PROTOTYPE LAYANAN *REMOTE ACCESS VIRTUAL PRIVATE NETWORK* (VPN) DENGAN METODE *SECURE SOCKET LAYER* (SSL)

HERWAN HERWANSYAH

JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU DAN KOMPUTER
UNIVERSITAS KOMPUTER INDONESIA
Jl. Dipati Ukur No. 112-114 Bandung
Email: h2s_cyber@yahoo.com

ABSTRAK

VPN (Virtual Private Network) adalah sebuah teknologi komunikasi yang memungkinkan pengguna untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal. Jaringan private ini seolah-olah sedang mengakses jaringan lokalnya tapi menggunakan jaringan publik. VPN memungkinkan untuk terbentuk suatu jaringan data private yang dapat diakses melalui jaringan publik seperti internet, dan hanya dapat diakses oleh pihak-pihak yang mempunyai otoritas. Remote Access VPN merupakan salah satu implementasi dari VPN yang berfungsi untuk melakukan akses jarak jauh (remote) terhadap suatu layanan private yang diakses melalui jaringan publik. Secure Socket Layer (SSL) VPN merupakan mekanisme protokol komunikasi data yang dapat digunakan pada remote access VPN dengan menggunakan konsep asymmetric encryption untuk mekanisme berbasis kunci dan sertifikat. Remote Access VPN melakukan proses komunikasi data yang menggunakan protokol SSL, akan melakukan enkripsi terhadap kunci dan enkripsi terhadap proses transfer data dari server menuju *client* maupun sebaliknya dengan menggunakan algoritma enkripsi, sehingga *host* yang terhubung dengan suatu jaringan VPN dapat melakukan koneksi yang aman.

Kata Kunci: VPN, *Remote Access*, SSL, Enkripsi.

---

1. PENDAHULUAN

1.1 Latar Belakang Masalah

Suatu jaringan idealnya dapat menghubungkan antartitik secara *any to any*. Di masa lalu, perusahaan yang hendak menghubungkan cabang-cabang kantornya dalam suatu jaringan akan mengunakan saluran sewa secara titik ke titik (*point to point*) yang tentu saja biayanya sangat besar.

Dalam sebuah jaringan komputer, keamanan di dalam pengiriman serta penerimaan data sangat penting untuk menjamin bahwa data yang dikirim tidak jatuh ke pihak ketiga, terutama jika data tersebut bersifat rahasia. Untuk itu perlu dilakukan implementasi metode-metode pengamanan data pada jaringan. Banyak metode yang dapat diimplementasikan, seperti penggunaan tanda tangan digital, enkripsi ataupun pemasangan firewall.

Seiring dengan maraknya penggunaan Internet, banyak perusahaan yang kemudian beralih menggunakan internet sebagai bagian dari jaringan mereka untuk menghemat biaya. Akan tetapi permasalahan keamanan masih menjadi faktor utama dalam reabilitas dalam suatu jaringan. *Virtual Private Network* (VPN) adalah salah satu cara untuk membuat sambungan *any to any* di atas jaringan publik seperti internet, tanpa klien yang satu dengan klien yang lain saling mengetahui yang merupakan suatu cara untuk membuat sebuah jaringan bersifat

"*private*" dan aman dengan menggunakan jaringan public.

Dewasa ini ada beberapa teknik yang dikenal untuk mengembangkan VPN di atas jaringan Internet yaitu *Point to Point Tunnelling Protocol* (PPTP), *Layer* 2 *Tunneling Protocol* (L2TP), *Secure Socket Layer/ Transport Layer Security* (SSL/TLS) dan *Internet Protocol Security* (IPSec). Kelompok kerja IPSec (di bawah area keamanan) berkonsentrasi pada proteksi lapisan jaringan dengan merancang mekanisme keamanan pengacakan (kriptografi). Mekanisme secara fleksibel dapat mendukung kombinasi dari autentifikasi, integritas, kontrol akses, dan kerahasiaan.

Pada VPN yang berbasis SSL, SSL VPN menggunakan algoritma *cryptographic* untuk mengenkripsi data sehingga hanya komputer-komputer yang berkomunikasi yang dapat membaca dan mengerti pesan yang dikirim. SSL mendukung berbagai algoritma enkripsi sehingga modifikasi terhadap aplikasi tidak dibutuhkan dan pengguna tidak perlu membuat sistem keamanan untuk setiap aplikasi atau setiap komputer. SSL merupakan salah satu solusi yang baik bagi *remote access* VPN atau pengguna yang bergerak (*mobile*). Sehingga dengan dibangunnya suatu layanan VPN yang berbasis SSL merupakan alternatif yang efektif untuk solusi keamanan untuk suatu jaringan.

