Progresif: Jurnal Ilmiah Komputer
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0877
p-ISSN: 0216-3284

Optimasi Pembagian Beban Dan Keamanan Jaringan Menggunakan *OpenVPN* Dengan OSPF *Routing Protocol*

Oky Tria Saputra[1*], Dadang Iskandar Mulyana[2], Yuma Akbar[3]
Program Studi Teknik Informatika, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika, Jakarta, Indonesia
[*]Email *Corresponding Author:* okytria@gmail.com

Abstract

Virtual Private Network (VPN) often we found to connect private networks securely through internet. One of the VPN that often we used OpenVPN. OpenVPN was one of the opensource application with high level security and compatible with a lot of operating system. For prevent Single Point of Failure (SPoF) need backup link so VPN still can be accessed when there's one link down. When there's 2 VPN link, we need to loadbalance it to make it optimized. For connect some network, we need routing protocol such as OSPF. Researcher will optimize load balance with two links of VPN with OSPF (Open Shortest Path First) used EVE-NG network simulator. When researcher did the test download file from FTP (File Transfer Protocol) Server with 200Megabyte to client1 and client2 got throughput 0,385 Mbps with 8 minutes 4 second with latency ping 65ms average. And 0,445 Mbps to client2 with duration 7 minutes 58 seconds with latency ping average 63ms.

Keywords: *OpenVPN; Loadbalance; Failover; Open Shortest Path First, Djikstra Algorithm*

Abstrak

Virtual Private Network (VPN) sering kita jumpai untuk menghubungkan jaringan pribadi secara aman melalui internet. Salah satu VPN yang sering digunakan yaitu *OpenVPN*. *OpenVPN* salah satu VPN gratis dengan tingkat keamanan tinggi serta kompatibel banyak Operating System. Untuk menghindari *Single Point of Failure* (SPoF) perlu adanya jalur backup sehingga vpn bisa diakses jika salah satu ISP terputus. Ketika ada dua jalur VPN supaya lebih optimal maka dibuatkan pembagian beban diantara dua jalur VPN. Untuk menghubungkan jaringan, menggunakan routing OSPF (*Open Shortest Path First*). OSPF dapat mengirimkan paket secara merata di kedua jalur yang berbeda. Peniliti akan mensimulasikan optimisasi pembagian beban 2 jalur VPN menggunakan OSPF di simulator EVE-NG. Pada saat dilakukan download file sebesar 200 Megabyte dari FTP (*File Transfer Protocol*) Server ke *client1* dan *client2* didapati *throughput* 0,385 Mbps sekitar 8 menit 4 detik pada *client1* dengan ping rata-rata 65ms dan 0,445 Mbps pada *client2* dengan waktu 7 menit 58 detik dan ping rata-rata 63ms.
Kata Kunci: *OpenVPN; Loadbalance; Failover; Open Shortest Path First; Algoritma Djikstra*

1. Pendahuluan

Internet saat ini menjadi sebuah kebutuhan masyarakat, hampir semua generasi menggunakan internet baik itu untuk berkomunikasi antara keluarga, bertukar data untuk keperluan bisnis, bermain *game*, kriptografi, *Metaverse* bahkan *content creator* yang saat ini sedang ramai dilakukan banyak orang.

Di dalam ranah bisnis, perusahaan yang memiliki oleh suatu kantor di beberapa lokasi membutuhkan ada nya bertukar data secara aman dan memiliki *up time* yang tinggi untuk menghindari adanya *downtime* dalam berkomunikasi antara kantor pusat dengan kantor cabang. Apalagi jika terdapat puluhan atau ratusan cabang yang tersebar.

Terdapat beberapa cara yang bisa dilakukan untuk menghubungkan jaringan kantor pusat dengan kantor cabang seperti Metro Ethernet, Satelit, atau Internet. Tapi untuk beberapa kasus masih banyak sekali yang menggunakan Internet karena biaya yang lebih murah dibandingkan layanan lain. Dengan adanya *Virtual Private Network*, dapat menghubungkan

jaringan dari suatu lokasi ke lokasi lain melalui jalur internet secara aman dengan enkripsi yang baik [1].

Ketika mendesain *Virtual Private Network* melalui Internet, jika hanya memiliki satu ISP di kantor pusat dan kantor cabang sebuah organisasi, maka ketika ISP tersebut mati, komunikasi antara kantor cabang dan pusat tidak bisa terjadi, maka perlu ada ISP *backup* sehingga ketika salah satu ISP mati, tetap bisa berkomunikasi antara kantor cabang dan kantor pusat. Jika kedua ISP hidup maka dengan pembagian beban akan diperoleh hasil yang maksimal dan efektif karena kedua ISP tersebut terbagi rata ketika pengiriman data dilakukan.

Makalah ini menyajikan model menghubungkan sebuah lokasi kantor cabang ke lokasi kantor pusat sebuah organisasi menggunakan 2 jalur VPN yang berbeda ISP, lalu akan di *loadbalance* sehingga kedua *link* tersebut dapat maksimal (sama rata). Pengujian dilakukan di PT. Integrasi Data Nusantara untuk menghubungkan kantor cabang di Semarang dengan kantor pusat di Jakarta.

