Implementasi Zero Trust Network Access (ZTNA) Menggunakan NetBird pada Lingkungan Cloud AWS

(Disusun untuk memenuhi tugas mata kuliah
Arsitektur Jaringan Modern)

Oleh Kelompok:

Catherine Nathania	(235150201111042)
Shinta Oktavia Ramadhani	(235150207111036)
I Made Deva Satria Wiguna Giri	(235150200111054)

Dosen:

Achmad Basuki, ST., MMG., Ph.D.

Program Studi S1 Teknik Informatika
Jurusan Teknik Informatika
Universitas Brawijaya
2025

KATA PENGANTAR

Puji syukur kami panjatkan kepada Tuhan yang Maha Esa atas segala rahmat dan karunia-Nya sehingga dapat terselesaikannya Proposal Project Akhir Mata Kuliah Arsitektur Jaringan Modern, dengan judul "**Implementasi *Zero Trust Network Access* (ZTNA) Menggunakan NetBird pada Lingkungan Cloud AWS**", sebagai salah satu persyaratan akademis dalam rangka menyelesaikan Mata Kuliah di Fakultas Ilmu Komputer

Proposal ini memaparkan tantangan keamanan siber modern yang semakin kompleks, khususnya dalam mendeteksi dan mengantisipasi ancaman internal maupun eksternal yang tidak terdeteksi oleh mekanisme keamanan tradisional. Dalam proposal ini, penulis membahas dan merancang pendekatan integratif antara arsitektur Zero Trust yang berfokus pada kontrol akses ketat dan verifikasi identitas, dengan teknologi analitik perilaku yang mampu mendeteksi anomali aktivitas pengguna secara adaptif dan dinamis.

Diharapkan bahwa integrasi ini dapat memberikan solusi keamanan yang lebih holistik dan responsif terhadap berbagai bentuk serangan siber, serta menjadi referensi bermanfaat bagi pengembangan sistem keamanan digital masa kini. Semoga Tuhan Yang Maha Esa memberikan balasan atas segala upaya yang telah dilakukan dan semoga proposal ini bermanfaat, baik bagi kami sendiri maupun pihak lain yang berkepentingan.

Malang, 10 Mei 2025

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era digital saat ini, organisasi dan perusahaan semakin banyak memanfaatkan layanan berbasis cloud untuk mendukung operasional harian. Perpindahan ke cloud membawa berbagai keuntungan seperti kemudahan skalabilitas, efisiensi biaya, dan aksesibilitas yang lebih baik. Namun, seiring berkembangnya teknologi, ancaman keamanan jaringan juga semakin kompleks dan tidak lagi dapat diatasi hanya dengan pendekatan keamanan tradisional yang mengandalkan perimeter security atau firewall semata.

Pada pendekatan tradisional, sistem keamanan jaringan bekerja dengan membangun "tembok" atau perimeter yang menganggap bahwa semua perangkat dan pengguna di dalam jaringan internal adalah tepercaya. Pendekatan ini memiliki kelemahan mendasar, terutama ketika organisasi memiliki banyak pengguna yang bekerja dari luar kantor (remote), menggunakan perangkat pribadi (BYOD), serta aplikasi dan server yang tersebar di berbagai lokasi, termasuk cloud publik. Model ini rentan terhadap serangan internal, penyalahgunaan akun, dan berbagai celah keamanan yang dapat dimanfaatkan penyerang.

Sebagai solusi modern, muncul konsep Zero Trust Network Access (ZTNA) yang menerapkan prinsip "*Never trust, always verify*." Konsep ini mengharuskan semua permintaan akses ke sumber daya jaringan untuk selalu diautentikasi, divalidasi, dan dipantau, tanpa memandang lokasi pengguna atau perangkat. Dengan demikian, kontrol akses berbasis identitas, enkripsi lalu lintas, serta kebijakan granular menjadi inti dari penerapan ZTNA.

Untuk membantu implementasi ZTNA di lingkungan cloud, tersedia berbagai alat dan platform. Salah satunya adalah NetBird, sebuah solusi open source yang memanfaatkan protokol VPN modern WireGuard untuk membangun konektivitas mesh yang terenkripsi antara endpoint dan resource. NetBird tidak

hanya berperan sebagai VPN, tetapi juga sebagai platform manajemen identitas dan kontrol akses yang mendukung penerapan Zero Trust secara lebih mudah dan fleksibel.

AWS (*Amazon Web Services*) menjadi pilihan infrastruktur cloud karena menyediakan kemudahan dalam penyediaan resource (seperti server aplikasi, database, dan server manajemen) serta mendukung kebutuhan skalabilitas dan keamanan yang sesuai dengan praktik industri. Dalam konteks pendidikan, melalui program AWS Academy, mahasiswa juga dapat memanfaatkan kredit cloud untuk belajar, bereksperimen, dan mengimplementasikan konsep arsitektur jaringan modern seperti ZTNA.

