Rancang Bangun Jaringan Pribadi Menggunakan OpenVPN

Charlie Brinsley[1], Yongky Fernando[2]

[1,2] Kompleks Maha Vihara Duta Maitreya,
Sungai Panas, Batam 29456, Kepulauan Riau - Indonesia
Email: charliebrinsley@outlook.com

Abstrak. OpenVPN adalah perangkat lunak gratis dengan sumber terbuka yang mengimplementasikan *virtual private network* (VPN), yang menyediakan fitur otentikasi dan enkripsi dalam komunikasi antar titik ke titik jaringan. Hal yang diutamakan dalam komunikasi di sebuah jaringan adalah menjaga keamanan dan privasi dalam komunikasi tersebut. Tetapi pertukaran maupun pengiriman data dan informasi antara pengguna tersebut rentan terdapat pengintaian dari pihak ketiga yang seharusnya tidak memperoleh akses terhadap komunikasi tersebut. Dalam penelitian ini akan dilakukan pembangunan server vpn yang menghubungkan client ke server, dimana nantinya client tersebut akan terhubung ke server vpn tersebut dalam jaringan pribadi. Dengan jaringan pribadi tersebut diharapkan komunikasi antara kedua perangkat tersebut aman dari peretas yang mencegat komunikasi atau privasi.

Kata kunci: *jaringan, jaringan pribadi, openvpn, vpn*

1 Pendahuluan

VPN menggunakan saluran pipa dari sub network yang mengenkrip dan mengenkapsulasi koneksi internet untuk menjaga komunikasi, data, lokasi, informasi [1][2]. Dalam pembahasan paper ini akan ditulis tahapan-tahapan dalam pembangunan jaringan pribadi menggunakan OpenVPN, dan diterapkan kepada perangkat yang terkoneksi di jaringan publik, Sehingga nantinya komunikasi antara kedua perangkat tersebut menjadi lebih aman dalam pertukaran data maupun informasi [3]. Jaringan internet yang begitu popular sekarang, banyak pengguna yang saling terhubung dalam suatu jaringan publik [4], dimana pertukaran maupun pengiriman data dan informasi antara pengguna pun sering terjadi, tetapi dalam pertukaran ataupun pengiriman data tersebut, sering kali terdapat pihak ketiga yang mengintai aktivitas tersebut. Hasil dari penelitian ini adalah data atau informasi dalam komunikasi tersebut diketahui oleh pihak yang seharusnya tidak memperoleh akses akan komunikasi tersebut [3][5]. Dengan jaringan pribadi tersebut maka komunikasi yang melewati jaringan tersebut akan dienkapsulasi sehingga akan mencegah peretasan yang mencegat komunikasi atau privasi.

Diterima 17 Oktober 2018, Direvisi 20 Oktober 2018, Diterima untuk dipublikasi 26 Oktober 2018

2 Tinjauan Pustaka

2.1 Jaringan

Jaringan mengacu pada proses total pembuatan dan penggunaan jaringan komputer. Jaringan berhubungan dengan perangkat keras, protokol dan perangkat lunak, termasuk teknologi kabel dan nirkabel juga dikenal sebagai praktik pengangkutan dan pertukaran data antara node melalui media bersama dalam suatu sistem informasi. Jaringan tidak hanya terdiri dari desain, konstruksi dan penggunaan jaringan, tetapi juga manajemen, pemeliharaan dan pengoperasian infrastruktur jaringan, perangkat lunak dan kebijakan [5].

- *Local Area Network* (LAN), Jaringan komputer di satu situs, biasanya di gedung perkantoran individual, yang bisa digunakan untuk berbagi sumber daya, seperti penyimpanan data dan printer [5].
- *Wide Area Network,* jaringan komputer yang menjangkau area yang sangat luas, seperti antar negara dan benua
- *Metropolitan Area Network*, jaringan komputer yang terdiri dari koneksi antar kota, kampus atau wilayah-wilayah kecil

2.2 VPN

VPN menggunakan saluran pipa dari sub network atau virtual ethernet melalui port tunggal udp atau tcp. VPN berfungsi dengan mengenkripsi koneksi Internet Anda untuk menjaga komunikasi, data, lokasi, dan informasi pribadi Anda saat online [6]. Layanan VPN dapat menukar alamat IP pribadi Anda dengan alamat IP server VPN, menciptakan tingkat privasi yang tidak dapat Anda capai saat berada di server publik. Saat menggunakan teknologi VPN (virtual private network), semua lalu lintas jaringan terenkapsulasi antara komputer klien dan server VPN. Dikarenakan komunikasi berada dalam sebuah yang disebut "terowongan", lorong ini mengenkripsi semua informasi yang dikirim melalui koneksi. Yang artinya setiap pengiriman dan penerimaan data saat menggunakan VPN, pengguna tidak perlu khawatir tentang peretas yang mencegat komunikasi atau membobol privasi [1][2].

