JSI : Jurnal Sistem Informasi *(E-Journal), VOL.12, NO.1, April 2020*
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsifasilkom@unsri.ac.id

Interkoneksi *Site-to-Site* dan *Remote Access* Menggunakan Virtual Private Network dan IP Security

Muhammad Arif[1], Ade Surya Budiman[2]
[1] Program Studi Teknik Informatika, STMIK Nusa Mandiri, Jakarta
[2] Program Studi Teknologi Komputer, FTI, Universitas Bina Sarana Informatika, Jakarta
[1]muhammad.arif2405@gmail.com, [2]ade.aum@bsi.ac.id

Abstrak

Interkoneksi antar lokasi jaringan komputer (site-to-site network) sangat diperlukan dalam kaitannya dengan pengembangan organisasi. Pengembangan organisasi baik perusahaan swasta maupun instansi pemerintah umumnya berimplikasi kepada penambahan atau perluasan wilayah kerja. Dengan wilayah kerja yang semakin luas, tentunya akan membutuhkan fleksibilitas dalam proses komunikasi data antar wilayah. Untuk menunjang fleksibilitas komunikasi data antar wilayah, jaringan komputer harus dibangun menyesuaikan dengan kebutuhan organisasi tersebut. PT. Sab'a System Solution merupakan sebuah perusahaan swasta yang memperluas wilayah kerja hingga ke Semarang. Jarak yang jauh antara kantor pusat di Jakarta dengan kantor cabang di Semarang, membutuhkan infrastruktur jaringan komputer yang tepat agar kedua site dapat saling terhubung dan dipergunakan dalam komunikasi data. Solusi yang paling efektif dan efisien untuk menghubungkan kedua site tersebut adalah dengan menerapkan site-to-site Virtual Private Network (VPN) dan remote-access VPN untuk menunjang kebutuhan komunikasi bagi mobile user. Dalam penelitian ini, analisa, perencanaan dan desain VPN dilakukan menggunakan software simulator, sekaligus juga untuk menguji efektifitasnya jika nantinya diterapkan pada interkoneksi site-to-site. VPN yang di desain dalam penelitian ini dipadukan dengan IP Security (IPSec) sebagai protokol penunjang keamanan VPN tunnel, ketika data ditransmisikan melalui jalur publik/internet. Dari hasil pengujian, menggunakan software simulator, komunikasi data antar site bisa berjalan dengan lancar serta data telah terenkripsi dengan aman ketika melintasi jalur publik/internet.

Kata kunci: *Site-to-site VPN, IP Security, Remote-Access VPN, Desain Jaringan*

Abstract

Interconnection between computer network locations (site-to-site network) is needed in relation to organizational development. The organizational development of both private companies and government agencies generally has implications for the addition or expansion of work areas. With an increasingly broad work area, of course, will require flexibility in the process of data communication between regions. To support the flexibility of data communication between regions, computer networks must be built to suit the needs of the organization. PT. Sab'a System Solution is a private company that expands the working area to Semarang. The great distance between the head office in Jakarta and the branch office in Semarang, requires proper computer network infrastructure so that the two sites can be connected and used in data communication. The most effective and efficient solution to connect the two sites is to implement a site-to-site Virtual Private Network (VPN) and remote-access VPN to support the communication needs of mobile users. In this research, VPN analysis, planning and design are carried out using a simulator software, as well as to test its effectiveness if it were applied in site-to-site interconnection. The VPN that was designed in this study was integrated with IP Security (IPSec) as a protocol to support VPN tunnel security, when data is transmitted through public / internet channels. From the test results, using the simulator software, data communication between sites can run smoothly and the data has been encrypted safely when crossing public / internet lines.

Keywords*: Site-to-site VPN, IP Security, Remote-Access VPN, Network Design*

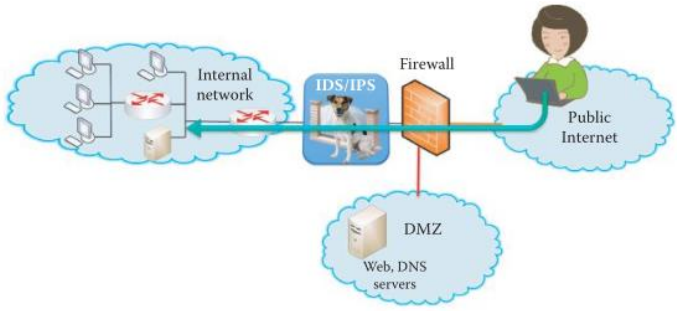
1. PENDAHULUAN

Interkoneksi antar komputer yang tanpa batasan jarak dan wilayah merupakan tujuan jangka panjang yang terus diperbaiki serta dikembangkan, dengan beragam metode dan teknologi. Jaringan Komputer yang merupakan terminologi dari interkoneksi

antar komputer, dipergunakan untuk memungkinkan beberapa *host* (perangkat) untuk bisa saling bertukar informasi [1].

