J-INTECH (Journal of Information and Technology)
Terakreditasi Kemendikbud SK No. 204/E/KPT/2022
E-ISSN: 2580-720X || P-ISSN: 2303-1425

Peningkatan Keamanan Jaringan *Virtual Private Network* Menggunakan Protokol IKE/IPSEC Berbasis Mikrotik

Annisa Dwi Prameswari[1*], Ronald David Marcus[2]

[1,2] S1 Sistem Informasi, Universitas Merdeka Malang, Jalan Terusan Dieng no 62-64, 65146, Jawa Timur, Indonesia

***Email Korespondensi:**
ronald.mangero@unmer.ac.id

Abstrak

Penelitian ini membahas beberapa protokol VPN (Virtual Private Network), yaitu PPTP, SSTP, L2TP, dan IPsec, serta analisis metode autentikasi yang digunakan pada masing – masing protokol. Metode yang digunakan pada penelitian ini adalah kualitaif dan melibatkan pengujian konektivitas, autentikasi dan konfigurasi yang digunakan pada setiap protokol VPN. Parameter yang digunakan pada penelitian ini yaitu kerumitan konfigurasi, fleksibilitas, keamanan dan waktu yang dibutuhkan untuk terhubung ke jaringan VPN. Pada protokol IKE/IPsec dilakukan analisis autentikasi perbandingan antara Pre-Shared Key dengan certificate. Autentikasi menggunakan sertificate terbukti lebih aman meskipun membutuhkan konfigurasi yang lebih rumit dibandingkan dengan Pre-Shared Key. . Hasil dari penelitian ini adalah penggunaan protokol IKE/Ipsec memiliki fleksibilitas dan keamanan yang baik. Algoritma yang ada pada protokol ini dapat dipilih sesuai dengan kebutuhan dan keamanan yang diinginkan.
Kata Kunci : Internet Key Exchange; IPsec; Mikrotik; Protokol VPN

Abstract

This research discusses protocols VPN (Virtual Private Network), namely PPTP, SSTP, L2TP, and IPsec, analyzes the authentication methods used in each protocol. The method used in this research is qualitative and involves testing the connectivity, authentication and configuration used in each VPN protocol. The parameters used in this research are configuration complexity, flexibility, security and the time required to connect to the VPN network. In the IKE/IPsec protocol, a comparison authentication analysis between Pre-Shared Key and certificate is carried out. Authentication using certificates is proven to be more secure even though it requires more complicated configuration compared to Pre-Shared Key. . The result of this research is the use of IKE / IPsec protocol has flexibility and good security. The algorithms in this protocol can be selected according to the needs and desired security.
Keywords: Internet Key Exchange; IPsec; Mikrotik; Protocol VPN

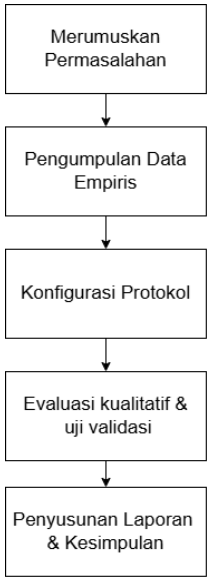
1. Pendahuluan

VPN (Virtual Private Network) sering digunakan oleh lembaga keuangan seperti bank, untuk menghubungkan antara kantor cabang dengan kantor pusat. Selain itu, antar bank juga memanfaatkan VOIP (Voice Over IP) untuk menjaga kerahasiaan dan keamanan data saat berkomunikasi. Dalam hal ini, bank memerlukan protokol keamanan VPN yang sangat kuat dan terenkripsi dengan baik, serta penggunaan protokol yang lebih optimal untuk mendukung aktivitas operasional transaksi.

Terdapat berbagai macam protokol VPN seperti PPTP, SSTP, L2TP, dan IPsec. Setiap VPN memiliki kelemahan dan kelebihannya masing masing. Meskipun protokol tersebut sudah banyak digunakan, namun dianggap kurang aman dan rentan terhadap serangan.

Pada penelitian "Analisis Perbandingan Performa QoS, PPTP, L2TP, SSTP dan IPsec Pada Jaringan VPN Menggunakan Mikrotik" yang dilakukan oleh Wa Ode Zamalia, L.M. Fid Aksara, dan Muh. Yamin, melakukan perbandingan menggunakan QoS. Didapatkan hasil bahwa protokol Ipsec lebih aman dibandingkan protokol VPN lainnya. Pada penelitian "Analisis dan Pengujian Permasalahan Pada Sistem Remote Access IPSec" oleh Arini, MT, dan Giri Patmono menjelaskan permasalahan keamanan pada jaringan VPN Remote Access menggunakan protokol IPsec. Berdasarkan penelitian tersebut maka masih banyak keamanan yang kurang optimal apabila hanya menggunakan protocol IPsec dalam mengamankan jaringan VPN. Maka, peneliti melakukan uji konektivitas dan konfigurasi VPN menggunakan IKE/IPsec. Penelitian ini juga menggunakan model koneksi remote access. Hal ini dilakukan untuk mengetahui fleksibilitas dan konfigurasi yang digunakan saat mengamankan sebuah jaringan.

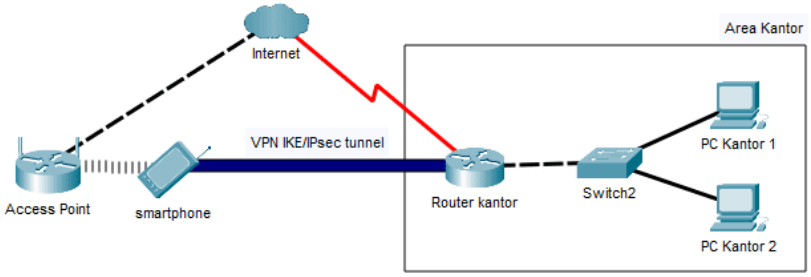
2. Metode Penelitian



Gambar 1. Diagram Metode Penelitian

Langkah pertama yang dilakukan adalah menentukan rumusan masalah pada penggunaan protokol VPN. Kemudian pengumpulan data dilakukan dengan studi pustaka mengenai jaringan VPN, macam – macam protokol, kelebihan dan kekurangan setiap protokol, serta cara kerja protokol VPN. Referensi didapatkan dari buku, jurnal, dan penelitian nasional maupun internasional.

