JURNAL SYNTAX ADMIRATION

Volume 4, No. 11, November 2023
p-ISSN 2722-7782 | e-ISSN 2722-5356
DOI: https://doi.org/10.46799/jsa.v4i11.757

INTEGRASI SERVER ON-PREMISE DENGAN SERVER CLOUD MENGGUNAKAN CLOUD VPN DAN MIKROTIK IPSEC UNTUK PENINGKATAN KEAMANAN KONEKSI

Hilmi Afifi Al-Atsari[1], Imam Suharjo[2]
Fakultas Teknologi Informasi, Universitas Mercu Buana, Yogyakarta
Email: [1]hilmiafifi12@gmail.com, [2]imam@mercubuana-yogya.ac.id

Abstract :
Dalam era digital yang terus berkembang, integrasi infrastruktur server onpremise dengan server cloud telah menjadi fokus penting bagi banyak perusahaan. Permasalahan yang dihadapi adalah mengenai koneksi yang menggunakan alamat IP publik secara langsung, yang seringkali rentan terhadap berbagai risiko keamanan dan ancaman siber. Oleh karena itu, penelitian ini bertujuan untuk mengidentifikasi dan mengatasi permasalahan utama yang muncul dalam integrasi ini. Dengan pemahaman yang lebih baik tentang tantangan tersebut, pengembang dan organisasi dapat meningkatkan keamanan infrastruktur server hibrid mereka. Metodologi penelitian ini menggunakan Mikrotik IPsec dan VPN Tunnel IKEv2 pada layanan Google Cloud. Pendekatan ini dimanfaatkan untuk meningkatkan keamanan koneksi antara server onpremise dan server cloud. Pertama, penulis melakukan konfigurasi Mikrotik IPsec di server onpremise dan mengatur VPN Tunnel IKEv2 pada layanan Google Cloud. Selanjutnya, penulis melakukan uji coba praktis dengan mengirimkan data antara kedua infrastruktur dan memonitor keamanan serta kestabilan koneksi. Dengan langkah-langkah ini, kami dapat mengevaluasi efektivitas solusi keamanan yang diimplementasikan dalam lingkungan server hibrid. Hasil penelitian menunjukkan bahwa pendekatan ini berhasil mengamankan koneksi antara kedua infrastruktur, mengurangi potensi risiko seperti sniffing, serangan port scanning, brute force, DDOS, dan ancaman siber lainnya. Selain itu, selama uji coba praktis, koneksi tetap stabil dan performa optimal, menunjukkan keefektifan solusi yang diusulkan dalam meningkatkan keamanan infrastruktur server hibrid. Hasil ini dapat memberikan bukti konkret bahwa penggunaan Mikrotik IPsec dan VPN Tunnel IKEv2 pada layanan Google Cloud dapat menjadi langkah yang efektif dalam mengamankan komunikasi antara server onpremise dan server cloud. Dengan demikian, penelitian ini memberikan panduan yang berharga bagi pengembang dan organisasi yang ingin mengimplementasikan solusi serupa.

Kata kunci: VPN, Mikrotik, IPsec, Tunnel, IKEv2, Keamanan Koneksi, Integrasi Server, Server Cloud, Infrastruktur Server.

Abstract:
In the ever-evolving digital era, integration of onpremise server infrastructure with cloud servers has become an important focus for many companies. The problem faced is regarding connections that use public IP addresses directly, which are often vulnerable to various security risks and cyber threats. Therefore, this research aims to identify and overcome the main problems that arise in this integration. With a better understanding of these challenges, developers and organizations can improve the security of their hybrid server infrastructure. The research methodology uses Mikrotik IPsec and VPN Tunnel IKEv2 on Google Cloud services. This approach is utilized to increase connection security between onpremise servers and cloud servers. First, the author configures Mikrotik IPsec on the onpremise server and sets up the IKEv2 VPN Tunnel on Google Cloud services. Next, the author carried out practical tests by sending data between the two infrastructures and monitoring the security and stability of the connection. With these steps, we can evaluate the effectiveness of security solutions implemented in a hybrid server environment. The research results show that this approach is successful in securing the connection between the two infrastructures, reducing potential risks such as sniffing, port scanning attacks, brute force, DDOS, and other cyber threats. Moreover, during practical trials, the connection remained stable and performed optimally, demonstrating the effectiveness of the proposed solution in improving the security of hybrid server infrastructure. These results can provide concrete evidence that using Mikrotik IPsec and VPN Tunnel IKEv2 on Google Cloud services can be an effective step in securing communications between onpremise servers and cloud servers. Thus, this research provides valuable guidance for developers and organizations looking to implement similar solutions.

Keywords: *VPN, Mikrotik, IPsec, Tunnel, IKEv2, Connection Security, Server Integration, Cloud Server, Server Infrastructure.*

PENDAHULUAN

Dalam konteks perkembangan teknologi yang pesat, integrasi infrastruktur server onpremise dengan server cloud telah menjadi perhatian utama bagi banyak perusahaan (Jamil & Rosihan, 2016). Model infrastruktur hibrida (hybrid infrastructure), yang menggabungkan server onpremise yang berada dalam lingkungan fisik perusahaan dengan server cloud yang memberikan fleksibilitas dan skalabilitas yang diperlukan, semakin menjadi pilihan populer (Rachmad et al., 2023). Namun, tantangan utama dalam konteks ini adalah keamanan. Banyak infrastruktur hibrida yang masih mengandalkan koneksi menggunakan alamat IP publik yang dapat diakses secara langsung dari internet. Hal ini akan menjadi penyebab infrastruktur tersebut rentan terhadap berbagai risiko keamanan dan ancaman siber.

Selain itu, beberapa perusahaan sering memiliki kebutuhan khusus seperti menjaga database server secara onpremise untuk alasan keamanan dan audit data. Namun,

perusahaan juga tetap ingin menjaga koneksi yang aman antara server onpremise dan server cloud tanpa harus membuka akses IP publik server secara langsung ke internet, yang dapat meningkatkan potensi risiko keamanan. Use case dari permasalahan ini seringkali terjadi di perusahaan yang memiliki server untuk diakses oleh tim internal saja, sehingga tidak perlu ekspose sumber daya mereka secara langsung ke internet. Oleh karena itu, diperlukan sebuah konsep yang dapat meningkatkan keamanan koneksi antara server onpremise dan server cloud. Konsep yang diusulkan adalah menggunakan metode IPsec + VPN Tunnel IKEv2 dengan memanfaatkan alamat IP internal untuk komunikasi antar VM.
Penelitian ini menyoroti akan pentingnya melindungi server onpremise dan server cloud dalam konteks keamanan siber yang terus berkembang. Dengan mengimplementasikan solusi keamanan yang tepat, perusahaan dapat menjaga data dan sistem mereka dari ancaman siber yang beragam dan memastikan bahwa infrastruktur server hibrida mereka tetap aman dan andal.

