PENERAPAN SISTEM KEAMANAN JARINGAN MENGGUNAKAN VPN DENGAN METODE PPTP PADA PT HINOKA SINERGI TANYO

Berliana Syela Fajrin[1], Priatno[2], Muhammad Ridwan Effendi
[1,2,] Universitas Bina Sarana Informatika,[3] Universitas Mohammad Husni Thamrin
[1]17190243@bsi.ac.id , [2]priatno@bsi.ac.id, [3] jundi79@gmail.com

Abstrak

PT Hinoka Sinergi Tanyo adalah sebuah perusahaan startup yang mengkhususkan diri dalam penjualan dan pemasaran kartu postpaid Indosat kepada UKM di seluruh Indonesia. Di tengah perkembangan pesat dalam bidang teknologi informasi, terutama dalam sektor telekomunikasi di Indonesia, PT Hinoka Sinergi Tanyo dihadapkan pada tantangan signifikan dalam hal keamanan sistem server komunikasinya. Perusahaan sangat mengandalkan server komunikasi sebagai pusat utama dalam pemasaran produk melalui jaringan telepon. Meskipun layanan telepon melalui jaringan internet yang sering dikenal dengan *Voice over internet protocol* (VoIP) telah menjadi alternatif yang lebih efisien, diperlukan perbaikan dalam sistem keamanan server komunikasi saat ini untuk melindungi data dari potensi kebocoran dan upaya akses yang tidak sah. Saat ini, akses ke server komunikasi masih terbuka untuk publik melalui penggunaan *Firewall* NAT. Oleh karena itu, solusi terbaik untuk meningkatkan tingkat keamanan sistem di PT Hinoka Sinergi Tanyo adalah melalui implementasi Virtual Private *Network* (VPN) dengan metode PPTP (Point to Point Tunneling Protocol). Dengan langkah ini, akses ke server komunikasi akan lebih terjaga privasinya dan hanya akan tersedia bagi pengguna yang sah yang ingin mengaksesnya dari lokasi jarak jauh.

Kata Kunci: Keamanan, *Firewall* NAT, VPN *(Virtual Private Network).*

Abstract

PT Hinoka Sinergi Tanyo is a startup company specializing in the sales and marketing of Indosat postpaid cards to SMEs throughout Indonesia. In the midst of rapid advancements in information technology, especially in the telecommunications sector in Indonesia, PT Hinoka Sinergi Tanyo faces significant challenges in the security of its communication server system. The company heavily relies on the communication server as the primary center for marketing products through telephone networks. While telephone services over the Internet, commonly known as Voice over internet protocol (VoIP), have become a more efficient alternative, improvements in the security of the current communication server system are needed to protect data from potential leaks and unauthorized access attempts. Currently, access to the communication server is still open to the public through the use of NAT firewalls. Therefore, the best solution to enhance the security level of the system at PT Hinoka Sinergi Tanyo is through the implementation of a Virtual Private Network (VPN) using the PPTP (Point to Point Tunneling Protocol) method. With this step, access to the communication server will be more private and only available to authorized users who wish to access it remotely..

Keywords: Security, firewall NAT, VPN (Virtual Private Network).

PENDAHULUAN

Berkembangnya teknologi komputer yang pesat, hal tersebut tidak mengurangi masalah yang terjadi pada jaringan komputer. Salah satu masalah yang terjadi pada jaringan komputer adalah sistem keamanan yang rentan mengalami sera-ngan hacker.(Jaya, Yuhandri, & Sumijan, 2020) Sistem ke-amanan pada jaringan komputer sangatlah penting, karena pertukaran data dapat terjadi kebocoran atau kebobolan data melalui jaringan publik oleh pihak luar yang tidak bertanggung jawab.(Dewi, 2020)

PT Hinoka Sinergi Tanyo merupakan perusahaan startup yang berfokus pada penjualan dan pemasaran kartu postpaid Indosat untuk para UMKM di Indonesia. Untuk memastikan operasi yang lancar dan produktivitas pada PT Hinoka Sinergi Tanyo memerlukan sistem server komunikasi yang aman untuk seluruh karyawan. Sistem keamanan yang sedang berjalan saat ini di PT Hinoka Sinergi Tanyo hanya menggunakan NAT *(Network Address Translation)* yang terkonfigurasi pada perangkat router di kantor untuk hak *remote* akses. (Mufida, Irawan, & Chrisnawati, 2017)

NAT *(Network Address Translation)* adalah teknologi jaringan yang mengubah alamat IP perangkat di dalam jaringan lokal saat terhubung ke Internet. Hal ini membuka potensi risiko bagi penyusup yang tidak memiliki izin akses ke server komunikasi PT Hinoka Sinergi Tanyo, yang dapat mengakibatkan kebocoran data, pembatasan akses ke server, atau bahkan penonaktifan akun dalam beberapa kasus.(Audrey, 2022) Ancaman ini muncul ketika individu yang tidak berizin secara berulang mencoba masuk dengan kombinasi username dan password yang salah. (Hidasaputra, 2021)

Masalah di PT Hinoka Sinergi Tanyo dapat diatasi dengan mengimple-mentasikan VPN menggunakan metode PPTP (Awaludin, Yasin, & Risyda, 2024). VPN *(Virtual Private Network)* adalah solusi yang efektif untuk mengatasi tantangan keamanan yang dihadapi dalam menghubungkan jaringan komputer yang terpisah dan berjauhan. (Phang & Setyaningsih, 2021)

VPN adalah solusi efektif untuk mengamankan komunikasi antara dua jaringan terpisah dengan dua jaringan yang berjauhan dapat terkoneksi dan terlihat seperti berada dalam satu jaringan internet yang besar (Awaludin & Yasin, 2020). Dengan cara ini, user yang di izinkan dapat mengakses sumber daya di kedua jaringan tersebut tanpa khawatir terjadi pelanggaran keamanan. (Putra, Indriyani, & Angraini, 2018)

PPTP merupakan singkatan dari Point to Point Tunneling Protocol yang merupakan sebuah protokol jaringan yang digunakan untuk mengamankan transfer data antara klien yang berlokasi jauh, de-ngan akses ke server perusahaan. (Satryawati, Pangestu, & Budiman, 2022)

Penerapannya melibatkan pembuat-an jaringan VPN menggunakan protokol TCP/IP yang sudah ada di jaringan PT Hinoka Sinergi Tanyo. (Hasibuan & Eko Suharyanto, 2021). Penulis akan menjelas-kan bagaimana sistem keamanan akan diterapkan di PT Hinoka Sinergi Tanyo menggunakan VPN dengan metode PPTP untuk memungkinkan pengelolaan server komunikasi dari jarak jauh dengan lebih efisien.

