 ISSN 2337-6805

IMPLEMENTASI VPN PADA JARINGAN INTRANET DENGAN KEAMANAN SSL BERBASIS MIKROTIK

VPN IMPLEMENTATION ON INTRANET NETWORKS WITH MICROTIC-BASED SSL SECURITY

Iin sundarmi [1], Andi Suprianto[2]
Program Studi Teknik Informatika, Fakultas Sains dan Teknologi Informasi
Institut Sains dan Teknologi Nasional
Jl. Moh. Kahfi II, Bhumi Srengseng Indah, Jagakarsa, Jakarta Selatan 12640
[1]sudarmiin@gmail.com, [2]andi.suprianto@ymail.com

ABSTRAKSI
Perkembangan bisnis saat sekarang ini, membuat perusahaan harus dapat melakukan pengolahan sistem informasi bisnis secara cepat dan aman serta mampu diakses dari manapun. Berbagai teknologi yang dikembangkan pada jaringan internet sudah mulai diimplemtasikan pada organisasi. Virtual Private Network (VPN) merupakan salah satu teknologi yang banyak digunakan oleh organisasi sebagai solusi atas kebutuhan kantor. VPN dengan keamanan SSL merupakan suatu tindakan yang tepat untuk mengamankan data dan informasi yang terhubung dengan internet, dimana untuk prosesnya pengiriman datanya telah di enkripsi terlebih dahulu jadi kecil kemungkinan data tersebut dibobol oleh pihak yang tidak bertanggung jawab
Kata Kunci : VPN, *Security*, SSL, *Network*, Mikrotik, *RouterOS*

ABSTRACT
Current business developments today, making the company should be able to process business information systems quickly and safely, and can be accessed from anywhere. Various technologies developed on the Internet network has begun are implemented in the organization. Virtual Private Network (VPN) is a technology that is widely used by organizations as a solution to the need for office needs. Keamaman SSL VPN with an appropriate action to secure the data and information connected to the Internet, in which to process data transmission has to be encrypted beforehand so small possibility that data is not compromised by the party responsible.
Keywords : VPN, *Security*, SSL, *Network*, Mikrotik, *RouterOS*

1. PENDAHULUAN

Perkembangan bisnis saat sekarang ini, membuat perusahaan harus dapat melakukan pengolahan sistem informasi bisnis secara cepat dan aman serta mampu diakses dari manapun. Berbagai teknologi yang dikembangkan pada jaringan internet sudah mulai diimplemtasikan pada organisasi. Virtual Private Network (VPN) merupakan salah satu teknologi yang banyak digunakan oleh organisasi sebagai solusi atas kebutuhan untuk kebutuhan kantor. Didalam suatu organisasi virtual private network berfungsi untuk menghubungkan kantor pusat dengan kantor cabang melalui jaringan public dengan membuat suatu jalur pribadi yang diumpamakan sebagai terowongan (tunnel) dengan menggunakan fasilitas jalur yang sudah tersedia (internet) yang memungkinkan dua cabang kantor untuk melakukan komunikasi secara aman.

Dari beberapa paper yang telah ada, salah satu paper yang ditulis oleh Geo San Iswara, Periyadi dan Setia Juli Irzal Ismail, yang berjudul Implementasi Protokol SSTP dalam membangun Server VPN Menggunakan Konfigurasi Routing Dan Remote Access Untuk Access Client Pada Windows Server 2008, dimana mereka meneliti sebuah permasalahan yaitu bagaimana melakukan konfigurasi server yang berfungsi sebagai Domain Controller, DNS server, dan file server pada private network. Serta melakukan pengujian VPN server yang telah dikonfigurasi dengan protocol SSTP dalam melakukan sharing file. [11]

Berdasarkan paper lain yang ditulis oleh Reza Aditya M.Ukhwarizman, Jurusan Sistem Informasi, STMIK PalComTech Palembang, yang berjudul Implementasi Rancangan Keamanan Jaringan Wireless dengan metode Secure Socket Layer (SSL) pada Bappeda Kabupaten Banyuasin, dimana mereka menggunakan metode SSL sebagai keamanan dari wireless internet, hal ini dikarenakan Bappeda belum memiliki server gateway dan sistem keamanan fasilitas internet.[12]

Berdasarkan dari beberapa referensi diatas tersebut, maka untuk mengatasi masalah yang terjadi terkait dengan keamanan, akan diangkat dalam skripsi kali ini yaitu Implementasi VPN

pada jaringan internet dengan keamanan SSL berbasis mikrotik. Yang menggunakan metode SSTP (Secure Socket Tunneling Protocol).

