JUDIS
Jurnal Multidisiplin Dan Sains
Vol. 2 No. 1 September 2025, pp.13-22
https://jurnal.compartdigital.com/index.php/judis

PENERAPAN ACCESS CONTROL LIST UNTUK KEAMANAN JARINGAN VIRTUAL LOCAL AREA NETWORK TERENSKRIPSI

Andi Irpan[1], Ilham Faisal [2]& Sarudin[3]
1,2,3) Teknik Informatika, Fakultas Teknik dan Komputer, Universitas Harapan Medan

*Coresponding Email: **Andredaulay67@gmail.com**

Abstrak

Penerapan Access Control List (ACL) merupakan salah satu strategi yang efektif untuk meningkatkan keamanan jaringan Virtual Local Area Network (VLAN) terenskripsi. VLAN menjadi komponen krusial dalam infrastruktur jaringan modern, namun memerlukan perlindungan yang cermat untuk mencegah akses yang tidak sah. Penelitian ini bertujuan untuk mengevaluasi dan menerapkan ACL sebagai mekanisme keamanan pada jaringan VLAN terenskripsi. Metodologi penelitian melibatkan analisis kebutuhan keamanan, perancangan konfigurasi ACL, implementasi pada perangkat jaringan, dan evaluasi kinerja sistem. Hasil eksperimen menunjukkan bahwa penerapan ACL secara efektif memitigasi risiko akses yang tidak sah dan serangan terhadap jaringan VLAN. Selain itu, penelitian ini juga mengidentifikasi pola akses yang umumnya digunakan oleh pengguna sah dan menyesuaikan konfigurasi ACL untuk memastikan ketersediaan layanan yang optimal. Dengan menerapkan ACL pada VLAN terenskripsi, pengguna dapat memperkuat keamanan jaringan mereka, melindungi data sensitif, dan mengurangi risiko terhadap serangan berbagai jenis. Temuan dari penelitian ini diharapkan dapat memberikan panduan praktis bagi administrator jaringan dalam meningkatkan keamanan VLAN terenskripsi melalui penerapan Access Control List.

Kata Kunci: Access control list, Virtual local area network, Encapsulasi

Abstract

Access Control List (ACL) implementation is one of the effective strategies to improve the security of encapsulated Virtual Local Area Network (VLAN) networks. VLANs are becoming a crucial component in modern network infrastructure, but require careful protection to prevent unauthorized access. This research aims to evaluate and implement ACLs as a security mechanism on encapsulated VLAN networks. The research methodology involves analyzing security requirements, designing ACL configurations, implementing on network devices, and evaluating system performance. The experimental results show that the implementation of ACLs effectively mitigates the risk of unauthorized access and attacks on VLAN networks. In addition, this research also identifies access patterns commonly used by authorized users and adjusts ACL configurations to ensure optimal service availability. By applying ACLs on encapsulated VLANs, users can enhance their network security, protect sensitive data, and reduce the risk against attacks of various types. The findings of this research are expected to provide practical guidance for network administrators in improving the security of encapsulated VLANs through the implementation of Access Control Lists.

Keywords: Access control list, Virtual local area network, Encapsulation

PENDAHULUAN

Dalam era digital yang gejolak ini, jaringan komputer telah menjadi tulang punggung utama dalam menghubungkan perangkat dan menyediakan akses ke sumber daya berharga seperti data, aplikasi, dan layanan. Namun, dengan perkembangan teknologi yang semakin pesat, ancaman terhadap keamanan jaringan juga semakin meningkat. Organisasi dan entitas

JUDIS
Jurnal Multidisiplin Dan Sains
Vol. 2 No. 1 September 2025, pp.13-22
https://jurnal.compartdigital.com/index.php/judis

lainnya terus berjuang untuk menjaga integritas dan kerahasiaan data mereka serta menghindari serangan yang dapat merusak operasional jaringan.

Salah satu cara untuk meningkatkan keamanan jaringan adalah dengan mengimplementasikan teknologi Access Control List (ACL). ACL adalah seperangkat aturan yang digunakan untuk mengatur akses ke sumber daya jaringan berdasarkan kriteria tertentu, seperti alamat IP, port, atau protokol. Dengan menggunakan ACL, administrator jaringan dapat membatasi akses pengguna ke sumber daya jaringan yang hanya dibutuhkan dan menghindari akses yang tidak sah.

