Paper

Pengamanan Koneksi Jaringan Lokal Terhadap Jaringan Publik Dengan Open VPN Pada Server Linux

Author: **Ummul Khair, Yuyun Dwi Lestari**

SNASTIKOM 10
Seminar Nasional Teknologi Informasi dan Komunikasi
UNIVERSITAS HARAPAN MEDAN 2012-2023
Program Studi Teknik Informatika
TEMA : DUNIA AKADEMIK DI ERA SOCIETY 5.0 : TANTANGAN DAN PELUANG
ISSN : 2964-1950

SNASTIKOM Ke 10 Tahun 2023
ISBN: 2964-1950

Pengamanan Koneksi Jaringan Lokal terhadap Jaringan Publik dengan OpenVPN pada Server Linux

Ummul Khair[1], Yuyun Dwi Lestari[2]
[1,2]Universitas Harapan, Medan, Indonesia
[1]ummulkhair@unhar.ac.id, [2]yuyundwilestari@unhar.ac.id

Abstrak

Keamanan jaringan internet sangat penting, karena jaringan internet merupakan jaringan yang bebas sehingga belum terjamin keamanannya. Dengan membangun jaringan private pada jaringan publik atau sering disebut Virtual Private Network (VPN) sehingga data dapat terjaga keamanannya dan terhindar dari kejahatan jaringan publik. Dengan adanya aplikasi OpenVPN yang menggunakan private keys, certificate atau username/password untuk melakukan authentikasi dalam membangun koneksi. Dimana protokol yang digunakan untuk enkripsi dalam jaringan OpenVPN menggunakan protokol Secure Socket Layer (SSL). Dengan membangun server OpenVPN, maka IP lokal yang sebenarnya berada pada sisi client berhasil disembunyikan dengan IP yang telah di share melalui server OpenVPN yang telah dibangun.
.

Kata Kunci: jaringan internet, jaringan private, VPN, OpenVPN, SSL

Abstract

Internet network security is very important, because the internet network is a free network so its security is not guaranteed. By building a private network on a public network or often called a Virtual Private Network (VPN), data can be kept secure and protected from public network crime. With the OpenVPN application which uses private keys, certificates or usernames/passwords to authenticate when establishing a connection. Where the protocol used for encryption in the OpenVPN network uses the Secure Socket Layer (SSL) protocol. By building an OpenVPN server, the local IP that is actually on the client side is successfully hidden with the IP that has been shared via the OpenVPN server that has been built..

Keywords: internet network, private network, VPN, OpenVPN, SSL

1. PENDAHULUAN

Dengan kemajuan zaman membuat suatu instansi, baik pemerintah maupun swasta harus dapat melakukan proses pengolahan sistem informasi yang cepat, tepat dan akurat. Sebuah instansi harus dapat memanfaatkan kemajuan teknologi dalam bidang komputer dan jaringan untuk dapat menghemat tenaga, waktu, biaya dan lain-lain. Untuk dapat mewujudkan hal tersebut, maka dukungan dari sisi infrastruktur jaringan pada sistem informasi dari instansi yang terkait sangat diperlukan. Dengan memanfaatkan penggunaan jaringan internet dapat membantu dalam mengatasi batasan jarak dan waktu. Kini seseorang dapat dengan mudah mengambil data atau mengolah data yang tersimpan di dalam jaringan lain. Contohnya jaringan di dalam sebuah instansi seperti perusahaan baik negeri atau swasta, juga dalam sebuah instansi yang bergerak dalam dunia pendidikan seperti sekolah dan perguruan tinggi, dari mana saja dan kapan saja. Hal tersebut dapat dilakukan jika jaringan tersebut terkoneksi dengan internet. [1]

Secara umum, VPN (Virtual Private Network) adalah sebuah proses dimana jaringan umum (public network atau internet) diamankan kemudian difungsikan menjadi sebuah jaringan privat (private network). Sebuah VPN tidak didefinisikan oleh rangkaian khusus atau router, tetapi didefinisikan oleh mekanisme keamanan dan prosedur-prosedur yang hanya mengizinkan penggunanya yang ditunjuk akses ke VPN dan informasi yang mengalir melaluinya. [2]

