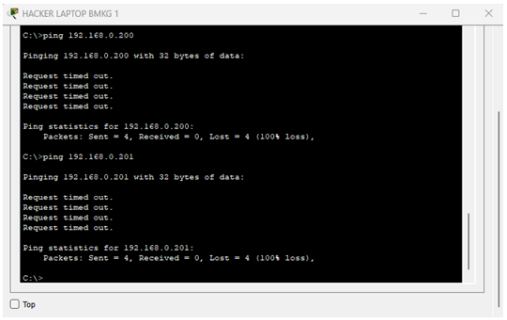


Hasil Ping dari Perangkat Hacker ke Server AWOS

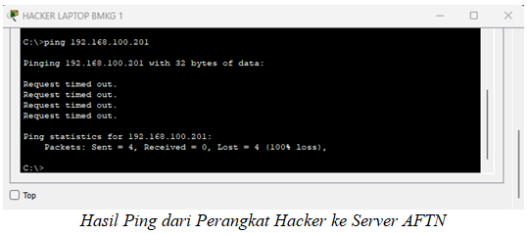
Gambar 8. Hasil Pengujian pada perangkat hacker pada area umum AirNav

Setelah penerapan firewall security port dan ACL maka akses perangkat hacker masih mendapatkan koneksi internet dibuktikan dengan perangkat masih dapat terkoneksi ke Router ISP AirNav sedangkan untuk koneksi ke server AFTN, server ATIS dan server AWOS telah terblokir.

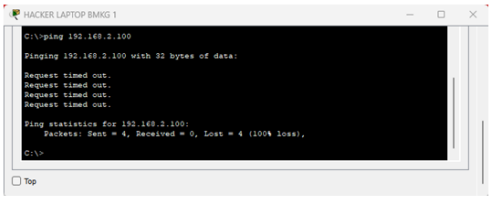
2. Perangkat hacker yang terhubung dengan access point area umum BMKG.



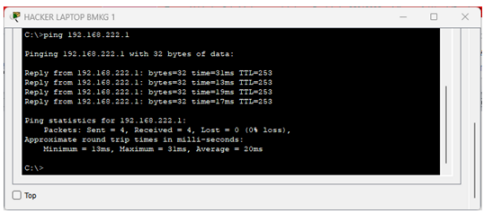
Hasil Ping dari Perangkat Hacker ke Server ATIS



Hasil Ping dari Perangkat Hacker ke Server AFTN



Hasil Ping dari Perangkat Hacker ke Server AWOS



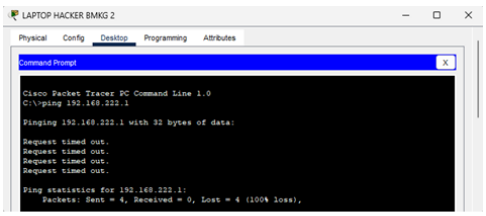
Hasil Ping dari Perangkat Hacker ke Router ISP BMKG

Gambar9. Hasil Pengujian pada perangkat hacker yang terhubung dengan access point area umum BMKG.

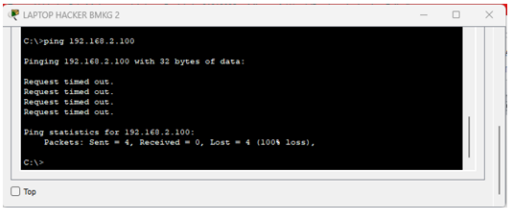
Setelah penerapan ACL pada router BMKG 2, perangkat hacker masih mendapatkan akses internet diketahui dengan hasil ping ke router ISP BMKG, sedangkan akses perangkat hacker ke server AWOS, server AFTN, dan server ATIS sepenuhnya diblokir.

3. Perangkat hacker yang terhubung dengan switch manageable BMKG.

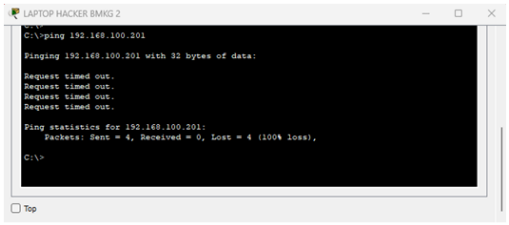
4.