2. Tinjauan Pustaka

Ada banyak tipe VPN yang sering digunakan saat ini, tapi penelitian dari [1] membahas tentang keamanan *OpenVPN* merupakan salah satu yang aman bisa digunakan untuk menghubungkan jaringan kantor pusat dengan kantor cabang. Penelitian dilakukan di Labolatorium Penelitian Teknik Informatika Universitas Ahmad Dahlan.

Beberapa pembahasan sudah dilakukan sebelum nya terkait optimisasi beban *Virtual Private Network* menggunakan OSPF. Salah satu nya dilakukan oleh [2]. Pengetesan dilakukan menggunakan protokol FTP dan UDP melalui *video streaming* VLC Media Player. Ketika menggunakan VPN GRE *Tunnel* kecepatan berkurang dikarenakan paket yang di enkripsi dan dekripsi. Hasil yang diberikan adalah OSPF *Load Balance* lebih baik dalam kecepatan, latensi, packet yang hilang dibandingkan tanpa Load Balancing. Tapi pembagian beban OSPF tersebut menggunakan GRE Tunnel yang tidak terenkripsi, sedangkan *OpenVPN* menenkripsi data secara aman dan bisa digunakan di lebih banyak *operating system* dibanding GRE *Tunnel*.

Dalam hal *survivabilitas*, penelitian yang dilakukan oleh [3] membahas bagaimana ketika membuat jaringan OSPF menggunakan *redundancy* jika terjadi nya kesalahan dalam jaringan OSPF. Jadi ketika ada jalur *redundacy* pada OSPF meningkatkan survivabilitas dalam jaringan OSPF.

Penelitian yang dilakukan oleh [4] membandingkan antara OpenVPN dengan IPSec pada jaringan berbasis IP Dinamis ditemukan bahwa kedua nya bisa berjalan dengan baik dan aman. Dengan ada nya fitur IP *Cloud* di MikroTik membuat walaupun menggunakan IP Dinamis tetap terhubung dengan baik setelah diadakan pengujian dengan sukses.

Loadbalance sering digunakan, salah satu nya pada penelitian [5] menggunakan *Equal Cost Multi Path* (ECMP) pada *Border Gateway Protocol* (BGP) dan OSPF. Setelah diuji ternyata BGP *load balance* nya lebih baik daripada OSPF. Jadi ketika salah satu *link* bermasalah akan tetap bisa dilewati jalur lain nya.

Komparasi dilakukan oleh [6] untuk membandingkan *Open Shortest Path First* (OSPF) pada *IP Networks* dengan *Multi Protocol Label Switching* (MPLS), bahwa ketika menggunakan VPLS pada jaringan MPLS ping dan latensi lebih baik dibandingkan hanya IP *Networks* saja dari sisi QoS, *jitter, latency*, dan lain nya yang sangat berguna untuk video streaming dari kantor pusat ke kantor cabang misal nya.

Ketika di analisa *routing* protokol dinamik pada penelitian [7] ternyata ditemukan bahwa RIPv2 cocok untuk skala kecil karena *hop* nya maksimal 15 saja, jika menggunakan *Enhanced Interior Gateway Protocol* [EIGRP] untuk konvergensi nya cepat dan terbaik tapi hanya untuk produk *Cisco* saja. Sedangkan yang bisa digunakan multi-vendor dan skala besar adalah OSPF yang bisa digunakan.

Dalam *wireless mesh*, untuk menghubungkan banyak *access point* secara *mesh*, perlu nya routing protokol terbaik untuk menghasilkan *latency* rendah, penelitian dilakukan oleh [8] dibandingkan beberapa *routing* protokol seperti RIP, OSPF, EIGRP. Ditemukan bahwa RIP hasil nya tidak jelas dan sering berubah, sedangkan OSPF memiliki *latency* yang kecil dan *throughput* yang besar dibandingkan yang lain. Disimpulkan bahwa OSPF merupakan routing protokol terbaik yang paling cocok untuk *wireless mesh*.

Salah satu yang sering digunakan ketika komunikasi antara kantor pusat dan cabang adalah *Voice over IP* (VoIP). Berfungsi untuk telpon menggunakan data atau internet secara gratis tanpa pulsa. Penelitian yang dilakukan oleh [9][10] bahwa *performance* OpenVPN

sangatlah stabil, tetapi perlu instalasi aplikasi OpenVPN pada laptop atau *handphone* langsung. Kalau tanpa OpenVPN sangatlah lemah nanti kalau disadap bisa terbaca, dengan kecepatan 100Mbps, data suara diterima dengan baik secara presentase 100%.

Penelitian lain dilakukan oleh [11] menggunakan OpenVPN serta OpenSSL untuk mengamankan lalu lintas data pribadi yang lewat pada Internet. Salah satu kelebihan OpenVPN dibanding yang lain adalah support untuk operating sistem yang kurang populer seperti FreeBSD, QNX, Solaris, Meemo, dan lain sebagai nya.