Dalam penelitian pertama dengan judul "Analisa Konektivitas Jaringan IPsec Dan OpenVPN Pada Jaringan Berbasis IP Dinamis," membahas isu-isu keamanan dalam jaringan internet yang saat ini menjadi kebutuhan vital bagi perusahaan. Mereka mencatat bahwa semakin banyak interkoneksi dengan jaringan luar, semakin besar potensi ancaman keamanan data. Oleh karena itu, penulis menyarankan penggunaan VPN sebagai solusi untuk menjaga keamanan data saat terhubung ke jaringan. VPN ini akan mengamankan data dengan mengirimkannya melalui sebuah tunnel yang menghubungkan antar jaringan dan melakukan enkripsi pada data tersebut. Dalam penelitian ini, penulis melakukan analisa terhadap konektivitas antara VPN IPSEC dan OpenVPN, menggunakan dua jaringan lokal di lokasi yang berbeda (Lokasi A dan B) sebagai objek pengujian (Setya & Sudaryanto, 2021).

Penelitian kedua yang berjudul "Rancang Bangun Jaringan VPN Berbasis IPSEC Menggunakan Mikrotik Routerboard Pada PT. Zahir Internasional" bertujuan untuk mengimplementasikan teknologi VPN berbasis IPSec menggunakan perangkat Mikrotik Routerboard di PT. Zahir Internasional. Latar belakangnya adalah kebutuhan akan keamanan dalam berbagi komunikasi dan informasi di perusahaan tersebut yang semakin meningkat seiring dengan penggunaan data yang tinggi. Masalah utama yang dihadapi adalah ketidakmampuan untuk berbagi data secara langsung antara kantor pusat dan cabang. Untuk mengatasi masalah ini, penelitian ini mengusulkan solusi berupa implementasi jaringan VPN berbasis IPSec menggunakan perangkat Mikrotik Routerboard (F. Sjafrina et al., 2019).

Kemudian penelitian ketiga membahas bagaimana algoritme enkripsi Blowfish dapat digunakan untuk meningkatkan kinerja VPN site-to-site. Penelitian tersebut berjudul "Optimasi IPSec Site to Site VPN Mikrotik Menggunakan Algoritme Enkripsi Blowfish". Latar belakang masalahnya adalah pentingnya menjaga keamanan data dalam komunikasi yang

semakin kompleks, sementara performa VPN juga harus tetap optimal. Penelitian ini dilakukan pada jaringan site-to-site IPsec VPN menggunakan simulator EVE-NG dengan membandingkan dua algoritma enkripsi, yaitu AES (Advanced Encryption Standard) dan Blowfish (Rahman et al., 2023).

Penelitian keempat yang berjudul "Protokol L2TP dan IPsec Sebagai Keamanan Jaringan Pada Dinas Kominfotik Sumatera Barat" mengangkat permasalahan keamanan jaringan di Kantor Dinas Komunikasi, Informatika, dan Statistik Sumatera Barat. Solusi yang ditawarkan adalah penerapan penggunaan teknologi keamanan jaringan VPN dengan metode L2TP (Layer 2 Tunneling Protocol) dan IPSec (Internet Protocol Security). Konfigurasi yang diterapkan berhasil meningkatkan keamanan jaringan, terutama dalam menghadapi serangan DDoS, sehingga server dapat tetap beroperasi secara efektif. Hasil penelitian ini menjadi sumber referensi berharga untuk permasalahan keamanan jaringan dengan solusi penggunaan L2TP dan IPsec (Laksamana et al., 2023).

Penelitian selanjutnya mengenai "Jaringan Virtual Private Network (VPN) Berbasis Mikrotik pada Kantor Kecamatan Marioriawa Kabupaten Soppeng". Penelitian ini bertujuan merancang dan mengimplementasikan jaringan Virtual Private Network (VPN) berbasis Mikrotik di Kantor Kecamatan Marioriawa. Latar belakang masalahnya adalah kebutuhan untuk memiliki jaringan internet yang aman dan terbebas dari gangguan peretasan, terutama karena berisi Data Induk Kependudukan warga Kecamatan Marioriawa yang harus dijaga kerahasiaannya. Solusi yang digunakan adalah metode PPTP (Point to Point Tunnel Protocol) yang diaplikasikan dalam Mikrotik Router, meskipun konfigurasi awalnya kompleks. Hasilnya adalah jaringan yang aman dengan data terenkripsi (Wardana et al., 2022).

Penelitian terakhir berjudul "Analisis Perbandingan Performansi QoS VPN Encryption Protocol Pada Jaringan Berbasis Hybrid Cloud" membahas tentang peningkatan keamanan dan performansi jaringan VPN pada sebuah grup perusahaan yang bergerak di sektor ritel dan industri dengan 975 toko yang tersebar di seluruh Indonesia. Perusahaan ini menggunakan jaringan hybrid cloud yang terdiri dari storage, database, SAP, dan aplikasi pendukung lainnya. Sebagian besar komunikasi antara toko cabang dan kantor pusat menggunakan VPN tunnel jenis EOIP, L2TP, PPTP, dan SSTP tanpa enkripsi yang maksimal, sehingga perlindungan data belum memenuhi standar ISO 27001. Perusahaan ini juga terdaftar sebagai penyelenggara sistem elektronik oleh Kominfo karena mengelola data pelanggan. Oleh karena itu, penelitian ini membandingkan tiga jenis VPN tunnel, yaitu L2TP/IPSec, OpenVPN, dan IKEv2/IPSec, untuk meningkatkan perlindungan data dan kualitas jaringan. Hasil penelitian menunjukkan bahwa IKEv2/IPSec memiliki nilai QoS yang lebih baik dengan throughput rata-rata 22 Mb/s, packet loss 0,12%, delay 0,408 ms, dan jitter 0,408 ms (Madhadi & Banowosari, 2021)

Definisi VPN

VPN (Virtual Private Network) merupakan sebuah koneksi virtual yang bersifat private karena pada dasarnya jaringan tidak terlihat secara fisik melainkan hanya berupa jaringan secara virtual, yang mana tidak semua orang dapat mengaksesnya (Sulistiyono, 2020); (Watrianthos & Nasution, 2018); . VPN (Virtual Private Network) digunakan untuk kegiatan seperti transmisi paket data, yang terenkripsi sehingga akan cukup sulit disadap oleh pihak yang tidak berwenang (Madhadi & Banowosari, 2021).

Menurut (F. Sjafrina et al., 2019) Virtual Private Network (VPN) adalah perluasan jaringan private pada jaringan public yang memungkinkan user dapat melakukan pengiriman dan mendapatkan informasi melalui lintas koneksi yang disatukan atau jaringan public yang seolah-olah sebagai koneksi langsung dengan sistem tertutup.

Pengertian lain mengenai Virtual Private Network (VPN) adalah sebuah jaringan private yang menghubungkan satu node jaringan ke node jaringan lainnya dengan menggunakan jaringan internet (Lukman & Bachtiar, 2018); (Khasanah & Utami, 2018). Data yang dilewatkan akan di encapsulation (dibungkus) dan dienkripsi supaya data tersebut terjamin kerahasiaannya. perusahaan (A. G. P. Sjafrina, 2019). Virtual Private Network (VPN) adalah fasilitas yang memungkinkan koneksi jarak jauh (remote access) menggunakan jaringan publik untuk akses Local Area Network (LAN) pada suatu perusahaan.

