Journal of Information Technology and Computer Science (INTECOMS)
Volume 6 Nomor 1, Juni 2023
e-ISSN : 2614-1574
p-ISSN : 2621-3249

RANCANG BANGUN KEAMANAN KONEKSI PRIBADI MELALUI OPEN VPN BERBASIS CLOUD

BUILD PRIVATE CONNECTION SECURITY THROUGH CLOUD-BASED OPEN VPN

Rahmad Milsa Pratama[1], Sri Wahyuni[2], Akhyar Lubis[3]
[1,2,3]Universitas Pembangunan Panca Budi
rahmadmilsa@gmail.com

ABSTRACT

Cybercrime experienced an increase during the pandemic that occurred in 2019; almost everything was carried out online. Most internet connections are still using public Wi-Fi networks. The habit of using open public Wi-Fi is very vulnerable to wiretapping from our activities. Virtual Private Network Network is an effort to provide privacy security when surfing the Internet so that it is almost untraceable. However, using a VPN, especially a free one, can allow third parties to commit data theft. Unclear funding, slow performance, bandwidth limitations, and data privacy issues. There are many reasons why we need our own configurable private VPN server. Current cloud technology support makes it possible to create private VPN servers that offer much better security and transparency than third-party VPNs. The purpose of this research is to provide VPN services with private infrastructure. The infrastructure to be built in this study uses VPC by integrating other services such as internet gateways, NAT gateways, elastic IP addresses, private subnets, and EC2 by integrating OpenVPN as a core VPN service. The OpenVPN used by the author is a free license with two simultaneous connections. The result of the implementation is that the infrastructure has been successfully built and is a solution when you still have to use a public Wi-Fi network to keep it safe

Keywoards*: VPN, AWS, Privacy, Infrastructure, Cloud Computing*

ABSTRAK

Kejahatan dunia maya mengalami peningkatan pada saat pandemi yang terjadi ditahun 2019 lalu, hampir seluruh hal dilaksanakan melalui online. Koneksi internet yang dilakukan sebagian besar masih memanfaatkan jaringan wi-fi publik. Kebiasaan menggunakan wifi publik yang terbuka sangat rentan terhadap penyadapan dari aktifitas yang kita lakukan. Jaringan Virtual Private Network merupakan upaya dalam memberikan keamanan privasi ketika berselancar di internet sehingga hampir tidak dapat dilacak. Namun, penggunaan VPN terutama yang gratis dapat memungkinkan pihak ketiga melakukan pencurian data. Pembiayaan yang tidak jelas, performa lambat, pembatasan bandwith dan masalah privasi data. Banyak alasan mengapa perlu adanya server vpn pribadi yang kita miliki sendiri dan dapat dikonfigurasi. Dukungan teknologi cloud saat ini memungkinkan untuk pembuatan vpn server secara pribadi yang menawarkan keamanan dan transparansi yang jauh lebih baik dari VPN pihak ketiga. Layanan Cloud Computing yang digunakna penulis adalah yaitu menggunakan Amazone Web Service (AWS). Tujuan dari penelelitian ini adalah menyediakan layanan vpn dengan infrastruktur secara pribadi. Infrastruktur yang akan dibangun pada penelitian ini menggunakan VPC dengan mengintegrasikan layanan lainnya seperti internet gateway, NAT gateway, elastic ip address, private subnet, EC2 dengan mengintegrasikan OpenVPN sebagai core layanan VPN. OpenVPN yang digunakan penulis adalah free lisensi dengan dua koneksi secara simultan. Hasil dari implementasi adalah infrastruktur berhasil dibangun dan menjadi solusi ketika tetap harus menggunakan jaringan wi-fi publik agar selalu tetap aman.

Kata Kunci: VPN, AWS, Privacy, Infrastruktur, Cloud Computing

PENDAHULUAN

Internet sudah menjadi kebutuhan dan menjadi peranan penting dalam mendapatkan informasi. Namun dibalik kemudahan tersebut menjadi ancaman bagi pengguna dari kejahatan dunia maya. Jumlah kejahatan dunia maya mengalami peningkatan (Mulya et al., 2021) sehingga menjadi ancaman terhadap serangan kebocoran data. Kejahatan dunia maya meningkat pada saat pandemi yang terjadi ditahun 2019 lalu, hampir seluruh hal dilaksanakan melalui online. Pandemi sangat berperan aktif dalam peningkatan kejahatan. Rata rata triwulan naik hingga mencapai sepuluh kali lipat dibandingkan

triwulan sebelum pandemi. (Mulya et al., 2021). Koneksi yang digunakan sebagian besar masih memanfaatkan jaringan wi-fi publik (Dekas, 2022).