Melalui proyek akhir ini, penulis dan tim ingin mengeksplorasi dan mengimplementasikan ZTNA menggunakan NetBird di lingkungan cloud AWS. Harapannya, implementasi ini dapat menjadi contoh nyata bagaimana Zero Trust dapat diterapkan untuk meningkatkan keamanan jaringan, sekaligus memberikan pengalaman praktis bagi mahasiswa dalam merancang, membangun, dan mengelola arsitektur jaringan modern yang lebih adaptif terhadap ancaman siber masa kini.

1.2 Identifikasi Masalah

Beberapa permasalahan utama yang dapat diidentifikasi dalam konteks Implementasi *Zero Trust Network Access* (ZTNA) Menggunakan NetBird pada Lingkungan Cloud AWS adalah sebagai berikut:

1. Keamanan jaringan tradisional yang masih mengandalkan perimeter security menjadi kurang efektif di era cloud dan kerja jarak jauh.
2. Banyak organisasi kesulitan menerapkan kontrol akses berbasis identitas yang granular dan terpusat.
3. Perlunya solusi modern seperti ZTNA yang dapat diterapkan dengan biaya dan kerumitan yang lebih rendah.

4. Minimnya pengalaman praktis mahasiswa dalam mengimplementasikan arsitektur Zero Trust di lingkungan cloud.

1.3 Rumusan Masalah

1. Bagaimana menyediakan akses yang aman dan terkontrol bagi pengguna jarak jauh (misalnya, karyawan yang bekerja dari rumah) ke sumber daya perusahaan?

2. Bagaimana mengamankan aset digital yang tersebar di berbagai lingkungan, seperti cloud publik (AWS) dan pusat data (datacenter) internal, dalam satu model keamanan yang koheren?

3. Bagaimana menerapkan prinsip least privilege (hak akses minimal), di mana pengguna hanya dapat mengakses sumber daya yang benar-benar mereka butuhkan untuk pekerjaan mereka?

1.4 Tujuan dan Manfaat Penelitian

Penelitian memiliki manfaat penelitian sebagai berikut:

1. Merancang dan mengimplementasikan sebuah prototipe arsitektur ZTNA yang fungsional.

2. Memanfaatkan layanan cloud Amazon Web Services (AWS) untuk menyimulasikan infrastruktur server.

3. Menggunakan Netbird sebagai control plane untuk membangun jaringan overlay yang aman berbasis WireGuard.

4. Mendemonstrasikan bagaimana server dapat diisolasi sepenuhnya dari internet publik namun tetap dapat diakses secara aman oleh pengguna berwenang.

5. Menguji skenario akses oleh banyak pengguna ke sumber daya yang tersegmentasi.

BAB II

TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 Zero Trust Network Access (ZTNA)

Zero Trust Network Access (ZTNA) adalah pendekatan keamanan jaringan modern yang berpijak pada prinsip *"Never trust, always verify"*. Dalam ZTNA, tidak ada pengguna atau perangkat yang secara otomatis dianggap tepercaya, meskipun berada di dalam jaringan internal. Setiap permintaan akses ke sumber daya harus melalui proses autentikasi dan otorisasi berbasis identitas, serta selalu diawasi dan dicatat (Rose et al., 2019). Penerapan ZTNA membantu mencegah serangan internal, meminimalkan dampak kebocoran data, dan mendukung model kerja jarak jauh.

2.1.2 Virtual Private Network (VPN) dan WireGuard

VPN adalah teknologi yang memungkinkan koneksi aman antara pengguna dan jaringan melalui saluran komunikasi terenkripsi. Salah satu protokol VPN modern adalah WireGuard, yang dirilis sebagai open source dan dikenal karena kesederhanaan, performa tinggi, serta penggunaan algoritma kriptografi mutakhir (Donenfeld, 2018). WireGuard dirancang lebih ringan dibanding protokol VPN tradisional seperti IPsec dan OpenVPN, sehingga cocok untuk implementasi modern termasuk mesh VPN.

2.1.3 Cloud Computing dan Layanan AWS

Cloud computing memungkinkan penyediaan infrastruktur, platform, dan perangkat lunak secara on-demand melalui internet. Amazon Web Services (AWS) adalah salah satu penyedia layanan cloud terbesar yang menyediakan layanan seperti Elastic Compute Cloud (EC2) untuk

server virtual, Virtual Private Cloud (VPC) untuk manajemen jaringan, dan IAM (Identity and Access Management) untuk keamanan. Cloud sangat mendukung penerapan arsitektur modern seperti ZTNA karena menyediakan skalabilitas dan fleksibilitas tinggi (Amazon, 2022).