VPN memiliki beberapa model koneksi. VPN site to site merupakan koneksi antara dua jaringan berbeda di lokasi yang berbeda melalui koneksi internet menggunakan keamanan VPN. Hal ini memungkinkan LAN pada suatu lokasi mengakses LAN pada lokasi lainnya. VPN remote access merupakan koneksi antara client dengan server jaringan. Sehingga seolah olah client berada pada jaringan yang sama dengan server yang akan di akses (Sulistiyono, 2020).



Gambar 2. Topologi jaringan VPN Remote Access

Topologi yang akan digunakan pada koneksi jaringan VPN remote access seperti pada Gambar 2. Terdapat komputer kantor yang terhubung ke internet melalui router kantor. Device di luar kantor terkoneksi ke internet. Device yang digunakan dapat berupa smartphone, laptop, atau PC. Device yang terkoneksi dengan internet akan membentuk tunnel ke router kantor. Hal ini membuat device dapat mengakses data yang ada pada komputer kantor meskipun berada di luar area kantor. Percobaan dilakukan beberapa kali menggunakan topologi yang sama dengan konfigurasi berbeda pada router kantor. Konfigurasi yang dilakukan adalah menggunanakan beberapa protokol VPN dan pada protokol IKE/IPsec dilakukan Konfigurasi menggunakan autentikasi Pre-Shared Key kemudian menggunakan konfigurasi autentikasi certificate. Kemudian melakukan koneksi hingga komputer atau device berhasil saling terkoneksi.

Metode penelitian yang digunakan adalah Kualitatif. Dimana penelitian berfokus pada pemahaman yang didapatkan dari pengalaman dan persepsi pada saat dilakukan penelitian. Data penelitian kualitatif didapatkan dari berbagai metode, yaitu wawancara, observasi dan studi pustaka (Shaheen et al., 2015)(Dr. Degdo Suprayitno et al., 2024).

Kriteria evaluasi kualitatif dan uji validasi yang digunakan dalam penelitian ini adalah mengukur Tingkat keamanan autentikasi dan enkripsi dari masing masing protokol. Membandingkan waktu koneksi ke jaringan VPN. Melakukan pengukuran tingkat kesulitan dalam konfigurasi setiap protokol VPN. Kemudian pada IKE/IPsec membandingkan menggunakan 2 autentikasi berbeda, sehingga dapat diketahui protokol IKE dengan autentikasi apa yang lebih optimal digunakan.

3. Hasil

Hasil yang didapatkan pada penelitian ini bedasarkan kriteria evaluasi kualitatif dan uji validasi adalah sebagai berikut.

Tabel 1. Perbedaan Protokol VPN

Nama Protokol	Autentikasi dan Enkripsi yang digunakan	Waktu Koneksi	Tingkat kerumitan Konfigurasi
PPTP	Username dan Password	CEPAT	Tidak Rumit
SSTP	Username, Password, certificate SSL	CEPAT	Lumayan Rumit
L2TP	Username, Password, IPsec key	CEPAT	Tidak Rumit
IPSec	Pre-Shared Key, Certificate Tandatangan digital	SEDANG	Cukup Rumit

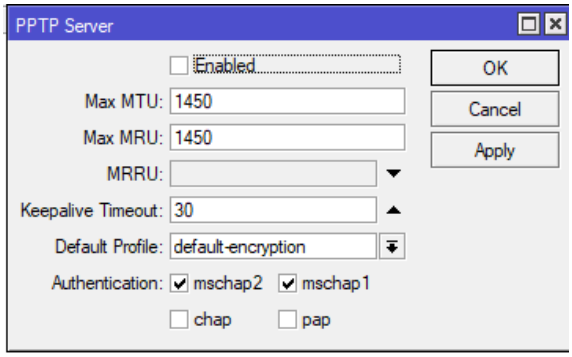
Pada protokol PPTP, client dapat terhubung dengan server VPN hanya dalam hitungan detik apabila username dan password yang dimasukkan benar. Sementara itu, pada protokol SSTP, setiap client akan mendapatkan certificate yang diberikan oleh server VPN, dan client harus menginstal certificate tersebut pada device yang akan digunakan untuk koneksi. Pada Protokol L2TP, client memasukkan password dua kali. Password pertama memverivikasi username dan password, sementara password kedua adalah Pre-Shared Key dari Ipsec. Pada protokol Ipsec, terdapat berbagai algoritma autentikasi dan enkripsi yang dapat dipilih sesuai kebutuhan dan seberapa rumit koneksi VPN yang akan dibuat. Pada saat client akan terkoneksi ke server VPN, akan melakukan beberapa cek sehingga waktu yang dibutuhkan untuk terkoneksi ke jaringan VPN akan lebih lama dibandingkan protokol VPN lainnya. Protokol PPTP dan SSTP saat ini sudah banyak dihilangkan pada device keluaran terbaru dan digantikan dengan protokol L2TP, Ipsec dan IKE.

Pada protokol IKE/Ipsec, pengggunaan autentikasi Pre-Shared Key lebih mudah saat melakukan konfigurasi pada server VPN, karena hanya memerlukan pembuatan Pre-shared Key yang digunakan oleh client untuk terhubung ke jaringan VPN. Namun, Jika menggunakan autentikasi certificate, pada server VPN harus membuatkan certificate client dan certificate server. Setiap certificate client hanya berlaku untuk satu device, sehingga akan merepotkan jika lebih dari satu device yang digunakan untuk terkoneksi ke jaringan VPN. Meskipun demikian, penggunaan autentikasi menggunakan certificate lebih aman dibandingkan menggunakan autentikasi Pre-Shared Key.

