INFOTRON
Informatics, Electronics and Control Engineering
1 (1) 2021 pp. 1-5
ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)
Jurnal Ilmiah Teknik Informatika, Elektronika dan Kontrol (Scientific Journal of Informatics, Electronics and Control Engineering)

Tersedia online di www.journal.unisma.ac.id

UNIVERSITAS ISLAM MALANG

S2-Accredited – SK No. 01/E/KPT/2021

Halaman journal tersedia di www.journal.unisma.ac.id:8080/index.php/infotron

ANALISA KONEKTIVITAS JARINGAN IPSEC DAN OPENVPN PADA JARINGAN BERBASIS IP DINAMIS

As' Ari Setya[a], *Aris Sudaryanto*[b]

[a]*Teknik Informatika, Universitas 17 Agustus 1945 Surabaya, Surabaya, Indonesia*

[b]*Teknik Informatika, Universitas 17 Agustus 1945 Surabaya, Surabaya, Indonesia*

email: [a] arisetya0@gmail.com, [b] *aris@untag-sby.ac.id*

INFORMASI ARTIKEL

Sejarah artikel:
Received 24 January 2020
Revised 30 April 2020
Accepted 2 December 2020
Available online xxx

Kata kunci: [Judul kata kunci]

VPN
IPSEC
OpenVPN
Konektivitas

Gaya IEEE dalam mengutip artikel ini: [rujukan?]
F. Fulan and F. Fulana, "Article Title," Register: Jurnal Ilmiah Teknologi Sistem Informasi, vol. 6, no. 1, pp. 1-10, 2020. [Isi judul kutipan]

A B S T R A K

Saat ini jaringan merupakan kebutuhan vital bagi setiap perusahaan. Dengan internet maka jaringan dapat terbentuk dan menghubungkan antar sektor atau divisi dalam perusahaan. Akan tetapi jaringan internet juga memiliki isu yang perlu diperhatikan, yaitu isu keamanan. Semakin banyak hubungan dengan jaringan luar maka tentu saja semakin besar potensi ancaman keamanan data. Salah satu solusi untuk tetap menjaga keamanan data selama terhubung dengan jaringan adalah menggunakan VPN. Dengan menggunakan VPN maka data akan dikirim melewati tunnel yang menghubungkan antar jaringan, serta dilakukan enkripsi pada data tersebut. Pada penelitian ini penulis melakukan analisa terhadap konektivitas antara VPN IPSEC dan OpenVPN. Pengujian dilakukan dengan menggunakan dua buah jaringan lokal pada dua lokasi berbeda (Lokasi A dan B), lalu masing masing diuji konektivitasnya ketika menggunakan VPN IPSEC maupun ketika menggunakan OpenVPN.

1 Pendahuluan

Saat ini jaringan internet merupakan salah satu tulang punggung keberhasilan bisnis suatu perusahaan. Untuk mencapai keterhubungan antar sektor yang efektif, memiliki performa maksimal, namun tetap dengan biaya yang minimal, maka diperlukan perencanaan perangkat yang baik. Selain itu, sangat penting untuk juga memperhatikan aspek keamanan untuk menjaga kerahasiaan data, demi mencegah kebocoran data atau bahkan pencurian. Salah satu dari konsep dari keamanan adalah kerahasiaan (*confidentiality*) yang berarti data hanya boleh diakses oleh individu yang memiliki otoritas / autentikasi terhadap data tersebut [1]. Untuk mencapai kerahasiaan sebagaimana dimaksud pada [1] maka diperlukan jalur yang aman di dalam jaringan yang menghubungkan antar lokasi.

Teknologi yang digunakan dalam jaringan internet publik adalah *DSL (Digital subscriber line). DSL* adalah teknologi yang menggunakan kabel tembaga untuk mendapatkan kecepatan data yang

F. Fulan, et. al./INFOTRON 1 (1) 2021 pp. 1-5
ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)

tinggi dengan menggunakan kabel tembaga [2], teknologi ini disebut juga sebagai teknologi broadband.

Salah satu kelemahan penggunaan jaringan internet publik adalah besarnya kemungkinan akses data oleh pihak lain atau pihak yang tidak seharusnya memiliki otoritas. Namun kelemahan tersebut mulai dapat ditutupi dengan teknologi VPN. *VPN* melakukan enkapsulasi dan enkripsi data yang dikirimkan, dan menggunakan autentikasi untuk memastikan hanya pengguna yang diperbolehkan yang dapat mengakses data tersebut [3].