Di sisi lain, Virtual Local Area Network (VLAN) adalah teknologi yang umum digunakan untuk mengatur jaringan dalam suatu organisasi. Dengan menggunakan VLAN, perangkat dalam jaringan dapat dikelompokkan ke dalam segmen-segmen yang berbeda, sehingga meningkatkan efisiensi pengaturan jaringan. Namun, keamanan jaringan VLAN terencapsulasi adalah aspek yang harus mendapatkan perhatian serius. Sementara banyak organisasi telah mengimplementasikan VLAN untuk meningkatkan efisiensi jaringan mereka, ada kebutuhan mendesak untuk memahami bagaimana teknologi Access Control List (ACL) dapat diintegrasikan dengan efektif dalam jaringan VLAN terencapsulasi. Masalah keamanan yang sering muncul dalam VLAN terencapsulasi meliputi serangan antar-VLAN, akses yang tidak sah ke sumber daya, dan risiko kebocoran data sensitif.

Sebagai hasilnya, penelitian ini bertujuan untuk mengatasi kebutuhan akan pemahaman yang lebih dalam tentang penerapan Access Control List (ACL) dalam keamanan jaringan Virtual Local Area Network terencapsulasi. Dalam penelitian ini, penulis akan menganalisis konsep ACL, mendemonstrasikan konfigurasi ACL pada perangkat jaringan yang mendukung VLAN terencapsulasi, dan menguji efektivitasnya dalam meningkatkan keamanan jaringan. Dengan memahami bagaimana ACL dapat diterapkan dalam jaringan VLAN terencapsulasi, diharapkan organisasi dan profesional jaringan dapat memperkuat sistem keamanan mereka dan melindungi data mereka dari ancaman yang ada dan yang akan datang.

JUDIS
Jurnal Multidisiplin Dan Sains
Vol. 2 No. 1 September 2025, pp.13-22
https://jurnal.compartdigital.com/index.php/judis

KAJIAN TEORI

Jaringan komputer dapat diklasifikasi menjadi dua jenis: jaringan kabel dan jaringan nirkabel. Dalam kasus jaringan kabel, diperlukan media fisik untuk tujuan pengangkutan informasi antar node. Untuk keperluan komunikasi digital di rumah dan di bisnis, kabel Ethernet digunakan untuk daya tahan yang baik dan juga biayanya yang rendah. Serat optik sekarang juga digunakan untuk transportasi data ke jarak yang jauh serta juga memiliki kecepatan yang jauh lebih cepat. Namun, dalam hal biaya, kabel Ethernet jauh lebih murah daripada serat optik.

Jaringan adalah interkoneksi sekumpulan perangkat yang mampu berkomunikasi. Dalam definisi ini, perangkat dapat menjadi *host* (atau sering disebut sebagai end system) seperti komputer, desktop, laptop, workstation, telepon seluler, atau sistem keamanan. Selain perangkat yang telah disebutkan, ada perangkat lain yang berfungsi sebagai penghubung antara jaringan yang satu dengan jaringan yang lain yaitu Router. Selanjutnya adalah *switch*, yaitu perangkat penghubung yang menyambungkan semua perangkat *end system* secara bersamaan. Ada juga perangkat yang digunakan untuk mengubah bentuk data, perangkat ini lebih dikenal dengan nama Modem (modulator-demodulator). Pada sebuah jaringan komputer semua perangkat yang telah disebutkan tadi dapat saling terhubung menggunakan media transmisi (kabel atau nirkabel) (Hartanto Tantriawan, 2023).

Dalam jaringan nirkabel, gelombang radio digunakan untuk mengangkut data di udara di mana perangkat dalam jaringan terhubung satu sama lain tanpa ada kabel di antaranya. WLAN atau LAN nirkabel adalah versi yang paling banyak digunakan dan terkenal yang digunakan untuk jaringan nirkabel. Ada juga beberapa alternatif di pasaran saat ini seperti satelit, Bluetooth, microwave, seluler dan banyak lagi (Medicine, 2019). Setelah mendefinisikan jaringan di bagian sebelumnya dan mendiskusikan struktur fisiknya, kita perlu membahas berbagai jenis jaringan yang kita jumpai di dunia saat ini.