Terhubung ke internet melalui jaringan wi-fi yang tidak aman menjadi target serangan dari pihak yang tidak bertanggung jawab (Astri Saraun, Arie S.M. Lumenta, 2021). Kebiasaan menggunakan wi-fi publik yang terbuka sangat rentan terhadap penyadapan dari aktifitas yang kita lakukan.

Jaringan Virtual Private Network merupakan upaya dalam memberikan keamanan privasi ketika mengakses website di internet sehingga hampir tidak dapat dilacak. VPN membangun koneksi yang aman dan terenkripsi sehingga akses ke website dapat dilakukan dengan aman (Mujiastuti & Prasetyo, 2021). VPN merupakan sarana untuk mengamankan dan memprivasikan pengiriman data pada infrastruktur yang tidak aman. Data yang dikirim dilakukan proses enkripsi dan deskripsi untuk menjaga kerahasiaan melalui jaringan publik. Proses ini yang dikenal dengan enkapsulasi atau tunneling (Usanto, 2021). VPN akan mengamankan komunikasi memanfaatkan jaringan publik menjadi jaringan privasi ke node lain yang jaraknya ribuan kilometer sehingga seolah kita berada ditempat lain. Keuntungan ini memungkinkan kebebasan online dalam mengakses aplikasi situs favorit saat berselancar di internet dengan aman.

Dibalik kelebihan dari VPN tersebut namun ada juga hal negatif selama bertahun tahun karena sejumlah alasan. Penggunaan VPN terutama yang gratis dapat memungkinkan pihak ketiga melakukan pencurian data (Taufieq, 2022). Pembiayaan yang tidak jelas, performa lambat, pembatasan bandwith, masalah privasi data. Penggunaan VPN dari pihak ketiga bermuara dari kurangnya kontrol yang kita yang tidak dapat dilakukan secara indepen menjalankan audit terhadap server orang lain. Banyak alasan mengapa perlu adanya server vpn pribadi yang kita miliki sendiri dan dapat dikonfigurasi. Dukungan teknologi cloud memungkinkan untuk pembuatan vpn server secara pribadi yang menawarkan keamanan dan transparansi yang jauh lebih baik dari VPN pihak ketiga.

Virtual Private Netwok (VPN) digunakan dalam mentransimisikan data secara aman dan anonim melalui jaringan publik dengan tujuan utama yaitu privasi, anonimitas dan keamanan. VPN melindungi data privasi menggunakan teknik enkripsi dalam menjaga kerahasian terutama saat terhubung melalui jaringan wifi publik. Koneksi VPN juga akan menyembunyikan alamat IP sehingga menjadi anonim di internet. OpenVPN adalah *open source* VPN Solution yang tersedia diberbagai platform sistem operasi dan juga platform publik. Open VPN mengandalkan OpenSLL yang memungkinkan dukungan TLS. IPSec adalah protokol yang terdiri dari dua protokol (Encapsulated Security Payload, Authentication Header) dan dua mode transport dan tunnel (Osswald et al., n.d.).

Open VPN tersedia berbagai platform diantaranya windows dan juga linux. OpenVPN menggunakan teknik enkripsi dengan algoritma *symmetric* dan *asymmetric*. Fungsi hash digunakan untuk mengamankan pesan atau yang dikenal dengan *digital signatures* (Skendzic & Kovacic, 2017).

Dukungan teknologi cloud computing dalam keamanan pribadi dapat diterapkan dengan membangun infrastruktur berbasis cloud dibandingkan dengan sistem konvensional. Cloud adalah tempat terjadinya banyak inovasi dan pertumbuhan teknologi akhir akhir ini. Teknologi yang menjadi inti dari semua operasi cloud adalah virtualiasi (A. Mishra, 2017). Salah satu service provider yang menyediakan layanan cloud computing adalah Amazon Web Service (AWS). Penggunaan layanan AWS berbasis cloud dan Open VPN pribadi dapat digunakan dalam perlindungan data, privasi, keamanan dan anonimitas. AWS

memiliki lebih dari 200 layanan unggulan yang ditawarkan secara lengkap dari pusat data secara global (Posey, 2021). Hal ini memungkinkan pengguna secara pribadi dapat membuat berbagai aplikasi pada platform komputasi awan.

