Nama: Yusril Rahardiansah

Kelas: C

NIM: 3411201076

Virtual Private Network

Virtual Private Network (VPN), merupakan sebuah jaringan yang dibuat untuk melakukan transaksi data yang telah dienkripsi antara dua atau lebih pengguna jaringan yang resmi. Jaringan VPN seluruhnya menggunakan internet sehingga faktor keamanan menjadi sangat penting. Beberapa serangan yang mungkin terjadi di jaringan internet adalah Denial of Service (DoS) attack, sniffing, spoofing, session hijacking, dan masih banyak lagi (Sari, 2011)

VPN merupakan paket solusi komunikasi data (baik berupa data suara, video, atau file digital lainnya) yang memberikan layanan berbasis IP ke *end user*. Layanan VPN dapat mengirimkan data antar-dua computer yang melewati jaringan publik, seperti Internet, sehingga seolah-olah terhubung secara *point-to-point*. (Sakiwan, 2010)

Perangkat keras VPN terdiri dari sebagai berikut. Pertama adalah VPN *Server*. Ini adalah sebuah perangkat jaringan yang menjalankan perangkat lunak *server*. Fungsi-fungsi utama pada VPN *servers* yaitu: menerima *request* dari koneksi VPN, melakukan negosiasi kebutuhan koneksi dan parameter, melakukan autentikasi dan otorisasi pada VPN *clients*, menerima data dari *client* atau meneruskan *request* data yang dilakukan *client*, serta berlaku sebagai titik akhir (*end point*) pada VPN *tunnel* dan koneksi. Yang kedua adalah VPN *Client*. Ini adalah mesin lokal maupun jarak jauh yang melakukan sebuah koneksi VPN pada sebuah VPN *server*, dan melakukan *login* pada sebuah jaringan jarak jauh setelah diautentikasi pada VPN *server*, yang kemudian dapat melakukan komunikasi (Trihadi et al., 2008)

OpenVPN adalah sebuah implementasi VPN *open source* yang menggunakan enkripsi SSL. Implementasi *user* OpenVPN tersedia untuk banyak sistem operasi, termasuk Linux, Windows 2000/XP atau yang lebih tinggi, OpenBSD, FreeBSD, NetBSD, Mac OS X, dan Solaris. Pada sebuah VPN, dia akan mengenkapsulasi semua trafik (termasuk protokol DNS dan protocol protokol lain) di tunnel yang terenkripsi, jadi bukan hanya satu port TCP saja. Kebanyakan orang merasa hal itu sangat memudahkan untuk dimengerti dan diatur daripada IPSEC (Triwanto & Setiawan, 2014)

*Routing* adalah proses dimana suatu router memforward paket ke jaringan yang dituju. Suatu router membuat keputusan berdasarkan IP address yang dituju oleh paket. Semua router menggunakan IP address tujuan untuk mengirim paket. Agar keputusan routing tersebut benar, router harus belajar bagaimana untuk mencapai tujuan. Ketika router menggunakan routing dinamis, informasi ini dipelajari dari router yang lain. Ketika menggunakan routing statis, seorang network administrator mengkonfigurasi informasi tentang jaringan yang ingin dituju secara manual. (Agus Widiana Putra & Pramartha, 2012)

PPTP merupakan *protocol* jaringan yang memungkinkan pengamanan *transfer* data dari remote *client* ke *server* pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP. Teknologi jaringan PPTP merupakan pengembangan dari *remote access Point-toPoint protocol* yang dikeluarkan oleh *Internet Engineering Task Force* (IETF). PPTP merupakan *protocol* jaringan yang merubah paket PPP menjadi IP datagram agar dapat di*transmisi*kan melalui intenet. PPTP juga dapat digunakan pada jaringan *private* LAN-toLAN (Nugroho et al., 2015)

Fungsi dari Teknologi VPN yaitu Autentikasi Sumber Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumbersumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya. Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain. (Chairul et al., 2016)

