RANCANG BANGUN FILE TRANSFER PROTOCOL (FTP) DENGAN PENGAMANAN OPEN SSL PADA JARINGAN VPN MIKROTIK DI SMKS DWIWARNA

Devi Ruwaida[1], Dian Kurnia[2]
Universitas Pembangunan Panca Budi
Jl. Jend. Gatot Subroto Km. 4,5 Sei Sikambing 20122 Medan
deviruwaida041095@gmail.com[1], diankurnia68@dosen.pancabudi.ac.id[2]

Abstrak — File Transfer Protocol (FTP) server merupakan jenis sistem yang menghubungkan hak pengakses (client) dan penyedia (server) dalam melakukan pertukaran data yang melewati port 21, yang semula ftp server berjalan pada protocol yang tidak terlindungi di dalam port 21, kemudian dengan OpenSSL ini di amankan agar data dapat sampai ke tujuan. Pada penelitian ini akan dibangun Rancang Bangun File Transfer Protocol (Ftp) Dengan Pengamanan Open Ssl Pada Jaringan Vpn Mikrotik Di SMKS Dwiwarna yang akan di konfigurasi pada debian 9.1 dengan di tambahnya pengaman sertifikat ssl , dengan harapan melindungi proses dalam pengiriman data dapat dengan aman dan ditambahkannya sistem VPN PPTP pada mikrotik akan lebih memberikan keamanan yang lebih baik lagi, dimana pemanfaatan Point-to-Point Tunneling Protocol (PPTP) suatu protokol jaringan yang bisa memungkinkan client dalam pengiriman data secara aman melalui remote client kepada server sekolah dibangunnya suatu virtual private network (VPN).

Kata kunci — FTP, Openssl, VPN, Mikrotik

I. PENDAHULUAN

Ilmu File Transfer Protocol (FTP) adalah protokol jaringan standar yang digunakan untuk mentransfer file komputer dari satu host ke host lain melalui jaringan berbasis TCP, seperti Internet. FTP dibangun di atas arsitektur server klien dan menggunakan kontrol terpisah dan koneksi data antara klien dan server. Pengguna APP dapat mengotentikasi dirinya dengan menggunakan protokol masuk yang jelas, biasanya dalam bentuk nama pengguna dan kata sandi, namun dapat terhubung secara anonim jika server dikonfigurasi untuk mengizinkannya Untuk transmisi aman yang melindungi username dan password, dan mengenkripsi isinya, FTP sering diamankan dengan SSL / TLS (FTPS) (Ranie, Leena, Preeti Narula dan Neeti Panchal, 2014).

FTP (File Tranfer Protocol) umumnya berfungsi sebagai media tukar menukar file atau data dalam suatu network yang menggunakan TCP koneksi. FTP yang digunakan menggunakan berbasis Open Source guna menunjang tingkat stabilitas tinggi dan tidak mudah terinfeksi virus dan malware. FTP merupakan metode protokol pilihan yang paling tepat dalam penyimpanan file/data secara cepat dalam proses upload dan download dari komputer server ke klien tanpa menggunakan flashdisk untuk mengambil data dari komputer server (Arman, Molavi, 2017).

SSL (Secure Socket Layer) diperlukan untuk menjaga proses autentikasi dan proses transfer data yang terlebih dahulu dienkripsi. SSL memiliki beberapa versi dan yang terbaru adalah SSLv3 namun pengembangan dari SSLv3 dinamakan TLS (Transfer Layer Security). TLS yang merupakan pengembangan SSL tidak luput juga dari serangan pihak ketiga, serangan tersebut dinamakan Padding Oracle On Downgraded Legacy Encryption (POODLE) yang memanfaatkan layanan yang dimiliki TLS yaitu Downgrade dance yang artinya ada penurunan tingkat keamanan dalam hal ini TLS ke protocol yang lebih rendah. Saat ini solusi untuk terhindar dari serangan POODLE adalah dengan menonaktifkan SSL dan hanya menggunakan TLS sebagai pengamanannya. Namun dengan menonaktifkan SSL pasti memiliki dampak tersendiri ketika client yang terhubung hanya mendukung SSL (Tehupeiory, Nardi, dan Dian W Chandra, 2016).