Penelitian dilakukan oleh [12] dari PT. Panen Lestari Internusa (SOGO) menghubungkan jaringan kantor cabang ke kantor pusat mereka menggunakan Metro *Ethernet*, tapi jika bermasalah, maka tidak ada nya jalur *backup*. Dengan ada nya *Speedy* maka dibuatkan *backup* internet dan *backup virtuap private network* menggunakan *WatchGuard.*

Analisis dilakukan oleh [13] dan [14] untuk menghubungkan kantor pusat dan kantor cabang nya menggunakan VPN, adapun yang dilakukan [13][14] menggunakan PPTP untuk menghubungkan antara kantor pusat dan cabang, tapi saat ini PPTP sudah mulai ditinggalkan karena sudah ada VPN yang lebih aman dibandingkan *virtuan private network* tersebut. Bahkan Apple sudah meniadakan PPTP semenjak 10.12 versi untuk macOS nya.

Pada penelitian [15] dibuatkan rancang bangun *Wide Area Network* (WAN) menggunakan *Cisco Packet Tracert* untuk menghubungkan beberapa *router* menggunakan VPN di *Packet Tracert* serta authentikasi terpusat menggunakan AAA (*Authentication, Authorization, Accounting*). Menggunakan protokol RADIUS untuk bisa authentikasi secara terpusat.

Perlunya pengiriman data *File Transfer Protocol* (FTP) membuat peneliti [16] merancang dan implementasi *virtual private network* menggunakan PPTP untuk bisa berkomunikasi ke jaringan lokal SMKS DWIWARNA. Dengan ada nya VPN ketika ada guru yang ingin akses data melalui FTP bisa dikirim atau diterima secara aman.

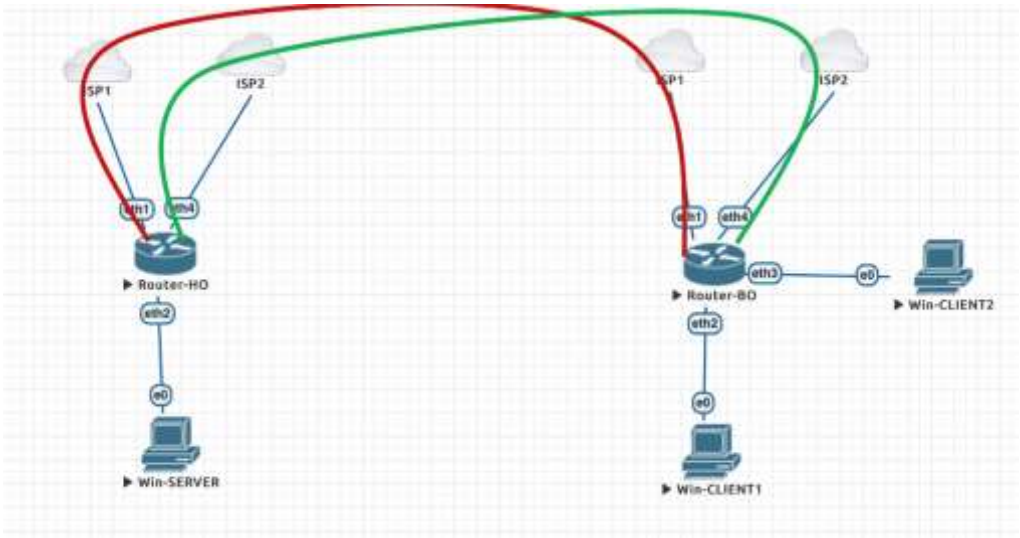
Sebuah perusahaan menggunakan Metronet Fiber Optik untuk menghubungkan suatu lokasi dengan lokasi lain nya. Peneliti [17] melakukan implementasi *failover* ketika metronet mati, menggunakan VPN berbasis PPTP. Tetapi PPTP sudah sangat lama sekali dan keamanan kurang baik, lebih baik menggunakan OpenVPN.

State of the art penelitian yang dilakukan saat ini yaitu penelitian [2] menggunakan gre tunnel tidak aman dan tidak multi-OS hanya OS tertentu, sedangkan pada penelitian kami menggunakan openVPN yang dipandang lebih aman dan universal OS.

3. Metodologi

3.1 Desain Topologi Jaringan

Sistem yang dibangun menggunakan lingkungan virtual EVE-NG terdapat 2 *router* dan 3 *host*. Setiap *router* terhubung ke 2 ISP, misalnya Telkom (5Mbps) dan Biznet (5Mbps). Tiap *Router* ada *client* yang berbeda misal nya *Head Office* dan *Branch Office*. *Router* yang akan digunakan untuk simulasi adalah MikroTik. Sedangkan Untuk *Client* nya menggunakan Windows 7. Gambar 1 merupakan rancangan topologi jaringan yang akan digunakan didalam penelitian:



Gambar 1. Topologi Jaringan *OpenVPN Loadbalance*

Pada Gambar 1, peneliti membuat design topologi menggunakan 1 *router* terhubung ke 2 ISP di *Router-Head Office* dan 1 *router* yang terhubung ke 2 ISP di *Router-Branc Offices*. Nanti dari *Router Branc Office* akan menkoneksikan OpenVPN *Client* ke *Router Head Office* sebanyak 2 koneksi OpenVPN, yang melewati ISP1 dan ISP2. Ketika terhubung dengan OSPF nanti akan dibuatkan routing, sehingga ketika *Client1* dan *Client2* ambil data dari Server akan terbagi secara merata kedua OpenVPN tersebut. Sehingga lebih optimal dan efisien serta aman dalam pengiriman dan penerimaan data dari *Server* ke *Client*.