2.3 OpenVPN

OpenVPN adalah perangkat lunak gratis dengan sumber terbuka yang mengimplementasikan *virtual private network* (VPN) untuk membuat koneksi / menjembatani antara suatu titik ke titik lainnya dalam akses jauh dengan dukungan keamanan jaringan [5][6][7]. Salah satu alasan open vpn menjadi sangat popular adalah fakta bahwa ia mendukung banyak system operasi utama. OpenVPN mundukung system operasi windows, macOS dan Linux serta platform seluler seperti android dan ios, tidak hanya itu OpenVPN juga mendukung platform yang kurang popular seperti FreeBSD, QNX, Solaris,

Maemo, dan Windows Mobile. Bahkan, ada penyedia OpenVPN komersial yang menggunakan protocol OpenVPN, dan mengubahnya menjadi klien VPN untuk penggunanya.

OpenVPN menggunakan pustaka OpenSSL, dimana OpenSSL merupakan sebuah pustaka perangkat lunak yang menyediakan keamanan dengan mengenkripsi saluran data jaringan hingga 256-bit dan mengontrol saluran tersebut[7][2]. OpenSLL mendukung enkripsi konvensional dalam Mode Static Key melalui PSK, dan juga keamanan kunci public melalui klien dan sertifikat server [5]. Ini memungkinkan OpenSSL untuk melakukan enkripsi dan otentikasi dan juga memungkinkan penggunaan cipher-cipher yang tersedia dalam paket OpenSSL. itulah juga merupakan salah satu keunggulan dari OpenVPN.

3 Tujuan Penelitian

Dikarenakan sering kali terdapat pengintaian ataupun pencurian informasi dan data dalam sebuah komunikasi di jaringan publik, Maka dilakukan penulisan tentang jaringan pribadi yang berfungsi menjaga komunikasi antara pengguna yang melewati jaringan publik tetap aman.

4 Metode Penelitian

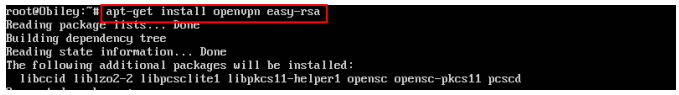
Metode yang digunakan dalam penelitian ini menggunakan metode penelitian tindakan, dimana akan dilakukan pembangunan jaringan vpn dan melihat langsung jalur trafik ketika menggunakan jaringan vpn dan tidak menggunakannya.

Perangkat yang digunakan dalam penelitian ini adalah:

1. Server intel xeon dengan sistem operasi Ubuntu Server Versi 16 sebagai server OpenVPN
2. Laptop dengan sistem operasi windows 10 sebagai client yang akan terkoneksi dengan OpenVPN

5 Hasil dan Pembahasan

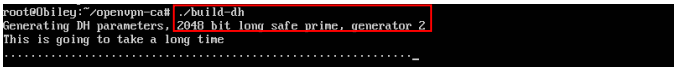
Pertama melakukan penginstalan paket openvpn dan easy-rsa, easy-rsa merupakan sertifikat CA(certificate authority) yang akan digunakan bersama OpenVPN nantinya.



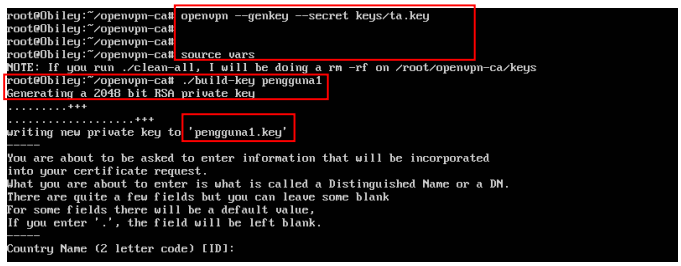
Gambar 1 instalasi paket openvpn dan easy-rsa

Membuat sertifikat dan pasangan kunci untuk server dan client yang akan digunakan sebagai autentikasi penghubung antara kedua perangkat tersebut

dengan perintah "/build-dh" pada terminal untuk menghasilkan kunci Diffie-Hellman, "openvpn –genkey –secret keys/ta.key" untuk membuat tanda tangan HMAC yang berguna untuk memperkuat kemampuan verifikasi integritas TLS server, Lalu dengan perintah "source vars" dan "./build-key pengguna1" untuk menghasilkan sertifikat dan key pair pengguna.