Definisi IPSec

IP Security (IPSec) merupakan sekumpulan standar protokol yang menyediakan keamanan dan kerahasiaan dalam pertukaran data di layer network (Hidayatulloh, 2014). Melalui IPSec keamanan jaringan komputer lebih terjamin karena menggunakan sistem autentifikasi yakni teknik otentikasi dan enkripsi. Otentikasi bertujuan untuk mengecek keaslian sumber paket data apakah benar paket yang dikirimkan seperti yang tertera di header paket atau merupakan paket dari sumber yang dipalsukan (spoofing). Teknik kedua IPSec adalah enkripsi, tujuannya untuk menjaga kerahasiaan (confidentiality) dari paket data yang dikirim yang artinya paket tersebut hanya boleh dibaca oleh penerima yang dituju. Proses enkripsi bekerja dengan cara mengubah data berbentuk teks biasa (plain text) menjadi kode acak yang tidak bisa dibaca (cipher text). Proses perubahan ini menggunakan algoritma enkripsi dan kunci enkripsi (encryption key) dimana kunci enkripsi tersebut disebut juga sebagai kunci kriptografi (cryptographic key) (Sjafrina et al., 2019).

Menurut (Arlan et al., 2016) Internet Protocol Security (IPSec) merupakan sebuah metode enkripsi yang digunakan untuk melindungi kerahasiaan, dan keutuhan data pengguna layanan di jaringan internet. IPSec merupakan jalur data antara komputer atau perangkat pengguna pada jaringan VPN, jalur data hanya bisa diakses dikedua ujung tunnel yang di enkapsulasi. Paket IPSec melewati satu ujung tunnel yang lain dan berisi paket data yang dipertukarkan antara pengguna lokal dengan jaringan private. Enkripsi paket data

dapat memastikan bahwa data tidak dapat dirusak dimanupulasi dan dibajak pihak ketiga yang berusaha mengakses data diluar koneksi IPSec.

Definisi IKEV2

IKEV2 adalah kombinasi protokol IKEV1, ISAKMP dan oakley. IKEV1 dan ISAKMP menentukan cara dua pihak tunnel membentuk security association. oakley memberikan kerahasiaan yang sempurna dengan menggunakan algoritma pertukaran kunci diffie-hellman. Pihak IKEV2 dapat mengidentifikasi diri mereka sendiri dengan certificate, yaitu protokol otentikasi yang diperluas, atau kunci yang dibagikan sebelumnya di kedua sisi tunnel, dengan menggunakan kunci yang dibagikan se- belumnya dalam bentuk kata sandi sederhana dan dikenal oleh kedua belah pihak. IKEV2 berfungsi dalam pertukaran pesan, setiap pesan permintaan yang valid akan memiliki satu pesan balasan yang sesuai. Setiap IKE SA memiliki initiator dan responder. Peran initiator diberikan kepada pihak yang mengirim permintaan Inisialisasi. Sesi IKE dimulai dengan bertukar pesan inisialisasi dan authentication. Setelah mengatur IKE SA, keduanya membuat lebih banyak SA atau mulai mentransfer informasi.

Mikrotik adalah nama perusahaan pemegang lisensi mikrotik yang berlokasi di Riga, ibukota Latvia (Jambak et al., 2022). Mikrotik menyediakan software dan hardware router mikrotik. Dengan mikrotik maka teknologi internet menjadi lebih cepat, handal dan terjangkau untuk kalangan pengguna yang lebih luas. Mikrotik RouterOS adalah sebuah software yang berfungsi mengubah PC (komputer) menjadi sebuah router. Mikrotik RouterOS layaknya IOS cisco yang diinstall di dalam Router Cisco, hanya saja IOS cisco tidak bisa diinstall di dalam komputer kecuali menggunakan emulator seperti GNS3 dan dinamis. Pada dasarnya RouterOS merupakan sistem operasi Mikrotik RouterBoard yang berbasis kernel Linux v2.6. Selain install di dalam PC, Mikrotik RouterOS juga bisa diinstall pada sebuah hardware khusus yang bernama RouterBoard. Ketika kita membeli sebuah Mikrotik RouterBoard biasanya sudah terinstall RouterOS di dalamnya.

Mikrotik router OS merupakan Operating System perangkat lunak yang dibentuk khusus pada jaringan router (Zamzami, 2013). Mikrotik Router dikembangkan dari kernel linux dan didesain dengan tujuan memberikan kemudahan kepada penggunanya. Manajemen bisa dilakukan dengan menggunakan aplikasi winbox. Mikrotik memberi service terhadap ISP untuk penggunan bantuan saluran internet di seluruh dunia.

METODE PENELITIAN

Pada bagian ini, penulis akan menjelaskan dengan rinci bahan-bahan yang digunakan dalam penelitian serta alat-alat yang diperlukan untuk menjalankan eksperimen dan implementasi dalam penelitian yang berjudul "Integrasi Server On-Premise dengan

Server Cloud menggunakan Cloud VPN dan MikroTik IPsec untuk Peningkatan Keamanan Koneksi."

Bahan yang akan digunakan dalam penelitian ini meliputi server onpremise, server cloud, metode, dan teknik dalam penelitian.

Bahan penelitian ini merinci konsep server onpremise yang menjadi fokus utama penelitian. Konsep ini akan didemonstrasikan melalui infrastruktur yang dibangun pada layanan Google Cloud dalam dua proyek GCP yang berbeda, yaitu (thanos-onprem) dan (thanos-cloud). Meskipun ini adalah demonstrasi prototipe, konsepnya relevan dengan infrastruktur fisik yang ada di lingkungan onpremise. Berikut adalah rinciannya:

Bahan penelitian ini mencakup server onpremise yang digunakan dalam penelitian. Server ini menjadi fokus utama penelitian dan mencakup:

- Spesifikasi Teknis Server On-Premise: Server ini merupakan perangkat fisik yang digunakan dalam lingkungan onpremise. Spesifikasi mencakup tipe perangkat keras, sistem operasi, serta konfigurasi jaringan yang relevan.
- Data Proses Bisnis: Data dan informasi yang mendeskripsikan proses bisnis yang menjadi obyek integrasi, seperti prosedur pembayaran gaji dan proses operasional lainnya yang relevan dengan tujuan penelitian.

Server Cloud juga menjadi bahan penelitian utama, berikut adalah cakupan bahan yang menjadi fokus utama:

- Penyedia Layanan Cloud: Penjelasan tentang penyedia layanan cloud yang digunakan yakni Google Cloud.
- Spesifikasi Server Cloud: Deskripsi spesifikasi server virtual yang digunakan di lingkungan cloud, termasuk jumlah sumber daya komputasi, sistem operasi, dan layanan yang digunakan dalam integrasi.

Alat yang akan digunakan dalam penelitian ini meliputi perangkat keras, perangkat lunak.

Dalam penelitian dibutuhkan perangkat keras dengan spesifikasi minimum seperti yang dapat dilihat pada Tabel 1.