METODE PENELITIAN

Dalam penelitian di PT Hinoka Sinergi Tanyo, penulis menemukan ke-butuhan untuk mengembangkan sistem keamanan server komunikasi mengguna-

kan VPN PPTP. Prosesnya melibatkan pengumpulan data, analisis, dan implementasi sistem keamanan dengan VPN PPTP.

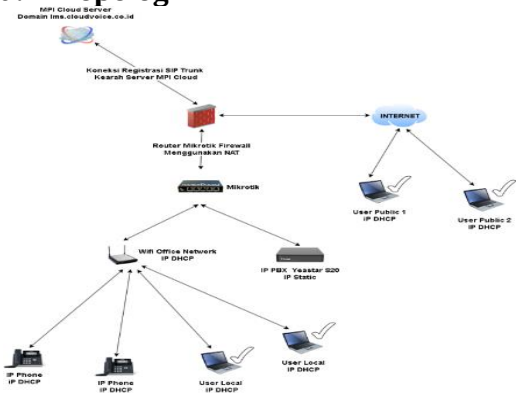
1. **Observasi**
   Pada tahap observasi ini penulis mulai melakukan pengamatan lang-sung ke PT Hinoka Sinergi Tanyo untuk dapat mengumpulkan data-data sebagai objek penelitian.
2. **Wawancara**
   Pada tahap wawancara, penulis akan melibatkan pertemuan secara tatap muka dengan pihak yang terlibat seperti *President Director, Operation Director*, Teknisi IT di PT Hinoka Sinergi Tanyo.
3. **Studi Pustaka**
   Penulis melakukan pengumpulan data dari jurnal-jurnal yang relevan dengan teori penelitian, yang akan digunakan sebagai referensi teori yang kuat dalam karya ilmiah. (Novianto & Munir, 2022)

HASIL DAN PEMBAHASAN

1. Analisa Jaringan Berjalan

Penulis telah mengidentifikasi beberapa masalah dalam skema jaringan internal yang perlu diperbaiki untuk meningkatkan keamanan. Oleh karena itu, akan dibuat skema jaringan usulan dengan menerapkan tingkat keamanan yang tinggi.

a. Topologi



Sumber : Penulis (2023)

Gambar 1. Topologi Jaringan Berjalan di PT Hinoka Sinergi Tanyo

PT Hinoka Sinergi Tanyo menggunakan topologi tree untuk menghubungkan server dengan perangkat-perangkat lainnya dan menggunakan jaringan WLAN untuk menggabungkan server yang berada di kantor ke jaringan internet.

b. Arsitektur Jaringan

Berikut adalah gambaran mengenai struktur jaringan di PT Hinoka Sinergi Tanyo, yang terdiri dari dua lantai pada kantor mereka dan telah dilengkapi dengan perangkat router MikroTik RouterOS tipe RB450G. Fungsi pada MikroTik ini adalah untuk membagi beban trafik jaringan (Awaludin & Gani, 2024). Kantor ini memiliki beberapa ruangan seperti marketing sales, IT, admin, *accounting, director,* dan wakil director. PT Hinoka Sinergi Tanyo memanfaatkan jaringan WLAN untuk menghubungkan *client* ke server dan antar *client* lain-nya. Kantor ini berlangganan layan-an Internet sebesar 20 Mbps dari penyedia layanan Internet Indihome. Rancangan sistem keamanan jaringan server komunikasi dikonfigurasi pada perangkat MikroTik di PT Hinoka Sinergi Tanyo. Spesifikasi alamat IP perangkat jaringan di PT Hinoka Sinergi Tanyo dapat dijelaskan sebagai berikut:

Tabel 1. Spesifikasi Jaringan Pada PT Hinoka Sinergi Tanyo

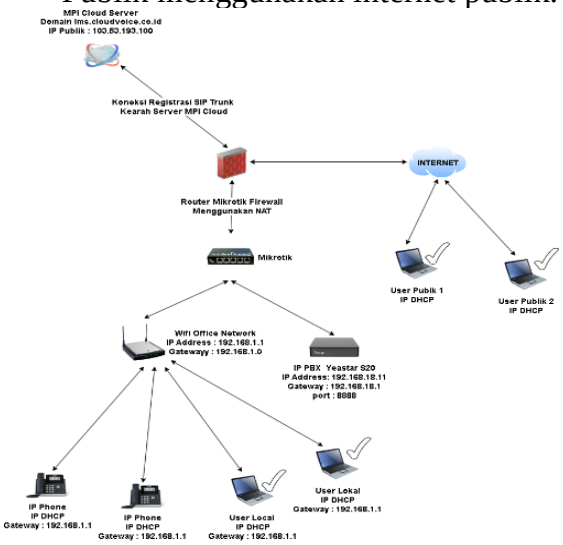
No	Details	IP *Address*	Gateway	Subnet Mask	DNS	IP Publik
1.	Server YeastarS20	192.168.18.11	192.168.18.1	255.225.255.0	8.8.8.8	-
2.	Router Mikrotik	172.110.13.28	172.110.13.1	255.225.255.0	8.8.8.8	-
3.	Cloud Voice	192.168.2.80	192.168.2.1	255.225.255.0	8.8.8.8	103.53.193.100
4.	*Accesspoint*	192.168.1.1	192.168.1.0	255.225.255.0	8.8.8.8	-
5.	User Lokal	IP DHCP	192.168.1.1	255.225.255.0	8.8.8.8	-
6.	User Publik	IP DHCP	192.168.1.1	255.225.255.0	8.8.8.8	-
7.	IP Phone	IP DHCP	192.168.1.1	255.225.255.0	8.8.8.8	-