3.2 Alur Implementasi dari Rancangan Topologi Jaringan

Adapun pembahasan umum dari masing-masing tahapan diatas adalah sebagai berikut:

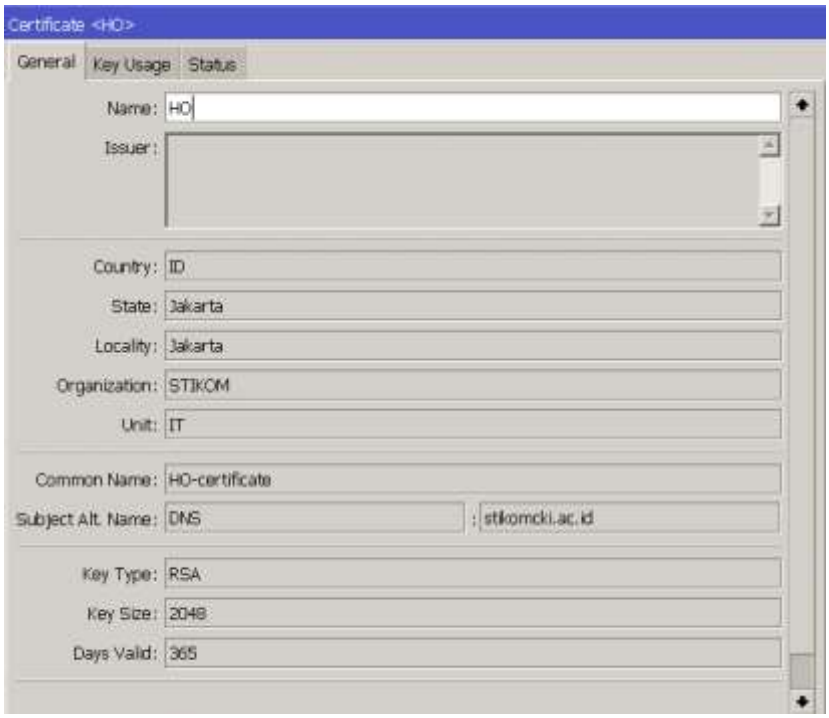
1. Tahapan dimulai dengan instalasi EVE-NG pada sebuah PC atau Server.
2. Selanjutnya membuat topologi jaringan dengan memasukan image MikroTik dan Windows 7 sebelum nya.
3. Setelah dibuatkan topologi jaringan, konfigurasi OpenVPN untuk menghubungkan kedua *router*.
4. Setelah terhubung, maka perlu mengaktifkan OSPF untuk bisa terhubung antara *Branch Offices* dengan *Head Offices*.
5. Untuk *loadbalance* akan dipastikan nilai *cost* nya sama.
6. Setelah *load balance* aktif, dilakukan pengujian dan analisis.
7. Hasil dari pengujian dan analisis.

Untuk menjalankan pengujian, peneliti mencoba mendesain topologi jaringan *point to point* menggunakan aplikasi EVE-NG *Network Simulator* apa saja yang dibutuhkan, menentukan IP Address yang akan digunakan setiap perangkat. Berikut proses tahapan pengujian:

1. EVE-NG *Network Simulator* untuk mendesain topologi jaringan dan memetakan *router* dan PC pada simulator
2. Wireshark menggunakan untuk menganalisa trafik paket yang lewat jalur internet pastikan terenkripsi dan aman.
3. FTP digunakan untuk simulasi pengiriman data dari *client* ke *server* menggunakan XLight FTP *Server* dan WinSCP *Client*
4. OSPF *metric* yaitu *cost* pada *routing* tabel.

4. Hasil dan Pembahasan

4.1 Membuat Sertifikat *Secure Socket Layer* pada MikroTik dan aktifkan OpenVPN Server

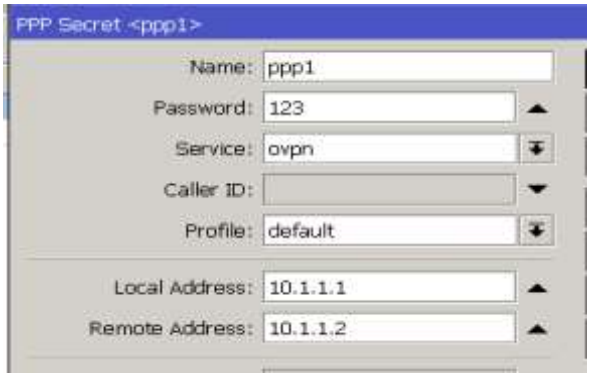


Gambar 2. Membuat sertifikat *Secure Socket Layer* (SSL) pada MikroTik

Biar *secure* dan aman, perlu dibuat self-sertifikat di MikroTik pusat terlebih dahulu untuk client nya juga dibuatkan. Setelah itu baru diaktifkan OpenVPN *Server* dengan memasukan sertifikat yang sudah dibuatkan tadi.