Jaringan komputer tidak hanya harus dapat menghubungkan pengguna yang berada pada lokasi berdekatan, namun jaringan komputer harus mampu menghubungkan pengguna yang berada di lokasi yang berjauhan. Sebuah organisasi dapat dengan mudah membangun infrastruktur jaringan yang berada di wilayah yang sama dan kecil. Tantangan terbesar bagi pengembangan infrastruktur jaringan komputer sebuah organisasi adalah bagaimana menghubungkan infrastruktur jaringan komputer antar wilayah yang berjauhan. Pemanfaatan infrastruktur jaringan komputer publik (*public internet*) menjadi solusi paling efektif dan efisien, ketimbang membangun infrastruktur milik sendiri yang membutuhkan investasi besar dalam perencanaan, pengembangan hingga perawatannya. Namun, keamanan menjadi isu yang sangat penting untuk bisa dikendalikan dalam penggunaan *public internet.* Untuk melindungi akses keluar masuk data organisasi ketika melewati *public internet* adalah dengan mengoperasikan sistem *Virtual Private Network* (VPN)

Banyak perusahaan mengoperasikan VPN yang memungkinkan pengguna jaringan mereka untuk mendapatkan akses terhadap sumber daya jaringan (*network resources*) dengan aman, ketika menggunakan perangkat *mobile* (seperti *laptop* dan *smartphone*) dari lokasi yang berjauhan (*remote*) maupun ketika berada di jaringan publik yang tidak dijamin keamanannya (*unsecured network*) [2]. Untuk menjamin keamanan jaringan internal (*internal network*) dari *public internet*, diperlukan *Firewall* yang merupakan "pagar pengaman" antara jaringan internal dengan *internal network*. Seperti terlihat dalam Gambar 1, keberadaan jalur VPN (VPN *tunnel*) memungkinkan *user* jaringan dari sebuah organisasi dapat berinteraksi dengan *internal network* kendati berada di *public internet* [3].



Gambar 1. Ilustrasi Penerapan VPN dari *Public Internet* [3].

VPN dirancang dengan menggunakan *tunneling,* otentikasi dan algoritma enkripsi sehingga mampu menyediakan kanal transmisi data virtual yang aman dan tersembunyi (*virtual hidden secure channel*), di dalam suatu jaringan publik atau internet [4]. Kanal trasmisi inilah yang disebut sebagai VPN *Tunnel*.

Konsep *Bring Your Own Device* (BYOD) dalam suatu organisasi menjadi sebuah filosofi yang terus berkembang penggunaannya. BYOD diperlukan untuk menunjang kinerja melalui kebebasan ruang gerak dan mobilitas karyawan, mengurangi biaya infrastruktur jaringan, merubah struktur ruang kerja dan meningkatkan kolaborasi antar karyawan [5]. Tantangan utama dari BYOD diantaranya adalah terkait keamanan informasi organisasi [6], yang bersumber dari potensi masalah keamanan akses data menggunakan *mobile device* melalui jalur internet atau jalur publik. Dalam hal ini VPN dapat diterapkan untuk memastikan keamanan jalur akses ke dalam server internal

perusahaan, dengan tujuan untuk memastikan otentikasi, otorisasi dan akuntabilitas pengakses jaringan internal perusahaan.

VPN telah diimplementasikan dalam banyak kasus dan tujuan, diantaranya adalah kemudahan dalam perbaikan data akademik kampus yang berada di beberapa *site* yang berjauhan, secara aman disertai dengan efisiensi dari sisi biaya [7], kemudahan dalam konsolidasi data sensitif seperti data keuangan siswa pada masing-masing unit sekolah yang bisa diakses secara *remote* antar jaringan sekolah [8], serta untuk menurunkan potensi serangan terhadap data selama proses transmisi data melalui jalur publik [9].

Mengarah kepada fungsionalitas yang lebih besar, efektifitas VPN untuk jaringan dengan jangkauan luas (*Wide Area Network*), dimana lokasi antar *site* sangat jauh (misalnya lintas kota atau lintas provinsi) bisa terus diuji dan diperbaiki. Hal ini terkait dengan kinerja transmisi data dan keamanan dalam proses transmisi data tersebut.

Mengacu kepada deskripsi yang telah dijabarkan tersebut, dalam penelitian ini, penulis melakukan perencanaan dan skema implementasi *site-to-site* VPN atau desain VPN, dengan studi kasus pada PT. Sab'a System Solution (selanjutnya dalam artikel ini disingkat sebagai PT. SSS). Jaringan komputer yang dimiliki PT. SSS tersegmentasi dalam dua *site* yang cukup berjauhan yaitu antara *site* Jakarta (kantor pusat) dan *site* Semarang (kantor cabang).

Selanjutnya, dalam penelitian ini juga dikembangkan pada uji coba penerapan *remote-access* VPN pada router yang terdapat di *site* Jakarta, khusunya bagi *mobile user* dalam kaitannya dengan penerapan BYOD dan *telecommuting workers*, utamanya dalam pengaksesan web server perusahaan. Metode keamanan yang digunakan pada desain *tunneling* VPN ini berupa *Internet Protocol Security* (IPSec). IPSec merupakan jenis *tunneling* VPN yang bekerja pada lapis arsitektur jaringan ke-3 (3rd *layer*) atau *Network* Layer, sehingga berperan dalam mengamankan data pada lapisan yang berada di atasnya. IPSec bertugas menjaga keamanan IP *datagram* ketika paket ditransmisikan, dikarenakan paket IP (IP *Package*) itu sendiri tidak memiliki keamanan, yang membuat isi dan alamat paket mudah diketahui [10].

2. METODE PENELITIAN

Metode yang dipakai dalam desain jaringan komputer PT. SSS ini mengacu kepada serangkaian tahapan yang diadaptasikan dari *System Development Life System* (SDLC) dalam lingkungan jaringan komputer, yang terdiri atas analisa kebutuhan, desain, instalasi/penerapan, pengujian dan evaluasi.