Sumber : Penulis (2023)

c. Skema Jaringan Berjalan

Skema jaringan PT Hinoka Sinergi Tanyo menggunakan cloud server dari PT Mulia Persada Indonesia untuk mengirimkan SIP Trunk ke server mereka. MikroTik sudah dikonfigurasi dengan *firewall* NAT untuk *remote access*, dan setiap *client* yang terhubung ke *access point* akan mendapatkan IP *Address* melalui DHCP, memudahkan proses perbaikan jika ada masalah.

Terlihat user publik 1 dan 2 dapat melakukan akses server, hal ini menjadi bukti bahwa menggunakan firwall NAT saja tidak cukup untuk melindungi server komunikasi yang berada di PT Hinoka Sinergi Tanyo, dampaknya pengguna manapun dapat mengakses server dengan IP Publik menggunakan internet publik.



Sumber : Penulis (2023)

Gambar 2. Skema Jaringan pada PT Hinoka Sinergi Tanyo

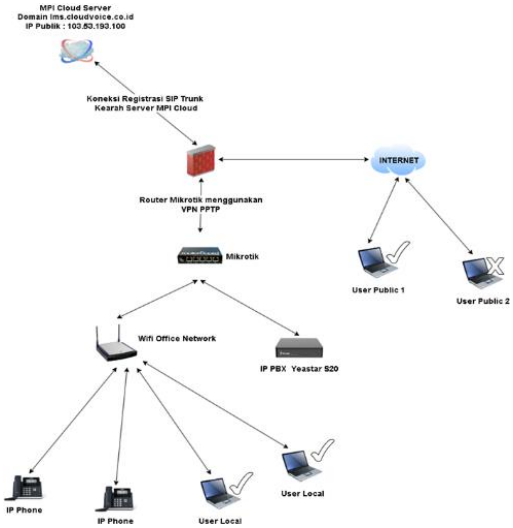
d. Kemanan Jaringan

PT Hinoka Sinergi Tanyo menggunakan antivirus untuk *Operating System (OS)* pada laptop *client* yaitu Smadav dan pada jaringan server menggunakan *Firewall* NAT yang terkonfigurasi di MikroTik. dengan kemanan jaringan yang sedang digunakan saat ini masih kurang untuk sistem keamananya. Setiap pengguna yang memiliki IP publik server Perusahaan dapat mengakses dimanapun menggunakan jaringan publik.

2. Rancangan Jaringan Usulan

Berikut adalah uraianpenjelasan mengenai rancangan jaringan yang mencakup implementasi keamanan melalui VPN PPTP di PT Hinoka Sinergi Tanyo.

a. Topologi



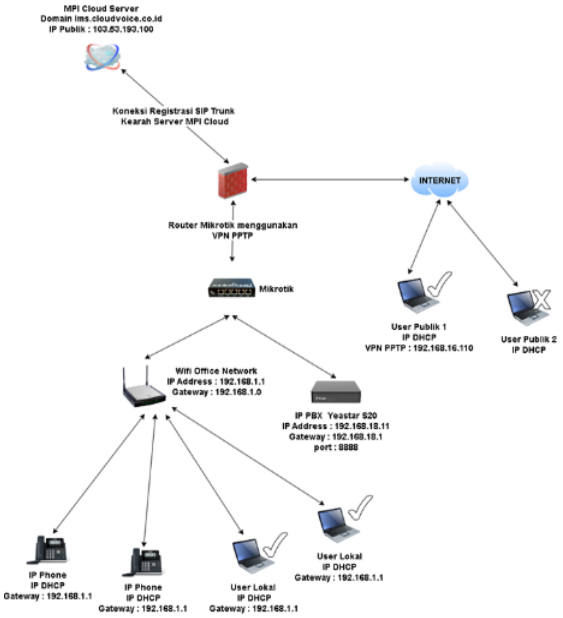
Sumber : Penulis (2023)

Gambar 3. Topologi Jaringan Usulan

PT Hinoka Sinergi Tanyo telah memanfaatkan jaringan yang mirip dengan yang sudah ada sebelumnya. Namun, perbedaannya terletak pada peningkatan aspek keamanan. Sebelumnya, perusahaan hanya mengandalkan *firewall* NAT, tetapi saat ini telah mengubah keamanan jaringannya dengan mengadopsi metode VPN PPTP. Hal ini dilakukan untuk menjadikan hak akses lebih private dan aman.

b. Skema Jaringan Berjalan

Skema jaringan usulan ini diperbarui dari skema jaringan yang sudah ada dengan mengganti *firewall* NAT menggunakan VPN PPTP. Ini dilakukan melalui penerapan akses jarak jauh melalui VPN dan pembuatan akun hanya untuk pengguna yang memiliki peran penting dalam mengakses server untuk meningkatkan keamanan server komunikasi. Terlihat pengguna publik 1 dapat mengakses server dikarenakan user publik 1 adalah pengguna yang sah dan user publik 2 pengguna yang tidak sah.



