*Journal of Information Technology and Computer Science (INTECOMS)*
Volume 9 Nomor 1, Tahun 2026
e-ISSN : 2614-1574
p-ISSN : 2621-3249

# IMPLEMENTASI ZERO TRUST NETWORK ACCESS (ZTNA) DALAM MENGAMANKAN JARINGAN SEKOLAH DENGAN SEGMENTASI VLAN DAN ROLE-BASED ACCESS CONTROL

## *IMPLEMENTATION OF ZERO TRUST NETWORK ACCESS (ZTNA) IN SECURING SCHOOL NETWORKS WITH VLAN SEGMENTATION AND ROLE-BASED ACCESS CONTROL*

**Yuma Akbar[1], Tegar Rizky Ardana[2]**
Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika[1,2]
tegarardana14@gmail.com[1]

***ABSTRACT***

*This research discusses the implementation of Zero Trust Network Access (ZTNA) to enhance network security in school environments through Virtual Local Area Network (VLAN) segmentation and Role-Based Access Control (RBAC). The main issue addressed is the lack of structured access control in school networks, which leads to vulnerabilities such as unauthorized access and lateral movement within the system. As a solution, this study designs a network system using MikroTik devices to segment traffic based on VLANs, assign access rights according to user roles (students, teachers, and administrators), and implement a captive portal as the primary authentication mechanism. The research applies an experimental method using EVE-NG as the simulation platform, with MikroTik Cloud Hosted Router (CHR) serving as the core device. Testing scenarios include VLAN isolation, role-based service access (e.g., CBT and database), and simulations of internal threats such as port scanning and spoofing. The expected outcome is a security system aligned with Zero Trust principles, in which all access is tightly controlled based on identity and user roles. This study offers a practical and cost-effective recommendation for implementing segmented and secure network infrastructure in educational institutions using MikroTik technology.*

***Keywords**: ZTNA, MikroTik, VLAN, RBAC, Captive Portal, School Network.*

**ABSTRAK**

Penelitian ini membahas penerapan *Zero Trust Network Access* (ZTNA) untuk meningkatkan keamanan jaringan sekolah melalui segmentasi *Virtual Local Area Network* (VLAN) dan pengendalian akses berbasis peran atau *Role-Based Access Control* (RBAC). Permasalahan yang diangkat adalah lemahnya sistem keamanan jaringan sekolah yang belum memiliki pembatasan akses pengguna secara terstruktur, sehingga rentan terhadap akses tidak sah dan gangguan internal. Sebagai solusi, penelitian ini merancang sistem jaringan yang memanfaatkan perangkat MikroTik untuk membagi trafik jaringan berdasarkan VLAN, mengatur hak akses sesuai peran pengguna (siswa, guru, dan admin), serta menerapkan *captive portal* sebagai autentikasi awal. Penelitian dilakukan menggunakan pendekatan eksperimen melalui simulasi jaringan di platform EVE-NG dengan MikroTik *Cloud Hosted Router* (CHR) sebagai perangkat utama. Pengujian dilakukan terhadap skenario isolasi antar-VLAN, pengaturan hak akses terhadap layanan seperti CBT dan *database*, serta simulasi ancaman internal seperti *port scanning* dan *spoofing*. Hasil yang diharapkan adalah terciptanya sistem keamanan jaringan yang sesuai prinsip *Zero Trust*, di mana setiap akses dikendalikan berdasarkan identitas dan peran pengguna. Penelitian ini memberikan rekomendasi penerapan sistem keamanan tersegmentasi yang terjangkau dan fleksibel bagi institusi pendidikan berbasis MikroTik.

**Kata Kunci:** ZTNA, Mikrotik, VLAN, RBAC, *Captive Portal*, Jaringan Sekolah

## PENDAHULUAN

Perkembangan teknologi informasi mendorong institusi pendidikan untuk mengintegrasikan infrastruktur jaringan dalam proses belajar mengajar. Namun, banyak sekolah masih menggunakan arsitektur jaringan tradisional tanpa segmentasi maupun kontrol akses memadai, sehingga seluruh perangkat dapat saling berkomunikasi tanpa batasan. Kondisi ini menimbulkan risiko seperti akses tidak sah, penyalahgunaan sumber daya, dan serangan internal.