Dalam Implementasinya VPN (Virtual Privet network) dibagi menjadi dua jenis yaitu remote access dan site-to-site VPN, VPN Remote access merupakan suatu cara meremote server atau host privet melalui jaringan public dengan aman. Sedangkan VPN site-to-site digunakan untuk menghubungkan dua tempat yang berjauhan, misal antara sekolah satu dengan sekolah lainnya (Fatoni, dan Dedi Irawan, 2015).

Dalam penelitian ini juga didasari oleh pengembang yang sudah melakukan penelitian dalam membangun FTP dengan SSL yang di lakukan oleh Molavi Arman berjudul Rancang Bangun Pengamanan FTP Server dengan Menggunakan Secure Sockets Layer, dengan adanya penelitian tersebut, peneliti akan menyederhanakan dan penambahan sedikit pengembangan yang sebelumnya menggunakan Ftp server dengan konfigurasi ssl, apache, php dan maria db, maka peneliti akan menambahkan adanya router mikrotik dengan konfigurasi Virtual Privet Network (VPN) dan tanpa adanya konfigurasi dalam php, apache atau mariadb. Dimana dalam pengembangan ini menggunakan

sistem mekanisme yang diberikan SSL langsung ke dalam pengamanan koneksi antara FTP Client dan FTP Server. Yang semula ProFTPD berjalan pada protocol yang tidak terlindungi di dalam port 21, kemudian dengan OpenSSL ini di amankan agar data dapat sampai ke tujuan secara aman dan pemanfaatan Point-to-Point Tunneling Protocol (PPTP) suatu protokol jaringan yang bisa memungkinkan client dalam pengiriman data secara aman melalui remote client kepada server sekolah dibangunnya suatu virtual private network (VPN).

II. METODOLOGI

Dalam Rancang Bangun File Transfer Protocol (Ftp) Dengan Pengamanan Open Ssl Pada Jaringan Vpn Mikrotik Di SMKS Dwiwarna terdapat bebrapa kebutuhan yang harus di penuhi yaitu sebagai berikut:

A. Analisa dalam Kebutuhan Software

Kebutuhan akan software dalam membangun penelitian ini di perlukan untuk kelancaran membangun penelitian yaitu sebagai berikut.

- Dengan menggunakan jenis operating system Linux Debian versi 9.1
- Pengkonfigurasi debian berupa bind9, Proftpd dan OpenSSL
- Konfigurasi VPN pada mikrotik router.
- Operasi sistem pengujian untuk client menggunakan Windows XP
- Aplikasi tambahan untuk pengujian berupa WinSCP dalam mengakses Ftp server yg terindentifikasi ssl dan winbox untuk konfigurasi router mikrotik

B. Analisa dalam Kebutuhan Hardware

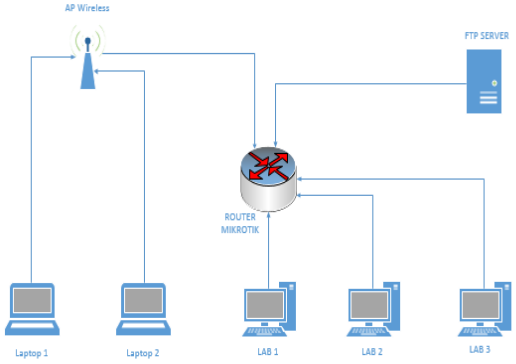
Kebutuhan Hardware dalam melancarkan penelitian ini yaitu sebagai berikut :

- PC berspesifikasi untuk server dengan Processor Intel Core i5 3.0 Ghz, Memori 4GB, DVD RW, keyboard dan monitor
- PC untuk Client dengan spesifikasi Intel Dual Core 2.5 Ghz, Memori 2GB, DVD RW, keyboard dan monitor
- Terdapat juga kebutuhan dalam perangkat jaringan menggunakan kabel UTP, Konektor RJ-45, switch, NIC, dan Router Mikrotik.