Akan tetapi, di dalam penelitian ini penulis membatasi lingkup penelitian hanya pada tahapan desain, maka tahapan instalasi/implementasi, pengujian fisik dan evaluasi tidak dilakukan. Untuk desain jaringan ini, penulis membagi tahapan desain kedalam rangkaian tahapan yang disebut sebagai Metode Desain Jaringan (*Network Design Methodologies*) yang terdiri atas 3 tahapan[11]:

a. Identifikasi kebutuhan jaringan, termasuk didalamnya kebutuhan pengguna (*Network and User Requirement*)

Dalam tahapan ini penulis melakukan analisa mengenai permasalahan dan kebutuhan dari organisasi yang merupakan objek penelitian ini. Analisa kebutuhan ini diperoleh dari data utama (*primary data*) yang bersumber dari hasil observasi dan wawancara dengan *stakeholder* terkait. Dari data utama tersebut, diperoleh *summary* kebutuhan jaringan dan pengguna adalah sebagai berikut:

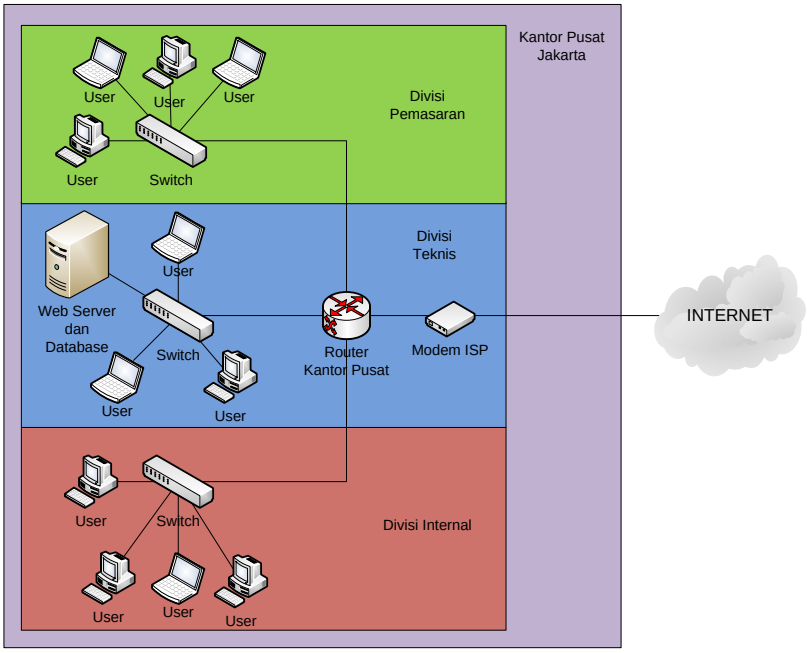
i. Organisasi harus memiliki interkoneksi antar *site*, yang memudahkan pengiriman dan penerimaan data antar lokasi yang berjauhan (dalam hal ini berbeda kota dan provinsi)

JSI : Jurnal Sistem Informasi *(E-Journal), VOL.12, NO.1, April 2020*
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsifasilkom@unsri.ac.id

ii. Jaringan harus menyediakan jalur lalu lintas data yang aman (*secure*) dan bisa dihandalkan (*reliable*)
iii. Server perusahaan harus dapat diakses melalui jaringan publik atau jaringan internet, untuk karyawan yang bekerja *remote* atau *telecommuting*.

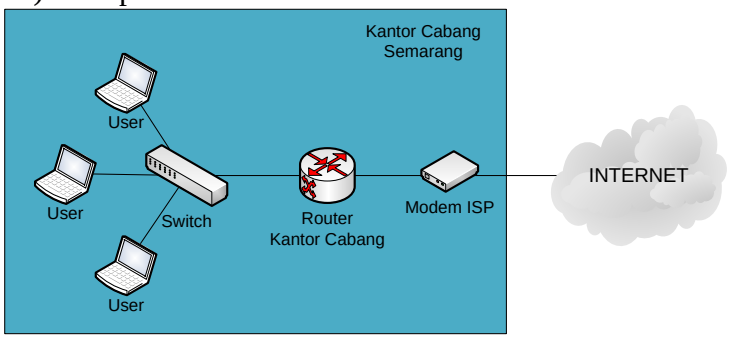
b. Pengenalan Karakter dari Jaringan Yang Dipergunakan Saat ini

Berikut ini merupakan skema masing-masing *site* yang akan dihubungkan menggunakan VPN *tunnel*. Pada gambar 2, diperlihatkan kantor pusat yang berada di Jakarta memiliki sebuah komputer server yang memberikan layanan web dan *database*. Setiap data harus disimpan pada server terpusat, sehingga untuk proses akses data juga akan bersumber dari pusat data yang sama. Karyawan juga bisa mengakses website perusahaan melalui web server yang terdapat di kantor pusat.



Gambar 2. Skema Jaringan Komputer Kantor Pusat Di Jakarta

Sebagai bagian dari strategi pengembangan bisnis perusahaan, di Semarang ditempatkan kantor cabang. Berbeda halnya dengan kantor pusat, lalu lintas jaringan di kantor cabang tidak melibatkan server sebagai penyimpanan data terpusat maupun penyedia layanan web, sebagaimana terlihat dalam Gambar 3. Akan tetapi, banyak data yang harus dikirimkan maupun diterima dari dan ke kantor pusat di Jakarta. Media surat elektronik (*e-mail*) merupakan sarana utama transmisi data antar dua *site* tersebut.

