JIKA (Jurnal of Informatics) UniversitasMuhammadiyah Tangerang *P ISSN : 2549-0710*
Vol 8 No.1, January 2024, pp 66-73 *E ISSN : 2722-2713*
DOI : 10.31000/jika.v8i1.9979

RANCANGAN VIRTUAL PRIVATE NETWORK PADA KANTOR PROLOV MENGGUNAKAN ZEROTIER

Enda Suhadi[1)], Toni Arifin[2)]
[1,2] Program Studi Teknik Informatika, Universitas Adhirajasa Reswara Sanjaya, Bandung
Antapani, Jl. Terusan Sekolah No.1-2, Cicaheum, Kota Bandung
Co Responden Email: endasuhadi@gmail.com

Article history
Received 03 Nov 2023
Revised 29 Nov 2023
Accepted 20 Dec 2023
Available online 27 Jan 2024

Keyword
VPN, VPS, ZeroTier, Virtualisasi

Abstract

The importance of safeguarding data in the current era of digitalization is directly linked to the threats posed by irresponsible entities, such as hackers. Cyber attacks, such as Man in The Middle (MiTM) and Distributed Denial of Service (DDoS), present serious potential risks that can result in information theft and disrupt server performance. MiTM, for instance, is a cyber action aimed at stealing data and monitoring the activities of victims by exploiting insecure internet connections. In the course of its operations, Prolov Office also utilizes internet networks; however, this practice exposes it to security risks due to sharing networks with general internet users when accessing the admin's Virtual Private Server. To address these risks, the implementation of a Virtual Private Network (VPN) is necessary to enhance data security. As a solution, Zerotier is employed as an open and encrypted platform. The objective of this research is to design clear and effective security policies.Following the implementation of Zerotier, the results indicate that Zerotier can function as an open-source VPN with encryption layers. This research has successfully increased the effectiveness of network security at Prolov Office, primarily because Zerotier can be monitored and controlled by administrators, providing convenience in network management.

Riwayat
Diterima 03 Nov 2023
Revisi 29 Nov 2023
Disetujui 20 Des 2023
Terbit 27 Jan 2024

Kata Kunci
VPN, VPS, ZeroTier, Virtualisasi

Abstrak

Pentingnya menjaga keamanan data di era digitalisasi saat ini dapat dihubungkan langsung dengan ancaman yang dihadapi dari pihak-pihak yang tidak bertanggung jawab, seperti hacker. Serangan siber, seperti Man in The Middle (MiTM) dan Distributed Denial of Service (DDoS), menjadi potensi serius yang dapat mencuri informasi serta merusak kinerja server. MiTM, sebagai contoh, merupakan tindakan siber yang bertujuan untuk mencuri data dan memantau aktivitas korban dengan memanfaatkan koneksi internet yang tidak aman. Kantor Prolov, dalam menjalankan operasionalnya, turut menggunakan jaringan internet, namun demikian, hal ini membawa risiko serangan karena berbagi jaringan dengan pengguna internet umum ketika mengakses Virtual Private Server admin. Untuk mengatasi risiko tersebut, diperlukan implementasi Virtual Private Network (VPN) guna memperkuat keamanan data. Sebagai solusi, digunakanlah Zerotier sebagai platform yang terbuka dan terenkripsi. Penelitian ini bertujuan untuk merancang kebijakan keamanan yang jelas dan efektif. Setelah penerapan Zerotier, hasilnya menunjukkan bahwa Zerotier dapat berfungsi sebagai VPN yang bersifat open-source dan memiliki lapisan enkripsi. Penelitian ini berhasil meningkatkan efektivitas keamanan jaringan di Kantor Prolov, terutama karena Zerotier dapat dipantau dan dikontrol oleh administrator, memberikan kemudahan dalam manajemen jaringan.

PENDAHULUAN

Data terhadap informasi yang tidak memiliki keamanan dalam jaringan publik rentan terhadap praktik kejahatan pencurian data dengan penyadapan atau peretasan oleh pihak yang tidak memiliki kepentingan (Mufida et al, 2017) atau kelompok maupun

individu yang tidak memiliki wewenang tanpa bertanggung jawab (Mufida et al, 2017) atau orang yang sama sekali tidak bertanggung jawab (Supriyanto, 2019)., dengan begitu kemanannya tidak menjamin terhadap data tersebut (Febrianti et al, 2021). Dari dasar tersebut, satu alternatif solusi yang ditawarkan yaitu dengan memanfaatkan VPN sebagai pihak ketiga dalam mengamankan jaringan (Patih et al, 2012). Virtual Private Network atau yang bisa disebut VPN, dapat mensimulasi atau meniru dua jaringan dengan lokasinya yang berjauhan untuk saling berkomunikasi dari satu jaringan dengan jaringan lain (Dewi & Sulistiyah, 2022) dengan begitu seolah-olah serangkaian jaringan tersebut berlokasi pada suatu jaringan internet bercakupan luas (Putra et al, 2018).