2.1.4 NetBird

NetBird adalah solusi open source yang menggabungkan WireGuard dengan sistem manajemen identitas dan kontrol akses terpusat. NetBird memudahkan penerapan mesh VPN dengan tampilan dashboard untuk administrator, memungkinkan pembuatan policy granular berbasis identitas, dan dapat di-deploy di cloud maupun on-premises. NetBird dirancang agar mudah diintegrasikan ke sistem yang ada, termasuk cloud public seperti AWS.

2.2 Kerangka Berpikir

Kerangka berpikir dalam proyek ini berangkat dari tantangan keamanan pada jaringan tradisional yang mengandalkan perimeter dan kepercayaan implisit antar perangkat internal. Model ini rentan terhadap serangan internal, lateral movement, dan kesulitan dalam menerapkan kontrol akses dinamis. Oleh karena itu, pendekatan Zero Trust Network Access (ZTNA) dipilih sebagai solusi karena menekankan pada autentikasi berkelanjutan dan otorisasi berdasarkan identitas. NetBird digunakan sebagai platform implementasi karena menyediakan solusi berbasis WireGuard yang ringan dan aman, serta kontrol akses yang dapat dikonfigurasi secara terpusat. Dengan memanfaatkan layanan AWS, proyek ini dapat menguji dan menerapkan solusi ZTNA dalam lingkungan cloud yang fleksibel dan dapat diskalakan.

2.3 Hipotesis

Hipotesis dalam proyek ini dirumuskan berdasarkan asumsi bahwa penerapan arsitektur ZTNA menggunakan NetBird dapat meningkatkan

keamanan jaringan cloud secara signifikan dibandingkan pendekatan tradisional. Hipotesis yang diajukan adalah sebagai berikut:

- H_0 (Hipotesis nol): Implementasi NetBird berbasis ZTNA tidak memberikan peningkatan signifikan terhadap keamanan jaringan cloud dibandingkan metode tradisional.

- H_1 (Hipotesis alternatif): Implementasi NetBird berbasis ZTNA memberikan peningkatan signifikan terhadap keamanan jaringan cloud, khususnya dalam hal kontrol akses, segmentasi lalu lintas, dan deteksi aktivitas anomali.

Uji hipotesis ini dilakukan melalui proses implementasi, pengujian kebijakan akses, serta observasi terhadap efektivitas sistem dalam membatasi akses dan mencatat log aktivitas.

BAB III

METODOLOGI PENELITIAN

Metodologi penelitian pada penyusunan tugas akhir ini bertujuan untuk memastikan bahwa proses integrasi analitik perilaku dengan "Arsitektur *Zero Trust*" berjalan secara terarah, terstruktur, dan sesuai dengan tujuan yang telah ditetapkan. Tahapan metodologi yang diterapkan meliputi:

3.1 Alur Penelitian

Tahapan penelitian ini meliputi:

1. Perancangan Sistem

   Merancang arsitektur ZTNA menggunakan Netbird pada infrastruktur hybrid cloud (AWS dan simulasi datacenter lokal) yang menggambarkan segmentasi sumber daya dan pengguna.
2. Penyediaan Infrastruktur

   Menyiapkan dua instance server virtual di AWS menggunakan Ubuntu Server 22.04 LTS sebagai Web Server dan CRM Server.
3. Instalasi dan Konfigurasi Netbird

   Menginstal agen Netbird di setiap perangkat (server dan laptop pengguna), serta menghubungkan semuanya ke dalam jaringan overlay Netbird menggunakan Setup Key.
4. Penerapan Kebijakan Akses

   Mengelola konektivitas peer-to-peer berdasarkan identitas pengguna dan kebijakan akses melalui dashboard Netbird.
5. Pengujian Skenario Akses

   Melakukan simulasi koneksi oleh beberapa pengguna ke sumber daya yang telah ditentukan dan memverifikasi keberhasilan atau penolakan akses sesuai dengan kebijakan yang ditetapkan.

3.2 Objek dan Ruang Lingkup

Objek dari proyek akhir ini adalah implementasi arsitektur Zero Trust Network Access (ZTNA) menggunakan Netbird dan Amazon Web Services (AWS). Fokus penelitian ini adalah pada pembangunan jaringan overlay yang aman, tersegmentasi, dan berbasis identitas untuk mendukung kebutuhan akses terhadap infrastruktur hybrid cloud.