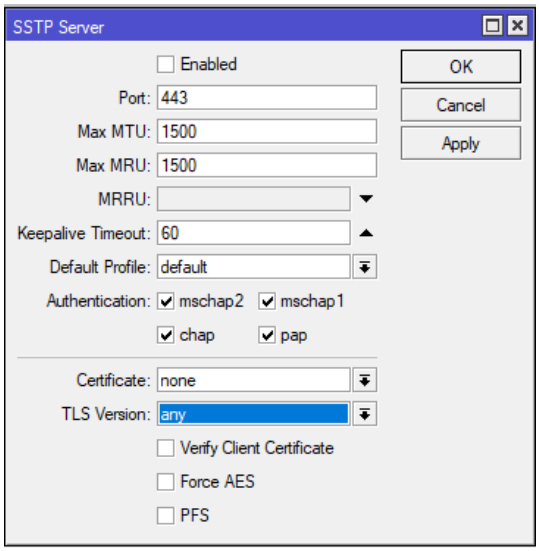
4. Pembahasan

Virtual Private Network (VPN) adalah dua jaringan berbeda yang disatukan menggunakan tunneling dan hanya beberapa orang saja yang diizinkan untuk mengakses data dalam jaringan tersebut (Tubagus Entus Madhadi & Lintang Yuniar Banowosari, 2021). VPN memanfaatkan jaringan publik yaitu internet. Hal ini dimanfaatkan oleh peretas untuk mencuri data penting yang ada pada jaringan (Nana, 2022).

Terdapat beberapa protokol yang dapat digunakan pada jaringan VPN. PPTP (Point to Point Tunneling Protocol) merupakan protokol yang memanfaatkan port TCP/IP. Username dan password digunakan untuk autentikasi client yang akan terhubung ke jaringan (Reza Arfind et al., 2023).



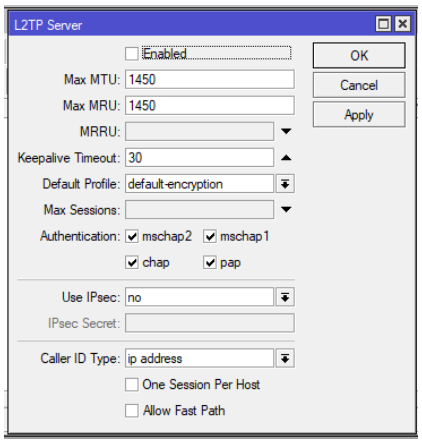
Gambar 3. PPTP Server



Gambar 4. SSTP Server

Konfigurasi yang harus dilakukan untuk PPTP server adalah mengaktifkan PPTP server, kemudian memilih konfigurasi profile, dan memilih autentikasi yang digunakan. Autentikasi yang ada pada PPTP ada beberapa, yaitu mschap2, mschap1, chap, dan pap. Kemudian melakukan konfigurasi secret. Konfigurasi ini digunakan untuk pengamanan saat user ingin terkoneksi dengan VPN PPTP. Konfigurasi PPTP client dilakukan dengan cara memasukkan IP publik dari PPTP server, kemudian memasukkan username dan password yang telah dibuat pada konfigurasi secret. Setelah kedua mikrotik terkoneksi, maka dilakukan konfigurasi routing agar LAN pada mikrotik PPTP server dapat terkoneksi dengan LAN pada mikrotik PPTP client. SSTP (Secure Socket Tunneling Protocol) merupakan protokol milik microsoft yang menggunakan SSL dan TCP (Raisul Azhar, 2017).

Konfigurasi yang dilakukan sama dengan VPN PPTP. Keamanan jaringan dapat ditambahkan dengan penggunaan certificate SSL. L2TP (Layer 2 Tunneling Protocol) merupakan gabungan protokol PPTP dengan L2F. Protokol ini memanfaatkan 2 macam tunneling, yaitu layer 2 Forwarding milik cisco dan PPTP milik microsoft (Usanto, 2021).

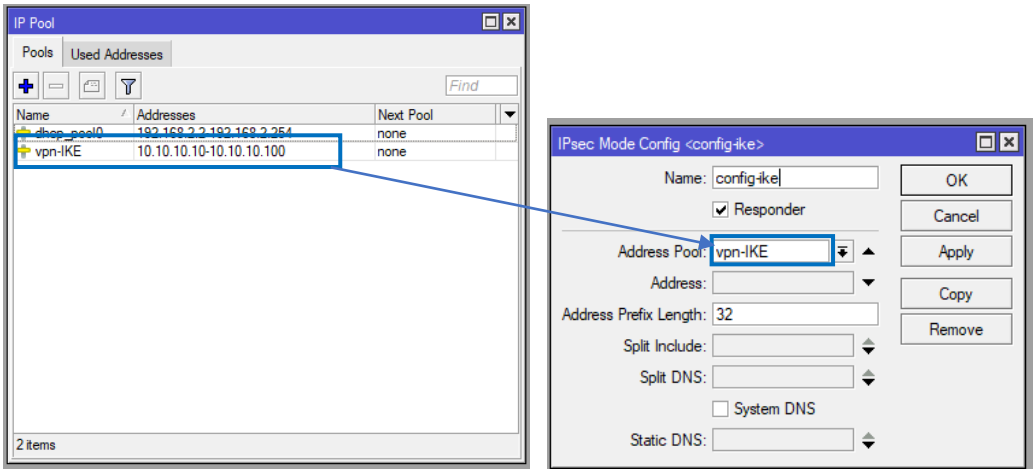


Gambar 5. L2TP Server

Penggunaan protokol L2TP sam dengan Protool PPTP, dimana membutuhkan username dan password untuk client terkoneksi dengan VPN server. Keamanan pada protokol ini diperkuat dengan penambahan penggunaan pre-shared key Ipsec.