Salah satu kelemahan utama adalah ketiadaan mekanisme autentikasi dan otorisasi berbasis peran. Pengguna seperti

siswa, guru, dan admin sering memiliki hak akses yang sama, padahal kebutuhan mereka berbeda. Penerapan Role-Based Access Control (RBAC) dapat membatasi akses hanya pada layanan relevan, sedangkan pendekatan modern seperti Zero Trust Network Access (ZTNA) menerapkan prinsip never trust, always verify untuk memverifikasi setiap permintaan berdasarkan identitas, perangkat, dan konteks.

Integrasi ZTNA dengan segmentasi jaringan berbasis Virtual LAN (VLAN) dan RBAC terbukti meningkatkan keamanan, namun kajian di lingkungan pendidikan masih terbatas, khususnya dengan perangkat MikroTik yang populer karena efisien dan terjangkau. Penelitian ini mengkaji perancangan dan implementasi ZTNA berbasis MikroTik dengan segmentasi VLAN dan RBAC untuk menciptakan sistem jaringan sekolah yang lebih aman, terkontrol, dan sesuai kebutuhan tiap peran pengguna.

## METODOLOGI

### 2.1 Pendekatan Penelitian

Penelitian ini menggunakan eksperimen terapan berbasis simulasi virtual dengan platform EVE-NG dan MikroTik Cloud Hosted Router (CHR). Fokus implementasi meliputi Zero Trust Network Access (ZTNA), segmentasi VLAN, dan Role-Based Access Control (RBAC) pada jaringan sekolah.

### 2.2 Tahapan Penelitian

1. Perancangan Topologi
   Merancang topologi jaringan sekolah secara virtual, mencakup kelompok pengguna (siswa, guru, admin), server CBT, dan database. Setiap kelompok ditempatkan pada VLAN terpisah, dihubungkan melalui MikroTik CHR.
2. Segmentasi VLAN
   Konfigurasi VLAN 10 (siswa), VLAN 20 (guru), dan VLAN 30 (admin), dengan IP dan DHCP server terpisah, untuk memisahkan trafik jaringan secara logis.
3. Pengaturan IP, NAT, dan Firewall
   Pemberian IP pada setiap VLAN, penerapan NAT untuk akses internet, dan konfigurasi firewall untuk membatasi komunikasi antar VLAN sesuai kebijakan keamanan.
4. Implementasi RBAC
   Pengaturan hak akses berbasis peran melalui captive portal (Hotspot MikroTik) dan kombinasi rule firewall. Akses layanan dibatasi sesuai role pengguna.
5. Penerapan ZTNA
   Prinsip *"Never Trust, Always Verify"* diterapkan melalui autentikasi berlapis (Hotspot + RBAC), memastikan verifikasi semua pengguna sebelum diberikan akses.
6. Simulasi dan Pengamatan
   Melakukan percobaan akses tiap role ke layanan (CBT, database, router), serta pencatatan log aktivitas untuk evaluasi.

### 2.3 Rancangan Pengujian

Pengujian meliputi:
a. Isolasi VLAN – memastikan komunikasi antar VLAN terblokir sesuai kebijakan.
b. Hak Akses (RBAC) – memverifikasi pembatasan layanan sesuai role.
c. Autentikasi (ZTNA) – menguji akses tanpa login untuk memastikan penolakan.
d. Keamanan Tambahan – simulasi serangan (port scanning, spoofing, bypass firewall).
e. Analisis Log – mengevaluasi kemampuan audit dan pelacakan akses.

