Implementasi Cisco ISE (Identity Service Engine) sebagai Network Access Control (NAC) untuk Meningkatkan Keamanan Akses Jaringan pada Simulasi Infrastruktur TI Modern

Ari Ramadhan, S. Kom, M. Kom.
NUPTK : 1633773674130282

Muhamad Rafif Hadi Kusmawan
2201 90346 018
Politeknik IDN, Bogor
muhammadkusmawanfx@gmail.com

ABSTRACT

The rapid development of information technology has increased the need for effective network security systems, especially in organizations with numerous users and devices connected to the network. Security threats such as unauthorized access, data theft, and cyber attacks have become major challenges in managing modern IT infrastructures. Therefore, a security solution capable of controlling network access centrally is required, one of which is the implementation of Network Access Control (NAC) using Cisco Identity Services Engine (ISE). This study aims to analyze the implementation of Cisco ISE in improving network access security within a modern IT infrastructure simulation. The research method used is an experimental method involving network topology design, system installation, security policy configuration, and testing of key Cisco ISE features such as Secure Access, Posture Compliance, and Device Administration using TACACS+. The results show that Cisco ISE is capable of identifying connected devices, performing user authentication and authorization, and automatically enforcing security policies based on user identity and device conditions. Therefore, the implementation of Cisco ISE can enhance network security, reduce the risk of unauthorized access, and support the implementation of identity-based and Zero Trust network security concepts

Keywords: Network Security, Cisco ISE, Network Access Control, Zero Trust, IT Infrastructure

ABSTRAK

Perkembangan teknologi informasi yang pesat meningkatkan kebutuhan akan sistem keamanan jaringan yang efektif, terutama pada organisasi dengan banyak

pengguna dan perangkat yang terhubung ke jaringan. Ancaman seperti akses tidak sah, pencurian data, dan serangan siber menjadi tantangan dalam pengelolaan infrastruktur jaringan modern. Oleh karena itu, diperlukan solusi keamanan yang mampu mengontrol akses jaringan secara terpusat, salah satunya melalui penerapan Network Access Control (NAC) menggunakan Cisco Identity Services Engine (ISE). Penelitian ini bertujuan untuk menganalisis implementasi Cisco ISE dalam meningkatkan keamanan akses jaringan pada simulasi infrastruktur TI modern. Metode penelitian yang digunakan adalah metode eksperimen melalui perancangan topologi jaringan, instalasi sistem, konfigurasi kebijakan keamanan, serta pengujian fitur Secure Access, Posture Compliance, dan Device Administration menggunakan TACACS+. Hasil penelitian menunjukkan bahwa Cisco ISE mampu melakukan identifikasi perangkat, autentikasi dan otorisasi pengguna, serta menerapkan kebijakan keamanan secara otomatis berdasarkan identitas dan kondisi perangkat. Dengan demikian, implementasi Cisco ISE dapat meningkatkan keamanan jaringan, mengurangi risiko akses tidak sah, serta mendukung penerapan konsep keamanan jaringan berbasis identitas dan Zero Trust.

Kata kunci: Network Security, Cisco ISE, Network Access Control, Zero Trust, Infrastruktur TI

Catatan : Nomor HP tidak akan dicantumkan, namun sebagai fast respon apabila perbaikan dan keputusan penerimaan jurnal sudah ada.
085157805655

A. Pendahuluan

Cisco Identitiy Service Engine (ISE) hadir dan menawarkan berbagai fitur yang dibutuhkan oleh industri. ISE merupakan salah satu NAC dan sudah banyak digunakan berbagai industri lainnya, ada banyak fitur ISE yang ditawarkan seperti autentikasi berbasis 802.1X, secure access, TACACS+, posture compliant, serta dapat monitoring endpoint user dengan otomatis dan secara real-time. Organisasi juga dapat menerapkan hak akses berdasarkan identitas dari pengguna, perangkat, dan lokasi. Dengan solusi tersebut, ISE merupakan salah satu hal yang penting dalam industri untuk

keamanan dengan berbasis Zero Trust.

