PERANCANGAN JARINGAN *VIRTUAL PRIVATE NETWORK (VPN)* MENGGUNAKAN KERANGKA KERJA NIST SP 800-113 DALAM MENDUKUNG KEAMANAN *E-GOVERNMENT*

[1] SOMANTRI, [2] MUHAMAD MUSLIH
[1] DEPARTEMEN TEKNIK INFORMATIKA UNIVERSITAS NUSA PUTRA, SUKABUMI, INDONESIA
[2] DEPARTEMEN SISTEM INFORMASI UNIVERSITAS NUSA PUTRA, SUKABUMI, INDONESIA
e-mail:[1] somantri@nusaputra.ac.id , [2] muhamad.muslih@nusaputra.ac.id

ABSTRACT

High mobility of employees at the Office of Communications and Information Technology requires facilities for communicate and process information when employees are outside the office. The facility is in the form of internet network, and employees who are outside the office can be connected in a computer network system. However, the internet network is a free network and can be accessed by anyone, so it has not guaranteed security. Data communications on the internet involves issues of security, ease and speed of transfer (data exchange). Designing Virtual Private Network Networks (VPNs) provides data confidentiality and security solution to internal resources located at the more secure Sukabumi City Office of Communication and Informatics (Diskominfo)

The research method I used in this research is Network Development Life Cycle (NDLC) method with framework NIST SP 800-113. The life cycle of network system implementation is defined in a number of phases. namely: analysis, design, simulation prototype, implementation, monitoring and management. The author uses SSL-based VPN (Security Socket Layer) in this implementation.

The results of this thesis research indicate that the application of Virtual Private Network (VPN) can streamline users in access network resources from outside network safely. The results also show that data send via VPN through a special path known as tunneling can not be detected by the sniffing program.

Keywords : VPN (Virtual Private Network), NIST SP 800-113, Network Development Life Cycle (NDLC), SSL, OpenVPN, e-government

1. PENDAHULUAN

Dewasa ini perkembangan teknologi dan informasi yang semakin pesat, dan kebutuhan akan pertukaran data yang tinggi baik sektor swasta, pemerintah maupun stakeholder. Perusahaan atau instansi pemerintah dengan mobilitas karyawan yang tinggi memerlukan fasilitas untuk melakukan komunikasi dan pengolahan informasi ketika karyawan berada diluar lingkup kantor, fasilitas tersebut berupa jaringan internet, dan karyawan yang berada diluar ruang lingkup kantor dapat terhubung dalam satu sistem jaringan komputer, namun jaringan internet merupakan jaringan yang bebas dan dapat diakses oleh siapa saja, sehingga belum terjamin keamanannya. Komunikasi data pada internet melibatkan masalah keamanan, kemudahan dan kecepatan transfer (pertukaran data). Hal ini yang harus diperhatikan oleh pemilik dan administrator sistem informasi suatu intansi pemerintahan dalam melakukan kegiatan di dunia internet, sehingga kerahasiaan

informasi suatu perusahaan atau intansi pemerintahan bisa terjaga dengan baik, kemudahan dan kecepatan (pertukaran data) bisa diimplementasikan sehingga dapat menjadi nilai lebih yang bisa berpengaruh pada cost.

Dalam penyelenggaraan kegiatan kepemerintahan, hampir semua lembaga pemerintah telah memiliki dukungan jaringan Teknologi Informasi untuk menunjang kegiatan operasional sehari-hari, selain itu bahkan sebagian sudah menerapkan e-government baik di tingkat pusat maupun di daerah. Seiring dengan perkembangan tersebut maka diperlukan Teknologi yang memungkinkan efisiensi lebih dan keamanan untuk dapat melakukan penyimpanan dan pertukaran data. Pertimbangan biaya yang cukup tinggi dalam pengembangan jaringan tertutup bagi intansi pemerintahan, sehingga ada pertimbangan untuk lebih memilih menggunakan jaringan publik (internet) bagi kepentingan operasionalnya untuk melakukan komunikasi dan pengolahan informasi baik untuk karyawan yang berada diluar lingkup kantor ataupun kantor-kantor dinas terkait.