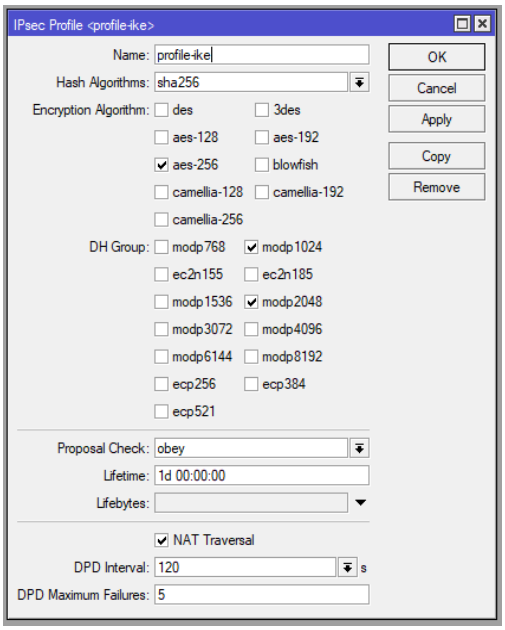
Protokol IP Security merupakan protokol keamanan menggunakan kunci kriptografi. Protokol ini bekerja pada layer 3 OSI layer (Zamalia et al., 2018). Ipsec menjamin keamanan kerahasiaan, integritas data, otentikasi, dan pertukaran kunci yang rahasia (Afifi Al-Atsari & Suharjo, 2023).

Internet Key Exchange (IKE) adalah protokol yang digunakan untuk membentuk Security Asosiation (SA) pada protokol VPN Ipsec (Marwa et al., 2013). IKE digunakan dalam mekanisme pertukaran kunci untuk membuat kunci kriptografi (Arini et al., 2015). Protokol IKE menggunakan Pre-Shared Key (PSK) dan sertifikat untuk autentikasi (Alsa'deh et al., 2013). IKE melakukan 2 fase untuk negosiasi keamanan. Fase 1 untuk membentuk IKE SA(Sadiqui, 2020). Pada fase ini, menegosiasikan algoritma kriptografi dan pertukaran Diffie-Helman. Pada fase 2 membentuk Ipsec SA (Sadiqui, 2020). Pada fase ini, melakukakan negosiasi layanan keamanan Ipsec berupa AH dan ESP (Perlman & Kaufman, 2000). Apabila fase 1 tidak berhasil melakukan negosiasi, maka tidak dapat melanjutkan ke fase 2 (Shaheen et al., 2015). Saat ini dikembangkan IKEv2 yang dapat mengatasi serangan Denial of Service (DoS) (Shaheen et al., 2015).



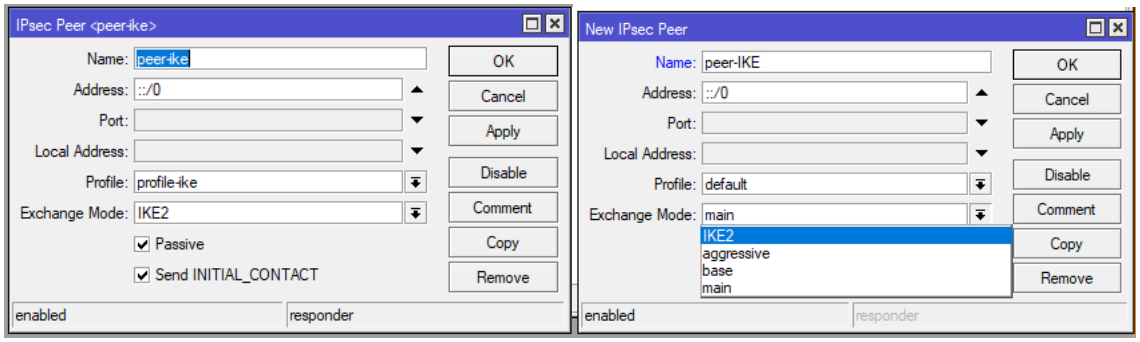
Gambar 6. Mode Ipsec Config

Konfigurasi Ipsec pada Router Mikrotik digunakan untuk menentukan konfigurasi yang digunakan. Apabila ingin memberikan IP khusus pada client yang terkoneksi dengan VPN server, maka harus membuat IP pool terlebih dahulu. Kemudian IP pool tersebut dimasukkan ke dalam address pool pada Ipsec Mode Config.



Gambar 7. Ipsec profile

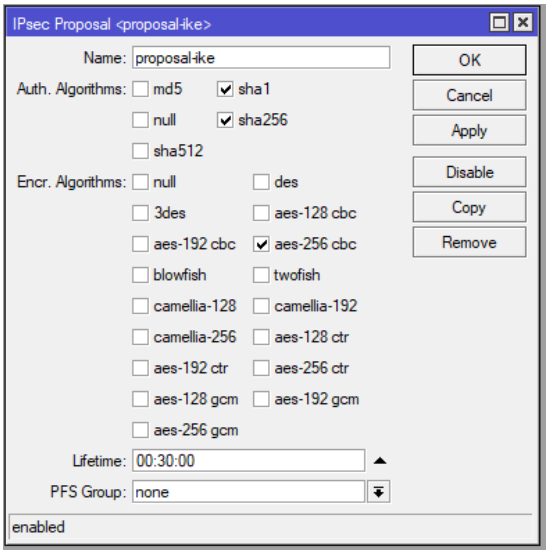
Konfigurasi Profile digunakan untuk fase 1 IPsec dalam pembuatan IKE SA. Konfigurasi profile digunakan untuk menentukan proses pertukaran kunci dan otentikasi awal koneksi. Pada Bagian ini, memilih algoritma hash, enkripsi dan DH group yang akan digunakan. Terdapat berbagai pilihan algoritma yang disediakan. Penggunaan algoritma tersebut dapat disesuaikan dengan kebutuhan keamanan VPN yang diinginkan. NAT Traversal digunakan untuk membantu IPsec melewati NAT (Network Address Translation) dikarenakan protokol ESP (Encapsulating Security Payload) pada IPsec tidak dapat dikenali oleh NAT.