Ruang lingkup penelitian meliputi:

1. Penerapan prinsip ZTNA dalam lingkungan hybrid (cloud dan lokal),
2. Instalasi dan konfigurasi Netbird sebagai platform kontrol akses dan jaringan privat,
3. Simulasi akses multi-user ke server yang tersegmentasi,
4. Pengujian efektivitas kontrol akses dan isolasi jaringan tanpa eksposur ke internet publik,
5. Penggunaan layanan AWS sebagai platform virtualisasi server.

3.3 Teknik Pengumpulan Data

Untuk mendukung pengembangan integrasi antara analitik perilaku dengan arsitektur Zero Trust, penelitian ini dilakukan melalui beberapa pendekatan utama, yaitu studi literatur, studi sistem sebelumnya, dan analisis sistem yang akan dirancang. Pendekatan ini dipilih agar penyusunan desain solusi dapat dilakukan secara sistematis berdasarkan referensi terpercaya serta praktik yang telah diterapkan sebelumnya.

1. Observasi Langsung

   Pengamatan langsung terhadap proses instalasi, konfigurasi, dan konektivitas antar perangkat dalam jaringan Netbird. Observasi

dilakukan untuk memastikan bahwa skenario akses yang dirancang sesuai dengan kebijakan yang telah diterapkan.

2. Dokumentasi Teknis dan Log Sistem

   Pengumpulan data berupa dokumentasi hasil konfigurasi, log aktivitas pengguna dari server, dan output dashboard Netbird. Log ini digunakan untuk menganalisis apakah koneksi berhasil, ditolak, atau diblokir sesuai kebijakan akses yang diterapkan.

3. Uji Coba Implementasi

   - Pengujian dilakukan dengan beberapa skenario seperti:
   - Akses satu pengguna ke satu server,
   - Akses dua pengguna ke dua server berbeda,
   - Akses dari IP publik untuk menguji apakah koneksi ditolak.
   - Hasil pengujian ini dicatat dan dievaluasi untuk mengetahui apakah implementasi sesuai dengan prinsip ZTNA.

4. Studi Literatur Pendukung

   Referensi dari dokumentasi resmi Netbird, artikel dan whitepaper mengenai ZTNA serta praktik implementasi arsitektur jaringan modern digunakan untuk mendukung rancangan dan konfigurasi sistem.

BAB IV

DESKRIPSI SOLUSI

4.1 Gambaran Umum

Solusi yang diusulkan adalah membangun jaringan privat virtual di atas infrastruktur fisik (AWS dan internet) menggunakan Netbird. Setiap komponen, baik itu server di cloud, server di datacenter, maupun laptop pengguna, menginstal agen Netbird. Agen ini menghubungkan setiap perangkat ke control plane Netbird untuk otentikasi dan pertukaran konfigurasi.

Setelah terhubung, Netbird menciptakan tunnel WireGuard yang terenkripsi secara peer-to-peer (P2P) langsung antar perangkat yang perlu berkomunikasi. Hal ini berarti lalu lintas data tidak perlu melewati server pusat, sehingga menghasilkan latensi rendah dan efisiensi tinggi. Akses ke sumber daya tidak lagi menggunakan IP publik, melainkan IP privat unik yang diberikan oleh Netbird, yang membuat seluruh infrastruktur "tidak terlihat" dari internet.

4.2 Alat dan Teknologi

- Cloud Provider
  Amazon Web Services (AWS), untuk penyediaan server virtual (EC2).
- Sistem Operasi Server
  Ubuntu Server 22.04 LTS.
- Platform ZTNA
  Netbird, sebagai control plane dan data plane overlay.
- Protokol Tunneling
  WireGuard.
- Layanan Server
  OpenSSH (untuk remote access), Nginx (untuk simulasi web server)

4.3 Fitur Utama

- Akses Berbasis Identitas
  Perangkat diautentikasi sebelum diizinkan masuk ke jaringan.

- Enkripsi End-to-End

  Semua lalu lintas diamankan menggunakan protokol WireGuard yang modern dan cepat.
- Isolasi Infrastruktur

  Server tidak memerlukan port terbuka ke internet, mengurangi permukaan serangan secara drastis.
- Manajemen Terpusat

  Kebijakan akses, pengguna, dan perangkat dikelola melalui dashboard Netbird.