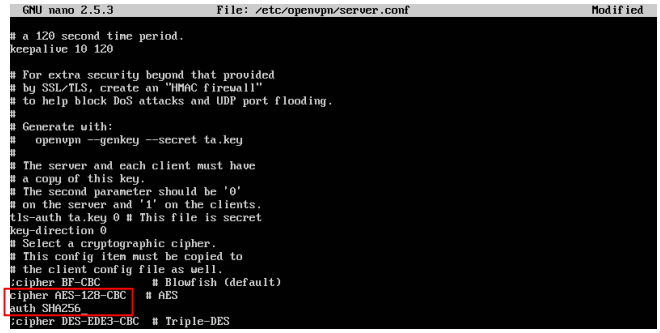


Gambar 2 pembuatan sertifikat server dan client



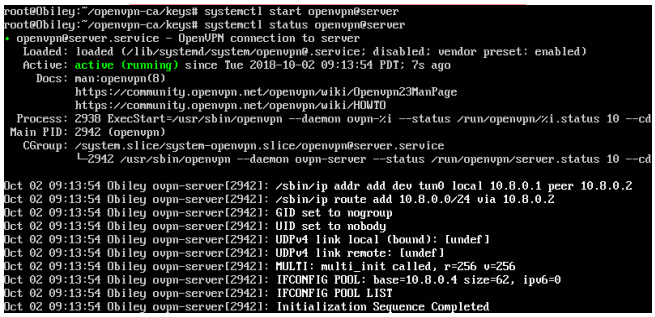
Gambar 3 pembuatan sertifikat server dan client

Setelah sertifikat telah berhasil dibuat, langkah selanjutnya menentukan tipe enkripsi dan chipper yang akan digunakan oleh VPN server tersebut dengan menambah baris "chipper AES-128-CBC" dan "auth SHA256" pada file konfigurasi OpenVPN.



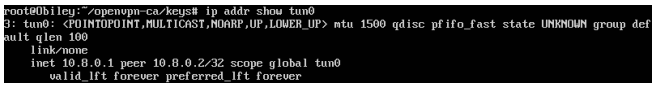
Gambar 4 konfigurasi tipe enkripsi dan chipper yang akan digunakan

Setelah semua konfigurasi telah selesai, OpenVPN server bisa dijalankan dengan perintah “systemctl start openvpn@server” dan “systemctl status openvpn@server” untuk mengecek status dari service OpenVPN.



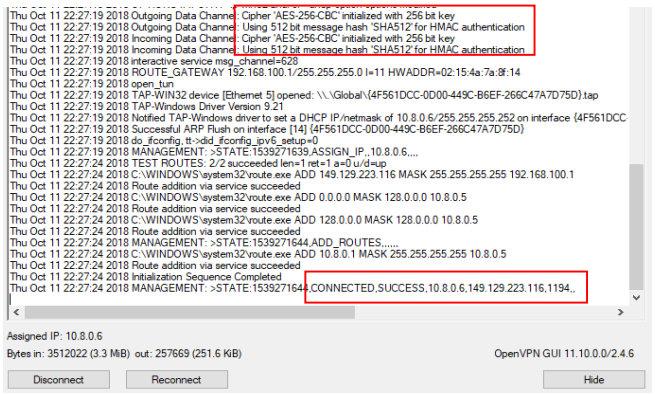
Gambar 5 status openvpn ketika dijalankan

Ketika layanan OpenVPN berjalan, Maka akan terbentuk suatu sub network private yang akan digunakan dalam interaksi semua client yang terkoneksi dalam jaringan tersebut dengan ip 10.8.0.1, bisa dilihat baris tampilan pada gambar 6 “inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0”.



Gambar 6 sub network layanan openvpn

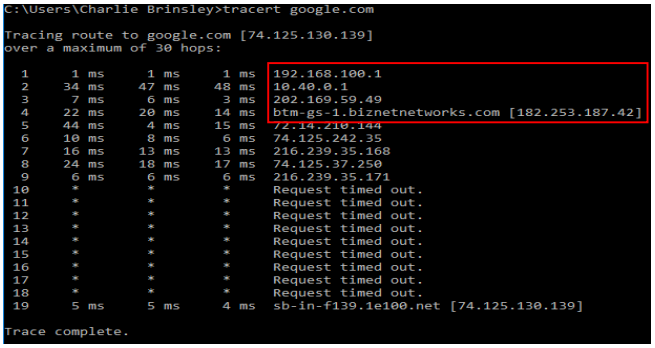
Setelah layanan di sisi telah berjalan, Maka dilakukan pengujian mengkoneksi



perangkat client ke jaringan tersebut.