B. Metode Penelitian

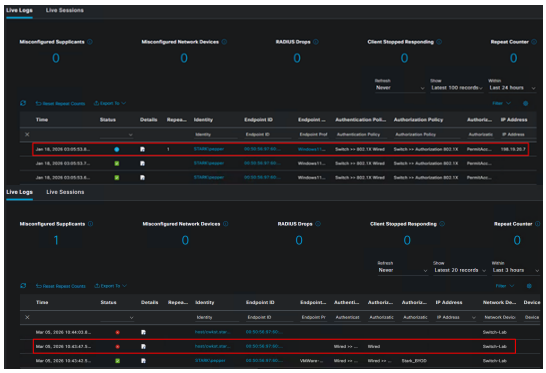
Dalam penerapan penelitian ini terdapat beberapa metodologi yang dilakukan untuk menyelesaikan permasalahan, Metode yang dilakukan dalam penelitian ini adalah dengan pengumpulan data sebagai berikut:

1. Observasi : Suatu kegiatan yang dilakukan oleh penulis untuk pengamatan langsung di lokasi penelitian untuk melakukan pengamatan dan mendapatkan data-data informasi yang dibutuhkan.
2. Studi Pustaka : Penulis mencari informasi yang berkaitan dengan permasalahan yang akan dibahas dalam buku-buku, harapan besar dapat membantu dalam penelitian ini.

C.Hasil Penelitian dan Pembahasan

1. Secure Access

Sebagian besar organisasi memulai dengan mengamankan jaringan nirkabel (wireless) mereka terlebih dahulu. Mengamankan jaringan wireless merupakan kebutuhan paling dasar bagi setiap organisasi. Dengan menggunakan Cisco ISE, administrator jaringan dapat mengamankan akses ke jaringan dengan hanya mengizinkan pengguna dan perangkat wireless yang telah terotorisasi — seperti ponsel, tablet, atau laptop, baik milik pribadi (BYOD) maupun milik organisasi, serta perangkat wireless lainnya — untuk terhubung ke jaringan dan kemudian menerapkan kebijakan keamanan yang berbeda. Autentikasi dan Otorisasi adalah fungsi inti dari ISE. Setiap sesi ISE dimulai dengan proses autentikasi, baik terhadap pengguna maupun perangkat.