Berdasarkan uraian latar belakang diatas, maka terdapat rumusan masalah sebagai berikut :

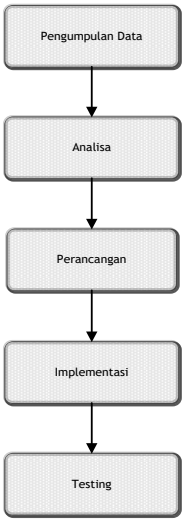
1. Membuat jaringan VPN (Virtual Private Network) dengan menggunakan metode SSTP berbasis Mikrotik.
2. Menerapkan SSL (Secure Socket Layer) sebagai keamanan pada jaringan tersebut.
3. Komunikasi antar server pusat dan kantor cabang tidak aman.

2. METODOLOGI PENELITIAN

Untuk mendapatkan keterangan dan data-data yang diperlukan guna memperoleh kebenaran ilmiah, maka dilakukan beberapa tahapan dapat dilihat pada gambar 1 :

Tahap Pengumpulan Literatur

Tahap ini dilakukan dengan cara studi lapangan, literatur dan wawancara untuk mendapatkan data-data yang dibutuhkan secara terperinci dari kasus yang ditangani oleh petugas lapangan.

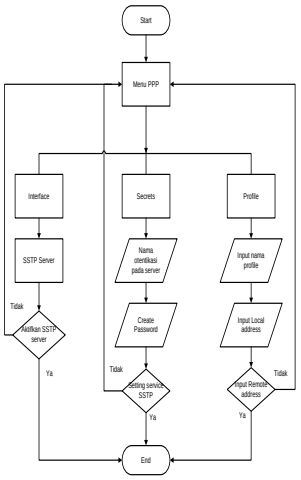


Gambar 1 Diagram System

Analisa Data

Flowchart Design PPP

Untuk memudahkan dalam melakukan Implementasi VPN terhadap SSL, akan digunakan PPP (Point to Point Protocol) sebuah protokol enkapsulasi paket jaringan yang banyak digunakan pada wide area network, dan protokol ini bekerja pada lapisan data link.



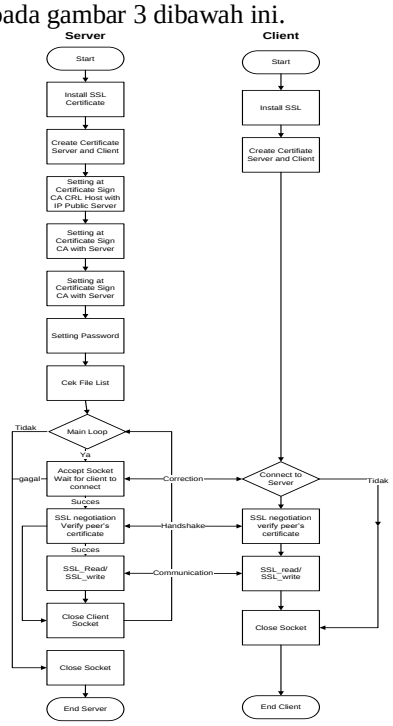
Gambar 2 Flowchart Design PPP

Ket ::

1. Pada menu PPP terdapat beberapa sub menu sebelum membangun VPN yang menggunakan metode SSTP.
2. Pada menu profile diperlukan input data yang berupa menetukan nama untuk identitas dari SSTP.
3. Pada menu Secrets diperlukan input data yang berupa nama untuk otentikasi pada Server dan Client setelah itu masukkan IP Address Local dari server dan Remote address dari client untuk mempermudah terhubungnya client jika terjadi kesalahan.
4. Pada menu Interface setting di SSTP server dan klik enabled untuk mengaktifkan SSTP tersebut.

Flowchart Certifikat SSL

Untuk Flowchart Certificate SSL bisa dilihat pada gambar 3 dibawah ini.