Sumber : Penulis (2023)

Gambar 4. Skema Jaringan Usulan PT Hinoka Sinergi Tanyo\

c. Keamanan Jaringan

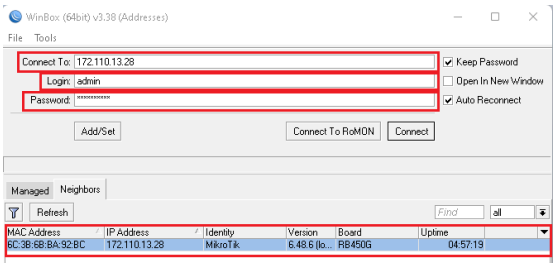
PT Hinoka Sinergi Tanyo sistem keamanan jaringan sebelumnya menggunakan *Firewall* NAT, sehingga tingkat keamanan kurang karena server masih dapat diakses oleh setiap pengguna. Maka di implementasikan penggunaan VPN PPTP untuk meningkatkan keamanan jaringan di PT Hinoka Sinergi Tanyo. PPTP memberikan tingkat enkripsi yang lebih baik dan mendukung protokol autentikasi seperti MS-CHAP dan CHAP, memastikan hanya pengguna sah yang dapat mengakses server yang berada di perusahaan.

3. Rancangan Aplikasi

Rancangan aplikasi yang diusulkan untuk mengatasi masalah di PT Hinoka Sinergi Tanyo adalah menerapkan sistem keamanan jaringan melalui VPN PPTP menggunakan perangkat MikroTik, termasuk RouterBoard R450G dan server Yeastar S20. Hal ini memungkinkan akses jaringan lokal melalui jaringan publik, memberikan akses pribadi ke server melalui IP lokal, dan hanya dapat diakses oleh pengguna dengan akun VPN. Penulis akan menjelaskan langkah-langkah pembuatan VPN PPTP *remote access* menggunakan MikroTik Router.

a. Konfigurasi VPN PPTP

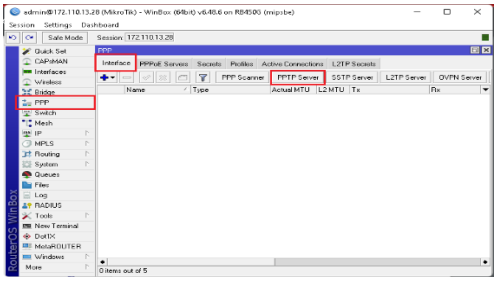
Masukkan IP router 172.110.13.28 dan username serta password.



Sunber : Penulis (2023)

Gambar 5. Login MikroTik menggunakan Winbox

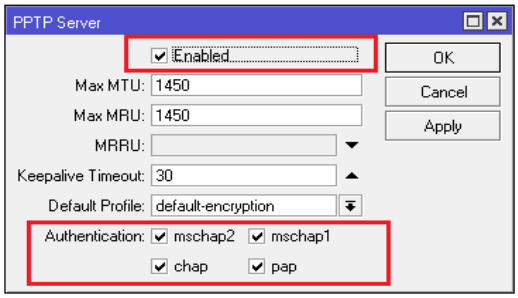
Masuk ke tab PPP lalu klik *interface* dan pilih PPTP Server



Sumber : Penulis

Gambar 5. Langkah membuat PPTP Server

Tandai kotak "*Enable*d" dan pilih opsi "PAP, MSCHAP1, CHAP, MSCHAP2" dalam kolom autentikasi sesi PPP di menu pengaturan autentikasi VPN.

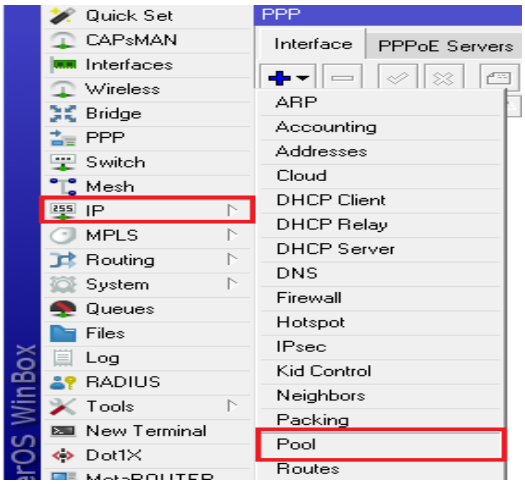


Sumber : Penulis (2023)

Gambar 7.Langkah membuat PPTP Server

b. Konfigurasi IP Pool

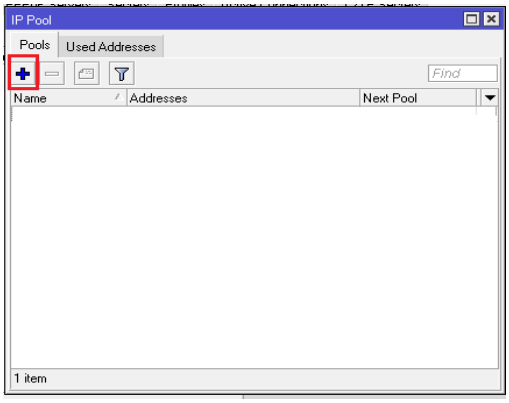
Buat IP Pool untuk *client* atau *exclude* IP *address* yang sudah di konfigurasi pada PPP Server dengan masuk ke tab lalu pilih IP Pool.



Sumber : Penulis (2023)

Gambar 8. Langkah melakukan konfigurasi IP Pool

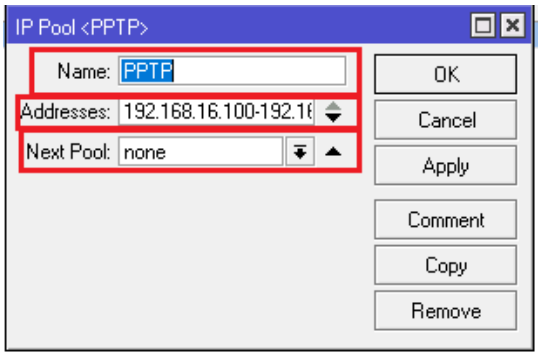
Klik tombol tanda add (+) pada jendela IP Pool.