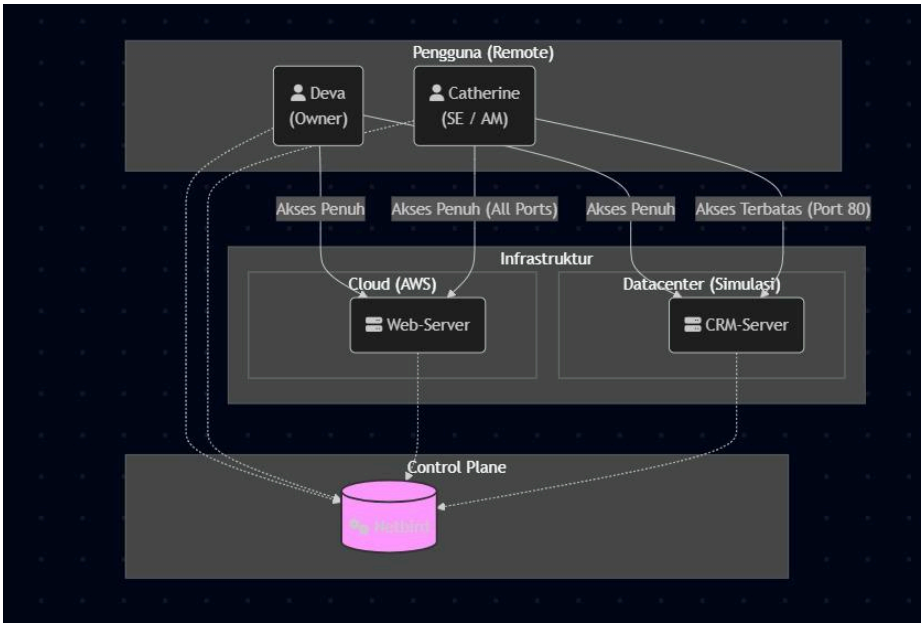
BAB V

PERANCANGAN SISTEM

5.1 Arsitektur Sistem

Arsitektur yang diimplementasikan mengikuti diagram di bawah ini, yang menyimulasikan lingkungan kerja hybrid.

Pengguna (Peers):



Gambar 1. Arsitektur Sistem ZTNA

Sumber Daya (Peers):

1. Cloud (AWS) berisi Web-Server.
2. Datacenter (Simulasi) berisi CRM-Server.

Control Plane:

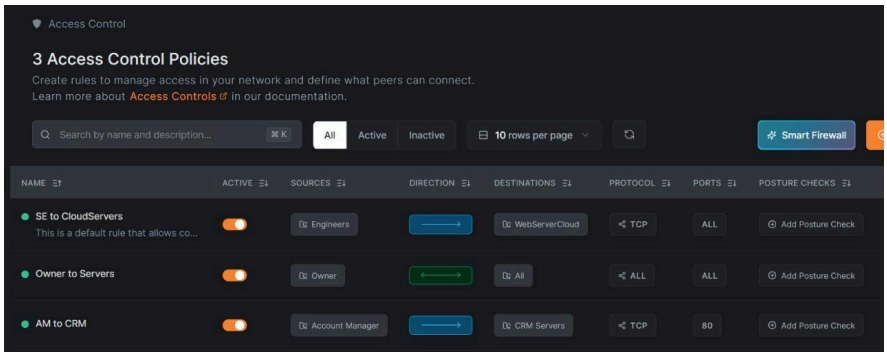
1. Netbird, mengatur otentikasi, kebijakan, dan distribusi kunci enkripsi untuk semua peer.
2. Diagram Alir Proses Koneksi Pengguna:
   - Pengguna menjalankan aplikasi Netbird di laptopnya.

- Aplikasi melakukan otentikasi ke Control Plane Netbird.
- Jika berhasil, perangkat mendapatkan IP privat unik dari Netbird dan daftar peer lain yang diizinkan.
- Pengguna mencoba mengakses server (misalnya via SSH) menggunakan IP Netbird server.
- Control Plane Netbird (melalui kebijakan) memastikan koneksi ini diizinkan.
- Sebuah tunnel WireGuard P2P yang terenkripsi dibuat langsung antara laptop pengguna dan server.
- Koneksi berhasil dan aman.