Berdasarkan beberapa penelitian [4] dan [5] menunjukkan bahwa teknologi *VPN* dapat diimplementasikan dalam lingkungan IP dinamis dengan menggunakan *DDNS*, kedua penelitian ini menggunakan jenis *VPN IPSEC*. Selain *IPSEC*, *OPENVPN* merupakan jenis *VPN* yang berbasis yang berbasis *SSL* yang memiliki tingkat keamanan yang hampir sama dengan *IPSEC*.

IPSEC dan *OPENVPN* dapat menjadi alternatif dalam membangun *VPN*. Pada penelitian ini, dilakukan analisa konektivitas dari *IPSEC* dan *OPENVPN* pada jaringan *VPN*, untuk menemukan jenis *VPN* dengan performa yang lebih baik.

2 Landasan Teori

Jaringan internet saat ini menjadi salah satu tulang punggung dalam operasional perusahaan. Namun meskipun begitu, terdapat isu isu yang sangat perlu diperhatikan, misalnya isu keamanan dan kerahasiaan data. Salah satu konsep dari keamanan data adalah kerahasiaan (*confidentiality*) yang artinya data hanya boleh diakses oleh pihak yang memiliki otoritas [1]. Salah satu metode yang dapat menjawab isu keamanan data pada jaringan adalah VPN, karena VPN melakukan enkapsulasi dan enkripsi terhadap data yang dikirimkan, serta melakukan autentifikasi terhadap penerima data [3].

Penggunaan VPN menghubungkan antar lokasi atau disebut site-to-site VPN telah dilakukan sejak dulu. Diantaranya penelitian yang dilakukan oleh Mubarok [6] yang membangun VPN dengan menggunakan fitur IP Cloud yang dimiliki mikrotik. Dalam penelitian ini protokol VPN yang digunakan untuk menghubungkan antar lokasi adalah PPTP dan menggunakan EOIP sebagai protokol untuk pembuatan tunnelnya.

Penelitian yang dilakukan oleh Haque dan Pamungkas [7] merupakan penelitian lanjutan berdasarkan oleh penelitian Mubarok. Penelitian lain yang dilakukan oleh Zacky menggunakan protokol VPN IPSEC dan L2TP sebagai protokol tunnelnya untuk menghubungkan jaringan antar lokasi . Dalam penelitian ini mengharuskan salah satu lokasi harus menggunakan IP Publik static.

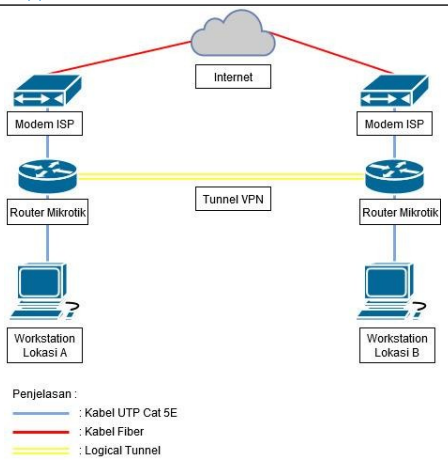
Penelitian lainnya mengenai penggunaan IPSEC adalah penelitian Firdhaus, Fatmawati, dan Wijonarko [5], yang mengimplementasikan site-to-site VPN dengan menggunakan IPSEC untuk menghubungkan jaringan di kementrian perhubungan [8]. Dalam penelitian ini menggunakan VPN IPSEC sebagai protokol VPN dan tunnelnya.

3 Metode Penelitian

Sistem yang digunakan dalam metode ini menggunakan dua perangkat router yang terhubung secara riil. Kedua router ini masing-masing terhubung dengan sebuah perangkat router ISP Indihome di dua lokasi yang berbeda. Namun kedua router mendapatkan IP lokal yang diberikan oleh router ISP secara default, sedangkan agar VPN dapat digunakan dibutuhkan IP Publik. Fungsi IP Publik ini adalah agar DDNS dari fitur IP Cloud Mikrotik dapat berfungsi dan digunakan sebagai alamat dial-up VPN.

Setelah kedua router Mikrotik mendapatkan IP Publik secara langsung dari router ISP, maka dibuat tunnel untuk masing-masing jaringan VPN. Dengan tunnel VPN IPSEC dan OpenVPN yang terhubung maka jaringan LAN dari kedua lokasi dapat melakukan ping secara langsung layaknya sebuah jaringan LAN yang berada dalam satu lokasi.

