PERANCANGAN DAN IMPLEMENTASI VIRTUAL PRIVATE NETWORK (VPN) MENGGUNAKAN PROTOKOL SSTP (SECURE SOCKET TUNNELING PROTOCOL) MIKROTIK DI FAKULTAS MIPA UNIVERSITAS TANJUNGPURA

Ikhwan Ruslianto[1], Uray Ristian[2]
[1,2]*Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Tanjungpura Pontianak, Kode Pos:78124, Pontianak-Kalimantan Barat, Indonesia.*
[1]*ikhwanruslianto@siskom.untan.ac.id,* [2]*urayristian@ siskom.untan.ac.id*

Abstrak—**Internet sudah menjadi bagian yang tidak terpisahkan dari aktivitas manusia sehari-hari. Dengan internet segala informasi bisa didapatkan dalam waktu yang cepat, dari berbagai penjuru dunia dapat saling berkomunikasi dan bertukar informasi. Akan tetapi dengan adanya internet, keterbukaan informasi menjadi hal yang biasa, walaupun terkadang ada informasi yang masih bersifat rahasia (confidentiality). Informasi dapat berupa apa saja, tidak terkecuali informasi dan data yang berkaitan dengan institusi pendidikan, Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Tanjungpura salah satunya. Di Fakultas MIPA sendiri ada beberapa informasi-informasi informasi yang hanya boleh diakses oleh kalangan tertentu saja. Misalnya ada beberapa aplikasi yang hanya dapat dibuka di lingkungan FMIPA saja maka dibuatlah mekanisme Virtual Private Network menggunakan protokol SSTP (Secure Socket Tunneling Protocol) agar Server dan aplikasi yang ada di lingkungan FMIPA dapat diakses menggunakan internet diluar lingkungan FMIPA. Konfigurasi SSTP dapat dilakukan menggunakan perangkat router mikrotik yang dihubungkan menggunakan perantara Virtual Private Server (VPS) yang ada di internet, kemudian diintegrasikan pada router mikrotik, sehingga kedua kondisi tersebut dapat saling berinteraksi seolah-olah pengguna berada dilingkungan FMIPA Untan.**

Kata Kunci— **VPS, SSTP, VPN.**

I. PENDAHULUAN

Internet merupakan komponen penting dalam perkembangan teknologi saat ini. Bahkan internet sudah menjadi kebutuhan primer dalam sebuah lembaga atau organisasi. Kehadiran internet dapat mempermudah manusia untuk saling berkomunikasi dan berkoordinasi satu sama lainnya. Keterbukaan akses internet dapat digunakan oleh semua kalangan, tidak terkecuali akses internet pada sebuah institusi pendidikan seperti halnya pada Universitas Tanjungpura. Universitas Tanjungpura merupakan salah universitas di Kalimantan Barat yang telah mengimplementasikan teknologi dan komunikasi dalam aktivitasnya. FMIPA merupakan salah satu fakultas di Universitas Tanjungpura yang telah memiliki sembilan (9) Program Studi yaitu Matematika, Fisika, Kimia, Sistem Informasi, Rekayasa Sistem Komputer, Geofisika, Ilmu Kelautan, Statistika dan Biologi.

FMIPA telah memiliki akses internet yang digunakan dalam proses belajar mengajar maupun dalam memberikan layanan kepada civitas akademika. Akan tetapi, akses internet di FMIPA masih dikelola sepenuhnya oleh Unit Pelaksana Teknis (UPT) Teknologi Informasi dan Komunikasi Universitas Tanjungpura sehingga sangat bergantung pada sumber daya manusia yang ada di UPT tersebut apabila terjadi gangguan. Banyaknya jumlah program studi dan mahasiswa yang ada di Universitas Tanjungpura dapat juga menjadi kendala kurang maksimalnya kecepatan akses internet di masing-masing fakultas, salah satunya FMIPA. Selain itu, keterbukaan akses internet dilingkungan FMIPA, sangat memungkinkan terjadinya pengasksesan data oleh pihak yang tidak berwenang, misalnya pencurian data, penyadapan bahkan sampai dilevel peretasan komputer maupun server. Dari permasalahan-permasalahan tersebut, sehingga perlu adanya suatu solusi untuk membuat kenyamanan dan keamanan dalam berselancar didunia maya dilingkungan FMIPA.

Berdasarkan permasalahan diatas, pada penelitian dilakukan suatu perancangan dan implementasi Virtual Private Network (VPS) untuk melakukan pengaksesan informasi yang bersifat krudensial dengan protokol SSTP (Secure Socket Tunneling Protocol) yang ada pada mikrotik sehingga dapat mengurangi permasalahan internet yang kurang maksimal dari sisi kecepatan akses serta keamanan lalu lintas data dilingkungan FMIPA Universitas Tanjungpura.