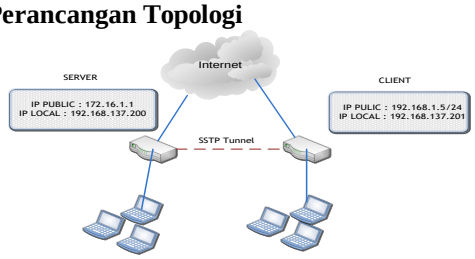
Gambar 3 Flowchart Sistem Certificate SSL

Penjelasan Flowchart gambar 3 terdapat beberapa langkah untuk membuat sertifikat pada SSL berikut untuk langkah-langkahnya :

1. Server
   a. Hal pertama yang dilakukan oleh server adalah Install SSL dan buat sertifikat untuk server dan client.
   b. Berikutnya adalah atur sertifikat pada sign CA CRL Host dengan mengisi IP Public dari server. Setelah selesai untuk client atur pada sing dan isikan dengan nama server.
   c. Selanjutnya yaitu isikan password pada button Export.
   d. Dan untuk mengetahui Sertifikat SSL yang telah dibuat bisa dilihat pada menu File List.
   e. Selanjutnya sertifikat akan melakukan putaran jika sertifikat diterima maka akan terhubung ke client, jika tidak sertifikat akan tertutup dan keluar dari server.
   f. Setelah sertifikat SSL diterima maka akan diverifikasi, dan SSL bisa dibaca atau ditulis / edit.
2. Client
   a. Setelah client mendapatkan SSL dari server maka yang harus dilakukan terutama menginstall SSL.
   b. Setelah buat sertifikat server dan client.
   c. Selanjutnya SSL client akan terhubung ke server, jika tidak SSL client akan tertutup dan keluar dari client.
   d. Proses selanjutnya yaitu setelah SSL diterima maka akan diverifikasi, dan SSL bisa dibaca atau ditulis.

3. HASIL DAN PEMBAHASAN

Perancangan Topologi

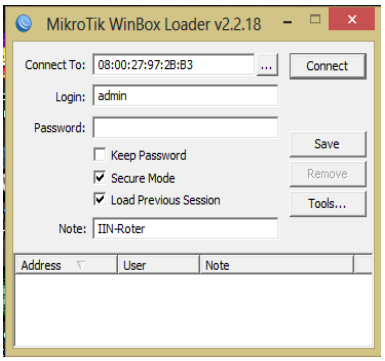


Implementasi Sistem

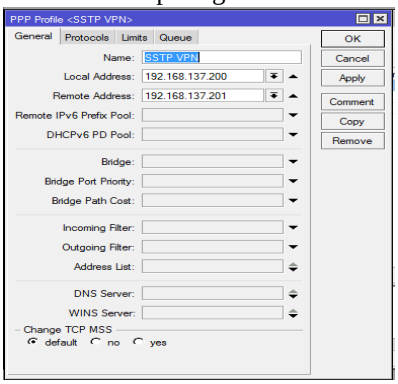
SSTP Server (Secure Socket Tunneling Protocol) pada router pertama

Pada implementasi VPN ini yaitu dengan cara menyetting SSTP server. Langkah-langkahnya sebagai berikut :

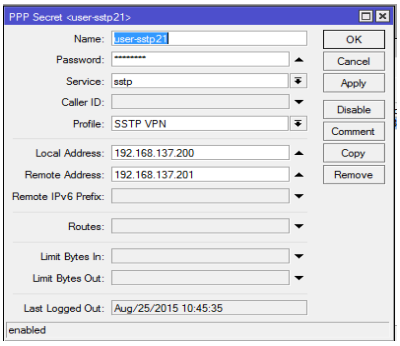
a. Login terlebih dahulu menggunakan winbox



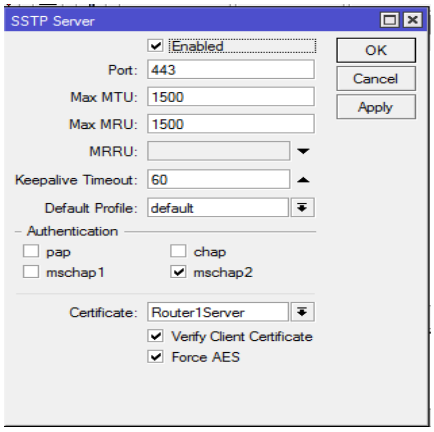
b. Setelah berhasil maka masuk ke menu PPP (Point to Point Protocol), setelah itu pilih submenu profile dan klik tanda plus (+), maka akan keluar seperti gambar dibawah ini.