## HASIL

### 3.1 Alat Penelitian

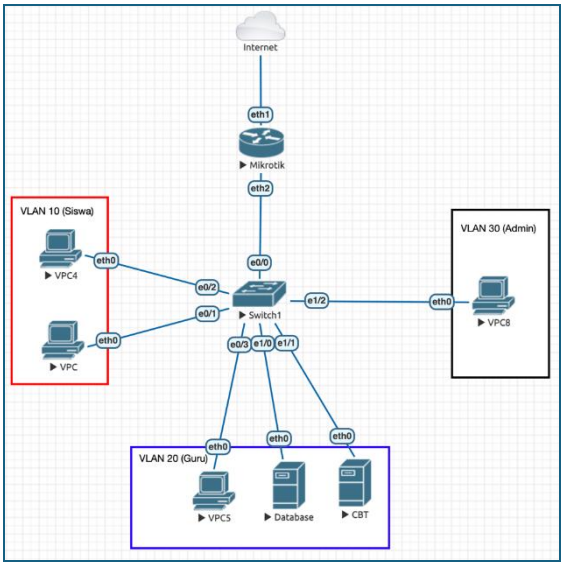
Penelitian ini dilaksanakan menggunakan laptop dengan spesifikasi prosesor Intel Core i5-6200U, RAM 16 GB, penyimpanan SSD 256 GB, dan sistem operasi Windows 11. Lingkungan simulasi dibangun dengan VMWare Workstation 17 Pro untuk menjalankan EVE-NG Community Edition, yang digunakan sebagai platform virtualisasi topologi jaringan. Perangkat utama yang

diimplementasikan adalah MikroTik RouterOS CHR, dipilih karena efisiensinya dalam penerapan VLAN, RBAC, dan captive portal dengan biaya yang relatif rendah.

### 3.2 Implementasi Sistem

Topologi jaringan yang dirancang merepresentasikan skenario jaringan sekolah dengan tiga kategori pengguna utama, yaitu:

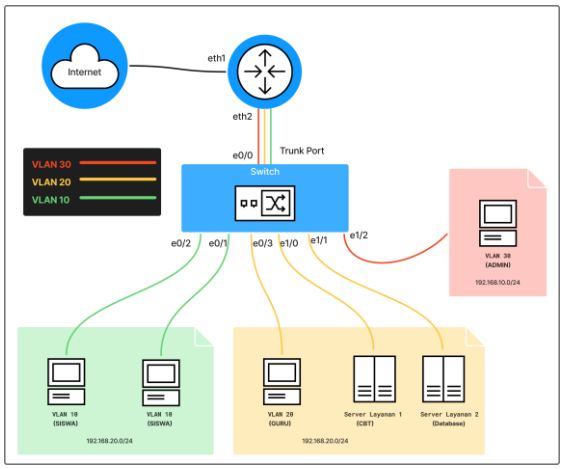
**VLAN 10 – Siswa**




**VLAN 20 – Guru**

```
/interface vlan
add interface=ether2 name=vlan10 vlan-id=10
add interface=ether2 name=vlan20 vlan-id=20
add interface=ether2 name=vlan30 vlan-id=30
```

**VLAN 30 – Admin**




Setiap VLAN memiliki subnet IP dan kebijakan akses yang berbeda. Konfigurasi DHCP Server pada MikroTik memastikan perangkat yang terhubung mendapatkan alamat IP sesuai VLAN-nya. NAT digunakan untuk menghubungkan seluruh VLAN ke internet.

Penerapan Role-Based Access Control (RBAC) dilakukan melalui fitur Hotspot MikroTik sebagai mekanisme autentikasi awal. Setiap pengguna wajib login melalui captive portal, dan berdasarkan kredensial yang dimasukkan, pengguna akan dimasukkan ke address list tertentu. Aturan firewall kemudian membatasi akses sesuai daftar ini. Misalnya:

Siswa hanya dapat mengakses internet umum dan platform pembelajaran daring.

Guru memiliki tambahan akses ke server ujian berbasis komputer (CBT) dan database sekolah.

Admin memiliki akses penuh termasuk ke seluruh VLAN.

Integrasi Zero Trust Network Access (ZTNA) dilakukan dengan menerapkan prinsip never trust, always verify. Meskipun perangkat sudah berada di VLAN yang sesuai, akses ke sumber daya tetap memerlukan verifikasi identitas pengguna dan perangkat.

3.3 Hasil Pengujian

Pengujian dilakukan dengan beberapa skenario berikut:

Segmentasi VLAN Berhasil

Perangkat pada VLAN berbeda tidak dapat saling ping atau mengakses layanan, kecuali jika firewall memberikan izin.