BAB VI

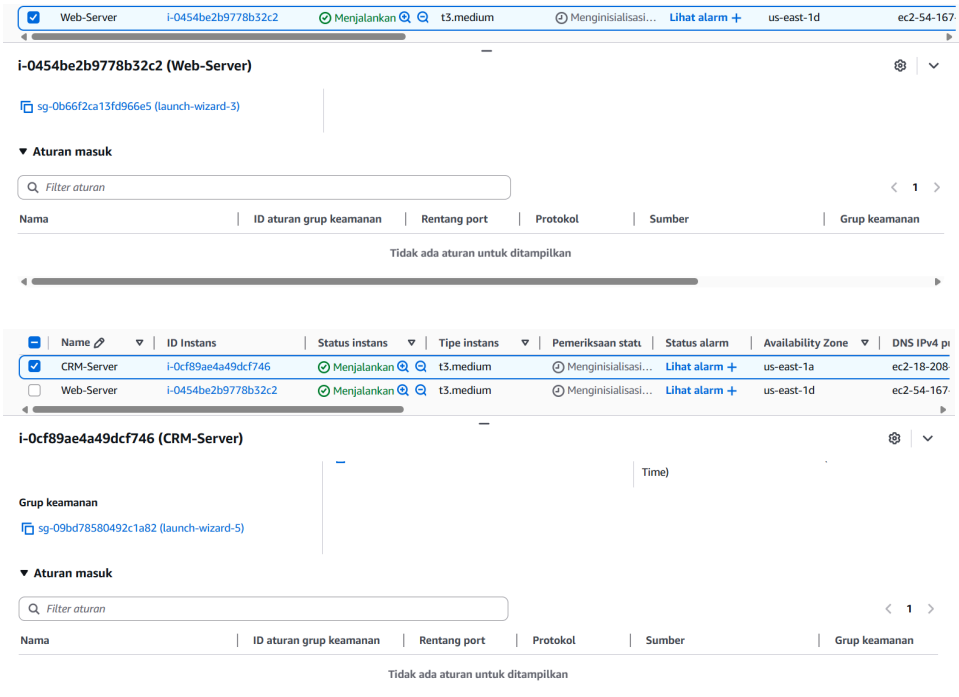
IMPLEMENTASI

6.1 Penjelasan Implementasi Komponen Utama



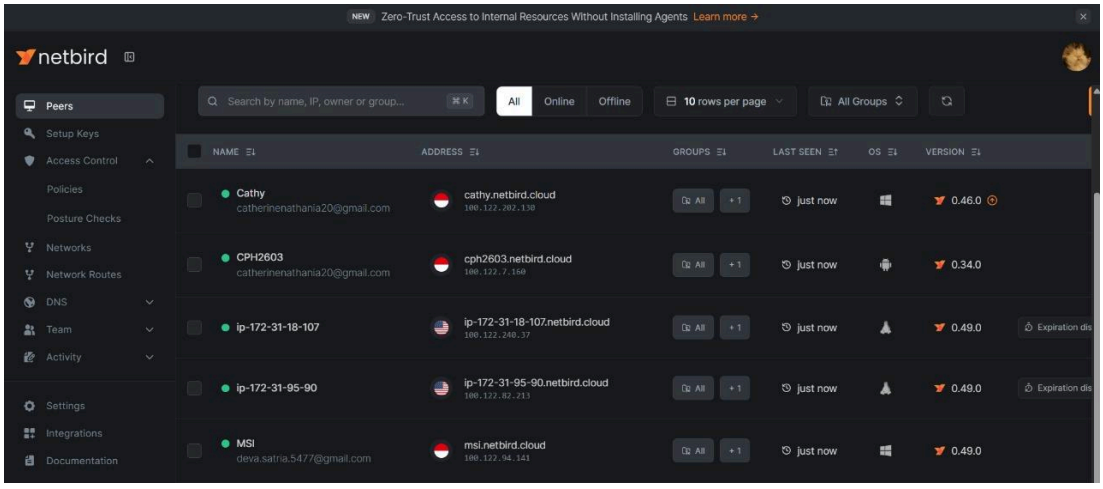
Gambar 2. Konfigurasi Kebijakan Akses di Netbird.

1. Penyediaan Infrastruktur: Dua instance EC2 t3.micro diluncurkan di AWS, masing-masing sebagai Web-Server dan CRM-Server.
2. Konfigurasi Netbird: Akun dibuat di Netbird dan Setup Key dibuat untuk pendaftaran perangkat.
3. Instalasi Agen Netbird: Agen diinstal pada kedua server dan pada laptop Deva serta Catherine.
4. Implementasi Kebijakan Akses: Grup pengguna (Owner, Software Engineer, Account Manager) dan grup server dibuat di Netbird. Kebijakan akses berikut diterapkan:
   - Grup Owner diizinkan mengakses semua grup server di semua port.
   - Grup Software Engineer diizinkan mengakses grup Web-Server di semua port.
   - Grup Account Manager diizinkan mengakses grup CRM-Server hanya pada port 80.
5. Pengamanan Akses: Setelah semua kebijakan terverifikasi, Security Group di AWS dikonfigurasi untuk memblokir semua port masuk dari internet publik.