1.2 Identifikasi Masalah

1. Bagaimana mengkonfigurasi *Remote Access* VPN dengan metode SSL.
2. Bagaimana membangun suatu layanan *Remote Access* VPN dengan metode SSL.
3. Bagaimana perbandingan layanan yang menggunakan *Remote Access* VPN yang menggunakan metode SSL dengan layanan yang tidak menggunakan VPN.

1.3 Maksud dan Tujuan

Maksud dari penulisan skripsi ini adalah untuk membangun suatu prototype layanan dari *Remote Access* VPN dengan metode SSL.

Tujuan yang akan dicapai dalam penelitian ini adalah:

1. Untuk menganalisis arsitektur dari VPN, terutama *Remote Access* VPN dengan metode SSL.
2. Untuk Mengimplementasikan suatu layanan yang berbasiskan *Remote Access* VPN dengan metode SSL.
3. Untuk membandingkan layanan yang menggunakan *Remote Access* VPN yang menggunakan metode SSL dengan jaringan yang tidak menggunakan VPN.

1.4 Batasan Masalah

1. Konfigurasi *Remote Access* VPN dengan metode SSL berupa konfigurasi pada sistem operasi.
2. Sistem operasi yang digunakan pada VPN *server* adalah Linux.
3. Implementasi konfigurasi *Remote Access* VPN dengan metode SSL berupa simulasi jaringan (*real network*) dengan menggunakan 2-4 komputer.
4. Koneksi *Remote Access* VPN apabila melewati internet pada bandwidth maksimal 256 Kbps.
5. VPN (*Virtual Private Network*) diimplementasikan dengan menggunakan IP versi 4 (IPv4).

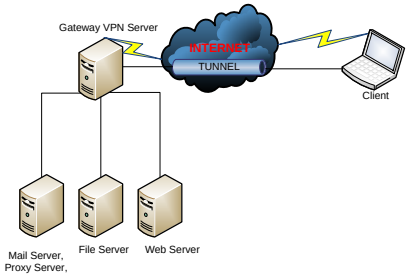
2. MODEL, ANALISIS, PERANCANGAN DAN IMPLEMENTASI

Remote Access Virtual Private Network biasanya digunakan untuk menguhubungkan pengguna yang *mobile* dari berbagai lokasi yang jauh (*remote*). Biasanya jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya.

2.1 Analisis

Remote Access merupakan sebuah kemampuan untuk mengakses *resource-resource* pada suatu layanan maupun jaringan komputer dari lokasi manapun. Penerapan *remote access* vpn akan memberikan sebuah kemampuan untuk mengakses *resource-resource* pada suatu layanan maupun jaringan komputer melalui jalur *private* yang lebih aman.

Model topologi jaringan *Remote Access Virtual Private Network* yang umum digunakan biasanya terdiri dari sebuah komputer sebagai *server* VPN, *server* pendukung lain seperti web server, file server, dan *server-server* yang lain dan komputer *client* dengan bentuk topologi seperti pada gambar 1 berikut:



Gambar 1. Topologi Remote Access VPN

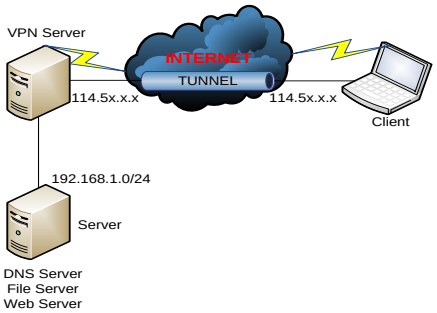
Secure Socket Layer (SSL) adalah protokol yang digunakan untuk berkomunikasi lewat internet secara aman. Teknologi SSL menggunakan konsep teknologi kriptografi kunci publik untuk bisa mencapai komunikasi yang aman antar *server* dan *client.*

Di dalam proses kerjanya, SSL terdiri dari beberapa fase, yaitu:

1. Negosiasi antar *peer* terhadap algoritma yang didukung oleh masing-masing *peer/endpoint* tersebut.
2. Pertukaran *Public Key* (*PKI*) untuk mekanisme enkripsi dan autentikasi berbasis sertifikat.
3. Enkripsi simetris maupun enkripsi asimetris

2.2 Perancangan

Perancangan Jaringan yang akan digunakan pada skripsi ini terdiri dari sebuah komputer sebagai *server* VPN, *server* dan komputer *client* dengan bentuk topologi seperti yang ditunjukan pada gambar 2:



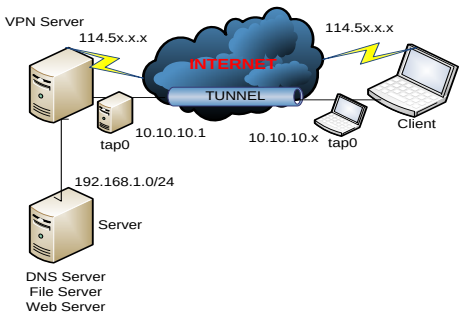
Gambar 2. *Simulasi Jaringan Remote Access VPN*