Jaringan komputer dan internet merupakan dua entitas yang saling terkait dan tidak dapat dipisahkan. Perangkat yang terkoneksi satu sama lain dapat digunakan untuk mengakses dan berbagi data dalam suatu sistem jaringan komputer. VPN, atau Virtual Private Network, adalah suatu jaringan pribadi yang beroperasi di dalam jaringan publik. Dengan VPN, individu yang memiliki otorisasi khusus dapat mengakses jaringan internal dari lokasi eksternal melalui internet. Ini memungkinkan pengguna untuk mencapai sumber daya dan data, serta memperoleh izin yang sama seolah-olah terhubung ke jaringan lokal di lokasi tersebut (Dewi et al., 2020; Subekti, 2020).

Prolov merupakan platform social commerce yang menjadi pionir di Indonesia dalam ranah properti. Platform ini berfungsi sebagai ekosistem digital bagi pengembang, pemasar, dan pembeli properti, baik untuk tujuan hunian maupun investasi. Prolov berdiri di Bandung sejak tahun 2016, bermula dari komunitas propertylovers yang memberikan ruang untuk belajar bersama, berbisnis, dan berbagi peluang bisnis di bidang properti. Hingga saat ini, Prolov telah berhasil membentuk lebih dari 2500 anggota yang tersebar dibanyak wilayah. Kolaborasinya melibatkan ratusan pengembang, bank nasional, kantor jasa penilai properti (kjpp), dan notaris. Melalui kerjasama ini, Prolov berhasil menjual lebih dari 3000 unit berbagai produk properti, termasuk hunian, ruko, rukos, gudang, kantor, hingga kavling. Platform ini menjadi wadah yang sukses untuk mempertemukan berbagai pihak dalam dunia properti. (Prolov,2023)

Prolov mengoperasikan server cloud menggunakan Virtual Private Server (VPS) yang terletak di infrastruktur server Alibaba. Saat ini, Prolov menghadapi tantangan keamanan terkait dengan ketiadaan langkah pengamanan pada bagian admin backend, menyebabkan potensi rentan terhadap serangan dari pihak yang tidak diinginkan. Untuk mengatasi permasalahan ini, Prolov memerlukan perancangan Virtual Private Network (VPN) yang dapat beroperasi di jaringan publik tanpa mengesampingkan aspek keamanan. Solusi ini diharapkan dapat meningkatkan perlindungan terhadap sistem backend, melindungi informasi sensitif, dan mencegah potensi penyusupan.

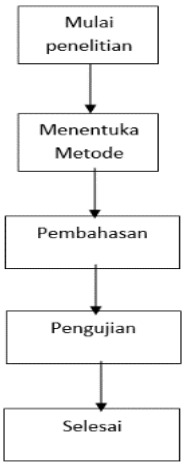
Sebagai bentuk pemikiran kritis terhadap masalah tersebut saya sebagai penulis membuat sebuah solusi, rekomendasi tersebut dengan penggunaan ZeroTier untuk VPN. ZeroTier dianggap cukup mudah dalam proses implementasinya, dimana pengguna atau perusahaan dalam hal ini adalah Prolov hanya perlu membuat akun di platform ZeroTier menggunakan alamat email. Dari akun ZeroTier, dapat dibuatkan sebuag jaringan baru yang dapat dihubungkan oleh setiap pengguna akhir melalui "Network ID" dari jaringan yang dibuat.

Pengguna akhir yang ingin terhubung ke jaringan hanya perlu menginstal aplikasi dari ZeroTier dan bergabung dengan "Network ID" yang telah dibuat sebelumnya. Dengan demikian, setiap pengguna akhir yang terhubung ke satu "Network ID" yang sama dapat berkomunikasi satu sama lain seolah-olah mereka terhubung dengan jaringan lokal kantor. ZeroTier diharapkan dapat menjadi sebuah solusi yang dapat diandalakan dengan jaminan yang telah banyak diketahuti terhadap kraman dan efisiensi dalam mengatasi masalah keamanan data pada bagian admin *back-end* di jaringan perusahaan Prolov. (Stefanus et al, 2022)

METODE PENELITIAN

Pada penelitian yang dilaksanakan oleh poenulis ini memiliki kerangka penelitian yang telah disusun oleh penulis, berikut adalah

kerangka penelitian yang telah disusun dan digunakan.