IV. IMPLEMENTASI DAN PENGUJIAN

A. Implementasi Dalam Penelitian

Penelitian ini mengimplementasikan pertukaran data melalui Ftp server yang menggunakan sistem mekanisme yang diberikan SSL dalam mengamankan koneksi antara FTP Client dan FTP Server yang semula ProFTPD berjalan pada protocol yang UnSecure di port 21 dengan adanya SSL ini dapat mengamankan data yang berjalan sampai ke tujuan dengan aman, Kemudian Point-to-Point Tunneling Protocol (PPTP) suatu protokol jaringan yang akan memungkinkan melakukan pengiriman data secara aman melalui remote client kepada server sekolah dengan membuat suatu virtual private network (VPN) mengarah pada jaringan data berbasis TCP/IP. Topologi dalam penelitian ini yaitu sebagai berikut :



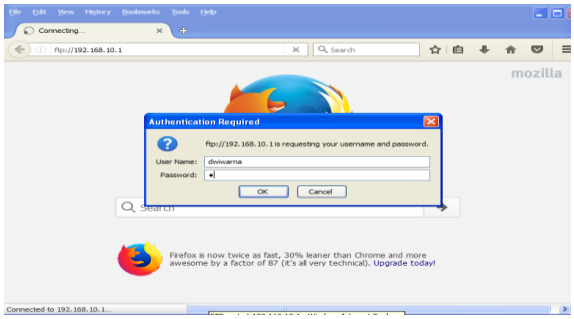
Gbr. 1 Topologi dalam membangun Ftp server

1. Pengkonfigurasian Proftpd Sebelum dapatnya sebuah hasil berhasil atau tidaknya pengujian proftpd, proftpd harus melalui tahap installasi dan pengkonfigurasian dengan perintah sebagai berikut :

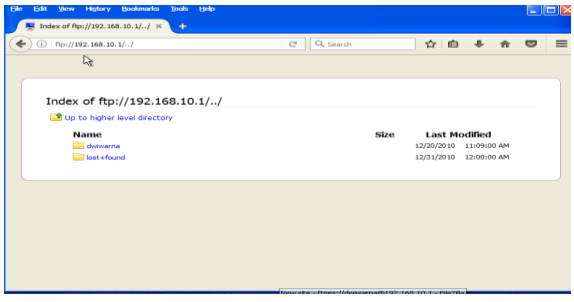
- tahap installasi paket

```
# apt-get install proftpd
```

- uji coba memanggil ftp://192.168.10.1 pada client bila paket sudah terinstall dengan cara menggunakan browser mozila hingga menampilkan tampilan login untuk masuk kedalam ftp server yang ada pada client seperti pada gambar di bawah :



Gbr. 2 Tampilan login ketika menguji ftp://192.168.10.1



Gbr. 3 Tampilan ketika berhasil login saat menguji ftp server

2. Pengkonfigurasian ssl Dalam tahap ini bagaimanan ftp server mendapatkan sertifikat ssl dengan melalui tahap installai openssl dan sedikit pengkonfigurasian perintah sebagai berikut :

- tahap membangun sertifikat ssl dengan menginstall paketnya terlebih dahulu berupa perintah :

```
# apt-get install openssl
```

- sebelum masuk kedalam membangun sertifikat ssl akan lebih baik membuat folder untuk menghindari error jika file yang nantinya di letakkan kedalam folder dengan nama ssl tidak kebingungan ketika di letakkan kedalam folder ssl tersebut dengan perintah :

```
#mkdir /etc/proftpd/ssl
```

- dan bila folder sudah di buat saatnya membuat sertifikat ssl dan setelah memasukkan perintah ini akan di minta untuk memasukkan data informasi untuk sertifikat, dengan printah :

```
# openssl req –x509 –nodes –days 365 –newkey rsa:2048 –keyout /etc/proftpd/ssl /dwiwarnakey –out /etc/proftpd/ssl /dwiwarna.cert
```

- tahap mengaktifkan Transport Layer Security (TLS) dengan perintah :