Trafik antar VLAN sepenuhnya terisolasi, mengurangi risiko serangan lateral.

Autentikasi dan Pembatasan Akses

Semua pengguna diarahkan ke captive portal saat pertama kali terhubung.

Hak akses diberikan sesuai peran: siswa → akses terbatas, guru → akses menengah, admin → akses penuh.

Efektivitas Firewall Filter

Aturan firewall memblokir upaya komunikasi yang tidak diotorisasi, termasuk uji coba port scanning dan spoofing.

Akses internet tetap berjalan tanpa hambatan untuk semua VLAN sesuai kebijakan.

Penerapan Prinsip ZTNA
Tidak ada akses yang diberikan hanya karena posisi dalam topologi jaringan; semua harus melalui autentikasi identitas.

Kebijakan dapat dengan mudah diubah atau diperluas sesuai kebutuhan keamanan.

Kelayakan Implementasi di Sekolah
Sistem ini dapat direplikasi di sekolah lain dengan biaya rendah, karena menggunakan perangkat MikroTik yang banyak tersedia.

Implementasi berbasis simulasi di EVE-NG memungkinkan uji coba tanpa mengganggu jaringan produksi.
Hasil ini membuktikan bahwa kombinasi VLAN + RBAC + ZTNA dapat secara signifikan meningkatkan keamanan jaringan sekolah, sekaligus tetap mempertahankan kemudahan akses sesuai kebutuhan masing-masing peran pengguna.

## KESIMPULAN DAN SARAN

Hasil perancangan, implementasi, dan pengujian sistem keamanan jaringan sekolah berbasis Zero Trust Network Access (ZTNA) dengan segmentasi VLAN dan Role-Based Access Control (RBAC) menggunakan MikroTik menunjukkan bahwa:

1. Segmentasi VLAN berhasil memisahkan jaringan menjadi tiga kelompok (siswa, guru, admin) yang terisolasi sehingga meminimalkan risiko akses tidak sah.
2. RBAC melalui captive portal membatasi akses sesuai peran: siswa hanya ke layanan tertentu, guru mendapat akses tambahan, dan admin memiliki akses penuh.
3. Prinsip ZTNA "Never Trust, Always Verify" berjalan efektif karena setiap pengguna wajib autentikasi sebelum mengakses jaringan.
4. Firewall memblokir trafik antar VLAN sesuai kebijakan, namun tetap mengizinkan akses internet setelah autentikasi.
5. Sistem log MikroTik memudahkan audit dan analisis keamanan dengan mencatat aktivitas serta upaya akses yang diblokir.

Secara keseluruhan, sistem ini meningkatkan keamanan jaringan sekolah dengan tetap menjaga efisiensi dan kemudahan pengelolaan.

### Saran

Untuk pengembangan lebih lanjut:

1. Integrasi dengan autentikasi eksternal (RADIUS/LDAP) untuk manajemen pengguna terpusat.
2. Penambahan enkripsi lalu lintas internal (IPsec/SSL VPN) sebagai lapisan keamanan tambahan.
3. Monitoring real-time dengan Zabbix atau The Dude untuk deteksi dini aktivitas mencurigakan.
4. Pengujian performa jaringan (latency, throughput, packet loss) untuk memastikan keamanan tidak mengorbankan kinerja.
5. Pelatihan rutin bagi administrator agar mampu memelihara, memperbarui kebijakan, dan melakukan troubleshooting mandiri.

## DAFTAR PUSTAKA

[1] Y. Kusnanto, M. A. Nugroho, and R. Kartadie, "IMPLEMENTASI ZERO

TRUST ARCHITECTURE UNTUK MENINGKATKAN KEAMANAN JARINGAN: PENDEKATAN BERBASIS SIMULASI," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 4, pp. 2357–2364, 2024, doi: 10.29100/jipi.v4i1.6943.