Tabel 1 Perangkat Keras

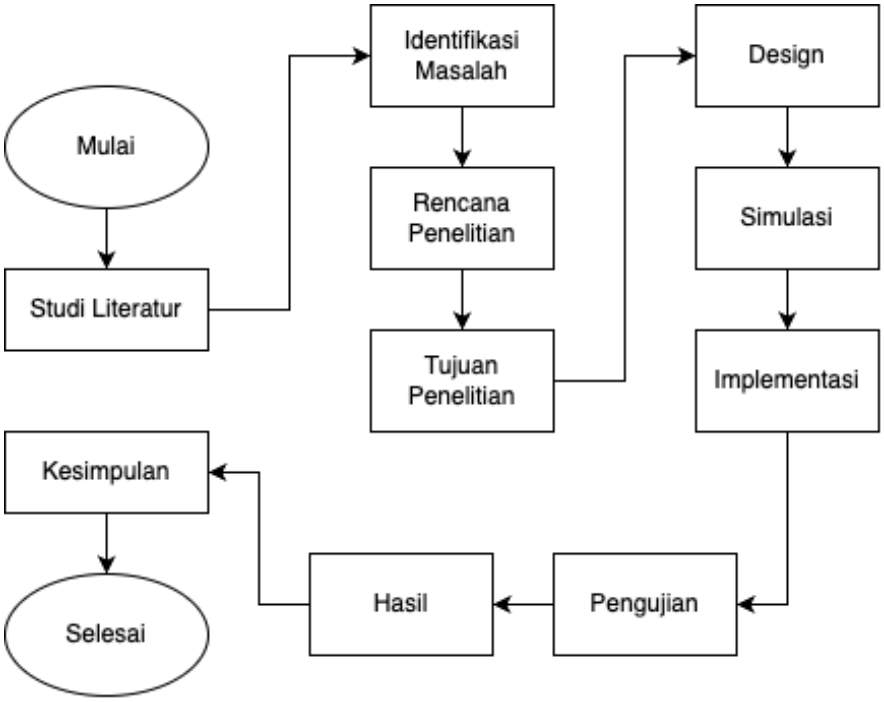
Hardware	Spesifikasi
Jenis Laptop	Macbook Air M2
Processor	Apple Silicone M2 CPU 8-core @3.5 GHz
Memory	8 GB
Storage	256 GB
Display	(2560 x 1664) 60Hz

Perangkat lunak yang digunakan dalam penelitian ini dapat dilihat pada Tabel 2.

Tabel 2 Perangkat Lunak

Software	Spesifikasi
Sistem Operasi	MacOS Sonoma versi 14.0
Web Browser	Google Chrome versi 117.0.59
Web Server	Nginx versi 1.21.4
Bahasa Pemrograman	PHP versi 7.4
Database Server	MySQL Server versi 8.0.34
Database Client	MySQL Client
Microsoft Word	Microsoft 365

Penelitian ini mengikuti serangkaian tahap-tahap untuk mencapai hasil yang diinginkan. Tahap-tahap penelitian ini digambarkan dalam Gambar 3.1.



Gambar 1 Jalan Penelitian

Selanjutnya jelaskan tahap-tahap yang tertera pada Gambar 3.1 tersebut, dipisah menjadi Sub-Bab, misalnya :

Pada tahap ini, penelitian dimulai dengan pemahaman mendalam tentang tantangan keamanan koneksi antara server on-premise dan server cloud. Ini melibatkan

pembelajaran tentang berbagai teknologi keamanan, termasuk Cloud VPN dan MikroTik IPsec. Penelitian literatur dan analisis informasi awal juga dilakukan untuk memahami konsep integrasi server on-premise dan cloud.

Tahap desain melibatkan perencanaan infrastruktur dan arsitektur yang akan digunakan dalam penelitian ini. Hal ini dibagi menjadi beberapa sub-bab:

Berikut merupakan topologi kondisi saat ini Sebuah perusahaan yang kondisi existing saat ini sudah memiliki hybrid infrastructure yakni onpremise server yang berada di internal gedung perusahaan dan cloud server yang berada di Google Cloud. Namun koneksi antara keduanya masih terekspose secara public menggunakan public IP Address yang mana less secure dari segi security.

Tahapan implementasi penelitian ini, penulis akan mendemonstrasikan kedua tipe infrastructure pada layanan Google Cloud Platform dengan cara memisahkannya kedalam project yang terpisah sehingga konsep onpremise dan cloud tetap akan berfungsi sebagai mana mestinya. Alasan penulis melakukan demonstrasi pada layanan Google Cloud Platform secara keseluruhan dikarenakan keterbatasan pengadaan akomodasi dalam hal lain yakni biaya, dimana pada layanan Google Cloud Platform menyediakan *free-trial* selama 90 hari untuk semua resource pada layanan tersebut. Project yang akan dibuat diberikan penamaan **(thanos-onprem)** dan **(thanos-cloud).** Project **(thanos-onprem)** digunakan untuk prototyping infrastructure onprem, kemudian project **(thanos-cloud)** digunakan untuk prototyping infrastructure cloud, sehingga kedua konsep infrastructure dibuat secara terpisah menggunakan 2 project berbeda, dimana langkah-langkahnya sebagai berikut:

1. Langkah pertama adalah memastikan infrastructure cloud telah tersedia. Penulis telah mempersiapkan infrastructure cloud pada Google Cloud Platform dengan nama project **(thanos-cloud)**, selanjutnya penulis membuat custom VPC network baru. VPC ini merupakan resource untuk membuat dan mengelola jaringan pribadi di lingkungan Google Cloud Platform, dimana VPC yang akan dibuat akan menggunakan IP range subnet 172.16.10.0/24
2. Langkah kedua membuat firewall rule untuk memfilter port mana saja yang boleh diizinkan, lalu mendefinisikan spesifik target tags firewall untuk diapply pada resource VM mana saja. Penulis mengizinkan port TCP 20, 21, 22, 80, 443, 888, 3306, 7800, 8291 beserta ICMP.
3. Membuat IP External Static dan IP Internal Static untuk kebutuhan IP Address pada VM web-server. IP External tidak dapat penulis definisikan secara manual. IP Internal dapat didefinisikan secara manual, untuk IP Internal yang digunakan adalah 172.16.10.10
4. Membuat IP External Static untuk kebutuhan IP Address pada Cloud VPN. IP External tidak dapat penulis definisikan secara manual.