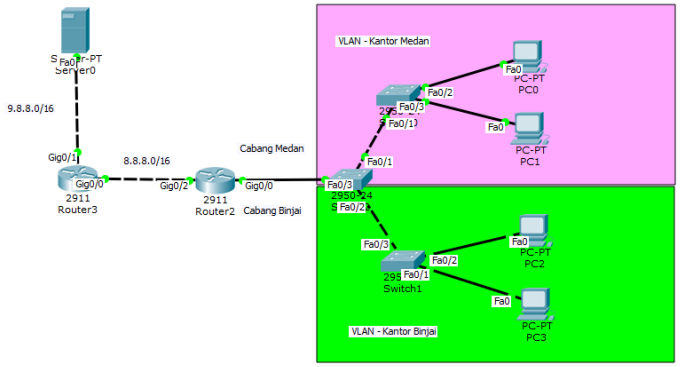
Kriteria membedakan satu jenis jaringan dari yang lain sulit dan terkadang membingungkan. Kami menggunakan beberapa kriteria seperti ukuran, cakupan geografis, dan kepemilikan untuk membuat perbedaan ini. Setelah membahas dua jenis jaringan, LAN dan WAN, kami mendefinisikan switching, yang digunakan untuk menghubungkan jaringan untuk

JUDIS
Jurnal Multidisiplin Dan Sains
Vol. 2 No. 1 September 2025, pp.13-22
https://jurnal.compartdigital.com/index.php/judis

membentuk internetwork (jaringan dari jaringan).

METODE PENELITIAN

Tahapan analisa selanjutnya adalah membangun skema jaringan yang digunakan sebagai pengujian jaringan enkapsulasi dan access list. Rancangan topologi jaringan yang akan digunakan pada penelitian ini dapat dilihat pada gambar dibawah ini.



Gambar 1. Rancangan topologi jaringan

Fungsi dan penggunaan perangkat pada rancangan jaringan diatas dapat dilihat pada tabel di bawah ini:

Tabel 1. Spesifikasi perangkat jaringan

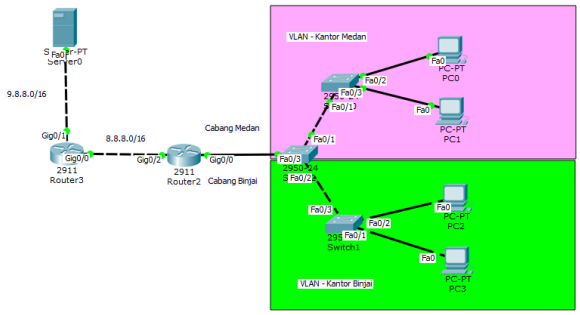
No	Device	Interface	Keterangan
1	Router0	Gigabitethernet0/0 Gigabitethernet0/1	- IP address: 8.8.8.0/8 SM: 255.0.0.0 - IP address: 9.8.8.0/8 SM: 255.0.0.0
2	Router1	Gigabitethernet0/0 Gigabitethernet0/1	- IP address: 200.100.10.0/24 SM: 255.255.255.0 - IP address: 201.100.10.0/24 SM: 255.255.255.252
3	Switch0	VLAN-1	VLAN number 100
4	Switch1	VLAN-1	VLAN number 110
5	Switch2	VLAN-1	VLAN number 120
6	Server-1	Fastethernet0	IP: 9.8.8.2/8 digunakan untuk *server*
7	PC0-PC3	-	IP: 200.100.10.2/24 SM: 255.255.255.0 IP: 201.100.10.2/24 SM: 255.255.255.0

JUDIS
Jurnal Multidisiplin Dan Sains
Vol. 2 No. 1 September 2025, pp.13-22
https://jurnal.compartdigital.com/index.php/judis

Tabel di atas menerangkan mengenai perangkat yang digunakan beserta penjelasan mengenai interface yang terdapat pada perangkat. Setelah memaparkan spesifikasi kebutuhan dari perangkat yang digunakan, selanjutnya dilakukan konfigurasi pada perangkat tersebut.