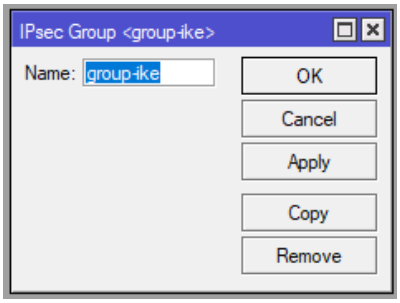
Gambar 8. IPsec Peer

Peer digunakan untuk menentukan mode yang akan digunakan. Terdapat beberapa pilihan mode. Main mode melakukan negosiasi dengan pengiriman yang aman dan membutuhkan sembilan kali pengiriman pesan, sedangkan aggressive mode dengan negosiasi dan pengiriman pesan lebih sedikit dengan mode main, sehingga proses koneksi dapat dilakukan lebih cepat. Namun mode ini tidak terlalu aman apabila digunakan. Mode IKE2 merupakan mode yang digunakan pada protokol IKEv2.

Terdapat pilihan penggunaan Passive dan send INITIAL_CONTACT. Passive digunakan untuk perangkat yang bertindak sebagai penerima koneksi. Apabila Passive digunakan, maka router bekerja dengan cara menunggu permintaan koneksi dari client. Send INITIAL_CONTACT digunakan untuk mengirimkan pesan bahwa pengirim memulai koneksi baru, sehingga apabila terdapat koneksi sebelumnya, maka akan diberhentikan atau dihapus untuk menghindari duplikasi koneksi antara dua perangkat. Keduanya dapat digunakan bersamaan.

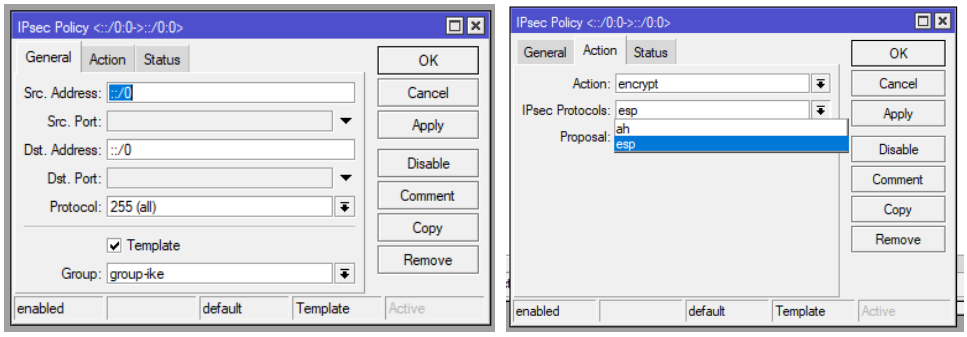


Gambar 9. IPsec Proposal



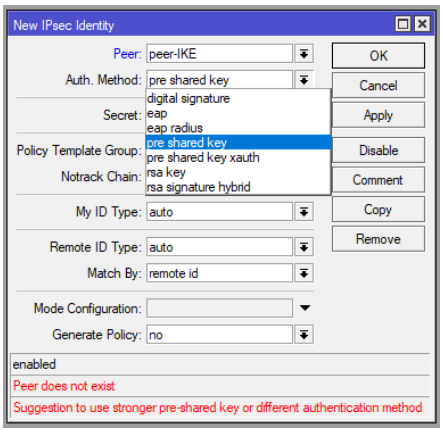
Gambar 10. IPsec Group

Pada bagian ini, memilih algoritma autentikasi dan enkripsi yang akan digunakan. Algoritma yang ada pada ipsec memiliki berbagai macam pilihan dan dapat menggunakan lebih dari satu algoritma sesuai dengan seberapa aman vpn yang akan dibuat. Lifetime digunakan untuk menentukan waktu pembuatan kunci baru setelah sesi berakhir. Proposal digunakan pada fase 2 IPsec dalam pembuatan IPsec SA. Group untuk membuat group yang akan digunakan pada saat konfigurasi IPsec.



Gambar 11. IPsec Policy

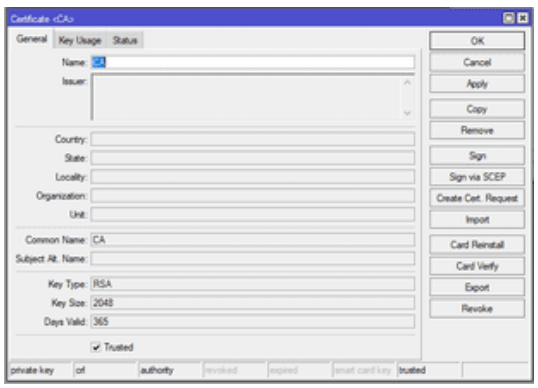
Policy digunakan untuk menentukan jalur yang akan dilindungi oleh IPsec. Tersedia pilihan Template agar memudahkan dalam melakukan konfigurasi. Src.Address digunakan untuk menentukan Alamat IP dari perangkat yang berlaku sebagai pengirim. Dst.Address digunakan untuk menentukan Alamat IP dari perangkat yang dituju. Pada Policy harus menentukan action yang digunakan,dan memilih IPsec Protokol yang terdiri dari AH dan ESP.



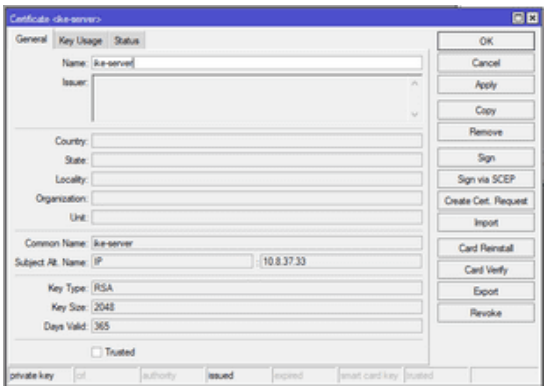
Gambar 12. IPsec Identity

Pada Identity digunakan untuk menentukan metode autentikasi yang akan digunakan. Gunakan Peer yang sudah dikonfigurasi. Metode autentikasi yang disediakan terdapat banyak pilihan dengan kerentanan dan efektifitas yang berbeda. Hal ini menentukan metode autentikasi yang digunakan oleh client saat akan terkoneksi ke VPN server.