Teknologi yang dapat membantu mengatasi masalah keamanan jaringan di internet adalah teknologi virtual private network. Secara umum, Virtual Private Network (VPN) adalah suatu proses berupa sebuah jaringan umum (public network atau internet) yang diamankan untuk difungsikan sebagai sebuah jaringan private (private network). VPN memungkinkan hubungan yang dilakukan antara user yang berada di luar kantor atau intansi terkait menjadi lebih ekonomis, selain itu koneksi vpn tidak terbatas hanya pada hubungan antara user yang berada di luar kantor dengan kantor saja, tetapi memberikan jaminan keamanan dan realibilitas yang hampir sama dengan jaringan pribadi. Penggunaan VPN menjamin keamanan yang tinggi karena koneksi dengan VPN dilakukan dengan menerapkan peralatan dengan metode autentifikasi yang berfungsi untuk memberi identitas kepada pemakai dan data yang dikirimkan lewat VPN dienkripsi.

2. KAJIAN PUSTAKA

Vulnerabulities of VPN using IPSec and Defensive Measures (Byeong-Ho Kang and Maricel O. Balitanas, 2009) menjelaskan bahwa keamanan data memainkan peranan penting di era bisnis modern yang proses transaksinya banyak menggunakan internet dan perangkat nirkabel. Penelitian yang dilakukan menyajikan kerentanan keamanan yang ditemukan di VPN dengan menggunakan IPSec serta rekomendasi kebijakan dalam penggunaan VPN sebagai metode pengamanan. Kebijakan yang disarankan adalah dengan implementasi VPN dengan konsentrator IPSec untuk karyawan, konsultan, kontraktor atau vendor dan para pekerja lainnya termasuk semua staff atau personel yang berhubungan dengan pihak ketiga kesemuannya memanfaatkan jaringan VPN untuk mengakses sumber daya yang ada di perusahaan.

Proposed Architecture for Implementing Privacy In Cloud Computing Using Grids And Virtual Private Network (N. Mahesh Kumar, K. Senthilkumar, 2013) menjelaskan implementasi jaringan vpn pada cloud computing yang berbasiskan site to site atau jaringan vpn dengan berbagai device.

Analisis Performansi Remote Access VPN Berbasis IPSec dan Berbasis SSL pada Jaringan IPv6
(Alex Yuasta1, Fazmah Arif Yulianto, S.T., M.T.2, Gandeva Bayu Satrya, S.T., M.T, 2014) Mengetahui hasil analisis dan pengujian terhadap analisis performansi remote access VPN berbasis IPSec dan SSL. The Impact of Virtual Private Network (VPN) on a Company's Network (J. Myles Powell, 2010) menjelaskan bagaimana dampak dan kontribusi dalam penggunaan VPN pada jaringan perusahaan. Analisa virtual private network menggunakan Openvpn dan point to point tunneling protocol.

Analisa virtual private network menggunakan Openvpn dan point to point tunneling protocol (Prihatin Oktivasari & Andri Budhi Utomo, 2016), Pengujian yang dilakukan pada performa menghasilkan perbedaan yang tidak begitu signifikan,

tetapi apabila diamati OpenVPN lebih unggul dari PPTP, hal ini ditunjukkan saat pengujian transfer file OpenVPN memiliki waktu lebih cepat. Sedangkan pada pengujian keamanan OpenVPN lebih unggul dari PPTP, hal ini dapat dilihat dari lebih banyaknya jumlah paket yang diterima oleh OpenVPN saat dilakukan serangan sebelum akhirnya mengalami gangguan pada service VPN.

Kajian Virtual Private Network (VPN) Lapan Dan Pemanfaatannya Dalam Mendukung Pengembangan E-Government (Sakiwan, Peneliti Pusat Analisis dan Informasi Kedirgantaraan, LAPAN, 2010) menjelaskan pengembangan VPN dapat mengoptimalkan komunikasi data antar Satker di lingkungan LAPAN. Dengan adanya pengembangan VPN ini maka kendala dalam pengiriman data dalam volume besar yang selama ini terjadi dapat diatasi, karena adanya karakteristik VPN yang memiliki kemampuan besar (broadband), sehingga jaringan ini dapat digunakan untuk mengirim data bervolume besar dengan cepat dan tepat.