Gambar 1. Kerangka penelitian

Pada gambar 1 kerangka penelitian yang digunakan adalah.

1. Langkah memulai penelitian adalah menetapkan ruang lingkup penelitian, yang berkaitan dengan permasalahan yang terdapat pada jaringan PT PROLOV.
2. Tahap selanjutnya adalah menentukan metode yang akan digunakan untuk menyelesaikan masalah pada jaringan. Dalam hal ini, metode yang dipilih adalah Zerotier.
3. Pada tahap ini, akan dilakukan pembahasan mengenai implementasi metode Zerotier pada jaringan PT PROLOV. Ini melibatkan analisis dan pemaparan mengenai bagaimana Zerotier akan diterapkan untuk mengatasi permasalahan yang ada.
4. Tahap pengujian merupakan langkah terakhir, di mana implementasi VPN dengan menggunakan Zerotier akan diuji untuk memastikan keberhasilan dan keamanan. Pengujian ini mencakup penilaian terhadap koneksi, kecepatan, serta efektivitas Zerotier sebagai pembatas jaringan.
5. Tahap terakhir ini menandakan penyelesaian dari seluruh proses penelitian, mulai dari penetapan ruang lingkup, pemilihan dari metode, pembahasan, hingga pengujian. Pada tahap ini, semua langkah penelitian telah dilaksanakan dan hasilnya dapat dievaluasi.

TUJUAN PENELITIAN

Melalui upaya yang berkelanjutan dan pemahaman yang mendalam tentang keamanan web, tujuan-tujuan ini dapat membantu melindungi situs web admin dari berbagai ancaman dan menjaga integritas serta kehandalan web admin. Berikut adalah tujuan penelitian:

1. Mengimplemenstasikan zerotier pada vps agar web admin dibagi akses nya dan lalu lintas jaringan lebih aman.
2. Mencoba mengimplementasikan metode zerotier dibandingkan dengan metode yang lainnya.
3. Mencegah akses yang tidak sah ke situs web admin seperti peretasan dan serangan brute force.
4. Memastikan bahwa hanya orang yang memiliki izin yang sesuai yang dapat mengakses dan mengelola situs web admin.

HASIL DAN PEMBAHASAN

Penelitian ini dibangun berdasarkan kerangka beberapa penelitian sebelumnya, salah satunya adalah jurnal penelitian yang berjudul "Rancangan Virtual Private Server Pada Kantor Kelurahan Menggunakan ZeroTier." Dalam penelitian tersebut, Kantor Kelurahan Banyuanyar menghadapi kendala karena menggunakan jaringan yang sama dengan pengguna internet umum, dan belum memiliki server utama sebagai database karena keterbatasan dana dan tenaga teknisi. Akibatnya, kegiatan staf dalam bekerja menjadi lamban dan kurang efektif. Oleh karena itu, diperlukan perancangan Virtual Private Server (VPS) untuk mendukung kinerja kantor kelurahan. Pendekatan yang diambil adalah menggunakan ZeroTier, sebuah solusi VPS dan VPN berbasis open source dengan teknologi terbaru. ZeroTier memungkinkan pengawasan dan kontrol oleh admin, memberikan kemudahan dalam manajemen jaringan.

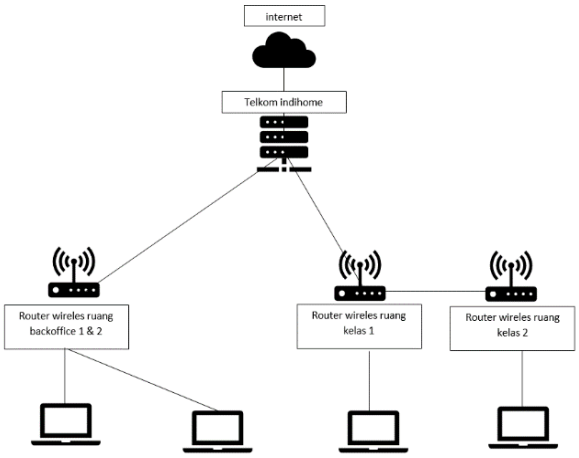
Dengan memanfaatkan jaringan internet yang terhubung ke seluruh desa, ditambah dengan dua server virtual yang dijalankan di

dalam ZeroTier sebagai VPS dan VPN, Kantor Kelurahan Banyuanyar dapat menjalankan fungsi dan tugasnya secara maksimal. Pemanfaatan jaringan yang tersebar di seluruh desa memungkinkan para staf mengakses Virtual Private Server ini di mana saja dan kapan saja tanpa kekhawatiran terkait keamanan. Dengan demikian, penelitian ini mengusulkan solusi yang dapat meningkatkan efisiensi dan efektivitas kinerja Kantor Kelurahan Banyuanyar.