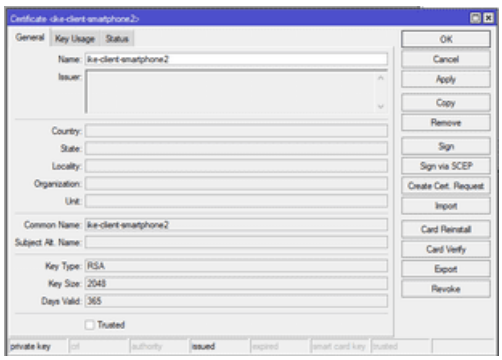
Autentikasi menggunakan Certificate menggunakan sertifikat yang ditandatangani secara digital untuk menambah keamanan saat client akan terkoneksi dengan VPN server. Mode ini menggunakan satu router mikrotik sebagai server VPN dan menerbitkan sertifikat untuk client. Sertifikat tersebut harus terinstal ke device yang akan terkoneksi dengan VPN server.



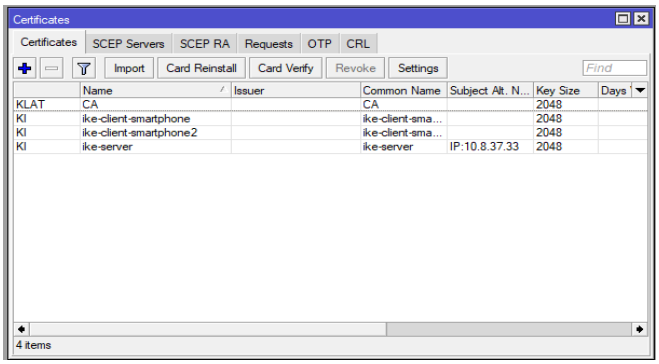
Gambar 13. Konfigurasi Certificate CA



Gambar 14. Konfigurasi Certificate Server

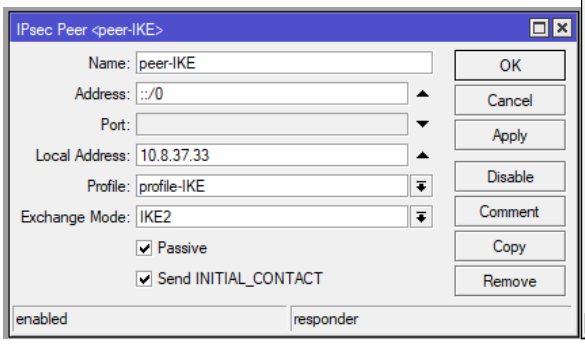


Gambar 15. Konfigurasi Sertifikat Client

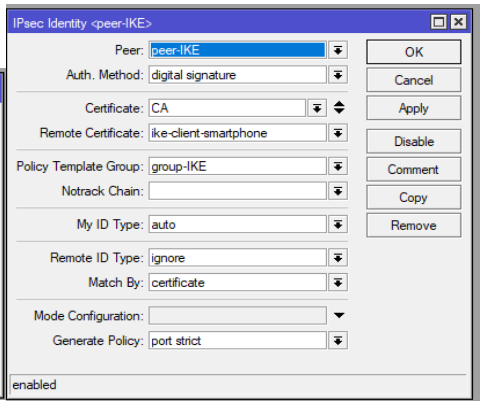


Gambar 16. Certificate yang Sudah Dibuat

Sertifikat dibuat oleh CA (Certificate Authority). Client dan server akan diberi sertifikat yang berisi kunci public dan ditandatangani oleh CA. Sertifikat tersebut digunakan untuk bertukar kunci public dan memverifikasi identitas kedua pihak.

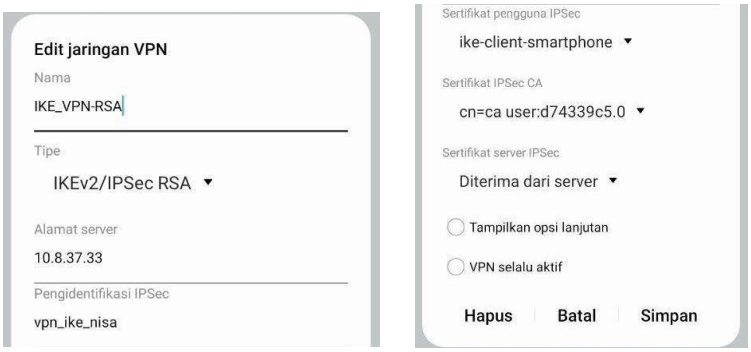


Gambar 17. Peer VPN Server Certificate



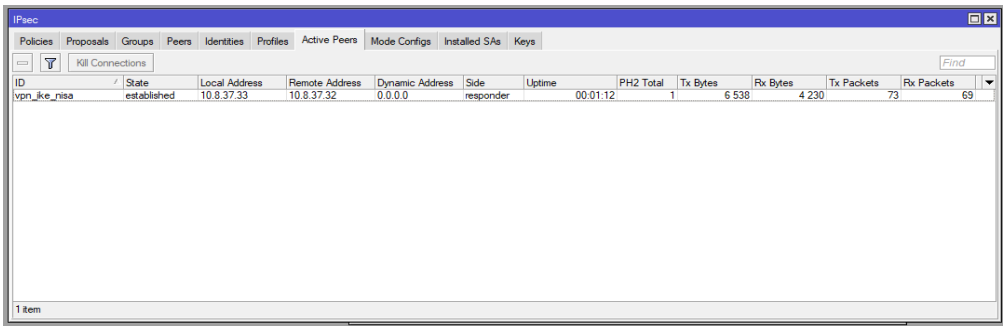
Gambar 18. Ipsec Identity VPN Server Certificate