Gambar 3. *Enabled* OpenVPN Server Dan Masukan Sertifikat Yang Dibuat.

Ketika mengaktifkan OpenVPN *Server*, jangan lupa dibagian *Certificate* kita pilih HO (sertifikat yang sudah kita buat), setelah itu di *ceklis Require CLient Certificate* untuk bisa memaksa *client* menggunakan sertifikat biar *secure* dan aman.

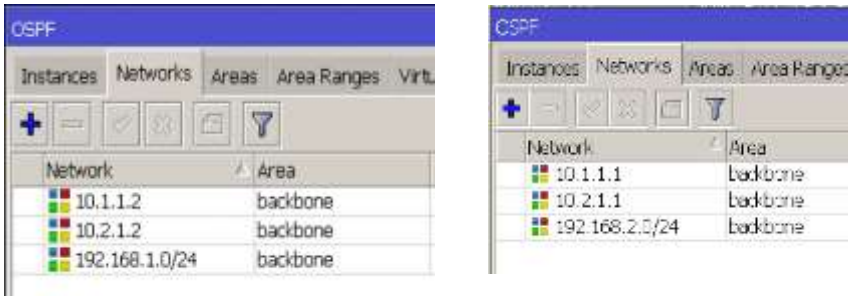


Gambar 4. Membuat *User* Dan *Password* Untuk *Client* OpenVPN Konek Ke *Server*.

Setelah diaktifkan, *client* nanti akan terhubung ke pusat menggunakan metode authentikasi *username* dan *password*. Maka dibuatkan *user* dan *password* nya terlebih dahulu pada menu PPP - *Secret* di MikroTik nya. Pada pilihan *service* kita gunakan OVPN.

Gambar 5. OpenVPN *Client* pada *Branch Office*

Pada *Branch Office* perlu melakukan authentikasi OpenVPN *Client* menggunakan *user* dan *password* yang sudah dibuatkan di OpenVPN *server*. Pada bagian *Connect to* masukan IP Public ISP1 pada *Head Office*, maka *Certificate*, masukan sertifikat yang sudah dibuat di pusat.

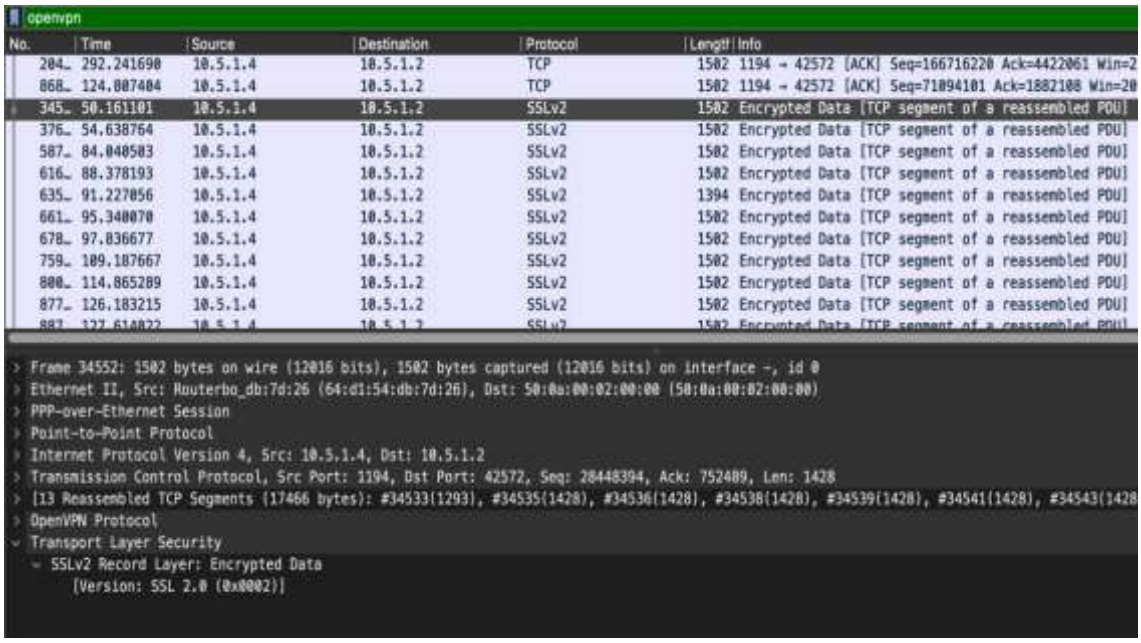


Gambar 6. Konfigurasi OSPF *Network* Untuk Menghubungkan Jaringan Kantor Pusat Dan Cabang.

Pada bagian akhir diakukan konfigurasi OSPF nya yang akan menghubungkan jaringan kantor pusat dengan kantor cabang menggunakan algorithma *Djikstra*, dan akan membagi trafik secara merata otomatis.