Mampu melakukan akses dengan jaringan secara *remote* dan mengefektifkan biaya karena menggunakan jaringan publik serta mengirimkan informasi yang bersifat rahasia seaman mungkin. VPN memberikan tingkat keamanan untuk berbagi informasi melalui, *confidentiality, integrity,* dan *authentication* (Haryan et al., 2015)

Konsep VPN Jaringan VPN menawarkan keamanan dan tidak terdeteksi dikarenakan IP yang digunakan adalah IP Public milik VPN *server*. Dengan adanya enkripsi dan dekripsi maka data yang lewat jaringan internet ini tidak dapat diakses oleh orang lain bahkan oleh *client* lain yang terhubung dengan *server* VPN. Kunci yang dibutuhkan untuk membuka enkripsi tersebut hanya diketahui oleh *server* VPN dan *client* yang terhubung dengannya. Dengan penggunaan enkripsi dan dekripsi itulah yang menyebabkan data yang lewat jaringan tidak dapat dimodifikasi dan dibaca sehingga keamanannya terjamin (Hendriana, 2012)

Teknologi *tunneling* merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya. Disebut *tunnel* (terowongan) karena koneksi *point-topoint* tersebut sebenarnya terbentuk dengan melintasi jaringan umum, namun koneksi tersebut tidak mempedulikan paket-paket data milik orang lain yang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya melayani transportasi data dari pembuatnya. Hal ini sama dengan penggunaan jalur *busway* yang pada dasarnya menggunakan jalan raya, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus. Koneksi *point-to-point* ini sesungguhnya tidak benar-benar ada, namun data yang dihantarkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat *point-to-point* (Oktivasari & Utomo, 2016)

DAFTAR PUSTAKA

Agus Widiana Putra, I., & Pramartha, C. (2012). Perancangan Implementasi Konsep Routing Dan Virtual Private Network Antara Webserver Moodle Dan Webserver Drupal. *JELIKU - Jurnal Elektronik Ilmu Komputer Universitas Udayana*, *1*(2), 99–103.

Chairul, U., Emilia, R., & Irfan. (2016). Perancangan Jaringan Keamanan Virtual Private Network ( VPN ) Siteto Site. *Perancangan Jaringan Keamanan Virtual Private Network (VPN)Siteto Site Chairul*, 23–30.

Haryan, D. B., Jafriyal, & Hendri, P. (2015). *Analisis Dan Perancangan Virtual Private Network Pada Pt. Bank DKI*. *1*(1), 50–71.

Hendriana, Y. (2012). Evaluasi Implementasi Keamanan Jaringan Virtual Private Network (VPN). *Serangan DoS Dengan Pingflood.*

Nugroho, I., Widada, B., & Kustanto. (2015). Perbandingan Performansi Jaringan Virtual Private Network Metode Point To Point Tunneling Protocol ( Pptp ) Dengan Metode Internet Protocol Security. *Jurnal TIKomSiN*, *3*(2), 1–9.

Oktivasari, P., & Utomo, A. B. (2016). *Analisa Virtual Private Network Menggunakan*. 185–202.

Sakiwan. (2010). Kajian Virtual Private Network (Vpn) Lapan Dan Pemanfaatannya Dalam Mendukung Pengembangan E-Government. *Berita Dirgantara*, *11*(4), 145–152.

Sari, M. W. (2011). Analisis Keamanan Jaringan Virtual Private Network (VPN) pada Sistem Online Microbanking. *Jurnal Teknik Informatika*, 1–12.

Trihadi, S., Budianto, F., & Arifin, W. (2008). Perancangan Virtual Private Network Dengan Server Linux Pada Pt. Dharma Guna Sakti. *CommIT (Communication and Information Technology) Journal*, *2*(1), 25. https://doi.org/10.21512/commit.v2i1.488

Triwanto, J., & Setiawan, E. A. (2014). Penggunaan Virtual Private Network Untuk Pengamanan Komunikasi Pada VoIP. *Tesla*, *16*(1), 25–32. https://www.journal.untar.ac.id/index.php/tesla/article/view/354/295