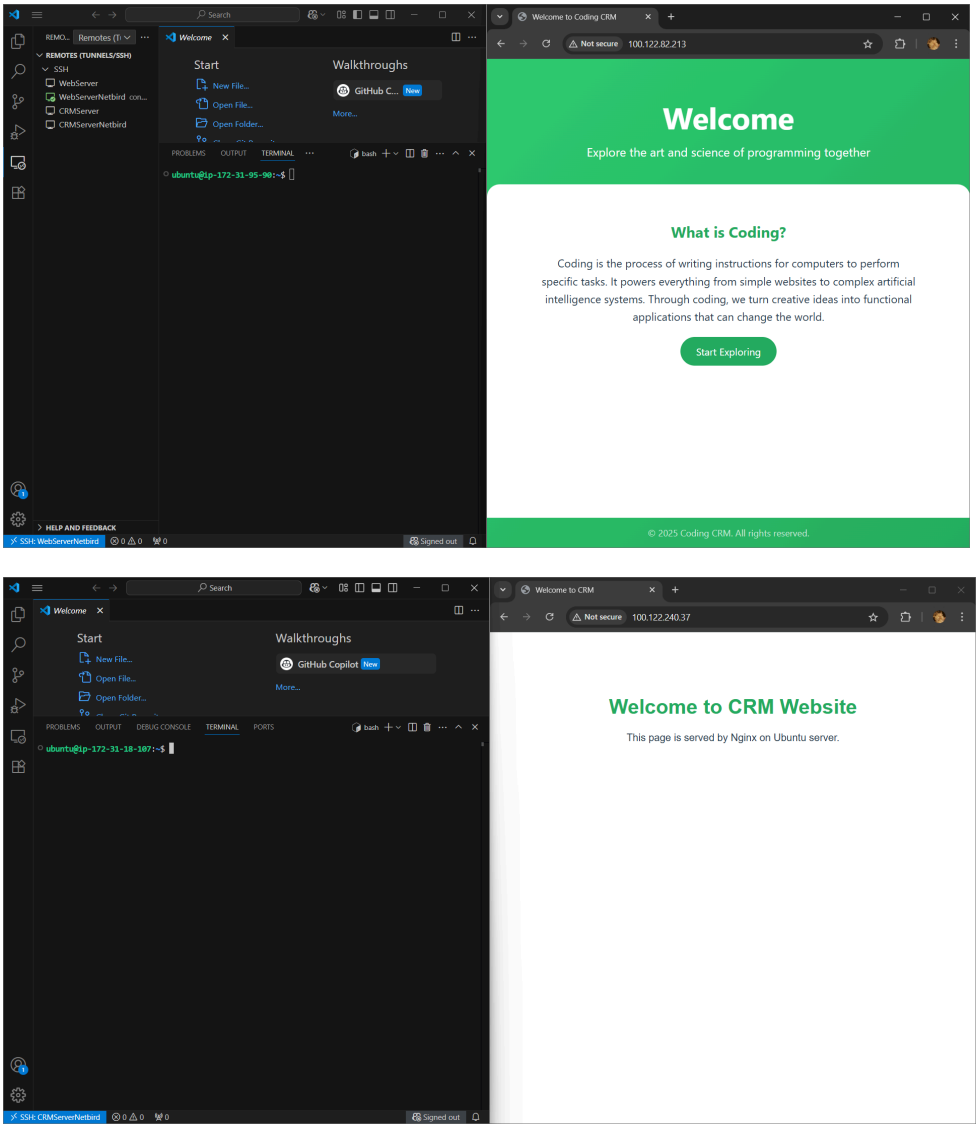
Gambar 3. Security Group

6.2 Demo Hasil Implementasi



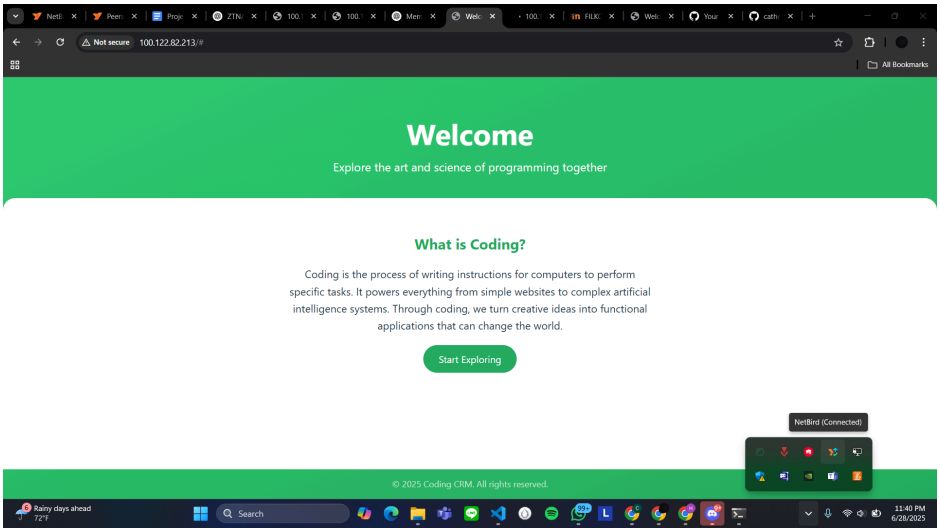
Gambar 4. Dashboard Peers Netbird

1. Skenario Deva (Owner): Deva berhasil melakukan koneksi SSH (port 22) dan mengakses halaman web (port 80) pada kedua server, Web-Server dan CRM-Server, membuktikan hak akses penuhnya.