Pada Local Address, diisi dengan IP Publik dari mikrotik. Gunakan mode IKE2, dan centang passive dan Send INITIAL_CONTACT. Hal ini digunakan karena router mikrotik berlaku sebagai penerima dan pengirim paket data. Metode autentikasi yang digunakan adalah digital signature. Gunakna certificate CA yang sudah dibuat. Pada remote certificate gunakan certificate client yang sudah dibuat. Gunakan match by certificate dan port yang digunakan adalah port strict. Port strict digunakan untuk memperkuat keamanan dengan cara memeriksa setiap port yang terkoneksi harus memiliki kesamaan dengan port yang digunakan pada saat koneksi awal. Namun hal ini dapat menimbulkan masalah apabila koneksi juga menggunakan NAT dikarenakan sulit untuk terkoneksi dengan jaringan VPN.

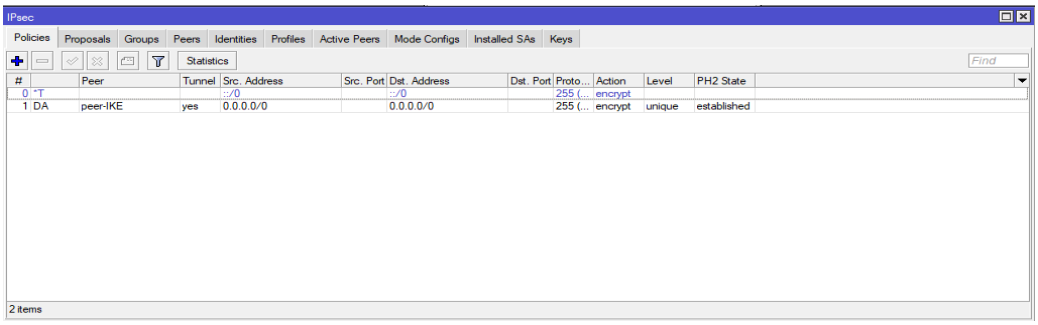


Gambar 19. Konfigurasi pada Device menggunakan Certificate

Nama digunakan untuk memberikan identitas nama koneksi vpn pada device. Pilih tipe IKEv2/Ipsec RSA, kemudian alamat server diisi dengan ip publik dari vpn server. Identifikasi Ipsec digunakna untuk memeberikan identitas device saat terkoneksi dengan vpn server. Gunakan sertifikat pengguna dan CA yang diberikan oleh server.

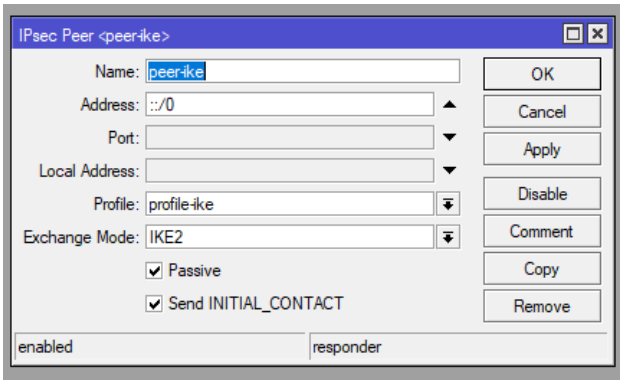


Gambar 20. Active Peers menggunakan Certificate

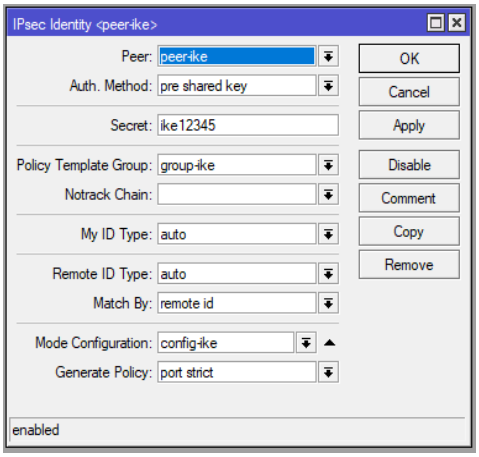


Gambar 21. Policies menggunakan Certificate

Apabila berhasil terkoneksi ke VPN server maka akan muncul seperti gambar 18 dan gambar 19. Metode autentikasi yang digunakan pada mode ini adalah Pre shared Key. Dimana client terkoneksi dengan VPN server menggunakan password yang telah dibuat.



Gambar 22. Peer VPN Server PSK

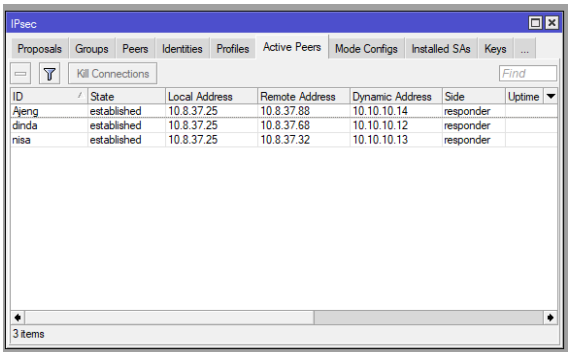


Gambar 23. Ipsec Identity VPN Server PSK

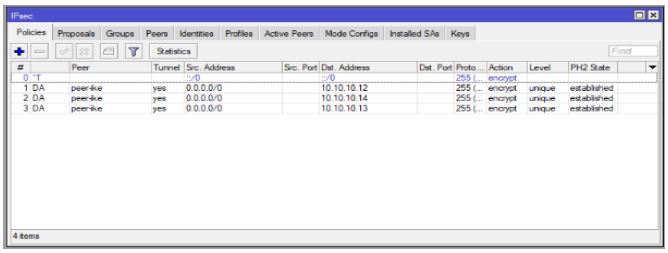
Gunakan profile yang sudah dibuat dan pilih exchange mode IKE2. Pada mode ini tidak perlu memasukkan IP Address apapun. Metode autentikasi yang digunakan adalah preshared key. Kemudian masukkan secret sebagai password client saat akan terkoneksi dengan server VPN. Gunakan port strict. Apabila menggunakan konfigurasi mode config, dapat dicantumkan pada konfigurasi tersebut.