Menurut penelitian selanjutnya adalah jurnal menurut (Putra et al, 2022) Dalam penelitian yang membahas "Penggunaan Virtual Private Network (VPN) pada PT SEMEN BATURAJA (PERSERO) TBK," ditemukan bahwa karyawan PT Semen Baturaja memiliki keinginan untuk terhubung ke jaringan lokal perusahaan di mana pun mereka berada. Oleh karena itu, VPN digunakan sebagai solusi untuk memudahkan para karyawan dalam mengakses jaringan tanpa adanya gangguan, memastikan akses yang lancar dan cepat di seluruh lokasi. Penggunaan Virtual Private Network (VPN) memberikan kemudahan bagi karyawan agar dapat langsung terhubung ke jaringan lokal PT Semen Baturaja tanpa hambatan. Fasilitas ini memainkan peran penting dalam mendukung mobilitas karyawan, memastikan bahwa mereka dapat mengakses sumber daya jaringan perusahaan dengan mudah dan aman dari lokasi mana pun. Dengan adanya VPN, karyawan dapat mengoptimalkan produktivitas mereka tanpa harus terbatas oleh lokasi fisik, sehingga memberikan nilai tambah dalam efisiensi operasional PT Semen Baturaja.

Menurut penelitian selanjutnya adalah jurnal menurut (Firmansyah *et al*, 2019) Dalam penelitian yang membahas "Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP," penggunaan VPN diimplementasikan dengan tujuan mengoptimalkan alokasi penggunaan bandwidth dan mengurangi risiko kebocoran paket data selama proses transfer. Salah satu metode yang umum digunakan adalah VPN IPsec tuneling, yang digunakan untuk menghubungkan berbagai lokasi menjadi satu kesatuan jaringan. Metode ini memastikan perlindungan data selama transfer, baik dari host ke host, network ke network, hingga network ke host, karena paket data yang ditransfer telah dienkripsi. Hasil pengujian jaringan menggunakan VPN dengan algoritma ISAKMP menunjukkan pengurangan hops pada jaringan yang menggunakan tunnel dengan time to live (TTL) sebesar 126, sedangkan jaringan tanpa tunnel memiliki nilai TTL sebesar 124. Temuan ini menunjukkan bahwa implementasi VPN dengan algoritma ISAKMP memberikan dampak positif terhadap performa jaringan dengan mengurangi jumlah hops, sehingga meningkatkan efisiensi transfer data antarlokasi. Selain itu, penggunaan algoritma enkripsi ISAKMP pada VPN juga berkontribusi pada keamanan data dengan memberikan lapisan perlindungan melalui enkripsi paket data yang ditransfer.

Setelah menganalisis jaringan di Prolov, ditemukan bahwa topologi jaringan tang digunakan mengadopsi struktur infrastruktur. Dalam struktur ini, komputer atau laptop terhubung langsung ke router. Untuk mendapatkan akses internet, semua ruangan di Prolov menggunakan layanan Internet Service Provider (ISP). Berikut adalah skema jaringan yang sedang berlaku di PT PROLOV.

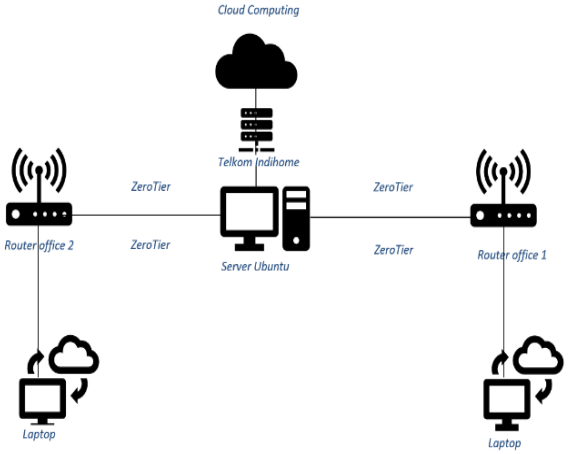


Gambar 3. Skema jaringan saat ini

Pada gambar 2 Skema jaringan saat ini terdiri atas:

a. Indihome digunakan sebagai penyedia layanan internet dengan kecepatan 50 Mbps.
b. Terdapat 3 buah router yang digunakan pada jaringan ini.
c. Ruang *backoffice* 1 dan & 2 berada pada lantai 1 di fasilitas PROLOV.
d. Sedangkan untuk ruang kelas 1 dan & 2 di fasilitas PROLOV berada pada lantai 2.