Sumber : Penulis (2023)

Gambar 9. Langkah melakukan konfigurasi IP Pool

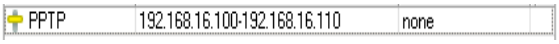
Setelah klik add pada jendela IP Pool, akan ditampilkan jendela *New* IP Pool, kemudian isi *Name* dan *Addresses* atau *range* IP sesuai kebutuhan. Pada konfigurasi VPN ini penulis memberikan *Name* PPTP dengan *range* 11 IP yang di mulai dari 192.168.16.100-192.168.16.110.
Setelah sudah di tentukan IP *range* nya klik *apply* dan OK.



Sumber : Penulis (2023)

Gambar 10.Langkah melakukan konfigurasi IP Pool

Berikut tampilan IP Pool yang sudah selesai

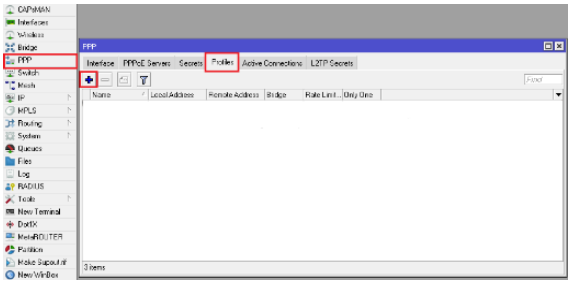


Sumber : Penulis (2023)

Gambar 11.Hasil IP yang sudah terkonfigurasi di IP Pool

c. Konfigurasi PPP Profiles

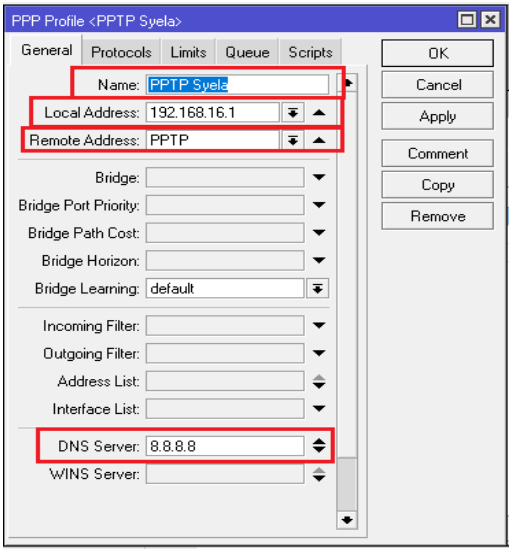
PPP Profiles adalah sebuah fitur yang memiliki peran untuk membuat template konfigurasi. Template ini mencakup pengaturan seperti Local dan *Remote Address*, penggunaan enkripsi, pembatasan kecepatan *(Rate Limit)*, aturan "Hanya Satu" *(Only One)*, antrian *(Queue)*, *firewall*, daftar alamat (*Address* List), dan sebagainya. Pilih tab PPP kemudian pilih *Profiles* klik tanda add (+)



Sumber : Penulis (2023)

Gambar 12. Langkah melakukan konfigurasi PPP Profiles

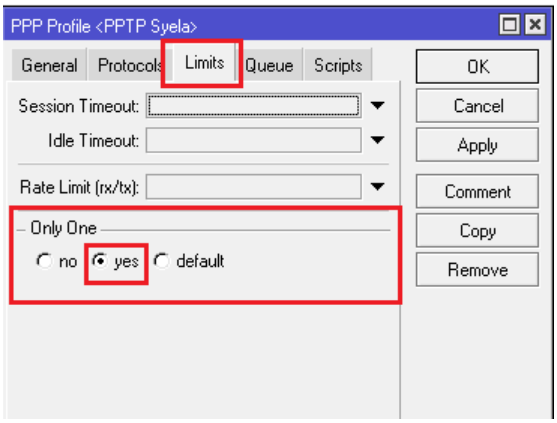
Kemudian pilih nama sesuai kebutuhan dan masukkan local *address* dengan menggunakan IP *gateway* dari IP Pool yang akan digunakan sebagai *remote* adddress pada PPP. Sebagai contoh, IP Pool yang telah dibuat memiliki *range* IP 192.168.16.100-192.168.192.168.16.110, sehingga IP *gateway* yang digunakan adalah 192.168.16.1, dan server DNS yang dipilih adalah 8.8.8.8.



Sumber : Penulis (2023)

Gambar 13. Langkah melakukan konfigurasi PPP Profiles

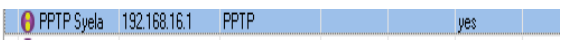
Langkah selanjutnya yaitu pillih tab *limits* dan pilih yes pada pengaturan *only one* sehingga akun VPN PPTP hanya dapat di akses oleh 1 pengguna.



Sumber : Penulis (2023)

Gambar 14. Langkah melakukan konfigurasi limits pada PPP profiles

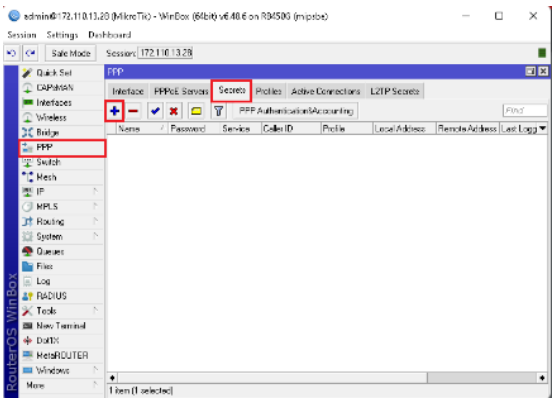
Kemudian klik apply dan OK, PPP Profiles sudah berhasul dibuat.