ISSN 2502-3357 (Online)
F. Fulan, et. al./INFOTRON 1 (1) 2021 pp. 1-5 ISSN 2503-0477 (Print)



Gambar 1. Topologi fisik

4 Hasil and Pembahasan

Untuk melihat dan membandingkan kemampuan IPSEC dan OPENVPN dalam hal konektivitas, maka dilakukan pengujian terhadap keduanya. Dalam pengujian terdapat dua buah LAN di dua lokasi berbeda, yaitu lokasi A dan lokasi B yang keduanya memiliki jaringan lokal. Pengujian pertama dilakukan ping sebanyak 15 kali untuk melihat apakah jaringan lokal di lokasi A dan lokasi B dapat terhubung dengan menggunakan IPSEC ataupun OPENVPN. Pengujian kedua dilakukan untuk memeriksa apakah paket dari jaringan LAN dari masing masing lokasi dapat melewati tunnel IPSEC maupun OPENVPN, caranya dengan melakukan pengujian traceroute.

Tabel 1. Tabel hasil pengujian konektivitas IPSEC

Lokasi	Pengujian	Hasil pengujian
Lokasi A	Melakukan ping dari router mikrotik ke alamat ip 192.168.100.1 yang terdapat pada router mikrotik	sukses
	Melakukan ping dari router ke alamat ip 192.168.100.250 yang terdapat pada laptop yang terhubung ke router mikrotik	sukses
	Melakukan ping dari laptop yang mendapatkan ip 192.168.101.250 mikrotik ke alamat ip 192.168.100.1 yang terdapat pada router mikrotik	sukses
	Melakukan ping dari laptop yang mendapatkan ip 192.168.101.250 ke alamat ip 192.168.100.253 yang terdapat pada laptop yang terhubung ke router mikrotik	sukses
	Melakukan traceroute dari laptop lokasi A ke alamat IP laptop lokasi B	sukses, namun hop yang dilewati disembunyikan
Lokasi B	Melakukan ping dari router mikrotik ke alamat ip 192.168.101.1 yang terdapat pada router mikrotik	sukses
	Melakukan ping dari router mikrotik ke alamat ip 192.168.101.253 yang terdapat pada laptop yang terhubung ke router mikrotik	sukses
	Melakukan ping dari laptop yang mendapatkan ip 192.168.100.253 mikrotik ke alamat ip 192.168.101.1 yang terdapat pada router mikrotik	sukses
	Melakukan ping dari laptop yang mendapatkan ip 192.168.100.253 ke alamat ip 192.168.101.250 yang terdapat pada laptop yang terhubung ke router mikrotik	sukses
	Prosentase Keberhasilan lokasi A dan lokasi B	100%

Hasil pengujian untuk IPSEC ditampilkan pada Tabel 1. Terlihat bahwa dengan menggunakan IPSEC pada lokasi A, ping antar router mikrotik di lokasi A berhasil dilakukan, ping dari router ke router mikrotik di lokasi A juga berhasil dilakukan, ping dari laptop ke router mikrotik lokasi A juga

F. Fulan, et. al./INFOTRON 1 (1) 2021 pp. 1-5
ISSN 2502-3357 (Online)
ISSN 2503-0477 (Print)

berhasil, ping antar laptop di lokasi A juga berhasil dilakukan, terakhir percobaan traceroute dari laptop di lokasi A ke laptop di lokasi B berhasil dilakukan meski hop yang dilewati disembunyikan. Keberhasilan yang sama juga didapatkan pada pengujian yang sama untuk lokasi B. Keseluruhan pengujian untuk IPSEC berhasil 100%.

Tabel 2. Tabel hasil pengujian konektivitas OPENVPN

Lokasi	Pengujian	Hasil pengujian
Lokasi A	Melakukan ping dari router mikrotik ke alamat ip 192.168.100.1 yang terdapat pada router mikrotik	sukses
	Melakukan ping dari router ke alamat ip 192.168.100.250 yang terdapat pada laptop yang terhubung ke router mikrotik	sukses
	Melakukan ping dari laptop yang mendapatkan ip 192.168.101.250 mikrotik ke alamat ip 192.168.100.1 yang terdapat pada router mikrotik	sukses
	Melakukan ping dari laptop yang mendapatkan ip 192.168.101.250 ke alamat ip 192.168.100.253 yang terdapat pada laptop yang terhubung ke router mikrotik	sukses
	Melakukan traceroute dari laptop lokasi A ke alamat IP laptop lokasi B	sukses, packet melewati 10.20.30.1
Lokasi B	Melakukan ping dari router mikrotik ke alamat ip 192.168.101.1 yang terdapat pada router mikrotik	sukses
	Melakukan ping dari router mikrotik ke alamat ip 192.168.101.253 yang terdapat pada laptop yang terhubung ke router mikrotik	sukses
	Melakukan ping dari laptop yang mendapatkan ip 192.168.100.253 mikrotik ke alamat ip 192.168.101.1 yang terdapat pada router mikrotik	sukses
	Melakukan ping dari laptop yang mendapatkan ip 192.168.100.253 ke alamat ip 192.168.101.250 yang terdapat pada laptop yang terhubung ke router mikrotik	sukses
	Prosentase Keberhasilan lokasi A dan lokasi B	100%