[2] J. Sujana, "Implementasi Virtual Local Area Network Dengan Basis Inter-Vlan Routing Menggunakan Mikrotik," *NetPLG Journal of Network and Computer Applications*, vol. 1, no. 1, 2022, [Online]. Available: https://jurnal.netplg.com/

[3] Y. Yuricha and I. K. Phan, "Penerapan Role Based Access Control dalam Sistem Supply Chain Management Berbasis Cloud," *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 3, no. 2, pp. 339–348, Nov. 2023, doi: 10.57152/malcom.v3i2.1259.

[4] A. Purwo Wicaksono, "Simulasi Virtual Local Area Network Menggunakan Packet Tracer (Simulation Virtual Local Area Network Using Packet Tracer)," *SAINTEKS*, vol. 15, no. 2, 2018.

[5] Seprianus Kenat, "Analisis Keamanan Jaringan Menggunakan Mikrotik Pada Lab Komputer STMIK Widuri," *Neptunus: Jurnal Ilmu Komputer Dan Teknologi Informasi*, vol. 2, no. 3, pp. 16–24, Jun. 2024, doi: 10.61132/neptunus.v2i3.177.

[6] D. Li, Z. Yang, S. Yu, M. Duan, and S. Yang, "A Micro-Segmentation Method Based on VLAN-VxLAN Mapping Technology," *Future Internet*, vol. 16, no. 9, p. 320, Sep. 2024, doi: 10.3390/fi16090320.

[7] Fatkhurrahman and Arita Witanti, "Optimasi Segmentasi Jaringan melalui Implementasi VLAN Dinamis pada Infrastruktur Kabel dan Nirkabel dengan MikroTik," *JEKIN - Jurnal Teknik Informatika*, vol. 4, no. 3, pp. 675–687, Aug. 2024, doi: 10.58794/jekin.v4i3.904.

[8] A. Darshane, "Advanced Network Security Concepts: Network Segmentation and Zero Trust Architecture," *International Journal of Engineering and Technology Research (IJETR)*, vol. 9, no. 2, pp. 379–386, 2024, doi: 10.5281/zenodo.13851178.

[9] S. Hartono and K. Yunan dan Bheta Agus Wardijono, "IMPLEMENTASI VLAN CISCO UNTUK PENGATURAN HAK AKSES PADA JARINGAN KOMPUTER SEKOLAH," *Seminar Nasional Teknologi Informasi dan Komunikasi STI&K (SeNTIK)*, vol. 7, no. 1, 2023.

[10] A. Marsehan, A. Amarto Wicaksono, S. I. Inkariski, and H. Artikel, "Perancangan Jaringan VLAN (Virtual Local Area Network) di SMK Pertanian Negeri 2 Tugumulyo," vol. 5, no. 1, 2025, doi: 10.47709/digitech.v5i1.5891.

[11] P. Adytia, "IMPLEMENTASI KEAMANAN JARINGAN LAN BERBASIS VLAN STUDI KASUS STMIK WIDYA CIPTA DHARMA," 2019.

[12] J. Singh, S. Rani, and V. Kumar, "Role-Based Access Control (RBAC) Enabled Secure and Efficient Data Processing Framework for IoT Networks," 2024. [Online]. Available: https://https://ijcnis.org/

[13] Y. Ajiji Makeri, G. T. Cirella, F. Javier Galas, H. Mohsin Jadah, and A. Olaniyi Adeniran, "Network Performance through Virtual Local Area Network (VLAN) Implementation & Enforcement on Network Security for Enterprise," *Int. J. Advanced Networking and Applications*, pp. 4750–4762, 2021.

[14] K. I. Ramadhan, "PERANCANGAN JARINGAN VLAN SEKOLAH

MENENGAH ATAS FATAHILLAH," 2024.

[15] S. Annigeri, "Use of Virtual LANs for Network Segmentation and Organization," *International Journal of Research in Engineering, Science and Management*, 2019.