Tabel 1. Alokasi IP Address

Device	IP Address	Publik/ Private	Interface
VPN *Server*	114.5x.x.x.	IP Publik	Modem HSDPA
	192.168.1.1	IP Private	Eth0
	10.10.10.1	IP VPN	Tap0
Server	192.168.1.100	IP Private	Eth0
Client	114.5x.x.x	IP Publik	Modem HSDPA
	10.10.10.x	IP VPN	Tap0

2.3 Implementasi

Pada implementasi *network* vpn, vpn *server* akan diberikan IP *address*-nya yaitu 10.10.10.1 dengan *subnet* 255.255.255.0 dan IP *address client* akan berada pada *range* 10.10.10.2-10.10.10.254 dengan *subnet* 255.255.255.0. Sehingga akan terbentuk topologi logik seperti yang ditunjukkan pada Gambar 3 dibawah ini:



Gambar 3. *Topologi Logik Remote Access VPN Berbasis SSL*

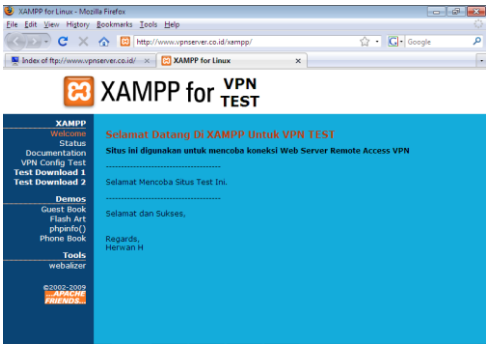
Dengan alokasi IP Adress sebagai berikut:

Tabel 1. Alokasi IP Address

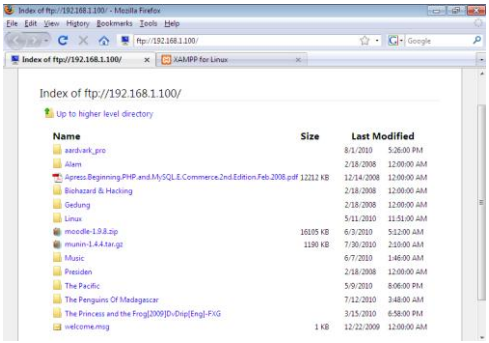
Device	IP Address	Publik/ Private	Interface
VPN *Server*	114.5x.x.x.	IP Publik	Modem HSDPA
	192.168.1.1	IP Private	Eth0
	10.10.10.1	IP VPN	Tap0
Server	192.168.1.100	IP Private	Eth0
Client	114.5x.x.x	IP Publik	Modem HSDPA
	10.10.10.x	IP VPN	Tap0

3. HASIL DAN DISKUSI

Pengujian dilakukan pada akses web server dan ftp server dengan yang terdapat di komputer *server*.

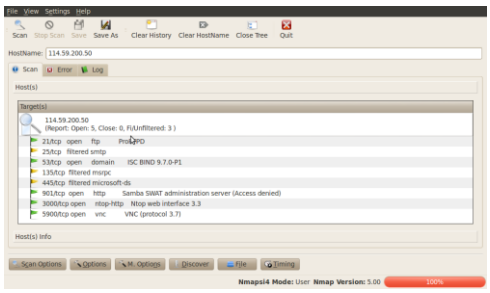


Gambar 4. *Akses Web Server*



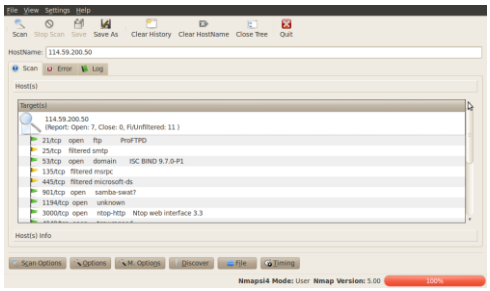
Gambar 5 *Akses FTP Server*

Pada hasil *scanning port* mode normal menunjukan bahwa terdapat 5 *port* yang terbuka, dan *port* VPN yang telah dibuat sebelumnya, yaitu *port* 1194 tidak tidak terdeteksi oleh Nmap



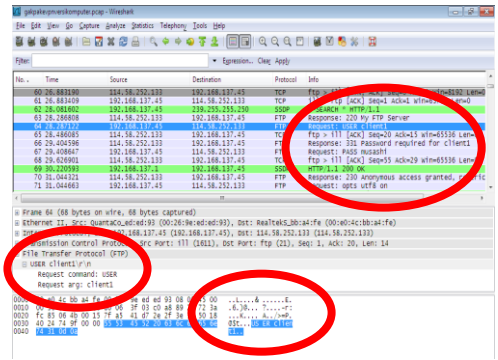
Gambar 6. *Scanning Port Mode Normal*

Sedangkan apabila melakukan *scanning port* terhadap vpn *server* dengan menggunakan mode all, maka akan terdeteksi 7 *port* yang terbuka, dan *port* vpn *server* (1194) terdeteksi oleh aplikasi Nmap, akan tetapi, aplikasi Nmap tidak dapat mengetahui informasi *port* 1194 tersebut dengan memnentukan jenis *port*-nya merupakan *port unknown*.