5. Langkah selanjutnya membuat VM web-server dengan Ubuntu 22.04 LTS sebagai Operating System, menambahkan network tags sesuai dengan nama target tags yang telah dibuat pada langkah pembuatan firewall rule.
6. Melakukan konfigurasi pada web-server, pada penelitian ini penulis akan menginstall aaPanel sebagai panel web-server dengan mengikuti panduan berikut: Setelah proses instalasi aaPanel selesai, selanjutnya penulis akan menginstall beberapa dependency seperti nginx, php54, php74, dan phpmMyAdmin
7. Kemudian melakukan setting remote database dari web-server ke database-server, penulis memasukkan IP Internal database-server yakni: 192.168.10.10
8. Selanjutnya penulis akan membuat website, yang mana penulis menggunakan domain yang sudah aktif, serta penulis telah mengarahkan dns domain tersebut mengarah ke IP External dari web-server. Website yang akan digunakan
9. Kemudian mengkonfigurasi file koneksi.php yang berisi konfigurasi untuk menghubungkan website pada web-server ke backend database-server
10. Selanjutnya penulis akan membuat Cloud VPN dengan memilih Classic VPN sebagai opsi pilihan:
    11. Selanjutnya mengisikan nama, deskripsi pada VPN gateway. Kemudian memilih network, region, dan IP External yang sebelumnya sudah dibuat untuk Cloud VPN
    12. Mengisikan nama, deskripsi, dan remote peer IP address dengan IP External mikrotik-server. Kemudian penulis memilih IKEv2, lalu menggenerate IKE pre shared key yang nanti akan digunakan pada saat setup IPsec pada mikrotik-server. Selain itu penulis memilih opsi routing route-based dan memasukkan IP Internal dari mikrotik-server serta database-server.
    13. Langkah terakhir pada Infrastructure Cloud adalah dengan membuat routing dari cloud ke onprem.
    14. Pada tahapan demonstrasi selanjutnya ini akan berfokus pada infrastructure onpremise yang mana penulis telah mempersiapkan infrastructure onpremise pada Google Cloud Platform dengan nama project **(thanos-onprem)**, selanjutnya penulis membuat custom VPC network baru. VPC ini merupakan resource untuk membuat dan mengelola jaringan pribadi di lingkungan Google Cloud Platform, dimana VPC yang akan dibuat akan menggunakan IP range subnet 192.168.10.0/24
    15. Langkah kedua membuat firewall rule untuk memfilter port mana saja yang boleh diizinkan, lalu mendefinisikan spesifik target tags firewall untuk diapply pada resource VM mana saja. Penulis mengizinkan port TCP 22, 80, 443, 3306, 8080, 8291 beserta ICMP.
    16. Membuat IP External Static dan IP Internal Static untuk kebutuhan IP Address pada VM mikrotik-server. IP External tidak dapat penulis definisikan secara manual. IP

Internal dapat didefinisikan secara manual, untuk IP Internal yang digunakan adalah 192.168.10.250

17. Membuat IP Internal Static untuk kebutuhan VM database-server, dimana untuk IP Internal yang digunakan adalah 172.16.10.10
18. Langkah selanjutnya membuat VM database-server dengan Ubuntu 22.04 LTS sebagai Operating System, menambahkan network tags sesuai dengan nama target tags yang telah dibuat pada langkah pembuatan firewall rule.
19. Setelah VM database-server terdeploy, penulis menginstall mysql-server dengan menjalankan command berikut pada terminal database-serverKemudian mengubah default password root mysql
20. Membuat user baru dan mengizinkan user baru tersebut untuk melakukan koneksi database secara remote
21. Kemudian download file .sh berikut dan jalankan script tersebut untuk mengizinkan koneksi database secara remote.
22. Tahap selanjutnya adalah membuat database dan mengimport database dummy ke database yang sudah disiapkan penulis
23. Langkah selanjutnya mengunduh RAW disk image Mikrotik CHR v6.49.10 pada website official berikut: https://mikrotik.com/download
24. Kemudian membuat Google Cloud Storage (Bucket) untuk kebutuhan upload RAW disk image Mikrotik yang sebelumnya telah didownload. Pada tahapan ini penulis perlu memberikan penamaan pada Bucket, location type, storage class, dan access control bucket tersebut.
25. Mengupload RAW disk image Mikrotik v6.49.10 ke GSC (Bucket)
26. Membuat image VMDK/VHD menggunakan RAW disk image Mikrotik v6.49.10 yang sudah diupload ke GSC (Bucket)
27. Melakukan konfigurasi mikrotik-server dimulai dari meremote mikrotik-server menggunakan software winbox
28. Melakukan konfigurasi IPsec pada menu IP > IPsec dengan membuat Profiles terlebih dahulu kemudian memilih Enkripsi Algoritma dan DH Group yang akan penulis digunakan:
29. Menambahkan IPsec Peers seperti berikut (isikan IP dari Cloud VPN), lalu pilih Profile yang sudah dibuat pada langkah sebelumnya, dan pilih Exchange Mode menggunakan IKEv2.
30. Kemudian setting IPsec Identity, pilih IPsec Peers yang sudah dibuat dengan auth method menggunakan pre shared key, lalu untuk secret isikan dengan secret IKEv2 yang didapat pada saat setup Cloud VPN nantinya. Setelah itu bisa memilih Policy Group Template yang sebelumnya sudah dibuat juga.

31. Membuat IPsec Proposal dengan Algorithms aes-256-cbc dan sha256
32. Membuat IPsec Policy. Pada tab General, penulis memilih Peer yang sebelumnya sudah dibuat, lalu mengenable Tunnel, dilanjutkan dengan memasukkan Source Address dengan Subnet IP Internal Infrastructure Onpremise, dan Destination Address dengan Subnet IP Internal Infrastructure Cloud.
33. Masih pada menu IPsec Policy, penulis berpindah ke tab menu Action. Pada menu tersebut penulis memilih Action Ecrypt, lalu memilih Proposal menggunakan Proposal yang sebelumnya sudah dibuat. Selanjutnya penulis berpindah tab ke Status untuk mengecek status konektivitas apakah sudah established atau belum.
34. Langkah terakhir adalah membuat routes dari onprem ke cloud

HASIL DAN PEMBAHASAN

Penelitian ini menghasilkan beberapa temuan penting terkait dengan integrasi server onpremise dan server cloud menggunakan teknologi Cloud VPN dan MikroTik IPsec. Berikut adalah beberapa hasil utama yang ditemukan:

Konfigurasi Infrastruktur On-Premise (thanos-onprem):

- Pada proyek (thanos-onprem), telah berhasil dikonfigurasi sebuah VM MikrotikCHR yang berfungsi sebagai perangkat pembangun IPsec Tunnel.
- MikrotikCHR telah dikonfigurasi dengan dua antarmuka, satu mengarah ke internet dan satu lainnya terhubung ke VM database menggunakan alamat IP internal.
- Firewall pada MikrotikCHR diatur untuk memberikan akses terbatas, sehingga hanya IP tertentu yang diizinkan untuk berkomunikasi.

Konfigurasi Infrastruktur On-Cloud (thanos-cloud):

- Pada proyek (thanos-cloud), telah berhasil dikonfigurasi sebuah VM yang berisi aplikasi front-end internal tanpa alamat IP publik.
- Terdapat konfigurasi Cloud VPN menggunakan Hybrid Connectivity, dengan penerapan kedua tipe VPN, yaitu Classic VPN dan HA VPN.
- Pilihan jatuh pada penggunaan Classic VPN untuk menghubungkan server onpremise dan cloud, yang membantu dalam melindungi koneksi.

Analisis dan Pembahasan

Pada bagian ini, kami akan melakukan analisis terhadap hasil penelitian dan membahas implikasinya. Hasil ini akan dianalisis dalam konteks metodologi penelitian yang digunakan, serta keamanan koneksi antara server onpremise dan cloud.

Keamanan Koneksi:

- Penggunaan Cloud VPN dan MikroTik IPsec telah meningkatkan keamanan koneksi antara server onpremise dan cloud secara signifikan. Alamat IP internal digunakan untuk koneksi, mengurangi risiko terpapar secara langsung ke internet.
- Implementasi IPsec memberikan enkripsi lalu lintas, menjaga integritas data, dan otentikasi, yang sangat penting dalam mengamankan koneksi jaringan.