II. METODOLOGI PENELITIAN

Tahapan-tahapan penelitian diperlukan dalam membangun metode penelitian. Sehingga hasil dari penelitian nantinya lebih prosedural dan relevan.

Adapun tahapan–tahapan dalam membangun metode penelitian adalah sebagai berikut :

A. Meteri penelitian

Adapun materi penelitian yang dibutuhkan dalam hal ini menyangkut :

1. Bahan Penelitian

Adapun bahan yang digunakan pada penelitian adalah :

a) Secure Socket Tunneling Protocol

SSTP adalah tembusan protokol yang tersedia pada platform Microsoft. Protokol ini berbasis pada kombinasi kedua teknologi, SSL dan TCP[2]. Teknologi SSL menjaminkan tingkat keamanan dengan transportasi dan integritas lalu lintas. SSL pada server kami di konfigurasi sedemikian rupa sehingga hanya metode enkripsi terbaik yang diaktifkan. SSTP bisa digunakan melalui firewall atau ISP throttling. Sejak SSTP beroperasi melalui TCP, dalam beberapa kasus akan dikendalikan IKEv2 atau protokol berbasis UDP lainnya. Secara keseluruhan, SSTP adalah pilihan terbaik dan dapat membantu menyelesaikan masalah konektivitas ataupun masalah kecepatan yang dimiliki. SSTP memiliki keunggulan dalam hal keamanan (Secure) dibanding dengan L2TP, PPTP dan PPP.

b) Virtual Private Network (VPN)

VPN adalah singkatan dari Virtual Private Network, yaitu sebuah terowongan Virtual (Virtual Tunnel) dari jaringan ke jaringan lain yang ter-enkripsi. VPN server dan VPN host saling ter-autentikasi. VPN mengkoneksikan dua jaringan seperti kantor - kantor cabang atau Remote User tunggal ke kantor[9]. Dalam melakukan transfer data dengan jaringan VPN, data dienkripsi dan dienkapsulasi sehingga keamanan data terjaga. Data yang ditransfer dilewatkan dalam sebuah tunnel sehingga seolah-olah memiliki saluran jaringan sendiri yang pada kenyataannya transfer data menggunakan jaringan internet atau jaringan publik[8].

2. Kebutuhan Penelitian

Adapun kebutuhan perangkat yang digunakan dalam Perancangan dan Implementasi Virtual Private Network (VPN) menggunakan Protokol SSTP (Secure Socket Tunneling Protocol) Mikrotik di Fakultas MIPA Universitas Tanjungpura. Pada penerapannya kebutuhan penelitian terbagi menjadi berikut:

a) Kebutuhan Perangkat Keras

Perangkat Keras (hardware) yang akan digunakan dalam perancangan topologi jaringan adalah Virtual Private Server (VPS) Mikrotik, Router Mikrotik, Switch Fiber Optik, Access Point Unifi, Unifi Security Gateway, Unifi Cloud Key, Switch Jet Stream

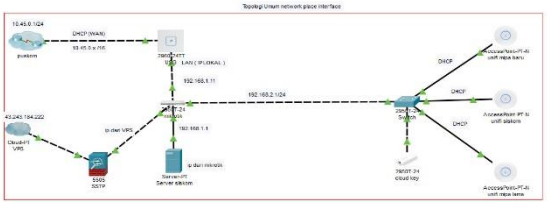
b) Kebutuhan Perangkat Lunak

Perangkat lunak (software) yang akan digunakan dalam perancangan dan implementasi sistem adalah sebagai berikut:

1. Windows 10
2. Xmind Pro 8 untuk mendesain rancangan sistem
3. Terminal (Command Prompt)
4. Trello untuk manajemen organisasi pekerjaan

B. Rancangan Penelitian

Prosedur penelitian yang dimaksud ialah proses yang dilakukan selama penelitian hingga akhir. Berupa alur rancangan pengerjaan sistem penelitian.



Gbr 1. Rancangan Penelitian

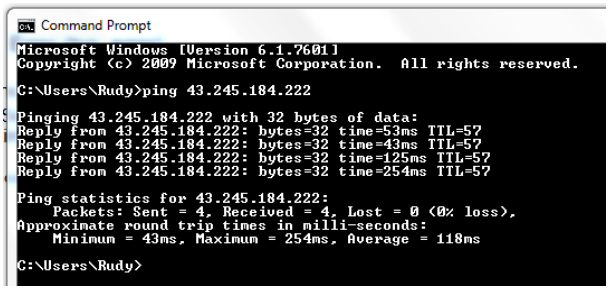
Topologi dimulai dengan jaringan Wide Area Network (WAN) yang bersumber dari Unit Pelaksana Teknis (UPT) Teknologi Informasi dan Komunikasi (TIK) Universitas menuju port WAN pada perangkat Unifi Security Gateway, kemudian perangkat tersebut menghubungkan jaringan ke router mikrotik sebagai pusat manajemen jaringan lokal pada lokasi Fakultas MIPA UNTAN. Perangkat mikrotik akan mengatur jalur pada jaringan lokal yang akan menghubungkan perangkat - perangkat yang di dalamnya seperti server aplikasi, dan masing - masing akses poin hotspot pada lingkungan FMIPA.