Amzone Web Service memiliki banyak layanan aws memiliki fungsi dan keunggulan yang berbeda pada setiap fiturnya(Nugroho & Mustofa, 2012). Adapun layanan produk AWS yang digunakan dalam membangun keamanan koneksi pribadi melalui open vpn server tersebut adalah VPC (Virtual Private Cloud) dan Amazon EC2 (S. Mishra et al., 2022). Virtual Private Cloud ini sangat mirip dengan jaringan tradisional yang nantinya dioperasikan pada pusat data. VPC menjadi bagian dari model jaringan yang berisi predikat, konstanta, dan aturan untuk mendeskripsikan komponen jaringan pada layanan amazone (Hutchison, 2022)

METODE

Langkah langkah yang dilakukan dalam pembangunan server pribadi VPN ini menggunakan metode *prototype*

Gambar 1. Metode Prototype

Pada tahap awal dilakukan *requirements* dalam proses pengumpulan data informasi terkait menyediakan layanan server secara pribadi yang dapat diterapkan, dikonfigurasi dan dimanfaatkan untuk perlindungan data dan privasi pengguna ke sumber internet yang terisolasi secara geografis terutama ketika memanfaatkan jaringan wi-fi publik. Pada fase kedua yaitu *quick design* dilakukan dengan mendesain topologi arsitektur jaringan (Putri et al., 2022).

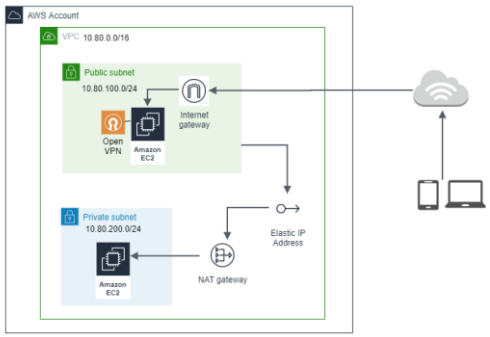
Desain topologi ini menjadi acuan dalam merancang sistem. Selanjutnya pada tahap ketiga yaitu *build prototype* dibangun sistem keamanan berdasarkan informasi yang dikumpulkan dari *quick design* dari rancangan sebelumnya.

Pada tahap ke empat dilakukan proses *evaluation* yaitu melakukan pengujian. Jika *prototype* yang dibangun tidak sesuai maka dilakukan perbaikan prototype. Pada tahap akhir *Refining Prototype* yaitu melakukan perbaikan terhadap prototype dari hasil evaluasi(Putri et al., 2022).

HASIL DAN PEMBAHASAN

Perancangan Topologi Infrastruktur

Pada gambar 2 menunjukkan desain infrastruktur yang dibangun berbasis cloud. Sistem ini dirancang dengan menggunakan dua buah komputer EC2 dan satu VPC.



Gambar 2. Topologi Infrastruktur Cloud

Skenario dari perancangan ini yaitu komputer atau smartphone pribadi yang terhubung ke internet masuk ke gateway akun aws cloud. Selanjutnya internet gateway akan mengarahkan permintaan publik melalui komputer server EC2 dengan subnet 10.80.100.0./24 permintaan ke server pribadi akan diarahkan ke elastik IP address melalui NAT gatewaty menuju server private subnet di 10.80.200.0/24.

Implementasi Sistem

Pembangunan infrastruktur keamanan koneksi pribadi melalui Open VPN menggunakan layanan Amazone Web Services (AWS). Beberapa layanan yang digunakan dalam membangun sistem keamanan vpn ini ditampilkan pada tabel 1.

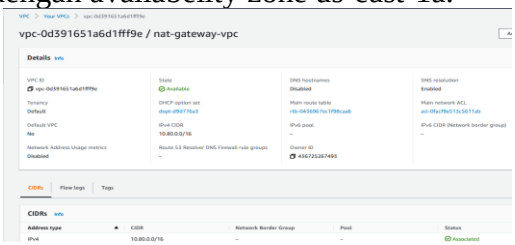
Tabel 1. Layanan AWS

Services	*Qty*	*Specification*
Amazon VPC	1	*enables launch AWS resources into a virtual*

		network. VPC create one region
Amazon EC2	2	*t2.micro, 1vCPU, 1GiB Memory, OpenVPN Access Server*

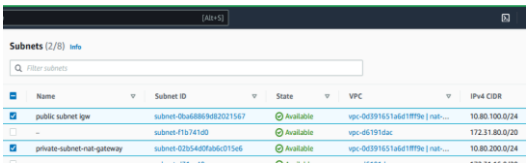
Implementasi VPC

Implementasi VPC dilakukan pada satu region yang berada di N.Virginia dengan availabelity zone us-east-1a.