VPN pada dasarnya bekerja dengan cara melakukan forwarding lalu lintas data yang ada di dalam jaringan internet. Jadi, ketika user mulai melakukan koneksi dengan internet, semua data dan arus transmisi yang melewati jaringan internet dapat diakses dengan mudah, tanpa khawatir

tidak dapat membuka situs-situs yang diblokir. Dengan menggunakan VPN, maka user nantinya akan melakukan koneksi dengan internet mirip seperti menggunakan jaringan lokal pribadi, sehingga lebih aman dan juga bisa mengakses banyak situs dari internet.

Jaringan VPN ini memberikan layanan yang bersifat private meskipun sebenarnya data atau informasi yang disampaikan melewati jaringan publik. Untuk proses pengenalan user oleh server diberikan suatu sistem yang disebut RADIUS (Remote Authentication Dial-In User Service). Hasil yang diperoleh adalah dihasilkannya rancang bangun RADIUS server yang memiliki proses Autentikasi, Accounting yang digabungkan dengan suatu bentuk jaringan yang berbasis VPN sehingga diharapkan tercipta suatu bentuk Security Network System yang mampu memberikan keamanan pengiriman data pada jaringan publik. [3]

Serangan yang cenderung bersifat *destruktif* (merusak) tersebut sudah selayaknya harus ditangkal dan dihindari agar tidak merugikan banyak pihak. Oleh karena itu sejumlah usaha pengamanan jaringan harus dilakukan oleh mereka yang berkepentingan. [4]

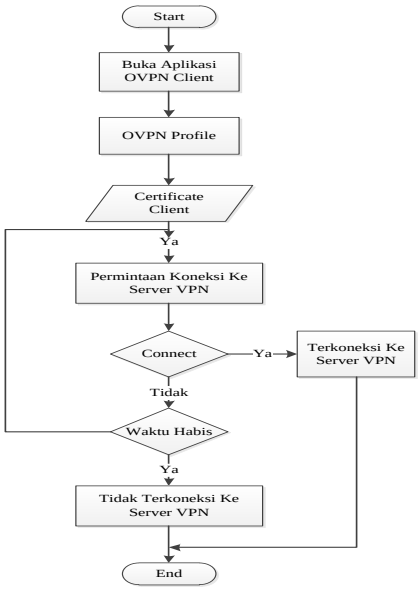
Jaringan LAN merupakan jaringan milik pribadi didalam sebuah kantor, gedung atau kampus yang berjarak sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan *workstation* dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumber daya (*resource,* misalnya *printer*) dan saling bertukar informasi.[5]

DARPA mengontak *Bolt, Beranek, and Newman* (BBN) untuk membangun TCP/IP untuk *Berkeley UNIX* di *University of California* di *Berkeley*, untuk mendistribusikan kode sumber bersama dengan sistem operasi *Berkeley Software Development* (BSD), pada tahun 1983 (4.2BSD). Mulai saat itu, TCP/IP menjadi terkenal di seluruh Universitas dan badan penelitian dan menjadi protokol standar untuk komunikasi.[6]

2. METODE PENELITIAN

2.1 Alur Kerja

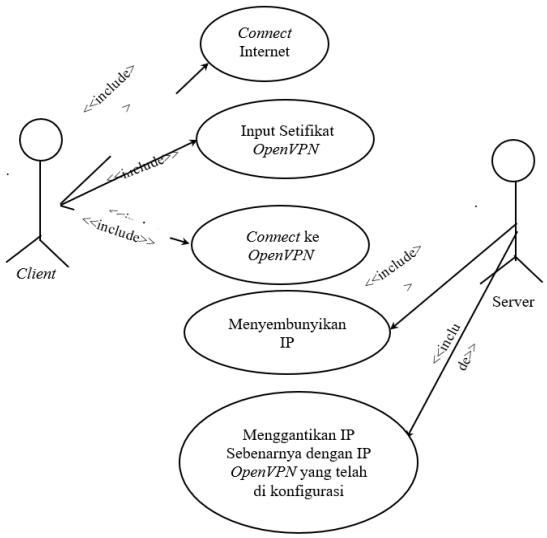
Flowchart alur kerja merupakan suatu langkah-langkah yang menggambarkan dari aliran kerja yang berlangsung untuk mendapatkan hasil akhir. Alur kerja dari VPN pada sistem ini dapat dilihat melalui *flowchart* gambar 1 di bawah ini:



Gambar 1. *Flowchart* Alur Kerja

2.2 Perancangan Sistem

Use Case Diagram digunakan untuk menggambarkan sistem dari sudut pandang pengguna sistem tersebut *(user).* sehingga pembuatan *use case diagram* lebih dititik beratkan pada fungsionalitas yang ada pada sistem, bukan berdasarkan alur atau urutan kejadian. Sebuah *use case diagram* mempresentasikan sebuah interaksi antara aktor dengan sistem. *Use case diagram* pada penelitian ini dapat dilihat pada Gambar 2 di bawah ini:

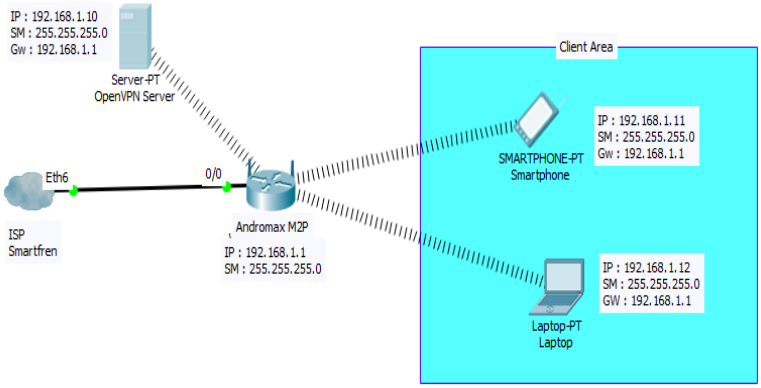


Gambar 2. *Use Case Diagram*

3. HASIL DAN PEMBAHASAN

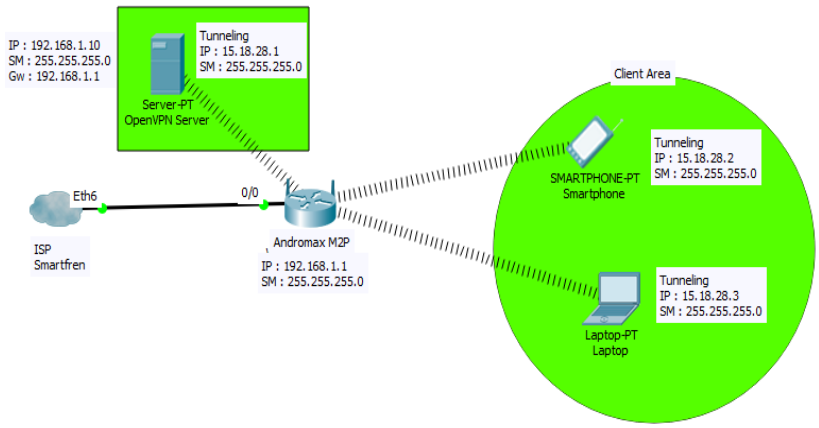
3.1 Hasil

Penggambaran skema topologi jaringan yang akan di implementasi pada penelitian ini menggunakan bantuan aplikasi *cisco packet tracer* versi 7.1 dapat dilihat pada gambar 3 di bawah ini:



Gambar 3. Topologi Jaringan Sebelum *Tunneling*

Sebelum terjadinya *tunneling* atau koneksi *client* kepada *server OpenVPN*, alokasi IP yang diberikan kepada masing-masing *client* di berikan berdasarkan IP yang telah di *setting* pada ISP modem *wirrelless andromax* yaitu 192.168.1.1 sebagai IP dari modem dan *gateway* bagi tiap-tiap perangkat *client* dengan *range* IP 192.168.1.10 s/d 192.168.1.20. dapat dilihat pada gambar 4 di bawah ini:



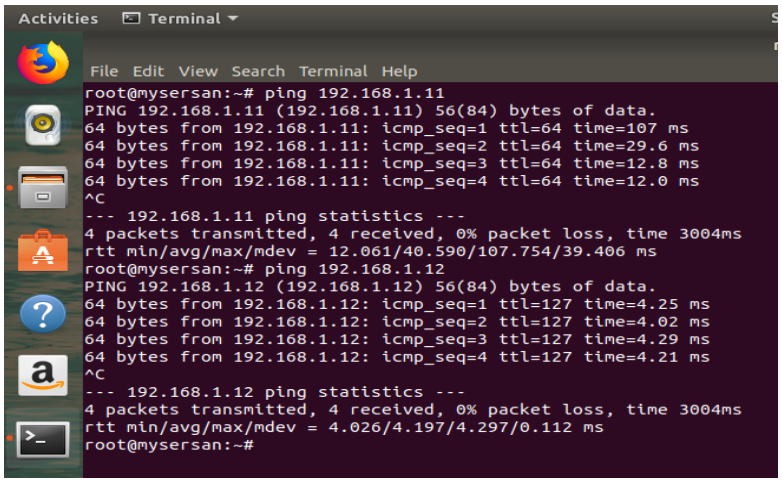
Gambar 4. Topologi Jaringan Setelah Terjadinya *Tunneling*

3.2 Pengujian sistem

Pengujian ini dilakukan untuk mengetahui kerja *Server* pada masing-masing *Client* dapat bekerja dengan baik antara lain pengujian status koneksi *OpenVPN*, pengujian *Ping Server* dan *Client* pada jalur publik dan jalur *tunneling*, dan pengujian pada aplikasi *web* untuk mendeteksi kebocoran IP, uji koneksi internet pada *client*, kemudian data hasil pengujian yang diperoleh nantinya akan dibahas untuk dijadikan dalam pengambilan kesimpulan.

a. Pengujian Koneksi Internet dan Alamat IP ISP Pada Terminal

Pada pengujian ini peneliti memanfaatkan utilitas ping pada terminal *server (linux)* ataupun *comand prompt* (CMD) pada *client (windows)* sebagai parameter keberhasilan suatu koneksi antara sistem baik untuk *client* kepada *server* ataupun koneksi *client* pada jaringan internet atau public.

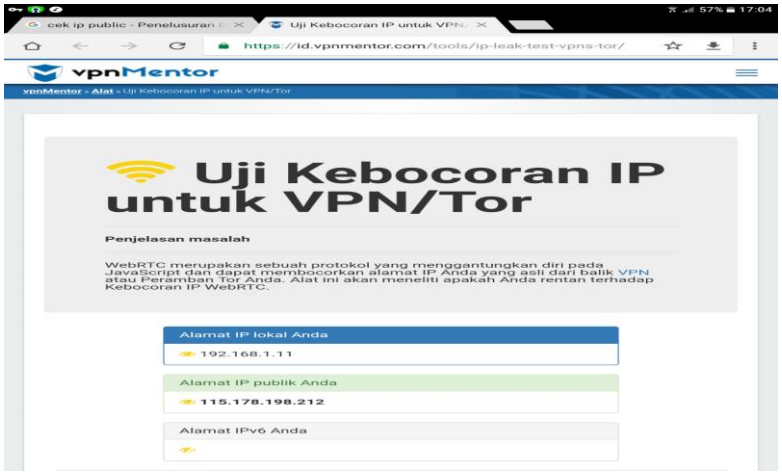


Gambar 5. Tes Koneksi Jaringan Ping Dari *Server* Ke *Client* Sebelum Terjadi *Tunneling*

ISBN: 2964-1950

b. Pengujian Kebocoran IP Melalui Aplikasi Web

Pada pengujian kali ini peneliti akan menguji sistem yang di bangun menggunakan beberapa aplikasi *web*. Peneliti mengambil dua sampel aplikasi *web* untuk menguji kekuatan sistem yang telah di bangun dengan dua sampel aplikasi *web* yang telah sangat teruji dan mempunyai rating yang sangat popular yaitu www.whatismyip.com dan id.vpnmentor.com dengan melakukan pengujian tersebut kita dapat mengetahui apakah ada terjadi kebocoran IP atau tidak setelah sistem di jalankan.