Permasalahan pada PT PROLOV saat ini adalah tidak ada pembatasan jaringan untuk mengakses ke *admin backend*, karena hal tersebut sangat rentan terhadap penyusupan. Berdasarkan permasalahan tersebut maka pemecahan masalah nya adalah membatasi jaringan untuk dapat mengakses web admin agar hanya orang tertentu saja yang dapat membukan halaman admin. Berikut skema jaringan usulan.



Gambar 3. Skema jaringan usulan

Pada gambar 3 setiap koneksi ke web admin harus melalui jaringan VPN yang sudah terdaftar di *management network* Zerotier.

Jaringan usulan merupakan salah satu gagasan yang dirancang penulis untuk mengatasi masalah yang sedang terjadi dari suatu jaringan komputer yang telah ada, dalam hal ini pembuatan jaringan Virtual Private Network (VPN) dan perubahan desain topologi jaringan komputer di Kantor Prolov.

Penulis mengusulkan untuk tetap memanfaatkan semua insfrastruktusr yang telah ada di Kantor Prolov dan mengusulkan untuk menambahkan jenis koneksi yang digunakan untuk membuka web admin menjadi VPN. Untuk menggunakan layanan VPN membutuhkan VPN server untuk jalur masuk koneksi dari internet. Sedangkan untuk infrastruktur yang sudah digunakan hanya ada sedikit perubahan dan konfigurasi untuk melakukan penyesuaian pada infrastruktur. Tipe VPN yang diusulkan adalah VPN dengan protokol ZeroTier agar terhubung ke server admin.

Pada penelitian ini penulis membuat implementasi jaringan *Virtual Private Network* menggunakan protokol ZeroTier berbasis dengan platform Linux ubuntu server 18.04 yang berfunsi sebagai server vpn.

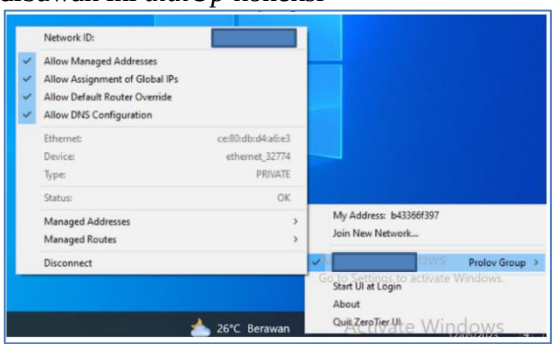
Dari hasil pengujian MITM (Man In The Middle) dengan menggunakan Cain Abel dan Wireshark, terungkap bahwa ketika melakukan uji ping ke alamat IP 8.8.8.8, aktivitas tersebut terpantau oleh Wireshark. Sebaliknya, saat uji coba dilakukan dengan menggunakan alamat IP dari ZeroTier, aktivitas tersebut tidak terlihat oleh Wireshark. Hal ini menunjukkan bahwa data yang dikirim melalui ZeroTier dapat dianggap aman. Kesimpulan ini sejalan dengan penjelasan yang terdapat di laman resmi ZeroTier ("ZeroTier.com"), yang menyatakan bahwa didalam tulisannya, ZeroTier mengimplementasikan tingkat keamanan yang tinggi hingga ke masa depan dengan menggunakan protokol kriptografi seperti SSL atau SSH.

PENGUJIAN JARINGAN AKHIR

Pada fase pengujian jaringan akhir ini, pelaksanaa evaluasi dilakukan setelah mengimplementasikan perubahan desain jaringan menggunakan VPN. Pengujian ini melibatkan langkah-langkah seperti melakukan koneksi dial-up ke ZeroTier, mengonfirmasi validitas koneksi di ZeroTier, melakukan ping ke koneksi domain server, mengakses domain melalui browser, dan memeriksa SSL di browser.