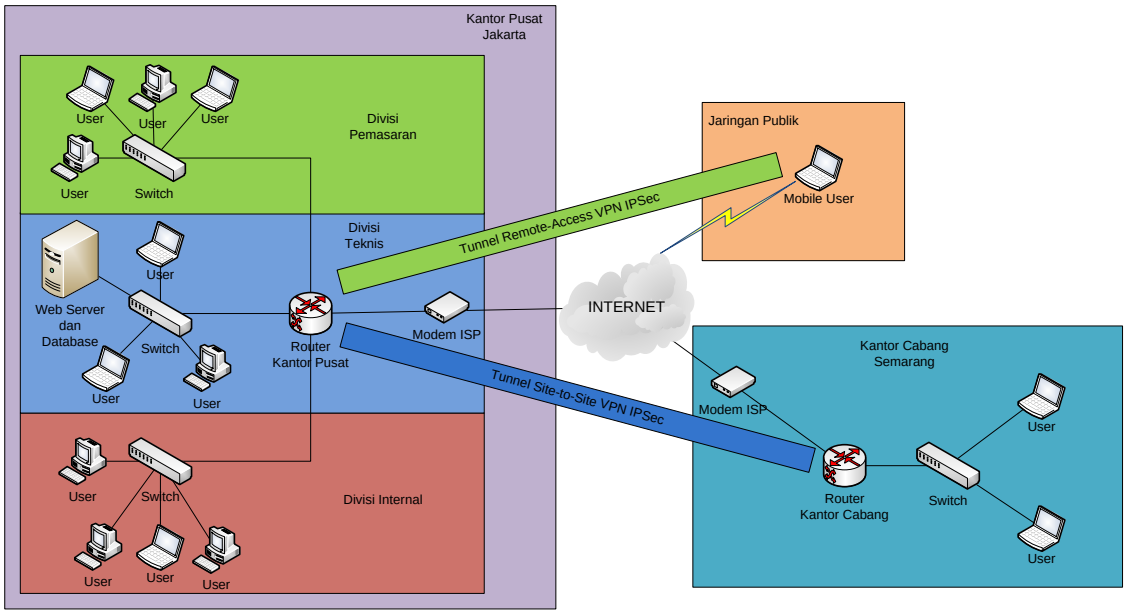


Gambar 4. Skema Jaringan Komputer Kantor Cabang di Semarang

Sebagai tambahan, di kedua *site* Router berperan juga sebagai DHCP *Server* yang memberikan layanan pemberian konfigurasi *host*, pada masing-masing *site*. Secara umum perangkat keras dan perangkat lunak yang terdapat di masing-masing *site* tetap bisa dipergunakan sebagaimana mestinya. Penambahan komponen keamanan jaringan hanya dibutuhkan untuk VPN *tunneling* yang menghubungkan antar *site*, yaitu nantinya akan menggunakan IPSec sebagai protokol keamanannya.

c. Desain Topologi Jaringan dan Solusi.

Mengacu kepada hasil identifikasi kebutuhan jaringan dan pengguna, serta mempertimbangkan karakteristik dari jaringan komputer di masing-masing *site*, penulis merancang desain topologi dan skema jaringan yang diusulkan untuk diterapkan dalam interkoneksi *site-to-site* PT. SSS.



Gambar 5. Desain Topologi Interkoneksi *Site-to-site VPN*

Skema jaringan secara fisik tidak mengalami perubahan. Perubahan yang dilakukan bersifat *logic* dengan menambahkan beberapa konfigurasi untuk membangun interkoneksi *site-to-site VPN*. Konfigurasi tersebut diterapkan pada perangkat *router* di kantor pusat Jakarta dan kantor cabang Semarang. Selain itu, *router* kantor pusat di Jakarta juga akan ditambahkan konfigurasi untuk dijadikan sebagai *remote-access VPN Server* dengan metode *IPSec*, agar bisa diakses secara aman oleh *mobile user* melalui jaringan publik (jaringan internet).

3. HASIL DAN PEMBAHASAN

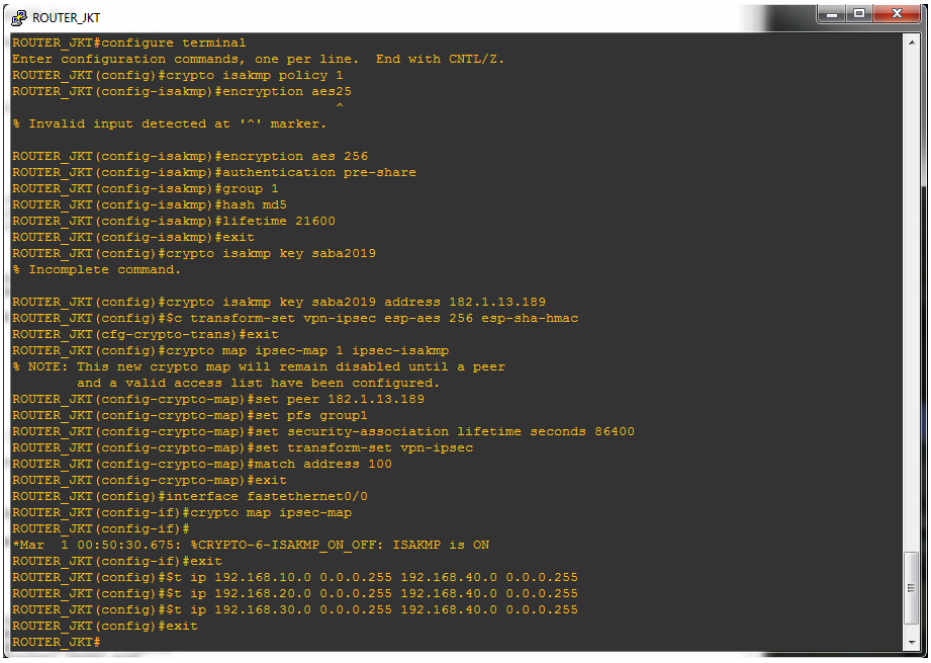
3.1. Konfigurasi *Site-to-Site VPN*

Untuk dapat menjalankan *site-to-site VPN*, perlu dilakukan konfigurasi pada setiap *router* di kantor pusat maupun kantor cabang. Router Jakarta dinamakan sebagai ROUTER_JKT, sedangkan Router di kantor cabang Semarang, dinamakan sebagai ROUTER_SMG.