Gambar 6. Pengujian Sebelum *Tunneling*

KESIMPULAN

Adapun kesimpulan yang dapat Peneliti sampaikan pada akhir Skripsi ini adalah sebagai berikut:

1. Penelitian proteksi jaringan lokal dari ancaman jaringan publik (internet) menggunakan sistem *OpenVPN* yang telah dibangun berhasil dilaksanakan dan diimplementasikan.
2. Dengan membangun *server OpenVPN* IP lokal yang sebenarnya berada pada sisi *client* berhasil disembunyikan ataupun dimanipulasi dengan IP yang telah di *share* melalui *server OpenVPN* yang telah dibangun. Akan tetapi hanya sebatas IP lokal saja yang bisa terproteksi sedangkan IP publik dan zona wilayah belum berhasil disembunyikan atau diproteksi secara maksimal.
3. Dengan membangun sistem proteksi perlindungan jaringan lokal dari acaman kejahatan pada jaringan publik (internet) menggunakan *server OpenVPN* kecepatan transfer data yang di berikan dari pihak provider atau ISP terjadi penurunan atau perlambatan, walaupun tidak terlalu terasa dan seknifikan. Akan tetapi penuruan kecepatan transfer tidak separah dengan metode VPN lainnya baik itu PPTP ataupun L2TP/IPSec yang sangat menguras *bandwith* sehingga membuat sistem transfer data menjadi sangat lambat.
4. Penggunaan *OpenVPN* sangat menjamin kerahasian dan keamanan data yang sedang ditransfer antar *user* ke u*ser* atau sekedar berselancar pada jaringan publik (internet) dikarenakan data yang berjalan telah dilindungin dengan *enkripsi* algoritma kriptografi yang telah di tanamkan dan di konfigurasi terlebih dahulu pada *server openVPN* yang dibangun.

DAFTAR PUSTAKA

[1] P. Oktivasari and A. B. Utomo, "Analisa Virtual Private Network Menggunakan OpenVPN Dan Point To Point Tunneling Protocol ISSN : 185-202," *J. Penelit. Komun. dan Opini Publik*, vol. 20, no. 2, pp. 185–202, 2016.

[2] F. D. I. Joko Triyono, Rr. Yuliana Rachmawati K, "Analisis Perbandingan Kinerja Jaringan VPN Berbasis Mikrotik Menggunakan Protokol PPTP Dan L2TP Sebagai Media Transfer Data ISSN : 2338-6312," *J. JARKOM*, vol. 1, no. 2, pp. 112–121, 2014.

[3] J. T. Ivan Joi Pramana, Naniek Widyastuti, "Implementasi Radius Server Pada Jaringan Virtual Private Network," *JARKOM*, vol. 1, no. 2, pp. 30–38, 2014.

[4] M. Mohamad Nurul Huda Monoarfa, Xaverius B.N. Najoan, ST., MT., Alicia A.E. Sinsuw, ST., "Analisa dan Implementasi Network Intrusion Prevention System di Jaringan Universitas Sam Ratulangi ISSN : 2301-8402," *E-Journal Tek. Elektro dan Komput.*, vol. 5, no. 4, pp. 34–45, 2016.

[5] D. S. Ramadhan and N. Mubarakah, "Perancangan Jaringan LAN Pada Gedung Perkantoran Dengan Menggunakan Software Cisco Packet Tracer," *SINGUDA ENSIKOM*, vol. 4, no. 3, 2013.

[6] S. Sukaridhoto, S. T. P. D, M. Arsitektur, and T. C. P. Ip, "Buku Jaringan Komputer I," 2014.