1. *DialUp koneksi*

DialUp koneksi merupakan tahap awal untuk dapat terhubung ke zero tier dengan cara memasukan uniqid di beri oleh admin jaringan. Jika berhasil terhubung akan menampilkan nama jaringan yang telah disetting di layanan zerotier. Berikut gambar dibawah ini *dialUp* koneksi

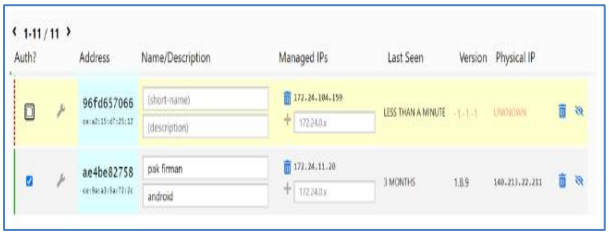


Gambar 4. *Dialup* koneksi

2. Validasi koneksi

JIKA (Jurnal of Informatics) UniversitasMuhammadiyah Tangerang *P ISSN : 2549-0710*
Vol 8 No.1, January 2024, pp 66-73 *E ISSN : 2722-2713*
DOI : 10.31000/jika.v8i1.9979

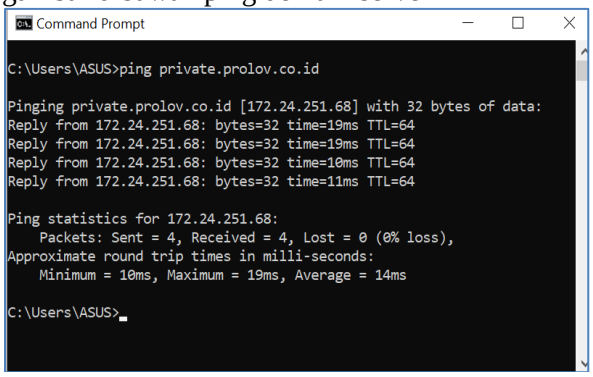
Validasi koneksi merupakan tahap selanjutnya setelah melakukan *DialUp* koneksi. Untuk membuat valid koneksi ceklis pada bagian *auth*. Berikut gambar dibawah ini validasi koneksi. Berikut ini gambar pengujian akhir validasi koneksi.



Gambar 4. Validasikoneksi

3. Ping domain server

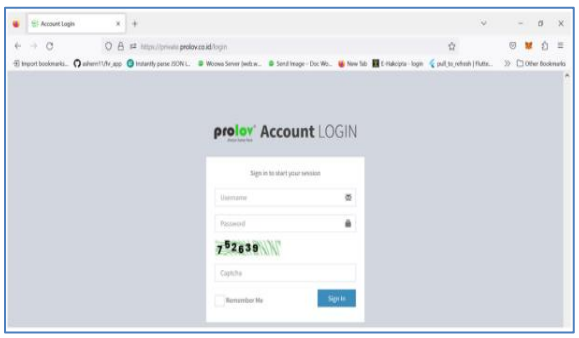
Ping yang dilakukan pada komputer client setelah menggunakan jaringan VPN akan mengalami perubahan IP, setelah terbentuknya VPN maka alamat ping akan di arahkan pada IP tunnel ZeroTier. Berikut gambar dibawah ping domain server



Gambar 5. Ping domain server

Akses domain

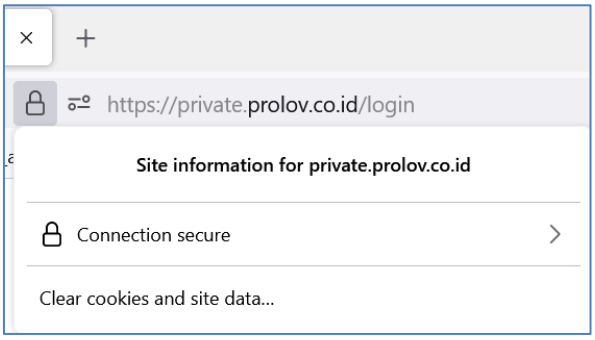
Akses domain di browser untuk melihat tampilan login di browser



Gambar 6. Akses domain *server*

5. Cek ssl

Pengecekan dilakukan agar diketahui apakah ssl sudah terinstall dengan benar. Jika ssl berhasil diinstall akan terdapat gembok di sebelah kiri domain.