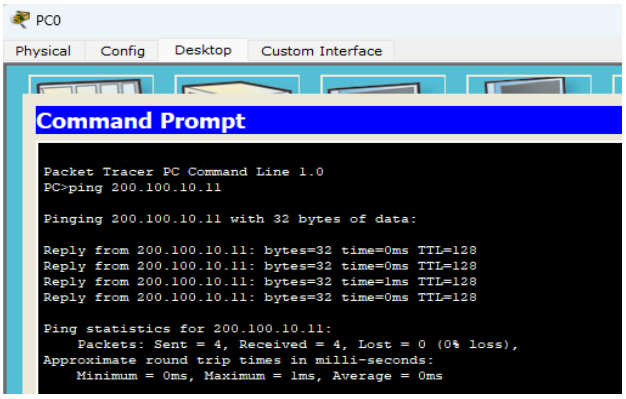
HASIL DAN PEMBAHASAN

Pengujian koneksi jaringan dilakukan untuk mengetahui sejauh mana keberhasilan konfigurasi yang telah dilakukan. Pengujian ini dilakukan dengan mengirimkan paket PING ke setiap device yang terkoneksi sebelum dilakukan accesslist. Berikut gambar skema jaringan yang akan diuji.



Gambar 2. Skema jaringan

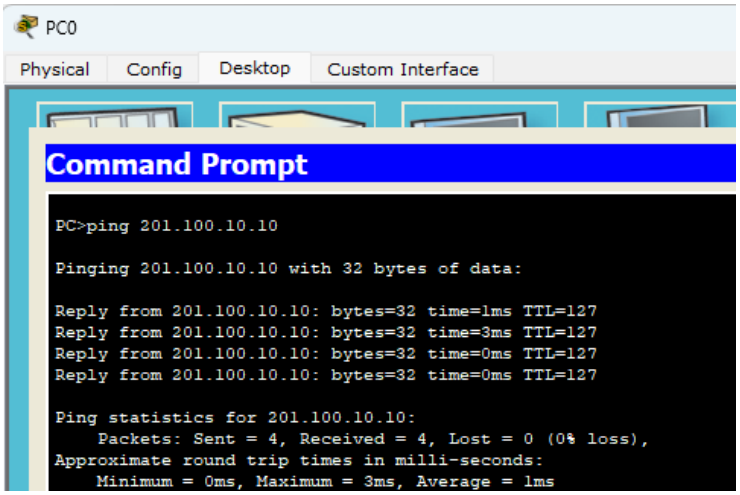
Pengujian pertama dilakukan pada perangkat PC0 ke perangkat PC1 yakni sebagai berikut.



Gambar 3. Pengujian PC0 ke PC1

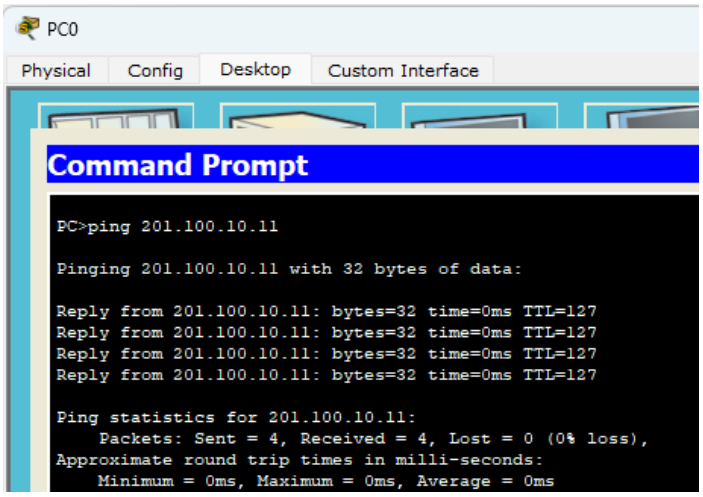
Selanjutnya dilakukan pengujian dari PC0 ke PC2 pada jaringan VLAN-Kantor Binjai. Jaringan ini merupakan jaringan yang berbeda segmen atau berbeda network. Ingat bahwa VLAN dapat diartika sebagai network.