Kemungkinan Ancaman Terhadap Keamanan:

- Dengan menggunakan metode ini, risiko seperti sniffing, bruteforce, dan serangan DDoS berkurang drastis. Koneksi kini lebih aman dari potensi serangan kejahatan siber

Skenario Use Case:

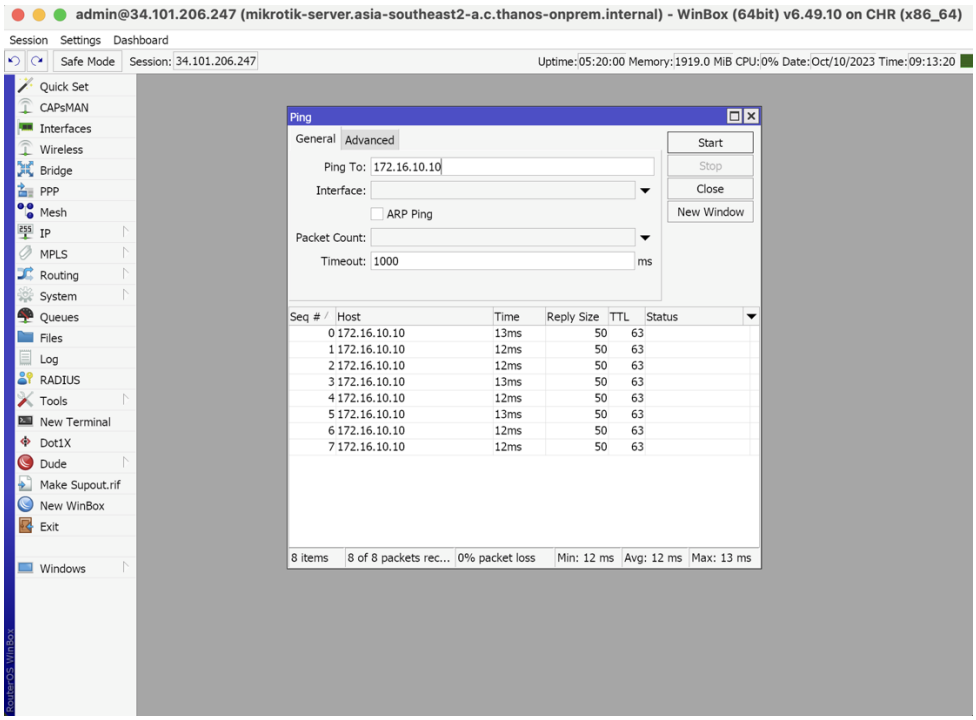
- Hasil penelitian ini memberikan wawasan pada situasi di mana perusahaan hanya diakses oleh tim internal, dan eksposur publik tidak diperlukan. Ini dapat menjadi panduan berharga bagi perusahaan dengan kebutuhan serupa.

Pengembangan dan Penerapan Lainnya:

- Hasil penelitian ini dapat diaplikasikan pada lingkungan yang lebih luas, baik onpremise maupun cloud. Penggunaan MikroTik dan Cloud VPN memberikan fleksibilitas dalam membangun koneksi yang aman.

Tes Konektivitas PING:

- Melakukan ping dari router **mikrotik-server** (onpremise) ke alamat ip internal **web-server** yang berada pada infrastructure cloud.



Gambar 1 PING mikrotik-server ke web-server

- Melakukan ping dari **database-server** (onpremise) ke ip internal **web-server** yang berada pada infrastructure cloud.

```
support@database-server:~$ ping 172.16.10.10 -c 10
PING 172.16.10.10 (172.16.10.10) 56(84) bytes of data.
64 bytes from 172.16.10.10: icmp_seq=1 ttl=62 time=17.1 ms
64 bytes from 172.16.10.10: icmp_seq=2 ttl=62 time=16.0 ms
64 bytes from 172.16.10.10: icmp_seq=3 ttl=62 time=16.1 ms
64 bytes from 172.16.10.10: icmp_seq=4 ttl=62 time=15.9 ms
64 bytes from 172.16.10.10: icmp_seq=5 ttl=62 time=16.0 ms
64 bytes from 172.16.10.10: icmp_seq=6 ttl=62 time=16.2 ms
64 bytes from 172.16.10.10: icmp_seq=7 ttl=62 time=16.0 ms
64 bytes from 172.16.10.10: icmp_seq=8 ttl=62 time=16.0 ms
64 bytes from 172.16.10.10: icmp_seq=9 ttl=62 time=16.2 ms
64 bytes from 172.16.10.10: icmp_seq=10 ttl=62 time=16.0 ms

--- 172.16.10.10 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9011ms
rtt min/avg/max/mdev = 15.942/16.170/17.141/0.335 ms
support@database-server:~$
```

Gambar 2 PING database-server ke web-server

- Melakukan ping dari **web-server** (cloud) ke ip internal **mikrotik-server** yang berada pada infrastructure onpremise.

```
support@web-server:~$ ping 192.168.10.250 -c 10
PING 192.168.10.250 (192.168.10.250) 56(84) bytes of data.
64 bytes from 192.168.10.250: icmp_seq=1 ttl=63 time=15.9 ms
64 bytes from 192.168.10.250: icmp_seq=2 ttl=63 time=13.7 ms
64 bytes from 192.168.10.250: icmp_seq=3 ttl=63 time=14.1 ms
64 bytes from 192.168.10.250: icmp_seq=4 ttl=63 time=14.0 ms
64 bytes from 192.168.10.250: icmp_seq=5 ttl=63 time=13.9 ms
64 bytes from 192.168.10.250: icmp_seq=6 ttl=63 time=13.7 ms
64 bytes from 192.168.10.250: icmp_seq=7 ttl=63 time=13.7 ms
64 bytes from 192.168.10.250: icmp_seq=8 ttl=63 time=13.8 ms
64 bytes from 192.168.10.250: icmp_seq=9 ttl=63 time=14.0 ms
64 bytes from 192.168.10.250: icmp_seq=10 ttl=63 time=13.7 ms

--- 192.168.10.250 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/mdev = 13.670/14.056/15.920/0.639 ms
support@web-server:~$
```

Gambar 3 PING web-server ke mikrotik-server

- Melakukan ping dari **web-server** (cloud) ke ip internal **database-server** yang berada pada infrastructure onpremise.

```
support@web-server:~$ ping 192.168.10.10 -c 10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
64 bytes from 192.168.10.10: icmp_seq=1 ttl=62 time=16.1 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=62 time=14.0 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=62 time=13.9 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=62 time=14.3 ms
64 bytes from 192.168.10.10: icmp_seq=5 ttl=62 time=13.9 ms
64 bytes from 192.168.10.10: icmp_seq=6 ttl=62 time=13.8 ms
64 bytes from 192.168.10.10: icmp_seq=7 ttl=62 time=14.0 ms
64 bytes from 192.168.10.10: icmp_seq=8 ttl=62 time=14.0 ms
64 bytes from 192.168.10.10: icmp_seq=9 ttl=62 time=14.0 ms
64 bytes from 192.168.10.10: icmp_seq=10 ttl=62 time=14.0 ms

--- 192.168.10.10 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9012ms
rtt min/avg/max/mdev = 13.792/14.196/16.126/0.656 ms
support@web-server:~$
```