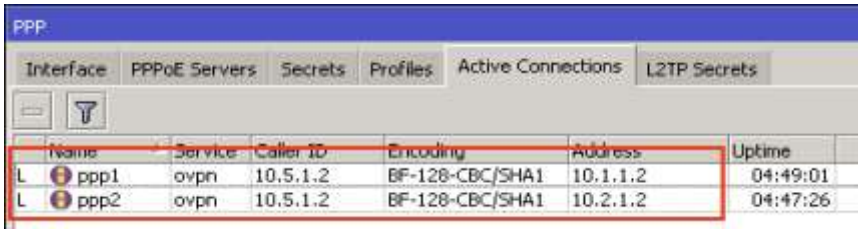
4.2 Hasil Akhir Pengujian

OpenVPN menggunakan OpenSSL yang membuat lalu lintas data dikirim secara aman, setelah OpenVPN terhubung, yang pertama kali peneliti cek adalah bagaimana lalu lintas data nya apakah aman, peneliti menggunakan aplikasi penyadap bernama *Wireshark* untuk melihat lalu lintas data ketika dikirim.



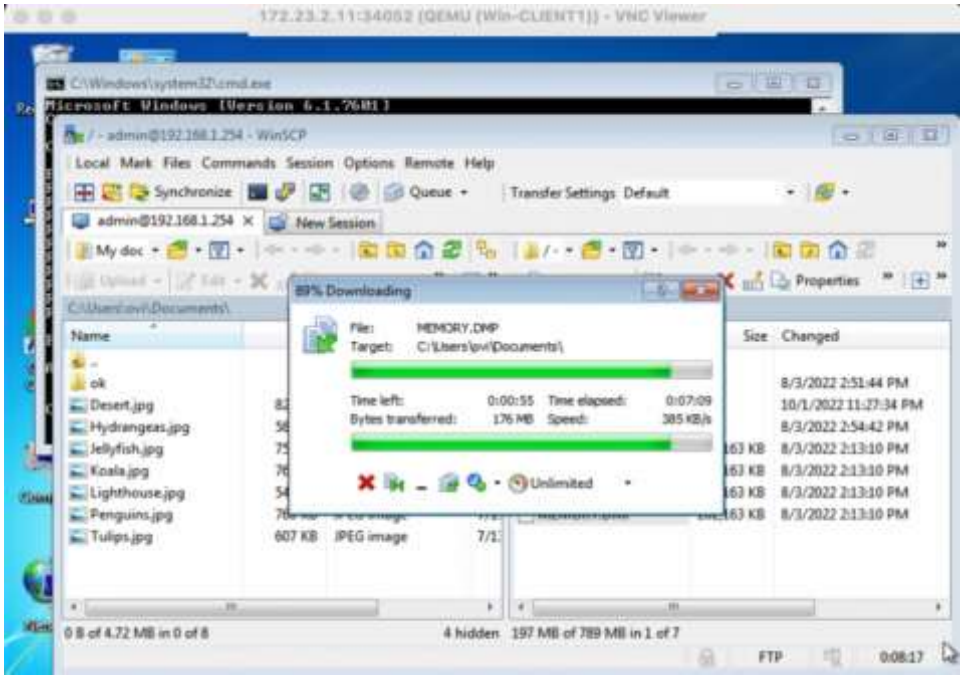
Gambar 7. Menjalankan *Wireshark* Untuk Melihat Trafik Dalam OpenVPN

Pada Gambar 7, bisa disimpulkan bahwa OpenVPN menggunakan SSLv2 *Encrypted* Data ketika mengirim atau menerima data. Jadi data tidak akan disadap karena di enkripsi dengan baik menggunakan *cipher blowfish128*.



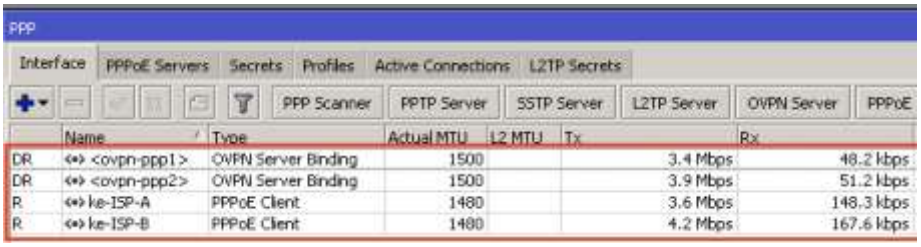
Gambar 8. *Encoding* BF-128-CBC/SHA1 pada OpenVPN

Terlihat pada Gambar 8 bahwa *encoding* yang digunakan lengkapnya BF-128-CBC/SHA1 pada OpenVPN client di kedua *user* yaitu ppp1 (ISP1) dan ppp2 (ISP2). Terlihat pada bagian *service* tertulis OVPN karena menggunakan OVPN bukan PPP lain nya.