Sumber : Penulis (2023)

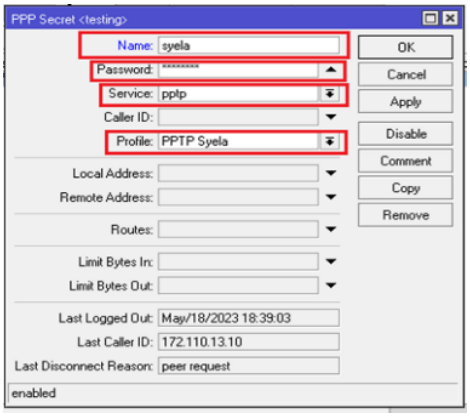
Gambar 15. Tampilan VPN server yang berhasil dibuat

d. Konfigurasi PPP dengan PPTP Secret
Masuk ke tab PPP kemudian pilih secret klik tanda add (+)



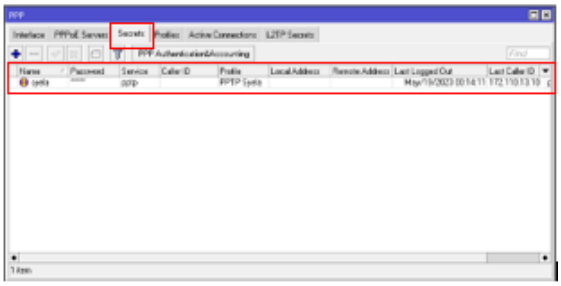
Sumber : Penulis (2023)
Gambar 16. Langkah melakukan konfigurasi PPP dengan PPTP Secret

Kemudian isi kolom *Name* dan *Password* sesuai kebutuhan, pilih service PPTP dan pilih profile PPP yang sudah dibuat sebelumnya klik *apply* dan OK.



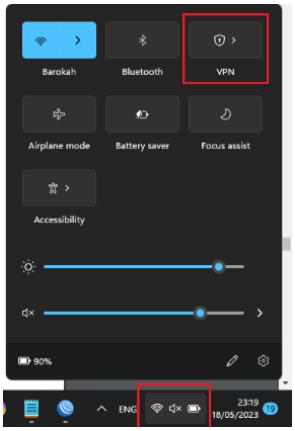
Sumber : Penulis (2023)
Gambar 17. Langkah melakukan konfigurasi PPP dengan PPTP secret

Berikut tampilan pada VPN PPTP yang sudah berhasil dibuat



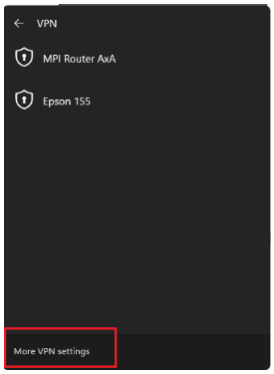
Sumber : Penulis (2023)
Gambar 18.Tampilan VPN PPTP yang sudah berhasil terkonfigurasi.

e. Konfigurasi *Client Remote*
Untuk menambahkan VPN yang sudah dibuat pada PC atau laptop teknisi IT, langkah-langkahnya adalah dengan mengklik ikon jaringan pada taskbar dan kemudian memilih *Network* & Internet *Setting*s. Pada gambar dibawah ini penulis menggunakan sistem OS *window*s 11, dan berikut adalah langkah-langkahnya:



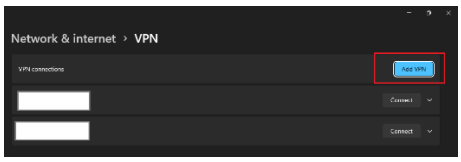
Sumber : Penulis (2023)
Gambar 19. Menambahkan akun VPN PPTP pada PC atau Laptop

Kemudian klik *more setting* VPN tampilan sebagai berikut.



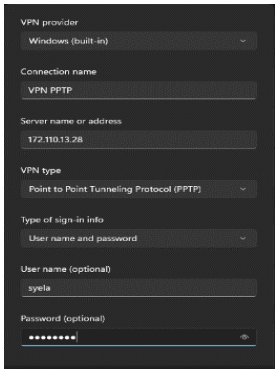
Sumber : Penulis (2023)
Gambar 20. Masuk ke VPN *setting* untuk menambahkan akun VPN

Setelah itu pilih tab Add VPN



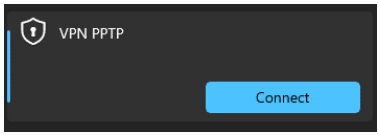
Sumber : Penulis (2023)
Gambar IV. 21.Add a new VPN

Pilih VPN provider *Windows* (built-in), isi Connection Name sesuai kebutuhan, server name or *address* dengan IP MikroTik, pilih VPN Type PPTP, dan sign in-info dengan *username* dan *password* yang telah dikonfigurasi di MikroTik.



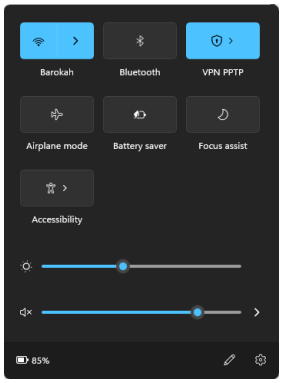
Sumber : Penulis (2023)
Gambar 22.Add a VPN Connection

Kemudian klik save, setelah berhasil di tambahkan VPN PPT klik tombol connect agar dapat terhubung.



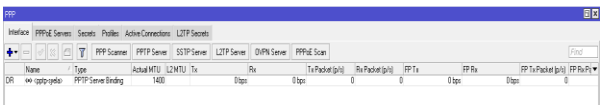
Sumber : Penulis (2023)
Gambar 22. VPN PPTP berhasil di tambahkan pada pc atau laptop

Berikut tampilan VPN PPTP yang sudah berhasil terhubung.



Sumber : Penulis (2023)
Gambar 23. VPN PPTP sudah berhasil terhubung pada PC atau Laptop

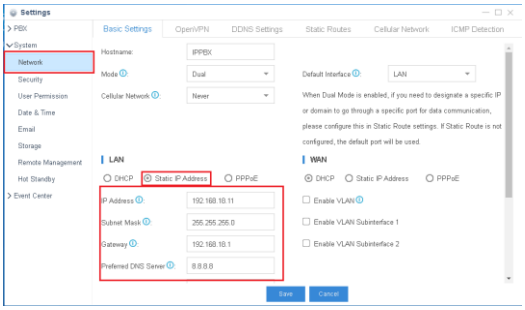
Ketika VPN PPTP diakifkan maka akan terbaca pada *interface* PPP di MikroTik.