Virtual Private Networks: A feasibility study of secure communications between remote locations. Mark Thomson, Lolita Mageramova, Alex Wikström, 2014, menjelaskan Perbandingan antara berbagai jenis VPN terkait waktu yang digunakan untuk menerapkan konfigurasi perangkat jaringan / pengguna akhir, biaya yang dikeluarkan dalam pengadaan peralatan / perangkat lunak tambahan untuk mengimplementasikan VPN, berdampak pada pengguna akhir, skalabilitas dan terakhir, fungsionalitas keseluruhan dari solusi VPN yang berkaitan dengan operasi bisnis sehari-hari.

3. METODOLOGI

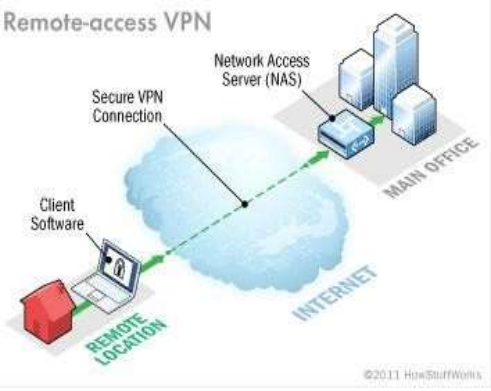
1. Virtual Private Network (VPN)

Virtual Private Network (VPN) adalah sebuah jaringan virtual, yang dibangun di atas sebuah jaringan fisik yang dapat menyediakan mekanisme komunikasi yang aman untuk data dan informasi IP yang ditransmisikan antar jaringan. Karena VPN dapat digunakan pada jaringan yang telah ada, seperti internet, maka VPN dapat memfasilitasi transfer data yang bersifat sensitif secara aman melalui jaringan publik. Cara ini kadang dapat menjadi lebih murah dibandingkan alternatif lain seperti jalur telekomunikasi privat yang khusus didirikan antar organisasi atau kantor cabang.[7]

2. Jenis implementasi VPN

a. *Remote Access* VPN

Remote access yang biasa juga disebut *virtual private dialup network* (VPDN), menghubungkan antara pengguna yang mobile dengan *local area network* (LAN). Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung kejaringan khusus perusahaannya dari berbagai lokasi yang jauh (*remote*) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan *enterprise service provider (ESP)*. ESP akan memberikan suatu *network access server* (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan *software client* untuk komputer komputer yang digunakan pegawai perusahaan tersebut.

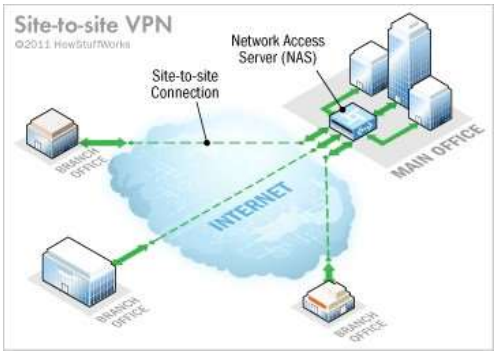


Gambar 1 Topologi Jaringan *VPN Remote Access*

b. Site to site VPN

Jenis implementasi VPN yang kedua adalah *site-to-site* VPN. Implementasi jenis ini menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra

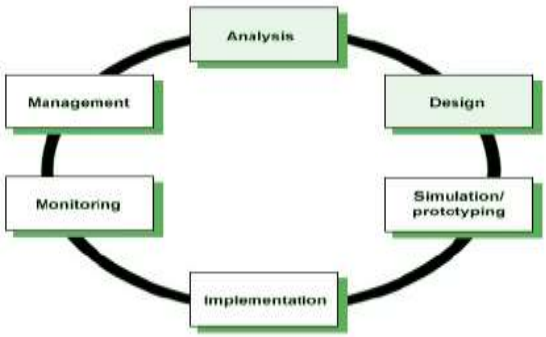
kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, supplier atau pelanggan) disebut *ekstranet*. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis *intranet site-to-site* VPN.



Gambar 2 Topologi Site to site VPN

c. Metode pengembangan sistem NDLC

Penulis menggunakan model pengembangan sistem NDLC *(Network Development Live Cycle*). Menurut Goldman dan Rawles [9], NDLC merupakan model kunci dibalik proses perancangan jaringan komputer. Seperti model pengembangan sistem untuk aplikasi perangkat lunak, NDLC terdiri dari elemen yang mendefinisikan fase, tahapan, langkah, atau mekanisme secara spesifik. Dari kata “cycle” (siklus) adalah kata kunci deskriptif dari siklus hidup pengembangan sistem jaringan yang menggambarkan secara eksplisit seluruh proses dan tahapan pengembangan sistem jaringan yang terus berkelanjutan.