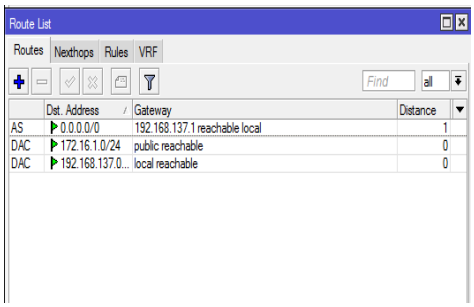
c. Setelah menyeting PPP Profile, lalu setting PPP Secrets yang digunakan untuk keperluan otentikasi pada client yang akan terhubung, seperti gambar dibawah ini



d. Pada gambar dibawah ini yaitu merupakan setting PPP Server, untuk mengaktifkan SSTP Server. Pindah kembali pada tab ”Interface” lalu klik pada tombol ”SSTP Server”, bericentang pada ”Enabled” untuk mengaktifkannya. Lalu pada ”Default Profile” pilih default, dan pada Authentication pilih machap2, setelah itu pilih pada ”Certificate” Router1Server yang sudah disetting pada system certificate, lalu centang pada ”Verify Client Certificate” dan ”Force AES”.



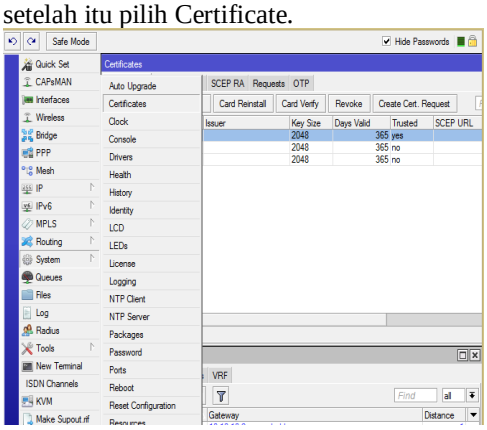
e. Dibawah ini merupakan list dari alamat IP address yang menghubungkan router 1 server dan router 2 client.



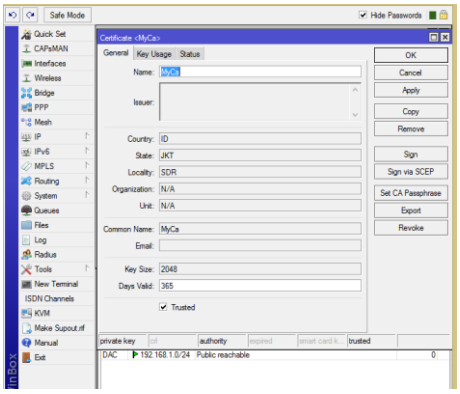
Certificate SSL (Secure Socket Layer)

a. Setting SSL (Secure Socket Layer)

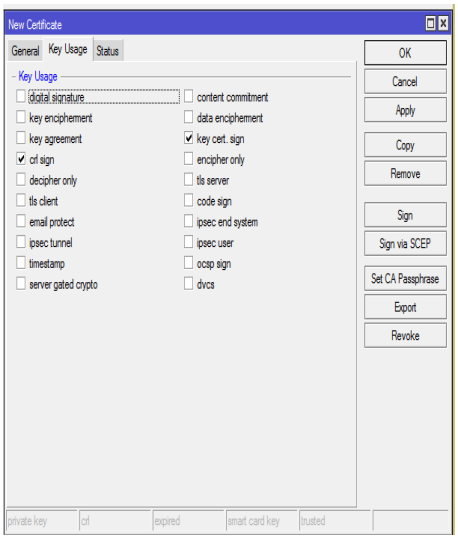
Pada gambar dibawah merupakan settingan pada SSL untuk membuat sertifikat baru. Dengan masuk ke winbox lalu pilih System setelah itu pilih Certificate.



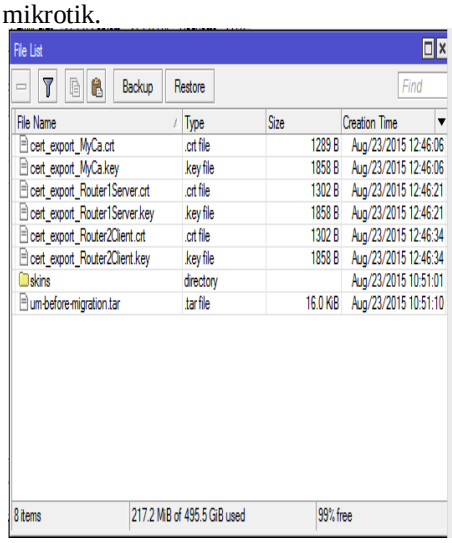
b. Setting New Certificate di winbox server, isi dikolom Name : MyCa (My Certificate), Country : ID (Indonesia), State : JKT (Jakarta), Localty : SDR (Sudirman). Untuk Key Size pilih 2048, karena untuk size 2048 untuk certificate SSL server dan client. Sedangkan size 1024 untuk hostpot.



c. Setelah settingan pertama di submenu General, lalu klik pada submenu Key Usage : klik pada pilihan crl sign dan key cert. Sign, key Usage ini berfungsi pada saat import dari router Server untuk membuat certificate di router client.