JUDIS
Jurnal Multidisiplin Dan Sains
Vol. 2 No. 1 September 2025, pp.13-22
https://jurnal.compartdigital.com/index.php/judis



Gambar 4.Pengujian PC0 ke PC2

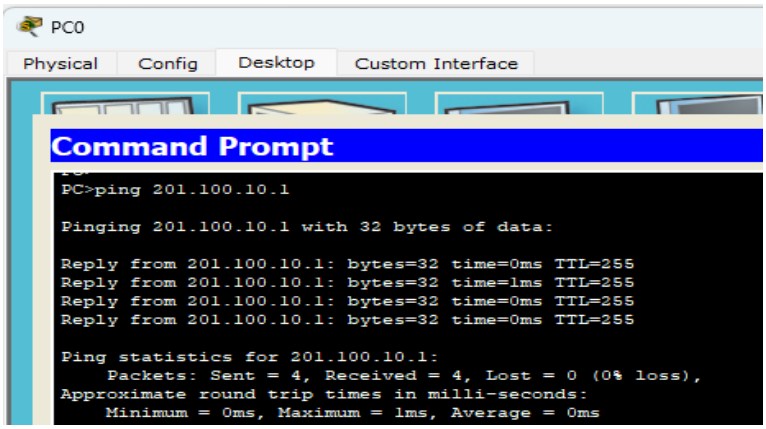
Dapat dilihat bahwa IP yang dituju oleh PC0 merupakan 201, sedangkat IP PC0 adalah 200. Hal ini tentu sudah berbeda network, namun tetap terhubung karena adanya gateway yakni router2. Kemudian dilakukan pengujian ke PC3 sebagai berikut.



Gambar 5. Pengujian PC0 ke PC3

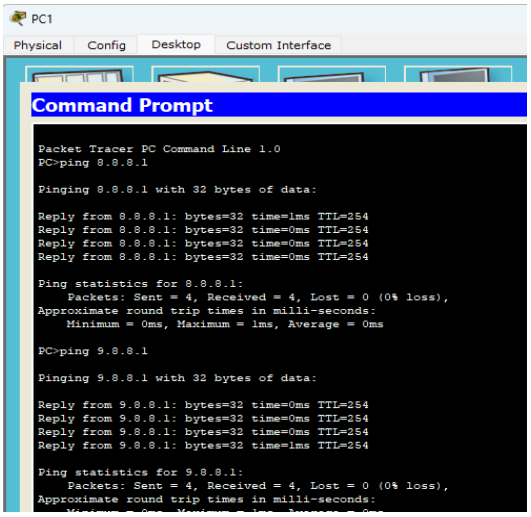
Pengujian ini dilakukan mewakili semua perangkat PC pada jaringan VLAN-Kantor Medan dan VLAN-Kantor Binjai. Oleh karena itu tidak perlu lagi dilakukan pengujian koneksi ke komputer sebaliknya. Akan tetapi pengujian terhadap router tetap harus dilakukan untuk mengujia apakat proses enkapsulasi berjalan dengan baik dan untuk memperlihatkan perbedaan setelah dilakukan proses akses list pada router. Pengujian PC0 ke router dapat dilihat pada gambar berikut.

JUDIS
Jurnal Multidisiplin Dan Sains
Vol. 2 No. 1 September 2025, pp.13-22
https://jurnal.compartdigital.com/index.php/judis



Gambar 6. Pengujian koneksi PC0 ke Router2

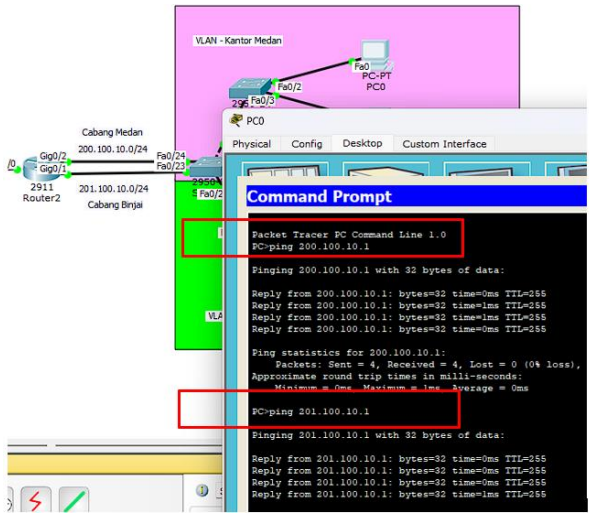
Selanjutnya dilakukan pengujian PC0 ke router3 dan server. Pengujian ini dilakukan sebelum dilakukan proses accesslist pada router. Pengujian ini dapat dilihat pada gambar dibawah ini.