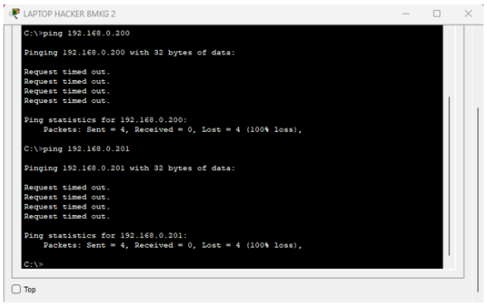
Hasil Ping dari Perangkat Hacker ke Router ISP BMKG



Hasil Ping dari Perangkat Hacker ke Server AWOS



Hasil Ping dari Perangkat Hacker ke Server AFTN

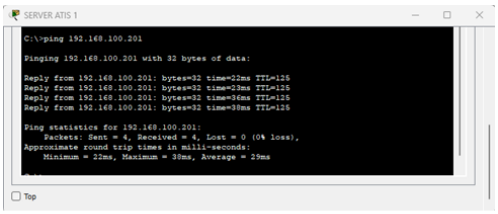


Hasil Ping dari Perangkat Hacker ke Server ATIS

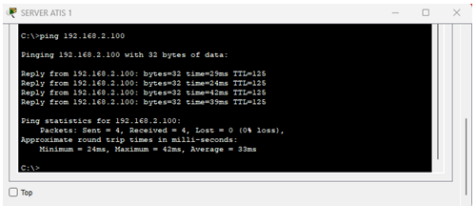
Gambar10. Hasil Pengujian pada perangkat hacker yang terhubung dengan switch manageable BMKG

Berdasarkan hasil pengujian setelah firewall security port diaktifkan maka switch manageable memblokir seluruh akses perangkat hacker karena alamat MAC perangkat hacker tidak terdaftar pada firewall security port.

5. Konektivitas server AWOS, AFTN dan server ATIS 1



Hasil Ping Test dari Server ATIS 1 ke Server AFTN



Hasil Ping Test dari Server ATIS 1 ke Server AWOS

Gambar11. Hasil Pengujian pada konektivitas server AWOS, AFTN dan server ATIS 1

Berdasarkan hasil pengujian yang dilakukan dengan metode ping test dari server ATIS 1 ke server AFTN dan server AWOS telah memverifikasi bahwa server AWOS dapat terkoneksi dan menerima data dari server AWOS setelah fitur firewall security port dan ACL diterapkan.

Kombinasi dari firewall security port dan ACL membentuk sistem pertahanan berlapis yang tangguh. Firewall port berfungsi pada level fisik, sedangkan ACL bekerja pada level logis dan protokol. Sistem pertahanan ini terbukti efektif dalam mencegah akses tidak sah, mengurangi risiko penyusupan, dan menjaga stabilitas serta integritas jaringan ATIS [13].

Ancaman umum seperti spoofing IP, port scanning, dan unauthorized remote access berhasil dicegah [14]. Selain itu, sistem keamanan yang diterapkan tidak mengganggu performa layanan utama. Server ATIS tetap dapat mengirimkan dan menerima data dari sumber resmi seperti BMKG tanpa hambatan. Hasil eksperimen ini membuktikan bahwa konfigurasi keamanan yang baik tidak hanya melindungi jaringan tetapi juga mempertahankan efisiensi layanan.

SIMPULAN

Firewall security port dan Access Control List (ACL) merupakan kombinasi solusi yang efektif dalam meningkatkan keamanan jaringan intranet Automatic Terminal Information Service (ATIS). Firewall port memberikan kontrol akses fisik melalui switch manageable,

sementara ACL menyaring lalu lintas data berdasarkan aturan yang ketat pada tingkat jaringan dan protokol.

Implementasi kedua fitur ini secara bersamaan memberikan perlindungan berlapis terhadap ancaman jaringan, mencegah akses tidak sah, serta menjaga kerahasiaan dan integritas data. Penelitian ini menunjukkan bahwa dengan penggunaan alat simulasi seperti Cisco Packet Tracer, konfigurasi dan dampak sistem keamanan dapat diuji secara realistis sebelum diterapkan pada sistem nyata.

Sebagai rekomendasi, disarankan agar pengelola jaringan ATIS menerapkan pendekatan keamanan menyeluruh yang mencakup penguatan di level fisik dan logis, serta ditambah dengan sistem deteksi intrusi (IDS), audit keamanan berkala, dan pelatihan keamanan jaringan bagi operator. Dengan demikian, jaringan ATIS dapat terjaga dari berbagai bentuk serangan siber dan tetap memberikan layanan informasi penerbangan yang aman dan andal.