Sistem yang akan dibuat adalah sebuah koneksi jaringan ke virtual private server pada jaringan publik menggunakan metode SSTP sehingga implementasi VPN dapat diterapkan pada topologi ini. Perangkat mikrotik akan menghubungkan jaringan lokal dengan virtual private server yang akan bertugas menghubungkan klien dari jaringan publik agar dapat mengakses jaringan lokal FMIPA UNTAN dengan menggunakan metode VPN.

III. HASIL DAN PEMBAHASAN

A. VPS

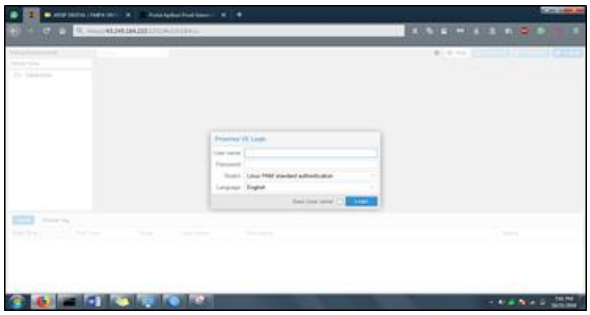
Pengujian dilakukan dengan melakukan ping ke VPS server untuk melihat apakah koneksi terbentuk. Pengujian ping dibuat ke alamat IP 43.245.184.222 yang merupakan IP server.



Gbr 2. Pengujian ping ke VPS server

B. SSTP

Perancangan Pengujian dilakukan dengan mengakses aplikasi yang berada pada server lokal agar mengindikasikan bahwa koneksi SSTP jaringan pribadi telah dibuat. Pengujian dilakukan pada IP 43.245.184.222 pada port 1232 yang merupakan alamat untuk aplikasi Proxmox.

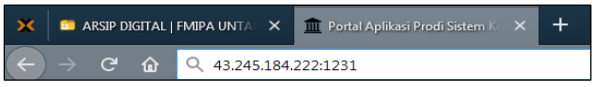


Gbr 3. Pengujian akses aplikasi yang berada pada server lokal

Client dapat mengakses aplikasi yang berada dalam server lokal pada jaringan lokal FMIPA. Pengakses tunnel "43.245.184.222" hanya yang diberikan akses oleh server. Sehingga host dapat mengakses ip publik untuk membuka aplikasi yang terdapat pada router lokal. Keamanan tersebut menjadi keunggulan dari metode SSTP (Secure Socket Tunneling Protocol) yang diimplementasikan pada penelitian.

Gbr 4. Client dapat mengakses aplikasi yang berada dalam server lokal

Aplikasi server lokal dapat diakses memalui jaringan publik memalui alamat ip VPS dengan metode SSTP yang telah diimplementasikan.

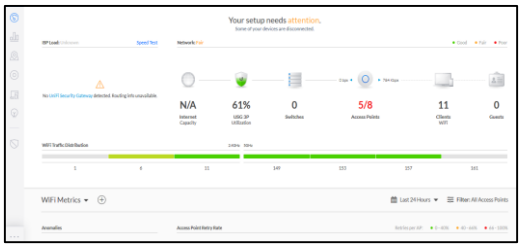


Gbr 5. Aplikasi server lokal dapat diakses memalui jaringan publik

Peranan VPS pada pengujian ini yaitu menghubungkan aplikasi lokal seperti portal siskom, arsip digital dan proxmox server dengan ip publik milik VPS. Akses tersebut berdasar pada ip VPS "43.245.184.222" dengan penambahan port ":" aplikasi.

C. Antarmuka

Sistem pemantauan memanfaatkan aplikasi yang terdapat pada perangkat unifi pada topologi yang digunakan.



Gbr 6. Monitoring perangkat unifi (akses point)

Berdasarkan Dashboard tersebut yang dipantau pada unifi dengan IP 10.45.27.121 dapat dilihat informasi terkait jaringan dapat dipantau pada sistem seperti jumlah perangkat.

Aplikasi diatas mempunyai fungsi monitoring perangkat unifi (akses point) dengan pembacaan yang mudah untuk orang awam (user friendly). Data diatas meliputi perangkat unifi yang terhubung, penggunaan data, monitoring host, anomali yang terjadi di jaringan dan monitoring kontrol unifi.