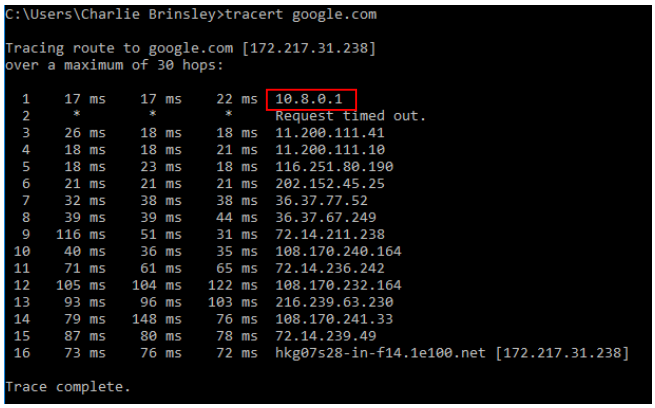
Gambar 7 status koneksi server openvpn dari sisi client

Dari gambar 7 bisa kita lihat bahwa koneksi dari sisi client ke server terenkripsi, bisa dilihat pada kotak merah pada gambar 7 “Cipher AES-256-CBC initialized with 256 bit key, Using 512 bit message hash SHA512 for HMAC authentication” dan berhasil terkoneksi ke jaringan sub network dari server OpenVPN dengan mendapatkan alamat ip 10.8.0.6, bisa dilihat pada kotak terakhir pada gambar 7 dengan tulisan “CONNECTED,SUCCESS,10.8.0.6, 149.129.223.116,1194”.



Gambar 8 trafik akses ke sebuah situs sebelum terkoneksi ke jaringan openvpn

Dari gambar 8 “btm-gs-1.biznetnetworks.com [182.253.187.42]”, bisa dilihat bahwa pengaksesan kesebuah situs tanpa terhubung kejaringan vpn, dimana jalur trafik pengiriman paket terbuka melewati jalur isp lalu ke jaringan publik.



Gambar 9 trafik akses ke sebuah situs sesudah terkoneksi ke jaringan openvpn

Dari gambar 9 bisa dilihat bahwa pengaksesan ke sebuah situs ketika terhubung kejaringan vpn, pengiriman paket akan dituju ke server OpenVPN “1 17ms 17ms 22ms 10.8.0.1, pada kotak merah gambar 9”, walaupun sebenarnya melewati jaringan publik, tetapi trafik tersebut terisolasi oleh jaringan pipa point to point sehingga keamanan paket tetap terjaga. Setelah itu baru paket tersebut lanjutkan ke situs tujuan oleh server OpenVPN.

6 Kesimpulan

Kelemahannya jika menggunakan jaringan internet tanpa vpn ialah dari pihak isp maupun pihak lainnya dapat mengintai data trafik yang dilakukan. Dengan membangun jaringan pribadi terbukti dapat meningkatkan keamanan dalam interaksi di sebuah jaringan publik dengan dukungan otentikasi dan enkripsi serta enkapsulasi yang disediakan. Dimana trafik yang dilakukan terenkapsulasi dari point ke point. Tetapi kelemahannya kecepatan trafik akan menurun, dikarenakan setiap trafik akan melalui server OpenVPN sebagai perantara.

7 Daftar Pusaka

[1] Pramana, I.J., Widyastuti, N., and Triyono, J., Implementasi Radius Server Pada Jaringan Virtual Private Network Jurnal Jarkom, Jurnal JARKOM, 1(2), pp. 122–130, 2014.

[2] Hasbi, M. & Badrul, M., "Jurnal Techno Nusa Mandiri Vol . XI No . 1 , Maret 2014 Penerapan metode Open VPN-Access server sebagai rancangan jaringan Wide Area Network Jurnal Techno Nusa Mandiri," vol. XI, no. 1, pp. 40–52, 2014.

[3] Patel, K. M., Science, S.C., & Science, C., "International Journal of Advance Engineering and Research, A Survey On Resource Allocation Mechanism In Cloud," pp. 70–74, 2015.

[4] Kurniawan, A., Riadi, I., & Luthfi, A., "Forensic analysis and prevent of cross site scripting in single victim attack using open web application security project (OWASP) framework," *J. Theor. Appl. Inf. Technol.*, 2017.

[5] Meyatmaja, E., & Syafrizal, M., "Perancangan Virtual Private Network Pada," *J. Dasi*, vol. 13, no. 4, pp. 11–16, 2012.

[6] Shahebaz, S., Madan, S., & Magare, S., "Review on protocols of Virtual Private Network," 2017.

[7] Rochim, A.F., &Martiyanto, A.S., "Desain dan Implementasi Web Proxy dan VPN Akses (Studi Kasus di Undip)," *J. Sist. Komput.*, vol. 1, no. 1, pp. 1–3, 2011.