Gambar 7. Pengujian PC1 ke router3 dan server

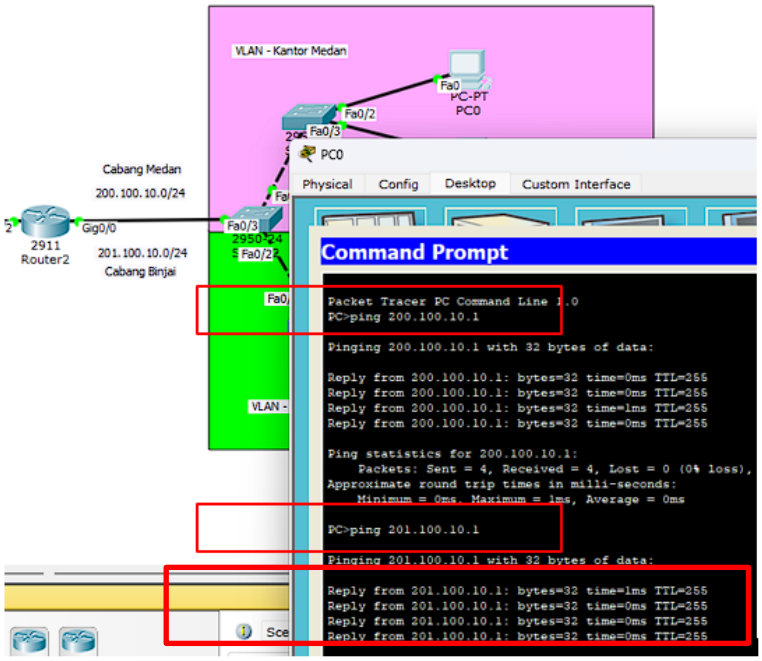
Pengujian enkapsulasi dilakukan untuk melihat sejauh mana pengaruh enkapsulasi terhadap koneksi pada jaringan. Pada dasarnya proses enkapsulasi ini adalah untuk efisiensi terhadap penggunaan interface pada router. Pengujian jaringan sebelum dilakukan proses enkapsulasi adalah sebagai berikut.

JUDIS
Jurnal Multidisiplin Dan Sains
Vol. 2 No. 1 September 2025, pp.13-22
https://jurnal.compartdigital.com/index.php/judis



Gambar 8. Pengujian sebelum proses encapsulation dot1q

Terlihat bahwa PC0 melakukan pengujian koneksi jaringan dengan mengirimkan paket PING ke router2 dengan IP 200.100.10.1/24 dan 201.100.10.1/24. Terlihat rata-rata transfer rate adalah 0 ms yang berarti bahwa rata-rata koneksi sangat baik. Setelah itu, dilakukan pengujian pada PC0 setelah dilakukan proses encapsulation dot1q. Pengujian ini dapat dilihat pada gambar berikut ini.



Gambar 9. Pengujian jaringan setelah dilakukan encapsulation dot1q

JUDIS
Jurnal Multidisiplin Dan Sains
Vol. 2 No. 1 September 2025, pp.13-22
https://jurnal.compartdigital.com/index.php/judis

Pada dasarnya hasil pengujian dan kecepatan transfer rate pada saat dilakukan proses enkapsulasi hampir sama dengan jaringan tanpa dilakukan proses enkapsulasi. Hal ini dapat dilihat pada gambar diatas bahwa rata-rata transfer rate pada pengujian adalah 0 ms sama dengan pengujian sebelumnya. Hal tersebut dapat dikatakan bahwa pengaruh enkapsulasi dan tanpa enkapsulasi terhadap transfer rate tidak begitu berpengaruh. Namun, hal tersebut perlu untuk diteliti terhadap jaringan yang lebih luas lagi, baik dari jaringan VLAN dan routing yang digunakan. Kemungkinan hal tersebut akan berpengaruh dikarenakan banyaknya jalur komunikasi yang terfokus hanya pada satu interface saja. Pada penelitian ini peneliti hanya berfokus pada implementasi dari enkapsulasi dan access list pada jaringan VLAN saja dan tidak membahas mengenai pengaruh enkapsulasi lebih jauh lagi.