Pada bagian awal konfigurasi, diberikan perintah yang menentukan mekanisme pertukaran *security key*, atau dengan kata lain memastikan kedua host yang akan dikoneksikan menyetujui penggunaan IPSec, ditandai dengan menentukan algoritma enkripsi yang dipergunakan [11]. Protokol ini dinamakan sebagai *Internet Security*

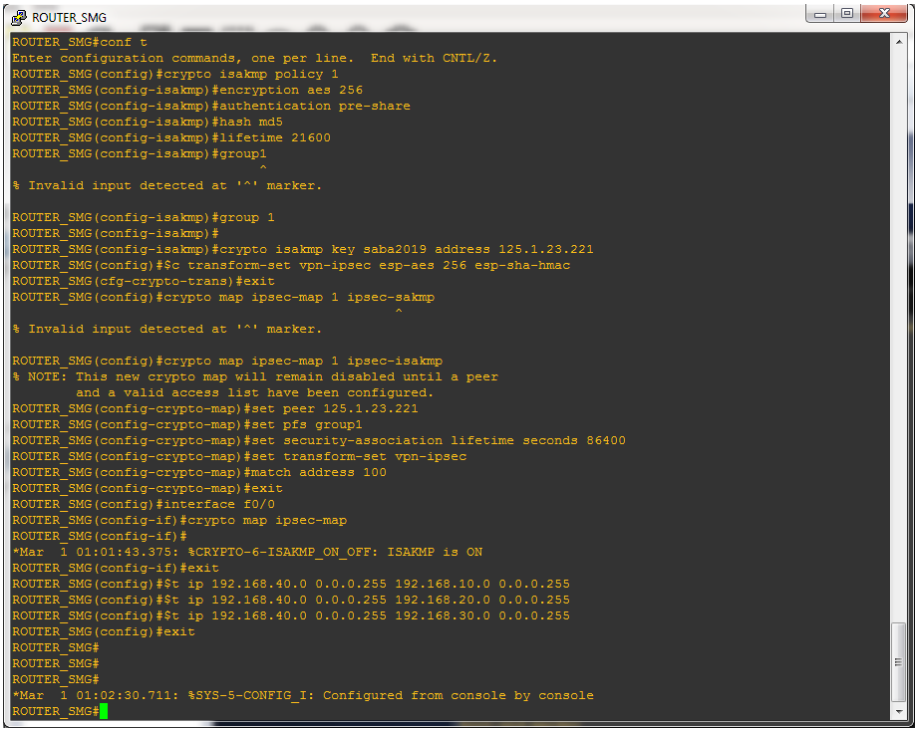
JSI : Jurnal Sistem Informasi *(E-Journal), VOL.12, NO.1, April 2020*
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsifasilkom@unsri.ac.id

Association dan Key Management Protocol (ISAKMP). Dalam kasus ini dipergunakan enkripsi Advanced Encryption Standard (AES) 256 bit. Konfigurasi diawalai dengan memasukkan perintah *crypto isakmp policy 1*. Didalam Gambar 6 terlihat konfigurasi lengkap yang dimasukkan di *router* kantor pusat Jakarta.



Gambar 6. Konfigurasi *Site-to-Site VPN* Kantor Pusat

Dengan konfigurasi yang hampir sama, untuk konfigurasi di kantor cabang diperlihatkan pada gambar 7.



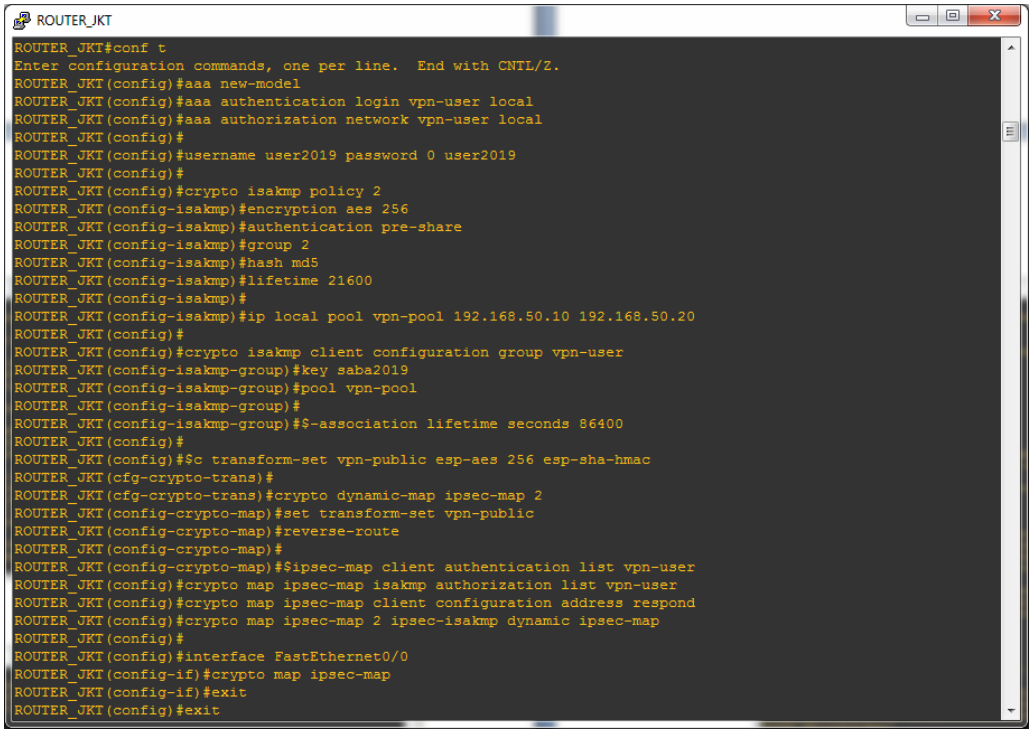
Gambar 7. Konfigurasi *Site-to-Site VPN* Kantor Cabang

JSI : Jurnal Sistem Informasi *(E-Journal), VOL.12, NO.1, April 2020*
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsifasilkom@unsri.ac.id

3.2. Konfigurasi Remote-access VPN

Selain difungsikan sebagai *site-to-site VPN*, router kantor pusat juga akan difungsikan sebagai *remote-access VPN server*. Hal ini dimaksud agar *mobile user* dapat terhubung dengan jaringan lokal kantor pusat melalui jaringan publik.