Hasil pengujian untuk OPENVPN ditampilkan pada Tabel 2. Terlihat bahwa dengan menggunakan OPENVPN pada lokasi A, ping antar router mikrotik di lokasi A berhasil dilakukan, ping dari router ke router mikrotik di lokasi A juga berhasil dilakukan, ping dari laptop ke router mikrotik lokasi A juga berhasil, ping antar laptop di lokasi A juga berhasil dilakukan, terakhir percobaan traceroute dari laptop di lokasi A ke laptop di lokasi B berhasil dan packet yang dikirimkan dapat lewat dengan sukses. Keberhasilan yang sama juga didapatkan pada pengujian yang sama untuk lokasi B. Keseluruhan pengujian untuk OPENVPN berhasil 100%.

5 Kesimpulan dan Saran

Berdasarkan pengujian yang telah dilakukan untuk membandingkan konektivitas antara penggunaan IPSEC dengan penggunaan OPENVPN, didapatkan hasil bahwa baik menggunakan IPSEC maupun menggunakan OPENVPN, keduanya menghasilkan konektivitas yang baik. Hal tersebut terbukti dari hasil pengujian konektivitas keduanya yang mencapai 100%.

Untuk penelitian selanjutnya, mungkin dapat dilakukan pengujian pengujian lainnya untuk membandingkan performa IPSEC dengan OPENVPN, misalnya pengukuran packet loss, delay dan lain lain. Jika pengujian lain sudah dilakukan dan diketahui mana yang lebih baik performanya, maka sistem kemungkinan dapat dikembangkan lagi dengan menerapkan otomatisasi jaringan, misalnya seperti menerapkan otomatisasi setting bonding [9] atau menerapkan sistem backup konfigurasi router secara otomatis[10].

ISSN 2502-3357 (Online)
F. Fulan, et. al./INFOTRON 1 (1) 2021 pp. 1-5 ISSN 2503-0477 (Print)

6 Referensi

[1] K. Barker and S. Morris, *CCNA Security 640-554 Official Cert Guide*. Cisco Press PP - Indianapolis, 2013.

[2] J. Cowley, *Communications and Networking : an Introduction*. Springer London PP - London, 2007.

[3] W. Panek, *MCSA Windows Server 2016 study guide : exam 70-741: Networking with Windows Server 2016*. Indianapolis, Indiana Sybex, A Wiley Brand, 2017.

[4] D. Kurnia, "Pemanfaatan Bettercap Sebagai Teknik Sniffing Pada Paket Trafik Jaringan Wifi," *Semin. Nas. Tek. UISU*, vol. 2, no. 1, pp. 83–85, 2019.

[5] C. E. Suharyanto and V. Gopama, "Pemanfaatan Mini Komputer Raspberry Sebagai Network Monitoring Tool Portable," *JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer)*, vol. 5, no. 1, pp. 133–138, 2019, doi: 10.33480/jitk.v5i1.707.

[6] D. F. Mubarok, "Implementasi EoIP over VPN di jaringan berbasis dynamic IP (studi kasus PT.Validata Teknologi)," *E-Journal*, vol. Vol. 4, no. No. 1, 2018.

[7] A. Z. F. Haque and W. H. Pamungkas, "Rancang Bangun Automated Virtual Private Network Menggunakan Jaringan Small Office Home Office (Soho) Di Pt . Satnetcom Balikpapan Design and Implementation of Automated Virtual Private Network Using Small Office Home Office (Soho) Network in Pt .," pp. 112–121, 2019.

[8] L. Firdhaus, Fatmawati, and B. Wijonarko, "Penerapan Vpn Ip Security Site To Site Di Kementrian Perhubungan," vol. 14, no. 1, pp. 13–20, 2019.

[9] K. Dria Perkasa, A. Sudaryanto, and E. Dwi Hartono, "Pengujian Bandwidth Pada Sistem Setting Bonding Otomatis Menggunakan Library Paramiko," *INFOTRON*, vol. 1, no. 1, pp. 1–5, 2021, [Online]. Available: http://riset.unisma.ac.id/index.php/INFOTRON/article/view/11215.

[10] M. Afrianto, D. Agus, and S. Aris, "SISTEM BACKUP KONFIGURASI ROUTER SECARA OTOMATIS DENGAN SHELL SCRIPT (STUDI KASUS : PT NETTOCYBER INDONESIA)," *KONVERGENSI*, vol. 15, no. 1, pp. 57–69, 2019, doi: https://doi.org/10.30996/konv.v15i1.2833.