SIMPULAN

Setelah melakukan pengujian dan implementasi terhadap jaringan maka penulis memaparkan beberapa kesimpulan pada penelitian ini. Kesimpulan tersebut adalah sebagai berikut.

1. Skripsi ini membahas implementasi Access Control List (ACL) sebagai strategi untuk meningkatkan keamanan jaringan Virtual Local Area Network (VLAN) yang terencapsulasi. Penelitian ini menyoroti pentingnya perlindungan terhadap jaringan VLAN dalam lingkungan terencapsulasi guna mencegah akses yang tidak sah dan potensi ancaman keamanan. Melalui penerapan ACL, kontrol akses yang tepat dapat diberlakukan, meningkatkan keamanan, dan memberikan perlindungan terhadap sumber daya jaringan.
2. Dalam penelitian ini, analisis keamanan jaringan VLAN terencapsulasi dilakukan untuk mengidentifikasi potensi kerentanan. Penerapan ACL kemudian diuji dan dievaluasi untuk melihat sejauh mana pengaruhnya terhadap keamanan jaringan. Hasil penelitian menunjukkan bahwa penerapan ACL mampu memberikan lapisan perlindungan tambahan yang signifikan terhadap ancaman keamanan

DAFTAR PUSTAKA

S. Agustini and A. Mudzakir, "Rancang Bangun Jaringan Komputer Dengan Bandwidth Management Menggunakan Teknik Brust Limit Dan Firewall Sebagai Pengaman

Jaringan," New Eng. Res. Oper., vol. 4, no. 3, pp. 189-195, 2019. [Online]. Available: https://nero.trunojoyo.ac.id/index.php/ner/article/view/138

A. Anwaridho and A. Supanto, "Simulasi Jaringan Wireless Dan Management Bandwidth Dengan Metode Firewall Mangle Dan Queue Tree Untuk Priority Traffic," J. Rekayasa Iktus, vol. 11, no. 1, pp. 73-78, 2022. [Online]. Available: https://ejournal.istn.ac.id/index.php/rekayasaiknsinformasi/article/view/1238

Alfred and J. Chandra, "Pemanfaatan Firewall pada Jaringan Komputer SMK Fadhilah," J. I D E A L S, vol. 1, no. 5, pp. 422-428, 2018. [Online]. Available: http://jom.fib.uad.ac.id/index.php/IDEALS/article/download/1037/263

Cisco, "Configuring Routing Between VLANs with IEEE 802.1Q," 2016. [Online]. Available: https://www.cisco.com/c/en/us/docs/ios/ios-lan/lan-switch/configuration/v2-5/lan-switch-cck-vlan-iec.html

T. Diansyah, I. Faisal, and D. Siregar, "Manajemen Pencegahan Serangan Jaringan Dan Serangan Dari Serangan Man In The Middle Attack," J. Rekayasa Komput. dan Inform., vol. 4, no. 1, pp. 224-233, 2022. [Online]. Available: https://ejournal.stmikbaramulia.ac.id/index.php/jrk/article/view/134

Fristanto and D. P. Utomo, "IMPLEMENTASI BANDWIDTH MANAGEMENT DAN FIREWALL SYSTEM MENGGUNAKAN MIKROTIK OS 2.9.7," Jarkom, vol. 2, no. 7, pp. 23-30, 2022. [Online]. Available: https://www.mikrotik.org/doc/download/1390

E. A. P. Hadimirawan, "Analisis Manajemen Bandwidth Menggunakan Metode Htb (Hierarchical Token Bucket) Pada Dinas Pariwisata Provinsi Lampung," J. Teknol. Pint., vol. 3, no. 5, 2023. [Online]. Available: http://teknologipintar.org/index.php/teknologipintar/article/download/405391

Mohammad Ferry Kurniawan and Sony Panca Budiarto, "Peningkatan Performa Jaringan Internet Rt Rw Net Di Dusun Warengan Desa Bubuk Menggunakan Metode Hierarchical Token Bucket," Jikom J. Inform. dan Komput., vol. 9, no. 1, pp. 72-90, 2022. [Online]. Available: https://doi.org/10.55794/jikom.v9i1.39