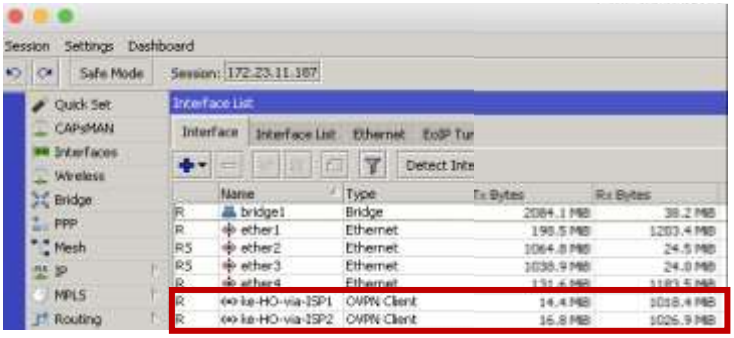
Gambar 9. FTP *Download* dari *Client1* ke *Server1*

Pada pengujiaan saat dilakukan *download file* sebesar 200Megabyte terlihat pada gambar x dan x dari komputer server1 ke *client1* dan *client2* dengan *throughput* 0,385 Mbps sekitar 8 menit 4 detik pada komputer *client1* dan 0,445 Mbps trafik selama 7 menit 58 detik masih normal dengan ping menggunakan beban rata-rata 63ms pada client1 dan rata-rata 65ms pada *client2* selama 100detik pertama proses *download* tidak mengalami kendala pada jaringan atau *Request Time Out* (RTO)



Gambar 10. *Loadbalance* Pada Kedua Jalur OpenVPN secara merata.

Pada gambar 10, ketika dilakukan proses FTP dari *Server1* ke *Client1* kedua jalur baik melewati ISP-A atau ISP-B terbagi secara merata. Jadi semisal total trafik 200Mb maka akan terbagi secara merata menjadi 100Mb lewat ISP1 dan 100Mb lewat ISP2 jadi lebih optimal.



Gambar 11. Hasil Trafik Terbagi Secara Merata

Pada Gambar 11 terlihat ketika 2000Mb file yang *download* totalnya akan terbagi secara merata 1000Mb akan lewat OpenVPN1 lewat ISP1 dan 1000Mb akan lewat OpenVPN2 lewat ISP2. Ketika salah satu VPN putus pun masih bisa berkomunikasi walaupun kecepatan akan berkurang 50%.

Setelah dilakukan pengujian, terbukti bahwa pembagian beban secara merata untuk interface OpenVPN-via-ISP1 dan OpenVPN-via-ISP2, dan pengiriman data dilakukan secara aman menggunakan encoding BF-128-CBC/SHA1 dibanding penelitian pembagian beban sebelum nya yang dilakukan oleh [2] yang hanya menggunakan GRE *Tunnel* yang tidak aman.

5. Simpulan

Jaringan *point to point* menggunakan OpenVPN dengan sertifikat dan BF-128-CBC/SHA1 dapat melakukan pertukaran data dan berjalan dengan lancar ketika terjadi komunikasi antara pusat dan cabang. OpenVPN dengan BF-128-CBC/SHA1 lebih *secure* dibanding PPTP atau L2TP karena menenkripsi paket dengan SSL. Pengujian Ping dengan beban rata-rata hasil yang didapatkan 63ms pada *client1* dan rata-rata 65ms pada *client2* selama 100detik pertama proses *download*, tidak mengalami kendala pada jaringan atau *reques time out* (RTO).

OSPF dengan *algorithma djikstra* mampu membagi beban trafik VPN melalui kedua ISP yang digunakan. Ketika salah satu OpenVPN dimatikan, maka speed berkurang 50% dan pengiriman data yang awal nya 7 menit bisa sampai 12 menit.

Beberapa rekomendasi yang perlu menjadi perhatian di masa mendatang adalah: (1) Terdapat beberapa PPP lain yang mudah di konfigurasikan seperti PPTP dan L2TP, tapi dari sisi keamanan lebih baik OpenVPN dengan sertifikat BF-128-CBC/SHA1. (2) Terdapat beberapa *routing protocol dynamic* lain nya yang bisa digunakan, salah satu diantaranya *Border Gateway Protocol* (BGP) atau *Enhanced Interior Gateway Protocol* (EIGRP) atau *Routing Information Protocol* (RIP) yang bisa jadi alternatif OSPF. (3) Lebih baik menggunakan *Loadbalance* pada OpenVPN ketika memiliki 2 ISP atau lebih karena OSPF akan membagi beban ke dua ISP. Jika hanya satu yang aktif saja, maka *speed* terasa lebih lambat dikarenakan kapasitas ISP yang digunakan, dan menghindari *Single Point of Failure*

Daftar Referensi

[1] M. Iqbal, I. Riadi, "Analysis of Security Virtual Private Network (VPN) Using OpenVPN," *International Journal of Cyber-Security and Digital Forensics (IJCSDF).*, Vol. 8, No. 1, pp. 58-65, 2019. http://dx.doi.org/10.17781/P002557

[2] N. F. N. Norazlan, R. A. Rahman, M. Kassim, and A. R. Mahmud, "Virtual Private Network Load Balancing Using OSPF Routing," *2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, pp. 164-169, Apr. 2020, doi: 10.1109/ iscaie47305.2020.9108802.