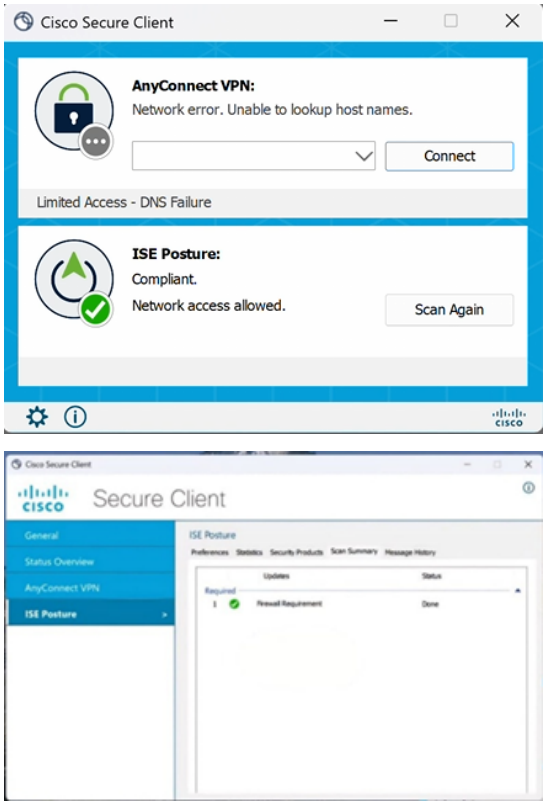
Gambar 1 Secure Access

2. Posture Compliant

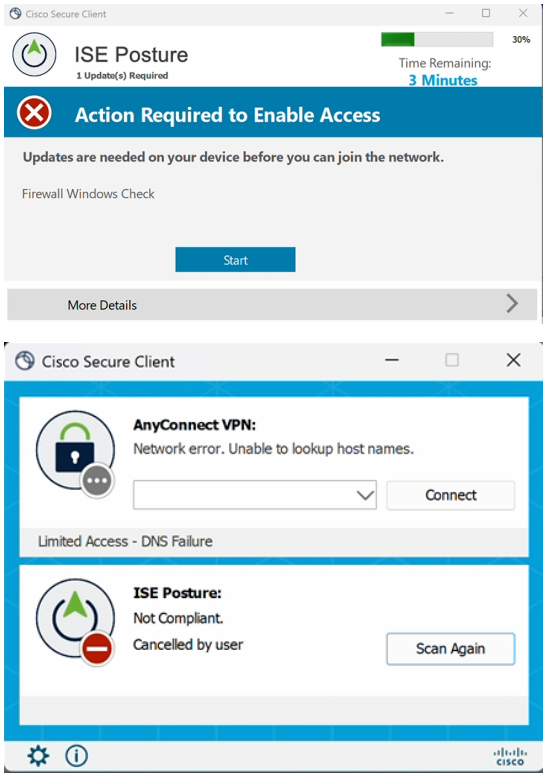
Posture memanfaatkan agen yang terpasang secara permanen maupun sementara untuk memeriksa kondisi internal perangkat (endpoint),

guna memastikan bahwa patch sistem operasi, antimalware, firewall, dan komponen lainnya sudah terpasang, diaktifkan, dan diperbarui sebelum perangkat tersebut diizinkan untuk mengakses jaringan.

Memiliki visibilitas yang baik terhadap perangkat mana saja yang patuh terhadap kebijakan perangkat lunak perusahaan saja tidak cukup — pelanggan mungkin ingin memberikan tingkat akses yang berbeda tergantung pada tingkat kepatuhan perangkat tersebut.



Gambar 2 Posturing Berhasil

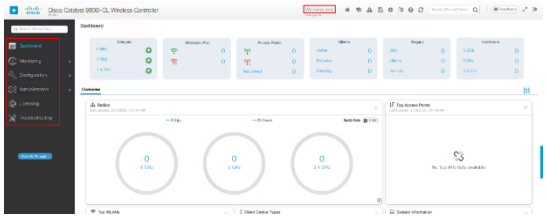


Gambar 3 Posturing Gagal

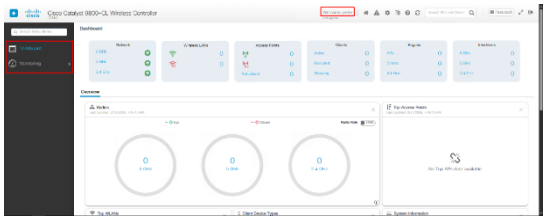
3. TACACS+/Device Admin

Cisco ISE mendukung administrasi perangkat menggunakan protokol keamanan TACACS+ untuk mengontrol dan mengaudit konfigurasi perangkat jaringan. Perangkat jaringan dikonfigurasi untuk meminta autentikasi dan otorisasi tindakan administrator perangkat kepada Cisco ISE, dan mengirimkan pesan akuntansi kepada Cisco ISE untuk mencatat tindakan tersebut. Hal ini memfasilitasi kontrol terperinci tentang siapa yang dapat mengakses perangkat jaringan mana dan mengubah pengaturan jaringan terkait. Administrator Cisco ISE dapat

membuat set kebijakan yang memungkinkan hasil TACACS, seperti set perintah dan profil shell, untuk dipilih dalam aturan kebijakan otorisasi dalam layanan akses administrasi perangkat. Node Pemantauan Cisco ISE menyediakan laporan lanjutan yang terkait dengan administrasi perangkat. Menu Pusat Kerja berisi semua halaman administrasi perangkat, yang bertindak sebagai titik awal tunggal bagi administrator ISE.



Gambar 3 TACACS+ Admin



Gambar 3 TACACS+ Non-Admin

E. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan mengenai implementasi sistem keamanan jaringan menggunakan Cisco Identity Services Engine (ISE) sebagai Network Access Control (NAC).

DAFTAR PUSTAKA

Jurnal :

F. Dali, “Sistem Keamanan Jaringan Menggunakan Cisco AnyConnect Dengan Metode Network Access Manager,” vol. 5, no. 1, 2021.