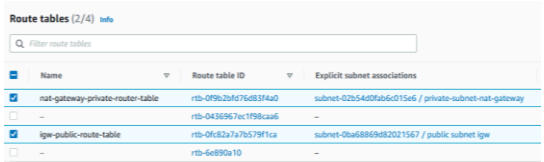


Gambar 3. VPC dengan availableity zone us-east-la

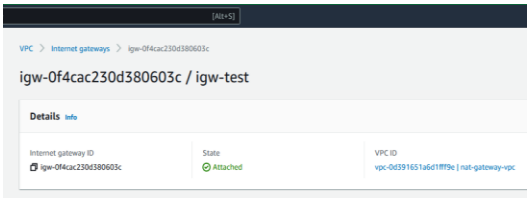
Beberapa pengaturan yang dilakukan pada VPS ini diantaranya 1).Menambahkan private subnet pada dan public subnet di VPC dengan region yang sama, 2). Menambahkan route table pada private subnet dan asscociate IT, 3). Menambahkan 1 NAT gateway dan 1 internet gateway 4). Launch 1 EC2 instance in private subnet 5). Melakukan pengecekan dari internet 6). Melakukan instalasi dan konfigurasi OPEN VPN pada Public EC2



Gambar 4. Menambahkan public subnet igw dan priate subnet nat gateway

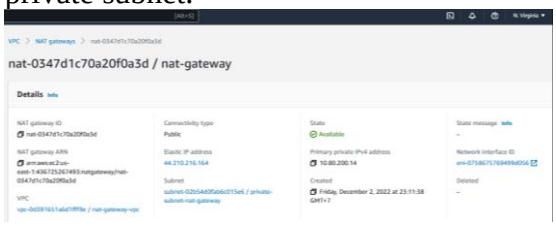


Gambar 5. Menambahkan route tables for nat-gateway public dan private



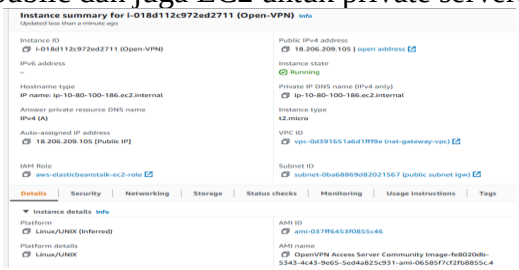
Gambar 6. Konfigurasi internet gatwaye dengan detach VPC

Pengaturan NAT gateway terhubung ke elastic IP menuju ke server private server yang berada di lokasi private subnet.

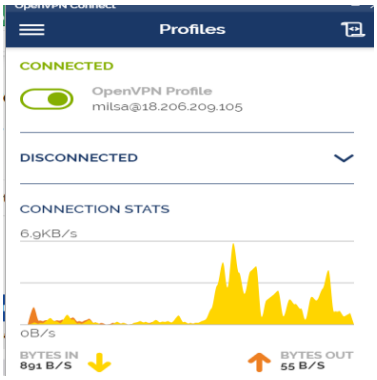


Gambar 7. Konfigurasi NAT Gateways

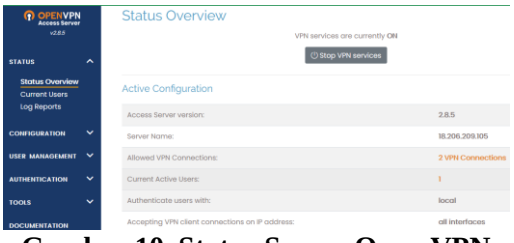
Pada server EC2 dilakukan implementasi Open VPN untuk akses public dan juga EC2 untuk private server.