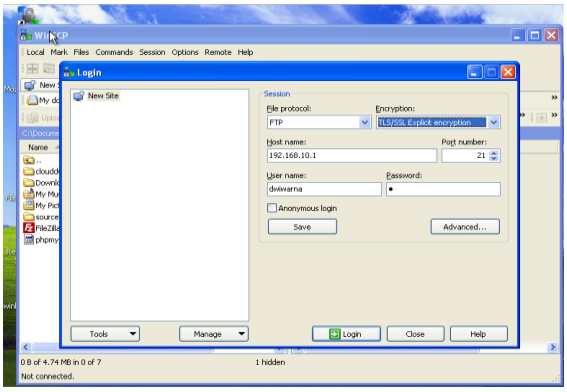
```
# nano /etc/proftpd/proftpd.conf
```

- kemudian cari script Include /etc/profptd/tls.conf lalu hilangkan tanda # dan dengan menambahkan beberapa script di bawah script Include /etc/proftpd/tls.conf dengan penambahan sebagai berikut :

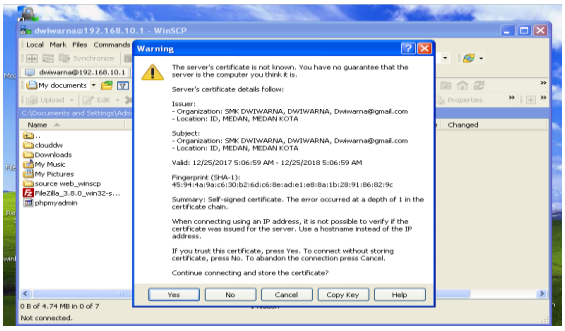
```
TLSEngine on
TLSLog /var/log/tlg.log
TLSProtocol SSLv3
TLSOptions NoCertRequest
TLSRSACertifitcateFile/etc/proftp/ssl/dwiwarna.cert
TLSRSACertificateKeyFile/etc/proftp/ssl/dwiwarna.key
TLSVerifyClient off
```

- kemudian simpan proftpd.conf dengan menekan Ctrl+x lalu Y dan enter setalah itu restart proftpd dengan perintah # systemctl restart proftpd

- uji coba sertifikat ssl pada ftp server dapat menggunakan software WinSCP pada client dengan membuka aplikasi WinSCP kemudian masukkan hostname, username dan password lalu login dan bila berhasil akan menampilkan infomasi bahwa ssl dapat di gunakan Seperti gambar berikut :



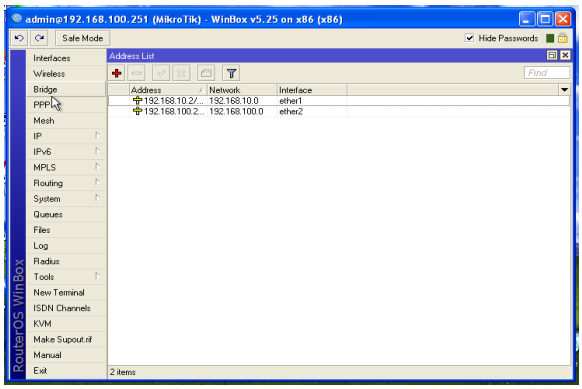
Gbr. 4 Tampilan awal WinSCP untuk login Ftp server



Gbr. 5 Tampilan pemberitahuan sertifikat ketika berhasil menguji ftp server malalui WinSCP

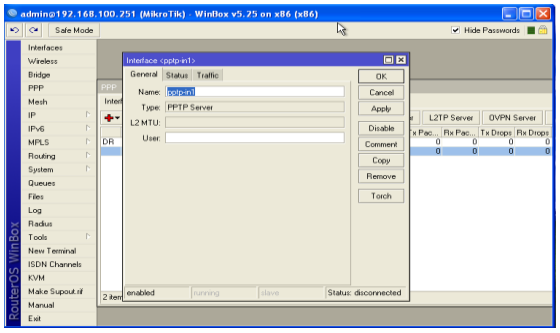
3. Membangun VPN PPTP pada mikrotik client harus terhubung dahulu dengan mikrotik untuk menjalankan software winbox yang berfungsi sebagai pengontrol atau pengkonfigurasi mikrotik router, tahap awal di lakukan dengan membuka software winbox dan login mikrotik seperti gambar berikut :