Gambar 6. Cek ssl

Keefektifan Keamanan Jaringan

Keefektifan keamanan jaringan melibatkan implementasi dan pemeliharaan beberapa lapisan keamanan. Kombinasi penggunaan teknologi terkini, kebijakan keamanan yang ketat, pemantauan yang aktif, serta kesadaran karyawan merupakan faktor-faktor kunci dalam menjaga integritas dan keamanan jaringan. Evaluasi rutin dan penyesuaian dengan ancaman keamanan yang berkembang akan menjadi kunci untuk tetap melangkah maju dalam melindungi informasi dan infrastruktur perusahaan. Mengevaluasi implementasi firewall untuk memblokir akses yang tidak sah dan melindungi jaringan dari serangan luar. Memastikan bahwa aturan firewall disusun dengan bijak untuk mengizinkan akses yang diperlukan dan memblokir yang tidak diinginkan.

Zerotier Dalam Aspek Manajemen Jaringan

ZeroTier adalah sebuah platform jaringan definisi perangkat lunak (SDN) yang memungkinkan pembentukan jaringan pribadi virtual yang aman dan terdistribusi melalui internet. Manfaat utama dari ZeroTier adalah sebagai berikut:

1. Koneksi Jarak Jauh yang Aman
   ZeroTier memungkinkan pengguna untuk menghubungkan perangkat dari berbagai lokasi secara aman melalui internet. Ini sangat berguna untuk tim yang bekerja jarak jauh atau organisasi yang memiliki cabang atau perangkat tersebar.
2. Keamanan Tinggi
   ZeroTier menggunakan enkripsi end-to-end yang kuat untuk melindungi lalu lintas

data, menjadikannya solusi yang aman untuk menghubungkan perangkat yang berbeda melalui jaringan internet yang tidak aman.

3. Sederhana dan Mudah Digunakan
   ZeroTier dirancang untuk mudah digunakan dan diatur, bahkan oleh pengguna yang tidak memiliki pengetahuan mendalam tentang jaringan. Ini memungkinkan pengguna untuk dengan cepat membuat jaringan pribadi virtual.
4. Kinerja yang Baik
   ZeroTier memiliki kinerja yang baik, yang membuatnya cocok untuk berbagai aplikasi, termasuk berbagi berkas, *streaming* media, dan aplikasi bisnis berat.
5. Skalabilitas
   Anda dapat dengan mudah menambahkan perangkat baru ke jaringan ZeroTier Anda saat kebutuhan tumbuh, menjadikannya solusi yang skalabel.
6. Dukungan untuk Berbagai Platform
   ZeroTier mendukung sejumlah platform, termasuk Windows, macOS, Linux, Android, iOS, dan berbagai perangkat Internet of Things (IoT).
7. Penghematan Biaya
   Dengan menggunakan ZeroTier, Anda dapat menghindari biaya infrastruktur fisik yang diperlukan untuk menghubungkan perangkat secara fisik, seperti sewa jalur khusus atau peralatan jaringan tambahan.
8. Kontrol Lebih Besar
   Anda memiliki kendali penuh atas jaringan pribadi virtual yang Anda buat dengan ZeroTier, termasuk pengaturan kebijakan akses dan otentikasi perangkat.
9. Isolasi Lalu Lintas
   Anda dapat mengisolasi lalu lintas antara perangkat dalam jaringan ZeroTier, memastikan bahwa data yang bergerak antara perangkat hanya dapat diakses oleh yang diizinkan.
10. Dukungan untuk Kasus Penggunaan yang Beragam
    ZeroTier dapat digunakan dalam berbagai kasus penggunaan, termasuk pengaturan VPN, konektivitas IoT, perusahaan terdistribusi, dan lain-lain.

KESIMPULAN

Berikut Kesimpulan penelitian ini
Sebelum menggunakan zerotier akses jaringan ke web admin dapat dengan

1. Sebelum menggunakan zerotier akses jaringan ke web admin dapat dengan mudah dibuka oleh orang lain yang terkoneksi ke internet tentu saja hal ini membuat tidak aman.
2. Setelah menggunakan zerotier akses untuk ke web admin menjadi lebih aman karena adanya proses otentikasi user terlebih dahulu karena adanya pembatasan jaringan oleh Zerotier
3. Kemudahan dalam mengkofigurasi Zerotier saat membuat jaringan VPN

SARAN

Saran yang diajukan untuk pengembangan lebih lanjut dari penelitian yang telah dilakukan, antara lain:

a. Dapat mengimplementasikan di os lain seperti windows karena pada penelitian ini di implementasikan di os linux
b. Dapat memanfaatkan dan mengimplementasikan fasilitas *Applicatin Programming Interface (api*) yang telah disediakan oleh zerotier.