IV. PEMBAHASAN

A. Kesimpulan

Berdasarkan pembahasan pada bab sebelumnya kesimpulan dari penelitian ini adalah sebagai berikut :

1. Penggunaan protokol SSTP pada mikrotik adalah metode untuk membuat jaringan privat di Fakultas MIPA Universitas Tanjungpura melewati jalur internet. Sehingga pengguna dapat mengaksesnya tanpa harus berada pada jaringan privat tersebut
2. Protokol SSTP yang di konfigurasi pada mikrotik dihubungkan dengan Virtual Privat Server (VPS) agar dapat diakses keluar dari jalur privat. SSTP dapat berjalan dengan baik bergantung pada kondisi dari VPS tersebut.
3. Pengguna dapat mengakses aplikasi yang tersedia di server Fakultas MIPA Universitas Tanjungpura tanpa harus berada pada jaringan di lingkungan tersebut. Dengan cara menambahkan port aplikasi pada alamat ip "43.245.184.222" aplikasi dapat ter-akses di jaringan publik.
4. Keunggulan dari protokol SSTP adalah keamanan dari socket tunneling atau komunikasi jaringan. Dengan demikian manajemen jalur komunikasi yang dilakukan pengguna yang melewati jalur privat akan diamankan oleh mikrotik dan komunikasi yang terjadi diamankan berdasarkan konfigurasi mikrotik dari admin jaringan.

Sehingga tingkat keamanan data yang dilakukan pengguna saat melakukan komunikasi melalui jalur SSTP bersifat rahasia (secure).

B. Saran

Adapun saran yang dapat diberikan untuk peningkatan sistem informasi tugas akhir yang telah dibuat adalah sebagai berikut :

1. Penggunaan satu portal port Virtual Privat server (VPN) menggunakan protokol SSTP untuk men-direct semua palikasi yang ada pada server. Sehingga pengguna hanya perlu mengakses alamat ip "43.245.184.222" sebagai portal untuk dapat membuka semua aplikasi yang ada.
2. Pada penelitian selanjutnya diharapkan adanya Penggunaan Virtual Privat Server (VPS) yang telah diberikan domain, sehingga pengguna tidak harus mengakses alamat ip SSTP "43.245.184.222" namun pengguna hanya perlu mengakses nama alamat SSTP misal "portal aplikasi Fakultas MIPA.
3. Melakukan penelitian lanjutan menggunakan berbagai macam metode VPN pada mikrotik (L2TP dan PPTP) agar dapat dibandingkan hasil dan keamanan layanan pada setiap metode yang berbeda.

REFERENSI

[1] Afrianto, I. & Setiawan, E. B., 2015. Kajian Virtual Private Network (Vpn) sebagai Sistem Pengamanan Data pada Jaringan Komputer. *Majalah Ilmiah UNIKOM*, 12(1), pp. 43-51.

[2] Farly, K. A., Najoan, X. B. N. & Lumenta, A. S. M., 2017. Perancangan dan Implementasi VPN Server dengan menggunakan Protokol SSTP (*Secure* Socket *Tunneling* Protocol) Studi Kasus Kampus Universitas Sam Ratulangi. *Teknik Informatika*, 11(1), pp. 1-7.

[3] Habibi, A. & Arifin, S., 2015. Membangun Jaringan Virtual Private Network (Vpn) dengan Metode *Tunneling* Menggunakan Mikrotik untuk Komunikasi Lokal Di Stmik Ppkia Pradnya Paramita Malang. *Teknologi Informasi*, 6(2), pp. 115-119.

[4] Halim, N. A., 2015. Penggunaan Media Internet di Kalangan Remaja. *Risalah*, 26(3), pp. 132-150.

[5] Khasanah, S. N., 2016. Keamanan Jaringan dengan Packet Filtering Firewall. *Khatulistiwa Informatika*, IV(2), pp. 182-191.

[6] Larasati, K. A. M., Nugroho, E. P. & Rizal, M. F., 2015. Implementasi *Remote* Desktop Melalui VPN Berbasis IPSec pada Smartphone dengan Menggunakan Vyatta OS. *Teknologi Informasi*, 2(2), pp. 40-44.

[7] Microsoft, 2009. *Microsoft.* [Online] Available at: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc779919(v=ws.10) [Accessed 21 05 2018].

[8] NCP, 2016. *NCP.* [Online] Available at: https://www.ncp-e.com/en/solutions/vpn-for-education [Accessed 21 Mei 2018].

[9] Schroder, C., 2009. *Linux Networking Cookbook.* 1 ed. New York: O'Really Media, Inc.

[10] Situmorang, J. R., 2012. Pemanfaatan Internet Sebagai New Media. *Administrasi Bisnis*, 8(1), pp. 73-87.