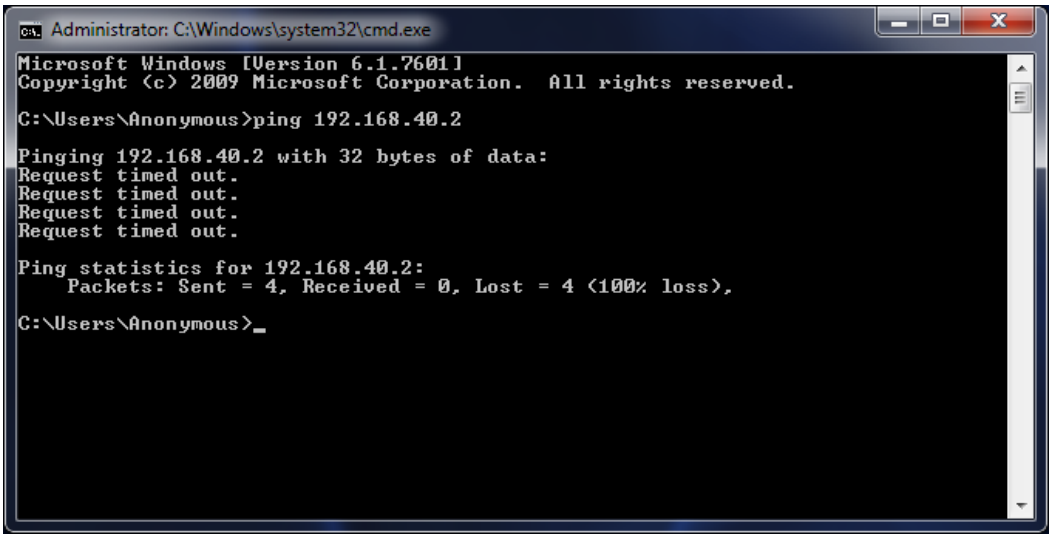
Untuk konfigurasi *remote-access VPN server* di kantor pusat Jakarta, diperlihatkan didalam gambar 8.



Gambar 8. Konfigurasi *Remote-Access VPN* Kantor Pusat

3.3. Pengujian Awal

Hasil uji *packet loss* dari jaringan lokal kantor pusat ke jaringan lokal kantor cabang dipergunakan perintah *ping* melalui panel *command prompt*, yang diperlihatkan dalam gambar 9.



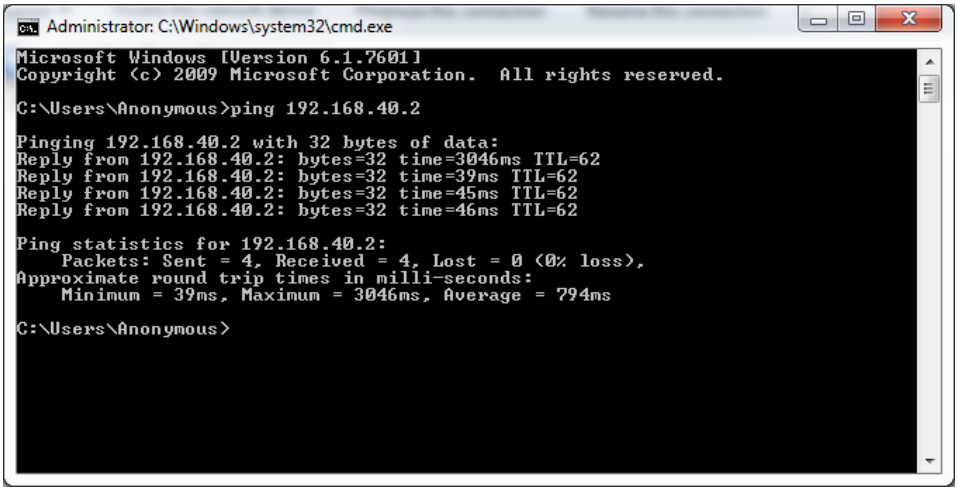
Gambar 9. Hasil Ping dari Kantor Pusat ke Kantor Cabang

JSI : Jurnal Sistem Informasi *(E-Journal), VOL.12, NO.1, April 2020*
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsifasilkom@unsri.ac.id

Dari hasil uji *packet loss* yang dilakukan, diperoleh data bahwa pengiriman packet dari tiap lokasi menunjukan hasil *100% loss*, yang berarti paket yang dikirim tidak sampai ke alamat tujuan. Ini membuktikan bahwa jaringan lokal kantor pusat dan jaringan lokal kantor cabang benar-benar tidak terhubung.