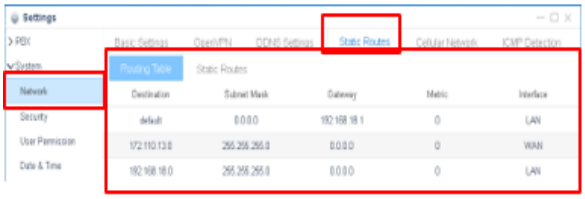
Sumber : Penulis (2023)
Gambar 24.Tampilan pada PPP *interface*
Ketika VPN PPTP sudah berhasil terhubung.

f. Konfigurasi server Yeastar S20 sebagai server komunikasi yang akan di berikan *remote access*.

Lakukan login ke web server, lalu konfigurasi dengan memilih tab *setting*s lalu pilih *network*, pada *network* pilihlah static IP *Address* kemudian isi IP *Address*, *subnet mask*, *gateway*, DNS.



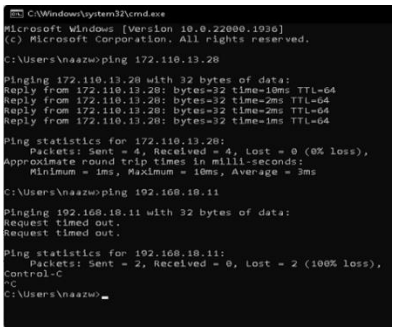
Sumber : Penulis (2023)
Gambar 25. Tampilan *setting network* pada server Yeastar S20 IPPBX



Sumber : Penulis (2023)
Gambar 26. IP *Address* yang sudah terdaftar pada server Yeastar S20 IPPBX

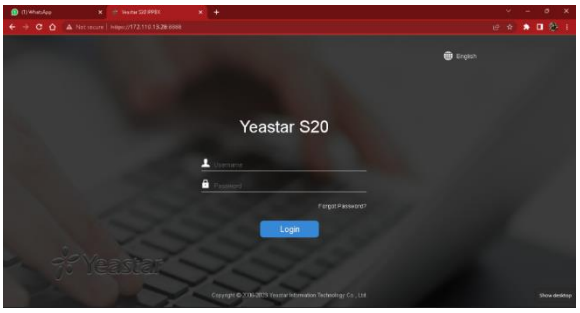
4. Pengujian Jaringan Awal

Tahap awal uji jaringan dilakukan sebelum mengimplementasikan jaringan yang diajukan. Diamati melalui pengujian koneksi menggunakan perintah PING di *Command prompt* dengan memanggil IP publik dan IP lokal server. Hasil pengujian menunjukkan bahwa sistem keamanan masih menggunakan *firewall* NAT, sehingga saat melakukan uji koneksi ke IP Publik (172.110.13.28) berhasil, namun uji koneksi ke IP Lokal server (192.168.18.11) tidak berhasil.



Sumber : Penulis (2023)
Gambar 27.Melakukan test koneksi IP Publik dan IP lokal server

Kemudian untuk akses server menjadi publik secara umum dengan menggunakan IP 172.110.13.28, sehingga siapapun yang mengetahui IP Publik server dapat diakses hal ini menyebabkan pengguna yang tidak sah dapat masuk ke server.

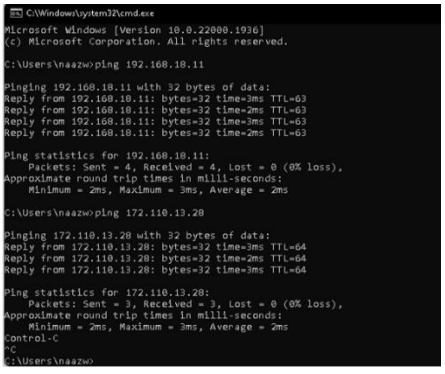


Sumber : Penulis (2023)
Gambar 28. Login akses server komunikasi menggunakan sistem keamanan *firewall* NAT

5. Pengujian Jaringan Akhir

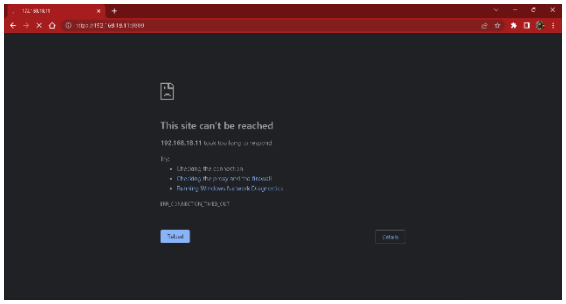
Tahapan uji akhir jaringan akan mengungkapkan hasil pelaksanaan sistem keamanan dengan VPN PPTP. Pengujian dilaksanakan dengan dua kondisi, yaitu mengakses server tanpa menggunakan VPN PPTP dan mengakses server dengan menggunakan VPN PPTP.

Pada gambar dibawah ini terlihat pada IP 172.110.13.28. berhasil terkoneksi dan IP 192.168.18.11 berhasil terkoneksi karena pada VPN PPTP sudah di aktifkan.



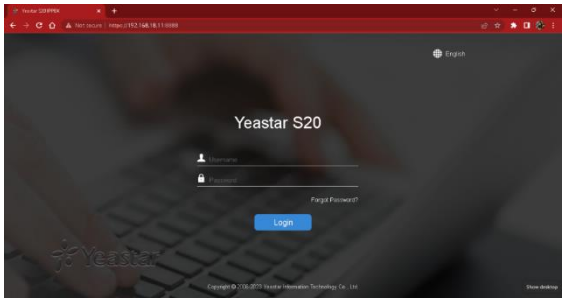
Sumber : Penulis (2023)
Gambar 29. Pengujian perintah PING di *command prompt* (CMD)

Pada gambar dibawah ini menampilkan akases server oleh pengguna yang tidak memiliki akun VPN PPTP atau tanpa VPN PPTP.



