

DAFTAR PUSTAKA

- [1] Müge Erel-Özçevik, “Token as a Service for Software-Defined Zero Trust Networking,” *Journal of Network and Systems Management*, vol. 33, no. 1, Dec. 2024, doi: <https://doi.org/10.1007/s10922-024-09894-w>.
- [2] S. Ahmadi, “Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities,” *Journal of Engineering Research and Reports*, vol. 26, no. 2, pp. 215–228, Feb. 2024, doi: <https://doi.org/10.9734/jerr/2024/v26i21083>.
- [3] J. A. Donenfeld, “WireGuard: Next Generation Kernel Network Tunnel,” *Proceedings 2017 Network and Distributed System Security Symposium*, 2017, doi: <https://doi.org/10.14722/ndss.2017.23160>.
- [4] C. Cremers, “Key Exchange in IPsec Revisited: Formal Analysis of IKEv1 and IKEv2,” *Lecture notes in computer science*, pp. 315–334, Jan. 2011, doi: https://doi.org/10.1007/978-3-642-23822-2_18.
- [5] J. Heino, C. Jalio, Antti Hakkala, and Seppo Virtanen, “JAPPI: An unsupervised endpoint application identification methodology for improved Zero Trust models, risk score calculations and threat detection,” *Computer Networks*, pp. 110606–110606, Jun. 2024, doi: <https://doi.org/10.1016/j.comnet.2024.110606>.
- [6] W. Yeoh, M. Liu, M. Shore, and F. Jiang, “Zero trust cybersecurity: Critical success factors and A maturity assessment framework,” *Computers & Security*, vol. 133, p. 103412, Oct. 2023, doi: <https://doi.org/10.1016/j.cose.2023.103412>.
- [7] J. Kindervag, “Making Leaders Successful Every Day Build Security Into Your Network’s DNA: The Zero Trust Network Architecture by John Kindervag for Security & Risk Professionals,” Nov. 2010. Available: https://www.actiac.org/system/files/Forrester_zero_trust_DNA.pdf

- [8] “Department of Defense (DoD) Zero Trust Reference Architecture Version 2.0 Prepared by the Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team CLEARED For Open Publication Department of Defense OFFICE OF PREPUBLICATION AND SECURITY REVIEW,” 2022. Available: [https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT_RA_v2.0\(U\)_Sep22.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf)
- [9] “Department of Defense Zero Trust Overlays Office of the Chief Information Officer CLEARED For Open Publication Department of Defense OFFICE OF PREPUBLICATION AND SECURITY REVIEW,” 2024. Available: <https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays.pdf>
- [10] S. P. Marsh, “Formalising trust as a computational concept,” *dspace.stir.ac.uk*, 1994. Available: <http://hdl.handle.net/1893/2010>
- [11] F. A. Qazi, "Study of Zero Trust Architecture for Applications and Network Security," 2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), Marietta, GA, USA, 2022, pp. 111-116, doi: 10.1109/HONET56683.2022.10019186.
- [12] Mr. Siddhesh Bhargude, “Privileged Access Management: Ensuring Security and Accountability,” *International Journal of Advanced Research in Science, Communication and Technology*, pp. 647–651, Jul. 2023, doi: <https://doi.org/10.48175/ijarset-12098>.

- [13] M. S. Ferdous and R. Poet, "A comparative analysis of Identity Management Systems," *2012 International Conference on High Performance Computing & Simulation (HPCS)*, Madrid, Spain, 2012, pp. 454-461, doi: 10.1109/HPCSim.2012.6266958.
- [14] M. Petit-Huguenin, G. Salgueiro, J. Rosenberg, D. Wing, R. Mahy, and P. Matthews, "Session Traversal Utilities for NAT (STUN)," Feb. 2020, doi: <https://doi.org/10.17487/rfc8489>.
- [15] P. Martinsen, T. Reddy, D. Wing, and V. Singh, "Measurement of Round-Trip Time and Fractional Loss Using Session Traversal Utilities for NAT (STUN)," Sep. 2016, doi: <https://doi.org/10.17487/rfc7982>.
- [16] M. Petit-Huguenin and G. Salgueiro, "Datagram Transport Layer Security (DTLS) as Transport for Session Traversal Utilities for NAT (STUN)," Aug. 2014, doi: <https://doi.org/10.17487/rfc7350>.
- [17] M. Petit-Huguenin, "Traversal Using Relays around NAT (TURN) Resolution Mechanism," Aug. 2010, doi: <https://doi.org/10.17487/rfc5928>.
- [18] M. Petit-Huguenin, S. Nandakumar, G. Salgueiro, and P. Jones, "Traversal Using Relays around NAT (TURN) Uniform Resource Identifiers," Nov. 2013, doi: <https://doi.org/10.17487/rfc7065>.
- [19] P. Matthews and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," *CiteSeer X (The Pennsylvania State University)*, Feb. 2020, doi: <https://doi.org/10.17487/rfc8656>.
- [20] J. Rosenberg, "Traversal Using Relays around NAT (TURN) Extensions for TCP Allocations," Nov. 2010, doi: <https://doi.org/10.17487/rfc6062>.