H. Fauzi, L. Widyawati, and K. Marzuki, “Analisa Penerapan Network Access Control (NAC) Untuk Keamanan Jaringan,” vol. 1, no. 1, pp. 2–5, 2025, doi: 10.30812/juteks.v1i1.5187.

D. Kus Heryadi et al., “Optimasi Keamanan Pada Jaringan Multi-Endpoint Access Menggunakan Network Access Control Berbasis Cisco Ise,” Jl. Kramat Raya, vol. ISSN, no. 2, pp. 2722–2713, 2021.

M. Fahsi, “802 . 1X and EAP evaluations in wired and wireless networks Avaliação 802 . 1X e EAP em redes com e sem fios Evaluaciones de 802 . 1X y EAP en redes cableadas e inalámbricas,” pp. 1–12, 2024, doi: 10.54021/seesv5n2-554.

V. Kodela, “Enhancing Industrial Network Security using Cisco ISE and Stealthwatch : A Case Study on Shopfloor Environment,” vol. 8, no. 3, pp. 1–7, 2023.

V. Bairy, F. R. Bank, and S. Francisco, “International Journal of Innovation Studies,” pp. 41–48.

K. Denzel, “A survey of security in zero trust network architectures,” vol. 22, no. February, pp. 182–214, 2025.

S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, “Security of Zero Trust Networks in Cloud Computing : A Comparative Review,” pp. 1–21, 2022.

R. Wpa-enterprise, T. A. Aji, M. Kurniawan, Y. Sutanto, A. A. Slameto, and R. A. Kristiary, “Jurnal Processor Perancangan Sistem Autentikasi Jaringan Nirkabel dan File Server,” vol. 20, no. 2, pp. 146–157, 2025.

S. Yiliyaer and Y. Kim, “Secure Access Service Edge : A Zero Trust Based Framework For Accessing Data Securely,” 2021.

T. Kaur, “Secure Access Service Edge (SASE): Extending Network Security to Client,” vol. 13, no. 7, 2024, doi: 10.15680/IJIRSET.2024.1307101.

Z. Senan, M. Attar, and S. Senan, “A Comprehensive Review of Zero Trust Network Architecture (ZTNA) and Deployment Frameworks,” vol. 11, no. 1, pp. 148–153, 2025.

N. Patel, “SECURE ACCESS SERVICE EDGE (SASE): EVALUATING THE IMPACT OF CONVEREGED NETWORK SECURITY ARCHITECTURES IN CLOUD COMPUTING,” vol. 11, no. 3, pp. 703–714, 2024.

H. O. N. J. U. N. Yoon, M. Fadli, and B. I. N. Zolkipli, “Conceptual Model for Remote Access Security Using Zero-Trust Network Access (ZTNA),” vol. 7, no. 4, pp. 28–34, 2024.

X. Chen, W. Feng, N. Ge, and Y. Zhang, “Zero Trust Architecture for 6G Security,” pp. 1–7.

N. Arun and M. Kesavan, “The Integration of Artificial Intelligence in Secure Access Service Edge : Enhancing Network Security and Performance,” pp. 460–466, 2024.

E. Stefano, F. Purun, and D. W. Chandra, “Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi) Analisis Keamanan DHCP Menggunakan RADIUS Accounting,” vol. 9, no. September, pp. 906–912, 2025.

K. Kamono, K. Mulumba, I. Meji, and K. Kayembe, “Study of Securing A Wireless Network with A Radius Server,” vol. 12, no. 03, pp. 4073–4090, 2024, doi: 10.47191/ijmcr/v12i3.01.

C. Alezander, O. Villanueva, and A. Roman-gonzalez, “International Journal of Advanced and Applied Sciences Implementation of a RADIUS server for access control through authentication in wireless networks,” vol. 10, no. 3, pp. 183–188, 2023.

R. Marin-lopez, O. Canovas, G. Lopez-millan, and F. Pereniguez-garcia, “SDN-AAA : Towards the

standard management of AAA infrastructures," pp. 1–7.