Gambar 24. Konfigurasi pada Device menggunakan PSK

Alamat server diisi IP publik dari VPN server. Pengindentifikasi IPSec digunakan untuk ID device yang terkoneksi dengan VPN server. Masukkan secret yang sudah ditentukan pada pra-bagi IPsec. Apabila client berhasil terkoneksi dengan VPN, maka akan muncul seperti pada gambar 25 dan pada gambar 26.



Gambar 25. Active Peers menggunakan PSK



Gambar 26. Policies menggunakan PSK

5. Kesimpulan

Berdasarkan hasil dari penelitian yang telah dilakukan, dapat disimpulkan bahwa penggunaan Protokol IKE/Ipsec pada jaringan VPN dikatakan aman, karena protokol ini menawarkan berbagai algoritma enkripsi dan autentikasi yang lebih kuat dibandingkan dengan protokol VPN lainnya. Selain itu, Protokol IKE/Ipsec juga memiliki fleksibilitas yang tinggi, karena dapat digunakan pada berbagai perangkat untuk membangun koneksi, seperti komputer dan smartphone. Protokol IKE/Ipsec didukung dengan dua autentikasi untuk mengamankan jaringan, yaitu Pre-Shared Key dan sertifikat yang memungkinkan pengamanan jaringan sesuai dengan kebutuhan dan Tingkat keamanan yang diinginkan.

Penelitian ini dapat dikembangkan lagi dengan meneliti pengujian pada kondisi jaringan tertentu, Penggunaan protokol IKE/IPsec pada perangkat lain, atau studi lebih lanjut mengenai algoritma enkripsi yang digunakan pada protokol IPsec.

Referensi

Afifi Al-Atsari, H., & Suharjo, I. (2023). Integrasi Server On-Premise dengan Server Cloud Menggunakan Cloud VPN dan Mikrotik Ipsec Untuk Peningkatan Keamanan Koneksi. *Jurnal Syntax Admiration*, *4*(11), 1977–1996. https://doi.org/10.46799/jsa.v4i11.757

Alsa'deh, A., Meinel, C., Westphal, F., Gawron, M., & Groneberg, B. (2013). CGA integration into IPsec/IKEv2 authentication. *SIN 2013 - Proceedings of the 6th International Conference on Security of Information and Networks*, 326–330. https://doi.org/10.1145/2523514.2527097

Arini, MT, & Patmono, G. (2015). Analisis dan Pengujian Permasalahan Pada Sistem Remote Access IPsec. *FST UIN Syarif Hidayatullah*.

Dr. Degdo Suprayitno, Dr. Ahmad, Tartila, Dr. Ir. H. Sa'dianoor, & Dr. Yuri Alfrin Aladdin. (2024). *METODOLOGI PENELITIAN KUALITATIF : Teori Komprehensif dan Referensi Wajib bagi Peneliti*. PT. Sonpedia Publishing Indonesia.

Marwa, A., Malika, B., & Nacira, G. (2013). Contribution to enhance IPSec security by a safe and efficient internet key exchange protocol. *2013 World Congress on Computer and Information Technology, WCCIT 2013*, 1–5. https://doi.org/10.1109/WCCIT.2013.6618745

Nana, D. I. M. (2022). Optimasi Keamanan Jaringan Point to Point Menggunakan VPN IPSec dan GRE. *Jurnal Jupiter*, *14*(2).

Perlman, R., & Kaufman, C. (2000). Key exchange in IPSec: analysis of IKE. In *IEEE Internet Computing*. https://doi.org/10.1109/4236.895016

Raisul Azhar. (2017). ANALISA QOS PADA JARINGAN SITE TO SITE VPN MENGGUNAKAN PROTOCOL SSTP. *Proceeding Seminar Nasional & Ilmu Sosial 2017*.

Reza Arfind, Hendra Supendar, & Riza Fahlapi. (2023). Perancangan Virtual Private Network Dengan Metode PPTP Menggunakan Mikrotik. *Jurnal Komputer Antartika*, *1*(3).

Sadiqui, A. (2020). *Computer Network Security*. ISTE. https://doi.org/10.1201/9781420093759.ch25

Shaheen, S. H., Yousaf, M., & Majeed, M. Y. (2015). Comparative analysis of Internet Key Exchange protocols. *International Conference on Information and Communication Technologies*. https://doi.org/10.1109/ICICT.2015.7469595

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. https://doi.org/10.30656/prosisko.v7i2.2523

Tubagus Entus Madhadi, & Lintang Yuniar Banowosari. (2021). Analisis Perbandingan Performasi QoS VPN Encryption Protocol Pada Jaringan Berbasis Hybrid Cloud. *Jurnal Ilmiah Komputasi*, *20*(1). https://doi.org/10.32409/jikstik.20.1.2695

Usanto, U. (2021). RANCANG BANGUN JARINGAN SITE TO SITE VPN (VIRTUAL PRIVATE NETWORK) DENGAN PROTOCOL OPENVPN. *JEIS: JURNAL ELEKTRO DAN INFORMATIKA SWADHARMA*, *1*(2), 55–65. https://doi.org/10.56486/jeis.vol1no2.180

Zamalia, W. O., Aksara, L. M. F., & Yamin, Muh. (2018). Analisis Perbandingan Performa Qos, Pptp, L2Tp, Sstp Dan Ipsec Pada Jaringan Vpn Menggunakan Mikrotik. *SemanTIK*, *4*(2), 29–36.