Gambar 4 PING mikrotik-server ke database-server

Tes Konektivitas Traceroute:

- Melakukan traceroute dari **database-server** (onpremise) ke alamat ip internal **web-server** yang berada pada infrastructure cloud.

```
support@database-server:~$ traceroute 172.16.10.10
traceroute to 172.16.10.10 (172.16.10.10), 30 hops max, 60 byte packets
 1  mikrotik-server.asia-southeast2-a.c.thanos-onprem.internal (192.168.10.250)  2.056 ms  2.012 ms  1.991 ms
```

Gambar 5 Traceroute database-server ke web-server

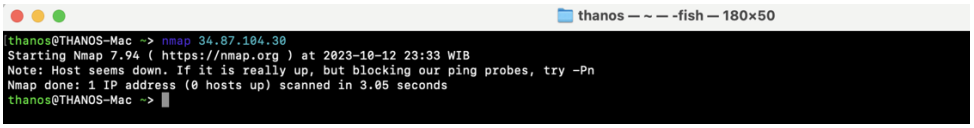
- Melakukan traceroute dari **web-server** (cloud) ke ip internal **database-server** yang berada pada infrastructure onpremise.

```
support@web-server:~$ traceroute -m 100 192.168.10.10
traceroute to 192.168.10.10 (192.168.10.10), 100 hops max, 60 byte packets
 1  * * *
 2  192.168.10.250 (192.168.10.250)  14.720 ms  14.699 ms  14.678 ms
 3  192.168.10.10 (192.168.10.10)  14.955 ms  14.927 ms  14.898 ms
support@web-server:~$
```

Gambar 6 Traceroute web-server ke database-server

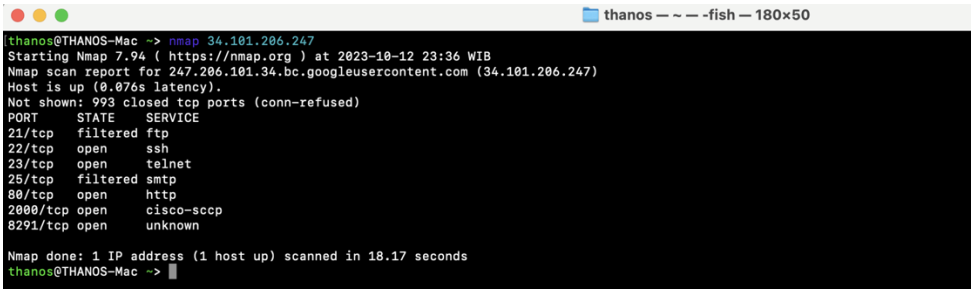
Tes Port Scanning:

- Melakukan nmap dari laptop ke alamat ip external **cloud-vpn** yang berada pada infrastructure cloud.



Gambar 7 Port Scan Laptop ke IP External Cloud VPN

- Melakukan nmap dari laptop ke alamat ip external **mikrotik-server** yang berada pada infrastructure onpremise.

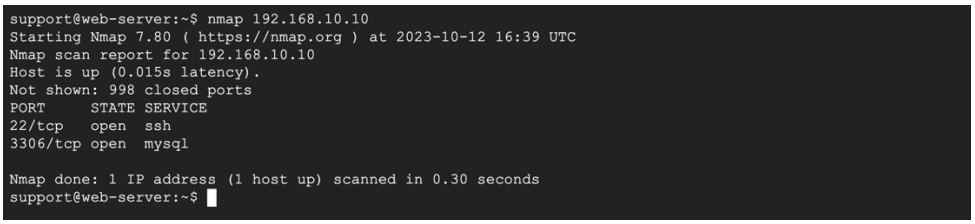


Gambar 8 Port Scan Laptop ke IP External mikrotik-server

- Melakukan nmap dari **web-server** (cloud) ke ip internal **mikrotik-server** yang berada pada infrastructure onpremise.

Gambar 9 Port Scan web-server ke IP Internal mikrotik-server

- Melakukan nmap dari **web-server** (cloud) ke ip internal **database-server** yang berada pada infrastructure onpremise.



Gambar 10 Port Scan web-server ke IP Internal database-server

- Melakukan nmap dari **database-server** (onpremise) ke ip internal **web-server** yang berada pada infrastructure cloud.

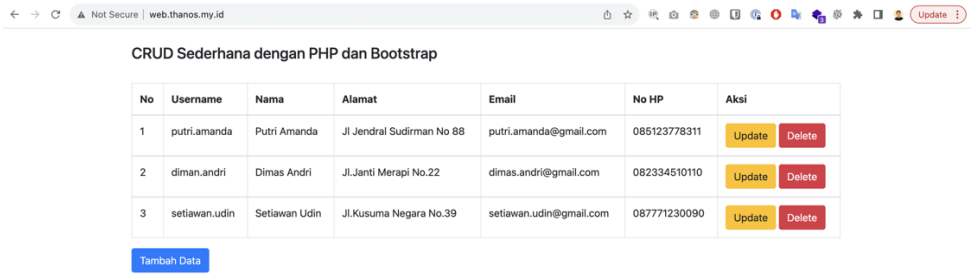
```
support@database-server:~$ nmap 172.16.10.10
Starting Nmap 7.80 ( https://nmap.org ) at 2023-10-12 16:41 UTC
Nmap scan report for 172.16.10.10
Host is up (0.016s latency).
Not shown: 994 filtered ports
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   closed ftp
22/tcp   open   ssh
80/tcp   open   http
888/tcp  open   accessbuilder
7800/tcp open   asr

Nmap done: 1 IP address (1 host up) scanned in 4.34 seconds
support@database-server:~$
```

Gambar 11 Port Scan database-server ke IP Internal web-server

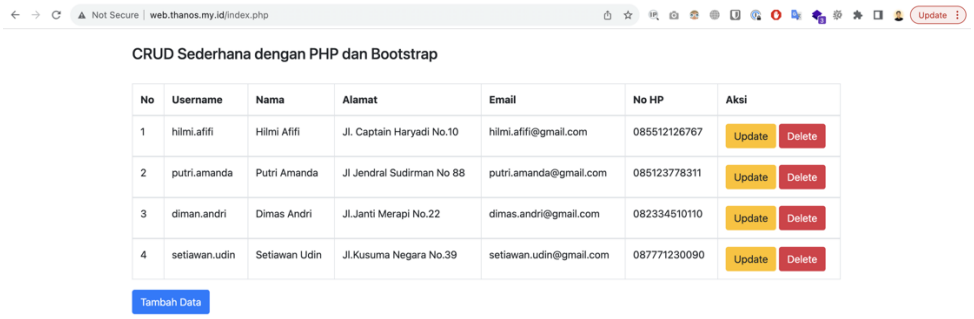
Tes Website CRUD:

- Kondisi saat ini website sudah dapat diakses dan menampilkan data yang berasal dari database-server



Gambar 12 Dashboard Website CRUD

- Kemudian kita coba menambahkan data dan berhasil sebagai berikut



Gambar 13 Test Fungsi CRUD

Demikianlah hasil penelitian ini menunjukkan bahwa integrasi server onpremise dengan server cloud menggunakan Cloud VPN dan MikroTik IPsec adalah solusi yang efektif dalam meningkatkan keamanan koneksi. Hasil penelitian ini dapat memberikan panduan bagi organisasi yang ingin mengimplementasikan solusi serupa dalam lingkungan mereka.