Gambar 5. Uji Coba Akses Deva ke Web-Server dan CRM-Server.

2. Skenario Catherine (Software Engineer): Catherine berhasil melakukan koneksi SSH dan mengakses halaman web pada Web-Server.

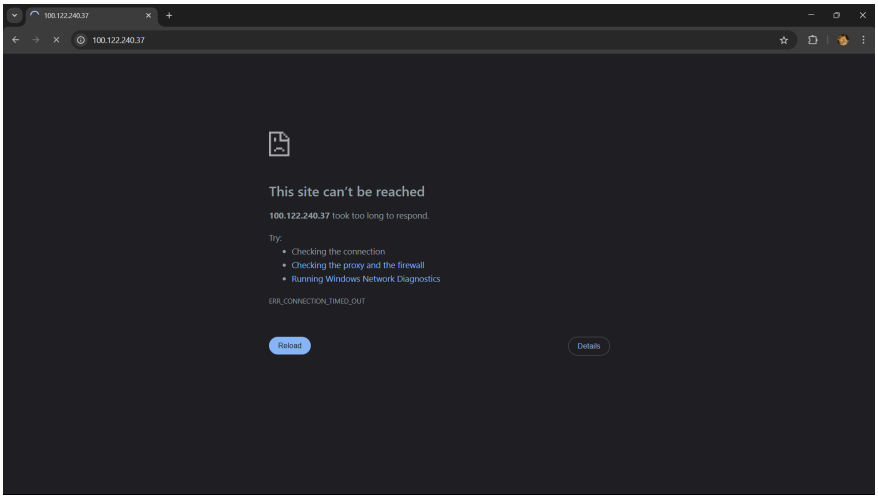


Gambar 6. Uji Coba Akses Catherine ke Web-Server.

3. Skenario Catherine (Account Manager): Catherine berhasil mengakses halaman web CRM-Server (port 80), namun koneksinya gagal (timeout) saat mencoba melakukan SSH (port 22) ke server yang sama. Ini membuktikan bahwa kebijakan pembatasan port bekerja dengan sempurna.

Gambar 7. Uji Coba Akses Catherine ke CRM-Server.

4. Uji Coba Akses Publik: Upaya untuk mengakses kedua server melalui IP Publik AWS gagal total, membuktikan bahwa infrastruktur telah berhasil diisolasi dari internet.



Gambar 8. Uji Coba Akses Publik

BAB V

PENUTUP

5.1 Kesimpulan

Proyek ini berhasil mengimplementasikan arsitektur Zero Trust Network Access (ZTNA) yang fungsional dan aman. Hasil utama yang dicapai adalah penerapan kebijakan akses granular berbasis peran pengguna, di mana hak akses dapat dibatasi hingga ke level port tertentu. Proyek ini membuktikan bahwa ZTNA merupakan solusi superior untuk mengamankan infrastruktur modern yang tersebar, memberikan kontrol yang lebih ketat dan visibilitas yang lebih baik dibandingkan model VPN tradisional.

5.2 Kendala yang Dihadapi

Keterbatasan Sumber Daya t2.micro: Ditemukan masalah timed out saat dua pengguna mencoba terhubung secara bersamaan ke Web-Server. Diagnosis menunjukkan ini disebabkan oleh habisnya CPU Credit pada instance t2.micro. Masalah ini berhasil diselesaikan dengan mengganti tipe instance ke t3.micro.

Instance "Macet": Ditemukan satu kasus di mana instance Web-Server menjadi tidak responsif bahkan setelah di-reboot. Solusi yang diambil adalah menghapus dan membuat ulang instance, yang merupakan demonstrasi praktis dari konsep immutable infrastructure.

5.3 Pengembangan Lanjutan

- Integrasi SSO: Mengintegrasikan Netbird dengan penyedia identitas (IdP) seperti Google Workspace atau Okta.
- Otomatisasi (Infrastructure as Code): Mengotomatiskan seluruh proses penyediaan dan konfigurasi menggunakan alat seperti Terraform atau AWS CloudFormation.
- Keamanan Tingkat Lanjut: Menerapkan pemantauan lalu lintas jaringan dan mengintegrasikan log akses dengan sistem SIEM.

LAMPIRAN

- **Link GitHub:**
  https://github.com/catherinenathania/AJM

- **Link Video YT:**
  https://drive.google.com/drive/folders/1L13-lBP_tBnGZndUAyFhUmPTXNzMcuNx?usp=sharing