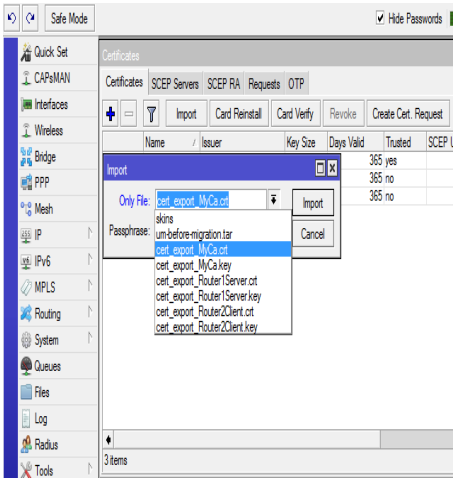


d. Setelah semua certificate untuk server dan client dibuat maka filenya akan seperti gambar dibawah ini. Menu pilihan ada di File pada mikrotik.

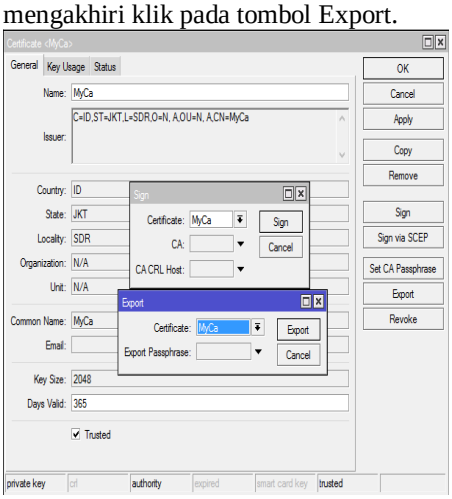


SSTP Client Certificate

a. Dibawah ini settingan dari certificate yang di export dari server Buka pada winbox atau router client.



b. Setelah di import maka pada kolom Issue tertera muncul tulisan C=ID,ST=JKT,L=SDR,O=N.A,CN=MyCa, dan untuk mengaktifkan nya pilih sign lalu klik pada CA CRL Host dengan IP Publik : 192.168.137.200 Kemudian pilih Export lalu isi Export Phassphrease : P@ssw0rd lalu untuk mengakhiri klik pada tombol Export.



4. SIMPULAN

1. Dengan menggunakan VPN dapat meremote jaringan kantor selama terhubung ke internet.
2. Komunikasi data antar server dan clinet menggunakan protokol SSL, sehingga lebih aman dalam proses transportasi data.

5. DAFTAR PUSTAKA

[1] Fernando, Hary. 2010, Studi dan Implementasi Sistem Keamanan Berbasis Web dengan Protokol SSL diserver Students Informatika ITB Departement Teknik Elektro, Program Studi Teknik Elektronika, Institut Teknologi Bandung. Via http://budi.insan.co.id/

[2] [2] Sofana, Iwan, Pengantar Jaringan Komputer dan CISCO CCNA. Bandung, Jawa Barat : Informatika, 2010.

[3] [3] Andi, Computer Networking : Andi, 2012.

[4] [4] Sofana, Iwan, CISCO CCNP dan Jaringan Komputer. Bandung, Jawa Barat : Informatika, 2012.

[5] [5] Sujalwo, Manajemen Jaringan Komputer Dengan Menggunakan Mikrotik Router, fki.ums.ac.id

[6] [6] W. Purbo, Onno. Buku Pintar Internet TCP/IP. PT. Elex Media Komputindo Kelompok Gramedia, Anggota IKAPI. Jakarta, 1998.

[7] http://www.academia.edu/11566305/Mikrotik_Training_Basic

[8] http://www.aryamaulana.com/2014/07/certificate-ssl-https-untuk-login.html

[9] https://nathangustiryan.wordpress.com/2010/04/16/step-by-step-membangun-vpn-server-dgn-mikrotik/

[10] http://www.academia.edu/9268513/SSL

[11] http://id.scribd.com/doc/160403573/Jurnal-Pa-Implementasi-Protokol-Sstp-Dalam-Membangun-Server-VPN-Menggunakan-Konfigurasi-Routing-Dan-Remote-Access-Untuk-Access-Client-Pada-Windows-Ser#scribd

[12] http://news.palcomtech.com/wp-content/uploads/2014/07/Jurnal_RezaUkhwarizman_ImplementasiRancanganKeamananJaringanWireless.pdf