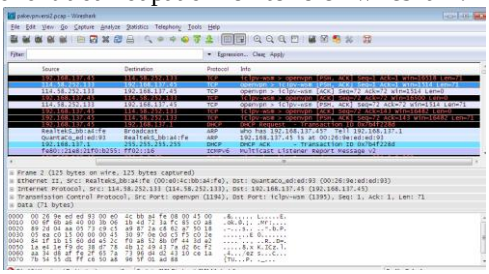
Gambar 7. *Scanning Port Mode All*

Hasil monitoring data terhadap jaringan yang tidak terkoneksi vpn, *client* yang melakukan akses terhadap ftp server, dapat diketahui username, password dan file yang digunakan untuk akses terhadap ftp server.



Gambar 8. *Monitoring Tanpa Melalui Remote Access VPN Berbasis SSL*

Pada proses monitoring data yang melalui *remote access* vpn yang berbasis SSL, username dan password yang digunakan oleh *client* untuk mengakses ftp *server* tidak diketahui, serta data yang di-*request* oleh *client* tidak dapat dimonitor oleh wireshark.



Gambar 9. *Monitoring Data Melalui VPN*

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

1. Konfigurasi *Remote Access Virtual Private Network* dengan metode dapat dilakukan dengan menggunakan openvpn yang telah mendukung untuk membangun jaringan VPN yang berbasis SSL.
2. Service-service seperti Web Server, FTP Server, DNS Server, dan server-server lainnya, dapat berjalan dengan baik dalam lingkungan *remote access* VPN yang berbasis SSL.
3. *Remote Access* VPN yang berbasis SSL akan melakukan enkripsi terhadap kunci dan proses transfer data dari *server* menuju *client* maupun sebaliknya.
4. SSL yang menjadi protokol yang digunakan pada *remote access* VPN memberikan mekanisme keamanan dengan salah satu bukti bahwa data yang dilewatkan melalui jalur VPN terbukti aman dengan tidak terdeteksinya informasi user dan data yang di-*request* oleh user.
5. Hasil *scanning port* terhadap VPN Server menunjukkan bahwa tidak terdeteksinya *port* yang di-*assign* untuk *remote access* VPN dalam mode normal dan tidak dapat diketahui jenis *service* yang digunakan pada *port* VPN server. Sehingga dapat dikatakan bahwa *remote access* VPN memberikan mekanisme keamanan terhadap sistem.

4.2 Saran

Untuk pengembangan lebih lanjut, perlu dilakukan analisis detail terhadap mekanisme pengujian keamanan *remote access virtual private network*, serta perbandingan protokol keamanan yang digunakan dalam lingkungan VPN.

5. DAFTAR PUSTAKA

[1] Bauer, Michael, 2003, *Building Secure Servers With Linux*, O'Reilly.

[2] Feilner, Markus, 2009, *Beginning OpenVPN 2.0.9: Build and Integrate Virtual Private Networks Using OpenVPN*, PACKT.

[3] Feilner, Markus, 2006, *OpenVPN:Building and Integrating Virtual Private Networks*, PACKT

[4] Negus, Cristoper, 2007, *Ubuntu Linux Toolbox*, WILEY.

[5] Sander, Van Vugt, 2006, *Beginning Ubuntu Server Administration: From Novice to Professional*, Apress

[6] Scott, Charlie, 1999, *Virtual Private Network 2nd Edition*, O'Reilly

[7] Scroder, Carla, 2007, *Linux Networking Cookbook*, O'Reilly.

[8] Steinberg, Joseph, 2005, *SSL VPN: Understanding, Evaluating, and Planning Secure, Web-Based Remote Access*, PACKT.

[9] Tanembaum,A.S., 2003, *Computer Networks*, Prentice Hall, NewJersey

[10] Irawan, Budhi., 2005, *Jaringan Komputer*. Graha Ilmu. Yogyakarta.

[11] _____, *Ubuntu Server Guide*, Canonical Ltd.

[12] _____, *Langkah Mudah Administrasi Jaringan Menggunakan Linux Ubuntu 9*, ANDI.