REFERENSI

AdhiSantoso, N., Maulidin, Z., DwiKurniawan, R., & YMI Tegal, S. (2022). Analisis Jaringan Komputer Menggunakan Teknologi Virtualisasi. *Jurnal MinfoPolgan*, *11*(2).

Almurayh, A. (n.d.). *Virtual Private Server*.

Andini, M. D., Amirulloh, M., &NoviantyMuchtar, H. (2020). *Penggunaan Aplikasi Virtual Private Network (VPN) Point To Point Tunneling Protocol (PPTP) dalam Mengakses Situs Terblokir* (Vol. 29, Issue 2). https://ditsti.itb.ac.id/layanan-vpn/

Ariyadi, T. (2018). *Mitigasi Keamanan*

Dynamic Host Control Protocl (DHCP) Untuk Mengurangi Serangan Pada Local Area Network (LAN).*3*(2).

DadiRiskiono, S. (2019). Analisis dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Networks (VPN). In *Jurnal TEKNOINFO* (Vol. 13, Issue 2).

Dewi, S., Riyadi, F., Suwastitaratu, T., & Hikmah, N. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *JurnalSains Dan Manajemen*, *8*(1).

Fitriawati, N., Herdiansah, A., Taufiq, R., & Destriana, R. (2022). IT Disaster Recovery Plan Dalam Mendukung Continuity Plan Saat Terjadi Force Majure. *JIKA (Jurnal Informatika)*, *6*(3), 249–255. https://doi.org/10.31000/jika.v6i3.6320

Hartono, S. B., &Niam, M. A. (2020). Client Server Sistem Informasi Aktivitas Penjualan *UKM Partner Cloth* (Vol. 19, Issue 2).

http://ejournal.upi.edu/index.php/manajerial/

Hasibuan, M., &EkoSuharyanto, C. (2021). Implementasi dan Perancangan VOIP Server Menggunakan Trixbox Opensource dan VPN Sebagai Pengamanan Antar Client. In *Jurnal COMASIE*.

Latifah, F. (n.d.). *Implementasi Virtual Private Network (VPN) dengan Otentikasi Server pada PT. Anugerah Tunggal Mandiri Jakarta* (Vol. 1).

http://www.mysecurecyberspace.com/encycl

Mujiastuti, R., &Prasetyo, I. (2021). *Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE*. www.google.com

Musril, H. A. (2019). Desain Virtual Private Network (VPN) Berbasis Open Shortest Path First (OSPF). *InfoTekJar (Jurnal Nasional Informatika Dan TeknologiJaringan)*, *3*(2), 83–88. https://doi.org/10.30743/infotekjar.v3i2.1055

Phang, V., &Setyaningsih, E. (n.d.).Perancangan Virtual Private Network DenganProtokol PPTP Menggunakan MikroTik Untuk Kebutuhan Remote Access. *Jurnal POLEKTRO: Jurnal Power Elektronik*, *10*(2), 2021.

Putra, T. G. S., &Widiasari, I. R. (2022).Rancangan Virtual Private Server Pada Kantor Kelurahan Menggunakan ZeroTier. *Building of Informatics, Technology and Science (BITS)*, *4*(2), 352–360. https://doi.org/10.47065/bits.v4i2.1810

Prolov. (2023). About Us Prolov. Retrieved Mei 19, 2023, from Prolov Website: https://prolov.co.id/

Ruslianto, I., & Ristian, U. (2019). *Perancangan dan Implementasi Virtual Private Network (VPN) Menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Mikrotik di Fakultas MIPA Universitas Tanjungpura* (Vol. 4, Issue 1).

Syarif1, R. F., &Sobari, I. A. (n.d.). *Implementasi Virtual Private Network (VPN) menggunakan Metode PPTP pada PT. Sinar Quality Internusa*.

Umaroh, L., &Rifauddin, M. (2020). *Implementasi Virtual Private Network (VPN) di Perpustakaan Universitas Islam Malang. Jurnal Dokumentasi dan Informasi. 41*(2), 193. https://doi.org/10.14203/j.baca.v41i2.531

Wahyudi, M., &AdiPurnama, R. (2019).*Analisis Performa Site to Site IP Security Virtual Private Network (VPN) Menggunakan Algoritma Enkripsi ISAKMP (Performance Analysis Site to Site IP Security Virtual Private Network (VPN) with Algorithm Encryption. ISAKMP*. Vol. 7, Issue 2.