[16] T. Rahman, "IMPLEMENTASI INTERFACE VIRTUAL LOCAL AREA NETWORK DAN FIREWALL PADA MIKROTIK DAN SWITCH MANAJEMEN," 2018, [Online]. Available: http://www.bsi.ac.id

[17] G. Budi Sulistyo, P. Widodo, and N. Hasan, "User Management and Authentication of Hotspot Using Mikrotik Hotspot Monitor at A Coffee Shop," *Indonesian Journal of Social Technology*, vol. 5, no. 12, p. 5815, 2024, [Online]. Available: http://jist.publikasiindonesia.id/

[18] M. Zulqifli and M. Asnawi Bahar, "PERANCANGAN SISTEM JARINGAN VLAN PADA SMP NEGERI 2 PASAR WAJO," 2023.

[19] G. T. Irawan, M. Djaohar, and M. Ficky Duskarnaen, "Perancangan Dan Implementasi Sistem Keamanan Jaringan Menggunakan Firewall dan Web Proxy Berbasis Mikrotik di SMA Negeri 1 Kota Sukabumi," *PINTER : Jurnal Pendidikan Teknik Informatika dan Komputer*, vol. 2, no. 1, pp. 27–32, Jun. 2018, doi: 10.21009/pinter.2.1.4.

[20] I. S. Yunika and I. N. Ichsan, "Quality of Service on Virtual Local Area Network (VLAN) in Campus Network," Jan. 2025. doi: https://doi.org/10.32520/stmsi.v14i1.4725.

[21] Y. D. Noviani, "Analisis Pengembangan Virtual Local Area Network (VLAN) di SMK Asy-Syarifiy Pandanwangi-Lumajang," vol. 02, pp. 61–66, 2020.

[22] N. Basta, M. Ikram, M. A. Kaafar, and A. Walker, "Towards a Zero-Trust Micro-segmentation Network Security Strategy: An Evaluation Framework," Nov. 2021, doi: 10.1109/NOMS54207.2022.9789888.

[23] S. Bakhri, A. Haidir, A. Syah, and M. Assari, "OPTIMASI NETWORK BERBASIS MULTI VLAN DAN NETWORK MONITOR PAESSLER ROUTER TRAFFIC GRAPHER DI MAKO KORBRIMOB POLRI," *884 Journal of Information System, Applied, Management, Accounting and Research. ( Printed)*, vol. 8, no. 4, pp. 884–894, 2024, doi: 10.52362/jisamar.v8i4.1642.

[24] T. Slattery, "How to implement network segmentation for better security | TechTarget," TechTarget. Accessed: Jun. 23, 2025. [Online]. Available: https://www.techtarget.com/searchnetworking/tip/How-to-implement-network-segmentation-for-better-security

[25] M. Dzaky Nurfaishal and Y. Akbar, "Analisis Efektivitas Keamanan Jaringan Layer 2: Port Security, VLAN Hopping, DHCP Snooping," Aug. 2024. doi: https://doi.org/10.35870/jimik.v5i3.975.

[26] A. Shomad, Y. Akbar, and D. I. Mulyana, "Implementasi Pembatasan Akses Sosial Media Menggunakan Layer 7 Protocol Pada Perangkat Mikrotik DI SMK IDN," *Journal of Informatics*, vol. 7, no. 1, pp. 27–38, Nov. 2022, doi: https://doi.org/10.51211/itbi.v7i1.1998.

[27] M. E. Saputra and Y. Akbar, "Analisis Penggunaan Metode XConnect Main and Backup Link Berbasis VPN MPLS Layer 2 pada Jaringan Metro-Ethernet," Sep. 2024. doi: https://doi.org/10.35870/jimik.v5i3.1009.

[28] E. Gilman and D. Barth, *Zero Trust Networks: Building Secure Systems in Untrusted Networks*, 1st ed. O'Reilly Media, Inc., 2017.
[29] R. Widjojo, *MikroTik Kung Fu : Kitab 1* , 3rd ed. Jasakom, 2019.
[30] T. Hart, *MikroTik Security Guide*. Independently published, 2017.
[31] J. Garbis and J. W. Chapman, *Zero Trust Security*, 1st ed. Berkeley, CA: Apress, 2021. doi: 10.1007/978-1-4842-6702-8.
[32] V. Zen, *Theory, Labs and Exercises for MikroTik RouterOS – Routing*, 1st ed. Independently published, 2019.