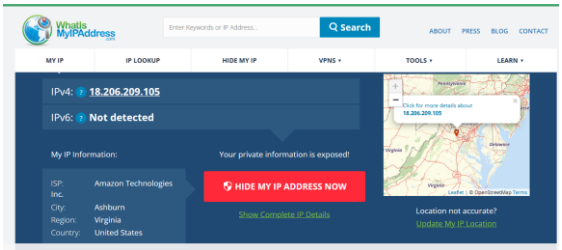
Gambar 8. Detail instance EC2 Open VPN



Gambar 9. Client Open VPN terhubung ke server VPN pada AWS



Gambar 10. Status Server Open VPN



Gambar 11. Personal user terkoneksi melalui IP address dari Virginia, US

SIMPULAN

Implementasi keamanan pribadi dengan menggunakan open vpn berhasil dilakukan. Pengguna dapat terhubung ke server open vpn pada lokasi Virginia, US. Percobaan melalui client berbasis windows dan juga mobile android dapat dilakukan dan terkoneksi ke server vpn. Ini sangat membantu dalam menjelajahi internet dengan aman yang dilindungi untuk menjaga privasi pada jaringan wifi. Open vpn ini dapat diakses dari jaringan mana saja baik itu pada jaringan wifi maupun jaringan internet selular.

DAFTAR PUSTAKA

Astri Saraun, Arie S.M. Lumenta, D. F. S. (2021). An Analysis of WLAN Security at the Minahasa Regency Office of Educational Affairs. *Jurnal Teknik Informatika Unsrat*, *17*(1), 19–26.

Dekas, R. (2022). Pengaruh Peningkatan Pemasangan Wi-Fi Di Kota Prabumulih. *Jurnal Neraca Peradaban*, *2*(1), 31–38. https://doi.org/10.55182/jnp.v2i1.90

Hutchison, D. (2022). *Computer Aided Verification 2022-1*.

Mishra, A. (2017). *Amazon web services for mobile developers : building Apps with AWS*.

Mishra, S., Kumar, M., Singh, N., & Dwivedi, S. (2022). A Survey on AWS Cloud Computing Security Challenges & Solutions. *Proceedings - 2022 6th International Conference on Intelligent Computing and Control Systems, ICICCS 2022*, 614–617. https://doi.org/10.1109/ICICCS53718.2022.9788254

Mujiastuti, R., & Prasetyo, I. (2021). Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE. *Prosiding Semnastek*, *November 2021*. https://jurnal.umj.ac.id/index.php/semnastek/article/view/11484

Mulya, N. B., Pradnyani, K. D. N., Wangi, A. L., Nugraha, A. A., & Rimadhani, T. D. (2021). Analisis Peningkatan Jumlah Kasus Cyber Attack Di Indonesia Pada Masa Pandemi Covid-19: *Prosiding Seminar Nasional Teknologi Dan Sistem Informasi*, *1*(1), 241–247. http://sitasi.upnjatim.ac.id/index.php/sitasi/article/view/188

Nugroho, A., & Mustofa, T. K. (2012). Implementasi Komputasi Awan Menggunakan Teknologi Google App Engine (Gae) Dan Amazon Web Services (Aws). *Jurnal Teknik Informatika*, *1*(1), 1–13. https://doi.org/10.35793/jti.1.1.2012.542

Osswald, L., Haeberle, M., & Menth, M. (n.d.). *Performance Comparison of VPN Solutions*. https://www.wireguard.com/.

Posey, B. (2021). *What is a Server?* https://www.techtarget.com/whatis/definition/server

Putri, C. M., Dani, U., Mulyana, D. A., Putri, Y. T., Fajri, K., Maulana, R. A., & Hamzah, M. L. (2022, June). Perancangan Sistem Informasi Pemesanan Menu Berbasis Web Menggunakan Agile Method. In *Prosiding Seminar Nasional Teknologi Informasi dan Bisnis* (pp. 94-98).

Putri, A., Syah, N. S., Oksama, M. H., Safiesza, Q. F. F., & Hamzah, M. L. (2022, June). Perancangan Sistem Informasi Manajemen Organisasi Mahasiswa Universitas Islam

Negeri Sultan Syarif Kasim Riau. In *Prosiding Seminar Nasional Teknologi Informasi dan Bisnis* (pp. 32-38).

Skendzic, A., & Kovacic, B. (2017). Open source system OpenVPN in a function of Virtual Private Network. *IOP Conference Series: Materials Science and Engineering*, *200*(1). https://doi.org/10.1088/1757-899X/200/1/012065

Taufieq, R. (2022). *Bahaya Memakai VPN Gratis untuk Mengakses Situs yang Diblokir Halaman all - Kompas.com*. Kompas.Com. https://www.kompas.com/tren/read/2022/07/31/060000265/bahaya-memakai-vpn-gratis-untuk-mengakses-situs-yang-diblokir?page=all

Usanto, S. (2021). *Rancang Bangun Jaringan Site To Site Vpn (Virtual Private*. *01*, 55–65.