- [21] P. Patil, T. Reddy, and D. Wing, “Traversal Using Relays around NAT (TURN) Server Auto Discovery,” Apr. 2017, doi: <https://doi.org/10.17487/rfc8155>.
- [22] M. Thomson, E. Mozilla, and S. Turner, “RFC 9001 Using TLS to Secure QUIC,” 2021, doi: <https://doi.org/10.17487/RFC9001>
- [23] W. Cui and M. Gou, “Design and Implementation of a SSH Proxy System Based on B/S Architecture,” *Journal of physics. Conference series*, vol. 2010, no. 1, pp. 012020–012020, Sep. 2021, doi: <https://doi.org/10.1088/1742-6596/2010/1/012020>.
- [24] V. Bhat, “Development of a Concept of a Modern Desktop-as-a-Service,” Oct. 14, 2021, doi: <https://doi.org/10.13140/RG.2.2.26025.93289>
- [25] Y. Kosuda and R. Sasaki, “Proposal and Implementation of SSH Client System Using Ajax,” *IFIP advances in information and communication technology*, pp. 184–196, Jan. 2009, doi: https://doi.org/10.1007/978-3-642-04280-5_16.
- [26] M. P. Kusuma and N. R. Rosyid, “Pengembangan Purwarupa Laboratorium Virtual Berbasis VMWare dengan Terraform,” *Journal of Internet and Software Engineering*, vol. 4, no. 1, pp. 23–31, May 2023, doi: <https://doi.org/10.22146/jise.v4i1.6510>.
- [27] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero trust architecture,” *NIST Special Publication 800-207*, Aug. 2020, doi: <https://doi.org/10.6028/nist.sp.800-207>.
- [28] G. Sharma, “Secure Remote Access IPSEC Virtual Private Network to University Network System,” *Journal of Computer Science Research*, vol. 3, no. 1, Feb. 2021, doi: <https://doi.org/10.30564/jcsr.v3i1.2730>.
- [29] S. D. Mediana, Lindawati, and M. Fadhli, “Implementing Zero Trust Model for SSH Security with kerberos and OpenLDAP,” *SISTEMASI*, vol. 12, no. 3, pp. 981–981, Sep. 2023, doi: <https://doi.org/10.32520/stmsi.v12i3.3330>.

- [30] D. Domakonda, “Secure Remote Access in CloudStack: Implementation and Performance Evaluation of an L2TP-over-IPsec VPN,” *The Eastasouth Journal of Information System and Computer Science*, vol. 1, no. 02, pp. 126–131, Dec. 2023, doi: <https://doi.org/10.58812/esiscs.v1i02.513>.
- [31] L. O. Sari and Helena, “Implementasi Virtual Private Network Menggunakan Layer 2 Tunneling Protocol Berbasis Mikrotik,” *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 4, no. 4, pp. 1496–1504, Sep. 2024, doi: <https://doi.org/10.57152/malcom.v4i4.1651>.
- [32] V. N. S. S. Chimakurthi, “The Challenge of Achieving Zero Trust Remote Access in Multi-Cloud Environment,” *ABC Journal of Advanced Research*, vol. 9, no. 2, pp. 89–102, Dec. 2020, doi: <https://doi.org/10.18034/abcjar.v9i2.608>.
- [33] H. J. Yoon and Mohamad Fadli Zolkipli, “Conceptual Model for Remote Access Security Using Zero-Trust Network Access (ZTNA),” *Borneo International Journal eISSN 2636-9826*, vol. 7, no. 4, pp. 28–34, 2024, Accessed: Apr. 20, 2025. [Online]. Available: <https://majmuah.com/journal/index.php/bij/article/view/665>
- [34] H. Nuruliansyah, “Penerapan Privileged Access Management Menggunakan One Identity Pada Sebuah Perusahaan,” *INOVA-TIF*, vol. 2, no. 1, pp. 12–21, Jan. 2020.
- [35] R. Azhari, “Developing Secure Privileged Access Management with Zero Trust,” *Rafif*, Feb. 12, 2025. <https://rafifdna.github.io/posts/pam-tri/>