Gbr. 6 Tampilan saat software di buka menampilan untuk login



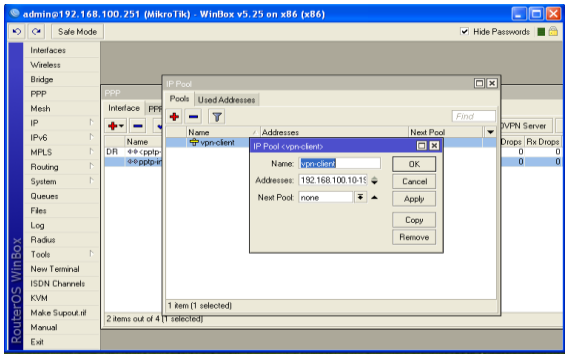
Gbr. 7 Tampilan pemberitahuan sertifikat ketika berhasil menguji ftp server malalui WinSCP

- tahap kedua melakukan konfigurasi menambahkan interface baru untuk PPTP Server dengan masuk pada menu PPP kemudian lalu kita akan masuk pada tampilan PPP terdapat beberapa menu lagi pilih menu interface pilih tombol + merah lalu pilih PPTP Server isi kan nama kemudian OK seperti pada gambar berikut :



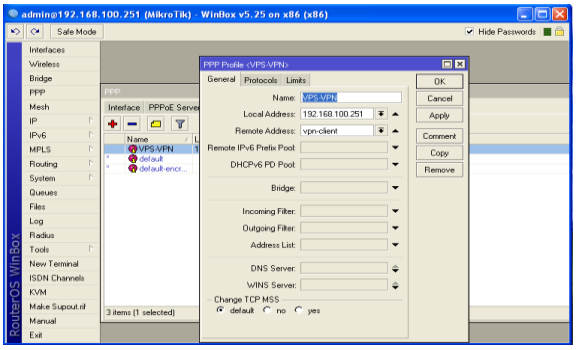
Gbr. 8 Tampilan konfigurasi penambhan interface VPN PPTP di winbox

- membuat IP pool untuk sebagai penampung jumlah IP address dengan mengklik menu IP kemudian pilih menu Pool kemudia pilih tombol + merah lalu masukkan name dan ip address dengan jumlah tamping yang di inginkan misalkan 192.168.100.20-192.168.100.30 seperti pada gambar berikut :



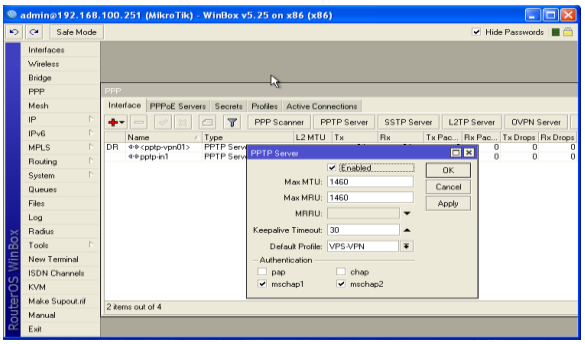
Gbr. 9 Tampilan konfigurasi IP Pool

- kemudian membuat sebuah profile dengan cara masih di terdapat pada menu PPP lalu kita akan masuk pada tampilan PPP terdapat beberapa menu lagi pilih menu profile pilih tombol + merah lalu masukkan name dan local address begitu jug dengan remote addresnya seperti pada gambar berikut :



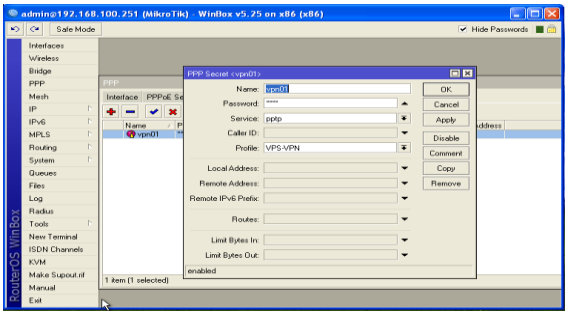
Gbr. 10 Tampilan konfigurasi Profile pada menu PPP di winbox