KESIMPULAN

Hasil penelitian ini mengungkapkan berbagai temuan penting terkait dengan integrasi server onpremise dan server cloud menggunakan teknologi Cloud VPN dan MikroTik IPsec.

Dalam konfigurasi on-premise, berhasil dilakukan konfigurasi VM MikrotikCHR sebagai perangkat pembangun IPsec Tunnel, dilengkapi dengan dua antarmuka yang satu mengarah ke internet dan yang lain terhubung ke VM database menggunakan alamat IP internal. Firewall pada MikrotikCHR diatur untuk memberikan akses terbatas hanya kepada IP tertentu. Pada sisi on-cloud, berhasil dikonfigurasi VM yang berisi aplikasi front-end di proyek thanos-cloud untuk terhubung ke back-end server di proyek thanos-onprem. Terapkan konfigurasi Cloud VPN Hybrid Connectivity dengan penggunaan tipe Classic VPN IKEv2, dengan keputusan menggunakan Classic VPN sebagai solusi untuk menghubungkan server on-premise dan cloud, membantu melindungi koneksi.

Dalam aspek keamanan koneksi, penggunaan Cloud VPN dan MikroTik IPsec secara signifikan meningkatkan keamanan koneksi antara server on-premise dan cloud. Penggunaan alamat IP internal mengurangi risiko eksposur langsung ke internet. Implementasi IPsec memberikan enkripsi lalu lintas, menjaga integritas data, dan otentikasi yang penting dalam mengamankan koneksi jaringan. Ancaman terhadap keamanan seperti sniffing, bruteforce, dan serangan DDoS berkurang secara signifikan, membuat koneksi lebih aman dari potensi serangan kejahatan siber.

Skenario use case di mana perusahaan hanya diakses oleh tim internal, dan eksposur publik tidak diperlukan, memberikan panduan berharga bagi perusahaan dengan kebutuhan serupa. Pengembangan dan penerapan lebih lanjut dari hasil penelitian ini dapat diaplikasikan pada lingkungan yang lebih luas, baik on-premise maupun cloud. Penggunaan MikroTik dan Cloud VPN memberikan fleksibilitas dalam membangun koneksi yang aman. Dengan demikian, penelitian ini menegaskan bahwa integrasi server on-premise dengan server cloud menggunakan Cloud VPN dan MikroTik IPsec adalah solusi efektif dalam meningkatkan keamanan koneksi, memberikan panduan bagi organisasi yang ingin mengimplementasikan solusi serupa dalam lingkungan mereka.

BIBLIOGRAFI

Arlan, R., Munadi, R., & Andini, N. (2016). Implementasi Dan Analisis Sistem Keamanan Ip Security (ipsec) Di Dalam Multi Protocol Label Switching-virtual Private Network (mpls-vpn) Pada Layanan Berbasis Ip Multimedia Subsystem (ims). *EProceedings of Engineering*, *3*(3).

Hidayatulloh, S. (2014). Analisis dan optimalisasi keamanan jaringan menggunakan protokol ipsec. *Jurnal Informatika*, *1*(2).

Jambak, A.-H., Aspriyono, H., & Al Akbar, A. (2022). Computer Network Management Using a Mikrotik Router at the Immigration Office Class I TPI Bengkulu City. *Jurnal Media Computer Science*, *1*(1), 7–13.

Jamil, M., & Rosihan, A. F. (2016). *Buku Ajar Cloud Computing*. Deepublish.

Khasanah, S. N., & Utami, L. A. (2018). Implementasi Failover Pada Jaringan WAN Berbasis VPN. *Jurnal Teknik Informatika STMIK Antar Bangsa, IV (1)*, 62–66.

Laksamana, P., Suharyanto, S., & Cahaya, Y. F. (2023). Determining factors of continuance intention in mobile payment: fintech industry perspective. *Asia Pacific Journal of Marketing and Logistics*, *35*(7), 1699–1718.

Lukman, A. M., & Bachtiar, Y. (2018). Analisis Sistem Pengelolaan, Pemeliharaan dan Keamanan Jaringan Internet Pada IT Telkom Purwokerto. *Jurnal Khatulistiwa Informatika*, *6*(2), 486692.

Madhadi, T. E., & Banowosari, L. Y. (2021). Analisis Perbandingan Performasi QoS VPN Encryption Protocol Pada Jaringan Berbasis Hybrid Cloud: Array. *Jurnal Ilmiah Komputasi*, *20*(1), 69–82.

Rachmad, Y. E., Dewantara, R., Junaidi, S., Firdaus, M., & Sulistianto, S. W. (2023). *MASTERING CLOUD COMPUTING (Foundations and Applications Programming)*. PT. Sonpedia Publishing Indonesia.

Rahman, I. K., Mulyana, D. I., & Akbar, Y. (2023). Optimasi IPSec Site to Site VPN Mikrotik menggunakan Algoritme Enkripsi Blowfish. *Progresif: Jurnal Ilmiah Komputer*, *19*(1), 145–154.

Setya, A. A., & Sudaryanto, A. (2021). Analisa Konektivitas Jaringan IPSEC Dan OpenVPN Pada Jaringan Berbasis IP Dinamis. *INFOTRON: Jurnal Ilmiah Teknik Informatika, Elektronika Dan Kontrol*, *1*(1), 1–5.

Sjafrina, A. G. P. (2019). The Impact of Money Politics on the High Costs of Election Winning and Political Corruption. *Journal of Anti-Corruption Integrity*, *5*(1), 43–53.

Sjafrina, F., Arnesia, P. D., & Aqim, A. (2019). Rancang Bangun Jaringan VPN Berbasis IPSec Menggunakan Microtic Routerboard pada PT. Zahir International. *Prosiding SeNTIK STI&K*, *3*.

Sulistiyono, S. (2020). Perancangan Jaringan Virtual Private Network Berbasis Ip Security Menggunakan Router Mikrotik. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 150–164.

Wardana, M. A., Nusri, A. Z., & Juliandika, J. (2022). Jaringan Virtual Private Network (Vpn) Berbasis Mikrotik Pada Kantor Kecamatan Marioriawa Kabupaten Soppeng. *Jurnal Ilmiah Sistem Informasi Dan Teknik Informatika (JISTI)*, *5*(2), 107–116.

Watrianthos, R., & Nasution, M. (2018). Analisa Kemampuan Transver Data Vpn Berbasis Open Source Pada Kondisi Encripsi-Dekscripsi Dan Komprensi-Dekomprensi. *INFORMATIKA*, *6*(1), 23–51.

Zamzami, N. F. (2013). Implementasi load balancing dan failover menggunakan mikrotik router os berdasarkan multihomed gateway pada warung internet" diga",". *DIGA"", Skripsi. UDINUS: Indonesia*.