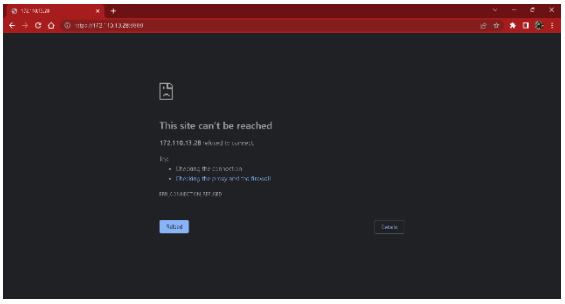
Sumber : Penulis (2023)
Gambar 30. pengujian akses server Yeastar S20 IPPBX Tanpa VPN PPTP

Pada gambar dibawah ini menampilkan akases server oleh pengguna yang sah memiliki akun VPN PPTP.



Sumber : Penulis (2023)
Gambar 31. Pengujian akses server Yeastar S20 IPPBX Menggunakan VPN PPTP

Pada gambar dibawah ini menampilkan akses server menggunakan IP Publik setelah dilakukan konfigurasi VPN PPTP pada router



Sumber : Penulis (2023)
Gambar 32. pengujian akses ke server Yeastar S20 IPPBX Menggunakan IP Publik

KESIMPULAN

Setelah mengevaluasi keamanan jaringan di PT Hinoka Sinergi Tanyo, kesimpulan penulis adalah bahwa penerapan sistem keamanan jaringan dengan VPN PPTP dapat memberikan akses server secara private, dan memberi kemudahan bagi teknisi IT dalam mengelola dan mengatasi masalah server perusahaan secara *remote* yang aman, tanpa perlu hadir secara fisik di lokasi. Kepada perusahaan untuk penggunaan VPN, yaitu:

1. Sosialisasikan kebijakan keamanan VPN kepada pengguna dan berikan pelatihan tentang penggunaan yang aman untuk tidak membagikan kredensial akses VPN kepada orang lain dan memastikan pengguna memahami pentingnya keamanan saat menggunakan VPN.
2. Menggunakan VPN L2TP IPsec untuk tingkat keamanan yang lebih baik.
3. Mengintergrasikan whitelist IP Address untuk memblokir IP Address yang tidak dikenali oleh server.

REFERENSI

Audrey, B. F. (2022). Virtual Private Network Menggunakan Point To Point Tunnel Protocol Berbasis Mikrotik: Virtual Private Network Menggunakan Point To Point Tunnel Protocol …. *Journal of Network and Computer Applications (ISSN …*, *1*(1), 1–8.

Awaludin, M., & Gani, A. (2024). Pemanfaatan kecerdasan buatan pada algoritma k-means klastering dan sentiment analysis terhadap strategi promosi yang sukses untuk penerimaan mahasiswa baru. *JSI (Jurnal Sistem Informasi) Universitas Suryadarma*, *11*(1), 1–6.

Awaludin, M., & Yasin, V. (2020). Application Of Oriented Fast And Rotated Brief (Orb) And Bruteforce Hamming In Library Opencv For Classification. *Journal of Information System, Applied, Managemgent, Accounting, and Reserarch*, *4*(3), 51–59.

Awaludin, M., Yasin, V., & Risyda, F. (2024). The Influence of Artificial Intelligence Technology, Infrastructure and Human Resource Competence on Internet Access Networks. *Inform : Jurnal Ilmiah Bidang Teknologi Informasi Dan Komunikasi*, *9*(2), 111–120. https://doi.org/10.25139/inform.v9i2.8109

Dewi, S. (2020). Keamanan Jaringan Menggunakan VPN (Virtual Private Network) Dengan Metode PPTP (Point To Point Tunneling Protocol) Pada Kantor Desa Kertaraharja Ciamis. *EVOLUSI : Jurnal Sains Dan Manajemen*, *8*(1), 128–139. https://doi.org/10.31294/evolusi.v8i1.7658

Hasibuan, M., & Eko Suharyanto, C. (2021). Implementasi Dan Perancangan Voip Server Menggunakan Trixbox Opensource Dan Vpn Sebagai Pengamanan Antar Client. *Jurnal Comasie*.

Hidasaputra, A. N. (2021). *Mengenal Konsep Gateway Dan Nat (Network Address Translation)*. 1–2.

Jaya, B., Yuhandri, Y., & Sumijan, S. (2020). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS). *Jurnal Sistim Informasi Dan Teknologi*, *2*, 115–123. https://doi.org/10.37034/jsisfotek.v2i4.32

Mufida, E., Irawan, D., & Chrisnawati, G. (2017). Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus pada Yayasan Teratai Global Jakarta. *Jurnal Matrik*, *16*(2), 9. https://doi.org/10.30812/matrik.v16i2.7

Novianto, M. A., & Munir, S. (2022). PERANCANGAN KEAMANAN JARINGAN NEXT-GENERATION FIREWALLMENGGUNAKAN ROUTER FORTINETPADA PT. ALODOKTER TEKNOLOGI SOLUSI. *Jurnal Informatika Terpadu*, *8*(2), 47–61.

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

Putra, J. L., Indriyani, L., & Angraini, Y. (2018). Penerapan Sistem Keamanan Jaringan Menggunakan VPN Dengan Metode PPTP Pada PT. Asri Pancawarna. *IJCIT (Indonesian Journal on Computer and Information Technology*, *3*(2), 260–267.

Satryawati, E., Pangestu, D. A., & Budiman, A. S. (2022). Implementasi Virtual Private Networ Menggunakan Point-To-Point Tunneling Protocol. *Jeis: Jurnal Elektro Dan Informatika Swadharma*, *2*(1), 36–42. https://doi.org/10.56486/jeis.vol2no1.160