- tahap selanjutnya yaitu mengaktifkan PPTP server yang terdapat pada menu PPP, pada tampilan PPP terdapat beberapa menu pilihan, pilih menu interface kemudian di sisi kanan terdapat tombol PPTP Server klik tombol tersebut kemudian ketika masuk dalam menu tersebut beri ceklis lah di bagian Enabled masukkan default profile dengan profile yang sudah di buat serperti pada gambar berikut :



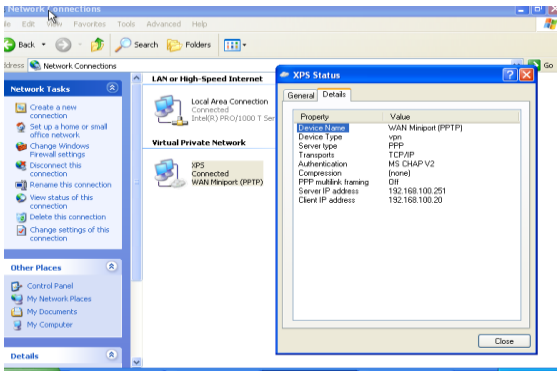
Gbr. 11 Tampilan mengaktifkan PPTP

- Langkah akhir membuat user VPN yang terdapat pada menu PPP didalam menu pilih lah menu Secrets kemudia profile pilih tombol + merah lalu masukkan name, password, Service dan profile seperti pada gambar berikut :



Gbr. 12 Tampilan konfigurasi membuat user VPN di winbox

- melakukan pengujian pada client dengan menggunakan operasi sistem windows XP seperti gambar berikut :



Gbr. 12 Tampilan hasil pengujian VPN pada client

V. PENUTUP

A. *Kesimpulan*

Dalam penenlitian rancang bangun file transfer protocol (ftp) dengan pengamanan open ssl pada jaringan vpn mikrotik di SMKS Dwiwarna ini di dapati kesimpulan kesimpulan yang dapat di ambil adalah sebagai berikut:

1. Dengan mekanisme ssl yang semula Prftpd berjalan pada protocol yang tidak terlindungi didalam port 21 sehingga bekerja dalam mengamankan koneksi antara Ftp Client dan Ftp Server.
2. Data yang akan di kirim dapat di jaga melalui proses transfer data yang lebih dahulu di enkripsi oleh ssl.
3. Membanding kan antara Ftp server yang menggunakan seritifikat ssl sebagai pengaman lebih aman dari pada Ftp server yang tidak memasang sertifikat sll
4. Dengan menggunakan VPN pada mikrotik dalam melakukan remote dan mengirim data lebih aman sebab berbasis Tcp/Ip

B. *Saran*

Dalam membangun penilitan ini harus adanya saran agar dapat di kembangkannya penelitian ini lebih baik lagi untuk saran dalam pengembangan ini kedepannya adalah sebagai berikut:

1. Dengan menambahkan Dns server dalam pengalamatan akan lebih baik tanpa harus rumit dalam mengingat semua alamat ip address
2. penambahan pada pengaksesan ip publik untuk internet sehingga pengaksesan lebih luas lagi

REFERENSI

[1] Ranie, Leena, Preeti Narula dan Neeti Panchal. 2014. Ftp- The File Transfer Protocol. International Journal of Research (UR), ISSN : 2348-6848

[2] Arman, Molvai. 2017.Rancang Bangun Pengamanan FTP Server dengan Menggunakan Secure Sockets Layer. Jurnal Integrasi, e-ISSN:2548-9828

[3] Tehupeiory, Nardi, dan Dian W Chandra. 2015. Analisis Perbandingan Mekanisme Secure Socket Layer (SSL) dan Transfer Layer Security (TLS) Pada Koneksi File Transfer Protocol (FTP) Server Ubuntu.

[4] Fatoni, dan Dedi Irawan, 2015. Implementasi jaringan vpn (virtual private network) site to site mikrotik router. Jurnal informatika, ISSN:2301-5632