SARAN

Berdasarkan hasil penelitian dan implementasi sistem keamanan yang dilakukan, terdapat beberapa saran yang dapat dipertimbangkan untuk pengembangan dan peningkatan sistem keamanan jaringan di masa depan. Pertama, perlu adanya evaluasi berkala terhadap konfigurasi firewall dan ACL yang diterapkan, karena ancaman siber terus berkembang seiring waktu. Evaluasi ini penting untuk memastikan bahwa aturan keamanan yang diterapkan masih relevan dan mampu menghadapi jenis serangan terbaru.

Kedua, disarankan untuk mengintegrasikan sistem keamanan yang lebih komprehensif seperti Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) untuk mendeteksi dan menanggulangi serangan secara real time. Penambahan sistem monitoring jaringan juga akan membantu dalam pelacakan aktivitas mencurigakan serta memberikan log audit yang akurat sebagai bahan evaluasi.

Ketiga, pelatihan rutin kepada personel teknis sangat penting untuk memastikan bahwa mereka memahami konfigurasi keamanan jaringan dan mampu merespons dengan cepat apabila terjadi gangguan atau serangan. Pemahaman yang baik terhadap perangkat lunak dan hardware yang digunakan akan meningkatkan ketahanan operasional sistem secara keseluruhan.

Terakhir, pendekatan keamanan harus diterapkan secara menyeluruh dan berlapis dengan melibatkan semua komponen jaringan, mulai dari perangkat keras, perangkat lunak, hingga kebijakan manajemen yang ketat. Dengan menerapkan strategi tersebut, diharapkan jaringan intranet ATIS dapat memberikan layanan yang lebih andal, aman, dan terlindungi dari berbagai potensi ancaman siber.

DAFTAR PUSTAKA

D. Dandegaokar, S. Katre, and S. V. More, “Automatic Terminal Information System (ATIS),” Int. J. Sci. Eng. Res., vol. 4, no. 4, 2016, [Online]. Available: https://www.ijser.in/archives/v4i4/IJSER15764.pdf?utm_source=chatgpt.com

W. Zhang, X. Li, and M. Chen, “A Study on Network Security via ACL Implementation,” IEEE Trans. Netw. Serv. Manag., 2020.

R. Gupta, D. Sharma, and N. Kumar, “Port Security Mechanisms in Network Switches,” J. Netw. Comput. Appl., pp. 231–245, 2022.

International Civil Aviation Organization (ICAO), Annex 11 to the Convention on International Civil Aviation – Air Traffic Services, 15th Editi. International Civil Aviation Organization (ICAO), 2019. [Online]. Available: https://www.icao.int/airnavigation

R. A. Al-Dhamari and M. Othman, “Design and Simulation of Network Security Using Cisco Packet Tracer,” vol. 11, no. 6, pp. 506–515, 2020, [Online]. Available: https://doi.org/10.14569/IJACSA.2020.0110659

S. McLeod, “Experimental Research,” Simply Psychol., 2019.

Cisco Systems, Cisco Networking Academy Course Materials on Access Control Lists (ACL). Cisco Systems, 2022. [Online]. Available: https://www.cisco.com

H. Chen, J. Wang, M. Zhang, and Z. Liu, A Comprehensive Study on Firewall and ACL Integration for Network Security. Journal of Information Security and Applications, 2018.

A. Kaur and S. Reddy, “Integration of Firewall and ACL for Enhanced Network Security,” Int. J. Comput. Appl., vol. 175,23, pp. 30–35, 2021.

J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed

Methods Approaches, 5th ed. Sage Publications, 2018.
D. Johnson, S. Williams, and A. Patel, "Advanced Network Defense Using Firewall and ACL," Int. J. Cyber-Security Digit. Forensics, pp. 57–68, 2021.
S. William, Principles of Network and Security. McGraw-Hill Education, 2018.
M.-H. Lee and J.-H. Kim, "Enhancing Firewall Performance in Modern Networks," pp. 102–110, 2019.
M. Raj and R. P. Gorthi, "Review on Modern Firewalls: Concepts, Types and Challenges," IEEE Xplore, 2020.