[3] D. S. Robbins, "Using Protocol Redundancy to Enhance OSPF Network System Survivability," *SoutheastCon 2018*, pp. 1-7, Apr. 01, 2018. doi: 10.1109/SECON. 2018.8479134

[4] A. A. Setya, A. Sudaryanto, "Analisa Konektivitas Jaringan IPSEC Dan OpenVPN Pada Jaringan Berbasis IP Dinamis," *INFOTRON: Jurnal Ilmiah Teknik Informatika, Elektronika dan Kontrol*, Vol. 1, No. 1, pp. 1-5, 2021. doi: http://dx.doi.org/10. 33474/infotron.v1i2

[5] A. Triwerdaya, D.T. Nugrahadi, M.I. Masdadi, I. Budiman, & A.R. Arrahimi, "Implementation of Load Balance Equal Cost Multi Path (ECMP) Between Routing Protocol Border Gateway Protocol (BGP) And Open Shortest Path First (OSPF) Using Dual Connection. *Journal of Data Science and Software Engineering*, vol. 1, no. 2, pp. 110-118, 2020.

[6] I. Nurhaida, D. Ramayanti, I. N. "Islamiyah, Performance Comparison based on Open Shortest Path First (OSPF) Routing Algorithm for IP Internet Networks," *Communications on Applied Electronics A scholarly Peer-reviewe scientific journal,* Vol. 7, No. 31, pp. 12-25, 2019. doi :10.5120/cae2019652838

[7] K. K. Wai, "Analysis Routing of RIP, EIGRP, and OSPF Routing Protocols in a Network," *International Journal of Trend in Scientific Research and Development (IJTSRD),* Vol. 3, No. 5, pp. 2484-2487, 2019. doi: 10.31142/ijtsrd27928.

[8] H. Kabir, Md. A. Kabir, S. Islam, M. G. Mortuza, and M. Mohiuddin, "Performance Analysis of Mesh Based Enterprise Network Using RIP, EIGRP and OSPF Routing Protocols," *Eng. Proc.* p. 47. Jan. 2021, doi: 10.3390/ecsa-8-11285.

[9] C. Aminoto, H. M. T. Alawiy, O. Melfazen, " Perancangan Voip Menggunakan Openvpn Pada Os Openwrt Sebagai Pengaman Jaringan Antar Client ", *Science Electrol,* Vol. 9, No. 1, pp. 6-15, 2018.

[10] R. E. Putro and I. R. Widiasari, "Analisis Keamanan Komunikasi VoIP Server Portable Dilengkapi OpenVPN Menggunakan Linux Asterisk," *Jurnal Media Informatika Budidarma,* Vol. 6, No. 2, pp. 943-951 2022, doi: 10.30865/mib.v6i2.3884.

[11] C. Brinsley and Y. Fernando, "Rancang Bangun Jaringan Pribadi Menggunakan OpenVPN,", *SYNTAX Jurnal Informatika,* Vol. 7, No. 2, pp. 87-93, 2018. DOI: 10.35706/syji.v7i2.1465

[12] K. Subandi, A. S. Aryani, "Analysis and Implementation of Backup Line Network Using Branch Office VPN and Speedy Internet Broadband," *Journal of Applied Science and Advanced Technology*, Vol. 1, No. 2, pp. 39-48, 2018, doi: 10.24853/JASAT.1.2.39-48.

[13] S.D. Amarudin, Riskiono, "Analisis Dan Desain Jalur Transmisi Jaringan Alternatif Menggunakan Virtual Private Network (VPN)", *Jurnal TEKNOINFO*, Vol. 13, No. 2, pp. 100-106, 2019. Doi: 10.33365/jti.v13i2.309

[14] A. Hidayat, "Analysis and Distance Access Design Far with Vpn Technology in Bmt Office. Mentari East Lampung.", *International Journal Information System and Computer Science (IJISCS),* Vol. 3, No. 2, pp. 64-71, 2019, DOI: 10.56327/ijiscs.v3i2

[15] S. Hidayatulloh and Wahyudin, "Perancangan Wide Area Network (WAN) Dengan Teknologi Virtual Private Network (VPN)," *Jurnal Teknik Komputer AMIK BSI*, Vo. 5, No. 1, pp. 7–14, 2019, doi: 10.31294/jtk.v4i2.

[16] D. Ruwaida and D. Kurnia, "Rancang Bangun File Transfer Protocol (FTP) Dengan Pengamanan Open SSL Pada Jaringan VPN Mikrotik Di SMKS Dwiwarna," *CESS (Journal*

of Computer Engineering System and Science), Vol. 3, No. 1, pp. 45-49, 2018. Doi: 10.24114/cess.v3i1.8267

[17] S. N. Khasanah and L. A. Utami, “Implementasi Failover Pada Jaringan WAN berbasis VPN,” *Jurnal Teknik Informatika STMIK Antar Bangsa*, Vol. IV, No. 1, pp. 62-66, Februari 2018.