3.4. Pengujian Akhir

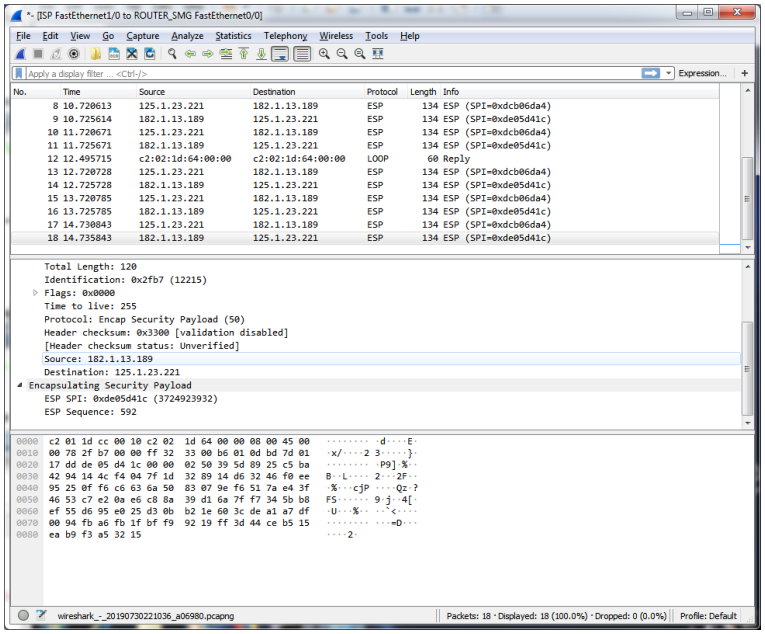
Pengujian jaringan akhir dilakukan setelah konfigurasi VPN IPSec sudah diterapkan pada masing-masing lokasi. Pengujian jaringan akhir dilakukan 2 tahap, yaitu pengujian jaringan *site-to-site VPN* dan pengujian jaringan *remote-access VPN*. Hasil pengujian untuk jaringan *site-to-site VPN* diperlihatkan didalam gambar 10.



Gambar 10. *Ping Test Site-to-Site VPN*

Uji packet loss yang dilakukan menunjukan hasil *0% loss*, hal ini berarti bahwa paket yang dikirimkan berhasil sampai ke alamat tujuan.

Pengujian selanjutnya dengan menggunakan aplikasi Wireshark untuk melihat apakah paket yang dikirimkan telah terenkripsi atau tidak.

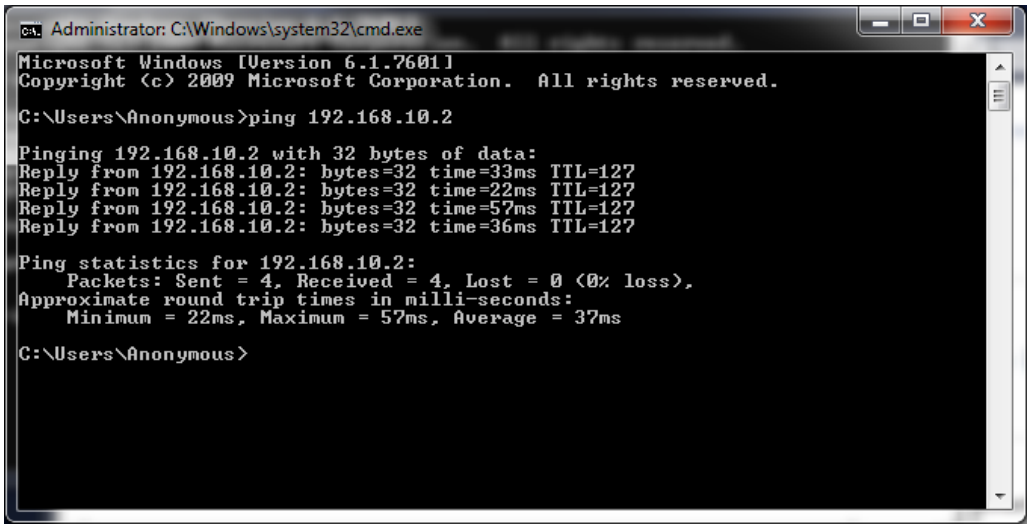


Gambar 11. Uji Wireshark *Site-to-SIte VPN*

JSI : Jurnal Sistem Informasi *(E-Journal), VOL.12, NO.1, April 2020*
ISSN Print : 2085-1588
ISSN Online :2355-4614
http://ejournal.unsri.ac.id/index.php/jsi/index
email: jsifasilkom@unsri.ac.id

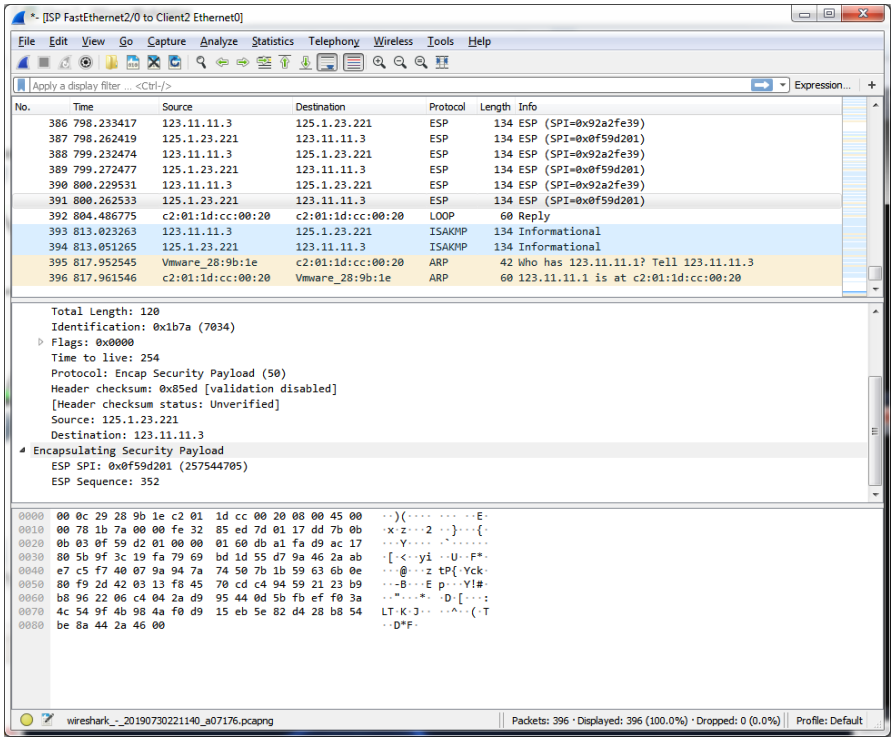
Hasil uji dengan menggunakan Wireshark yang diperlihatkan dalam gambar 11, menunjukkan bahwa paket yang dikirimkan sudah terenkripsi didalam protokol *Encapsulating Security Payload* (*ESP*), sehingga paket tidak mudah diketahui isinya. Selain itu, alamat IP asal dan tujuan sebenarnya dari paket yang dikirim juga tidak bisa diketahui, hanya diketahui alamat IP asal dan tujuan penghubung *tunnel*.

Langkah selanjutnya adalah pengujian jaringan *remote-access VPN*. Pengujian *remote-access VPN* juga dilakukan dengan cara yang sama, yaitu *packet loss test* dan pengujian dengan menggunakan *Wireshark*.



Gambar 12. *Ping Test Remote-Access VPN*

Pada pengujian *packet loss* seperti ditunjukkan pada gambar 12 diatas, didapatkan hasil berupa *0% loss* yang berarti paket yang dikirim juga berhasil sampai ke alamat tujuan.



Gambar 13. Uji Wireshark *Remote-Access VPN*

Untuk pengujian dengan menggunakan Wireshark, didapatkan hasil seperti ditunjukkan dalam gambar 13, bahwa koneksi yang dibangun sudah terenkripsi menggunakan ISAKMP dan ESP.

4. KESIMPULAN

Dari penelitian yang telah dilakukan oleh penulis, dapat disimpulkan beberapa hal berikut:

a. Interkoneksi antar lokasi jaringan (site-to-site network) dapat diterapkan dengan menggunakan Virtual Private Network (VPN), dengan mempertimbangkan fleksibilitas dan penunjang keamanan yang diberikan.
b. IP *Security* (IPSec) merupakan salah satu protokol keamanan yang dapat dipilih untuk membangun VPN *tunnel*, dengan menggunakan proses enkripsi data.
c. Dari hasil pengujian terhadap desain *site-to-site* VPN, terlihat bahwa komunikasi data dapat berjalan lancar meskipun menggunakan jalur publik/internet.
d. Dari hasil pengujian juga terlihat bahwa *remote-access* VPN dapat berjalan dengan baik ketika diakses dari jalur publik/internet oleh *mobile user*.

Untuk penelitian selanjutnya, dapat dilakukan pengujian konektifitas dengan menggunakan protokol keamanan selain IPSec maupun menggabungkan dengan protokol keamanan pada layer diatasnya seperti TLS dan SSH. Disamping, itu dapat pula diujicobakan pada interkoneksi lebih dari 2 site.

REFERENCES

[1] O. Bonaventure, *Computer Networking: Principles , Protocols and Practice (Release 0.25)*. The Saylor Foundation, 2011.
[2] E. Tetz, *Cisco Networking All-in-One For Dummies*. Hoboken, NJ: John Wiley & Sons, Inc, 2011.
[3] C.-H. (John) Wu and J. D. Irwin, *Introduction to Computer Networks and Cybersecurity*. Boca Raton, FL: CRC Press (Taylor & Francis Group, LLC), 2013.
[4] A. Uskov, N. A. Serdyukova, V. I. Serdyukov, C. Heinemann, and A. Byerly, "Multi Objective Optimization of VPN Design By Linear Programming With Risks Models," *Int. J. Knowledge-Base Intell. Eng. Syst.*, vol. 20, pp. 175–188, 2016.
[5] P. Chountalas and A. Karagiorgos, "Bring Your Own Device Philosophy From The User's Perspective: An Empirical Investigation," in *Proceedings of the 2nd HOBA International Conference - Vol.1 (ISBN: 978-960-538-950-5)*, 2015, pp. 1–12.
[6] M. Al Askar and K. N. Shen, "Understanding Bring Your Own Device (BYOD) and Employee Information Security Behaviors from A Work-Life Domain Perspective," in *Twenty-second Americas Conference on Information Systems*, 2016, pp. 1–10.
[7] I. K. S. Satwika and I. M. Sukafona, "Analisis Quality Of Service Jaringan Virtual Private Network (VPN) di STMIK STIKOM Indonesia," *J. Ilm. Inform.*, vol. 7, no. 1, pp. 60–66, 2019.
[8] E. Mufida, D. Irawan, and G. Chrisnawati, "Remote Site Mikrotik VPN Dengan Point To Point Tunneling Protocol (PPTP) Studi Kasus Pada Yayasan Teratai Global Jakarta," *Matrik*, vol. 16, no. 2, pp. 9–19, 2017.

[9] H. Sujadi and A. Burhanuddin, "Rancang Bangun Keamanan Data Jaringan Komputer Dengan Menggunakan Metode IPSec VPN (Studi Kasus: PT.Agrabudi Komunika)," *Infotech*, vol. 3, no. 2, pp. 10–15, 2017.

[10] W. O. Zamalia, L. M. F. Aksara, and M. Yamin, "Analisis Perbandingan Performa QoS, PPTP, L2TP, SSTP Dan IPSec Pada Jaringan VPN Menggunakan Mikrotik," *SemanTIK*, vol. 4, no. 2, pp. 29–36, 2018.

[11] Cisco, *Cisco Security Appliance Command Line Configuration Guide*, Software V. San Jose, CA, USA: www.cisco.com, 2008.