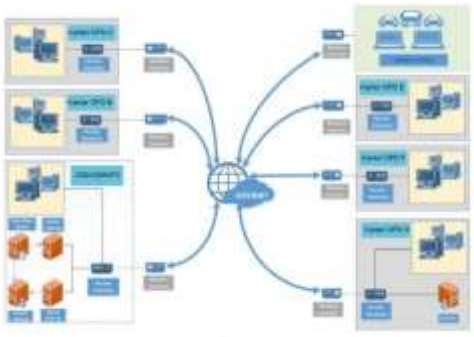


Gambar 3 *Network Development Life Cycle*

4. HASIL DAN PEMBAHASAN

1. Perancangan Topologi Jaringan Setelah diterapkan VPN

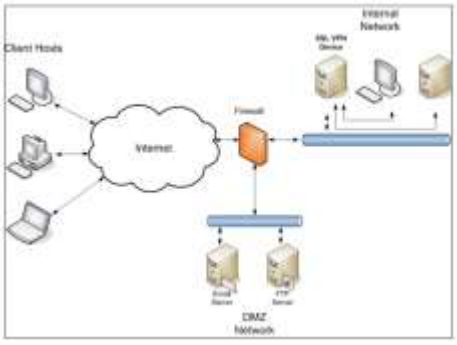
Perancangan ini berdasarkan konsep dan gambaran yang menjelaskan perangkat sebenarnya dalam suatu sistem yang penulis gambarkan dengan topologi sebagai berikut:



Gambar 4 Topologi Jaringan setelah diterapkan VPN

2. Penempatan Perangkat dan Konfigurasi Firewall

Penempatan Device untuk VPN seperti gambar dibawah ini:



Gambar 5 Penempatan Firewall

Pada gambar diatas Menempatkan perangkat VPN di jaringan internal. Opsi ini menempatkan perangkat VPN sepenuhnya di dalam jaringan internal di belakang *firewall*. Port TCP 443 untuk alamat SSL VPN harus dibuka di firewall untuk mengakses perangkat. Meskipun tidak ditunjukkan dalam diagram, penem-

patan firewall tambahan antara perangkat SSL VPN dan jaringan internal lainnya sangat disarankan. Untuk memastikan perlindungan front-end dan back-end untuk perangkat SSL VPN.

Penggunaan Kerangka kerja (framework) NIST Special Publication 800-113 mampu mendeskripsikan penggunaan SSL Virtual Private Network secara komperehensif, serta memiliki tahapan-tahapan secara menyeluruh.

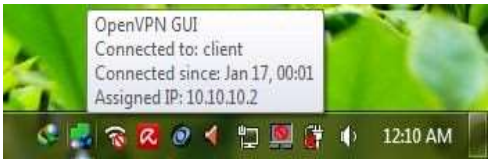
Pengujian

Pada penelitian ini dilakukan pengujian terhadap *Virtual Private Network* dengan beberapa skenario. Simulasi akan dilakukan melalui jaringan internet, dengan arsitektur simulasi seperti yang telah dirancang.

Skenario Pengujian

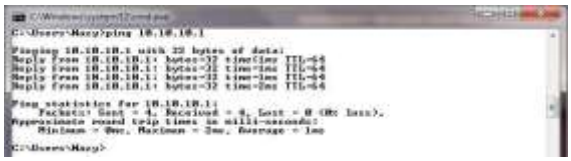
Pada skenario pengujian akan dilakukan terhadap konektivitas remote access VPN yang berbasis SSL. Adapun skenario-skenario yang dilakukan adalah sebagai berikut:

1. Pengujian Startup VPN (*Startup Server dan Startup Client*), pengujian bertujuan apakah konfigurasi yang telah dilakukan pada server maupun client telah benar atau tidak.



Gambar 6. Pengujian Startup VPN Client

2. Pengujian Koneksi VPN yang berupa tes koneksi PING (untuk melakukan pengecekan konektivitas pada komputer yang saling terhubung) dan TCPdump (tool untuk memantau dan menangkap *traffic* jaringan yang melewati *interface host).*

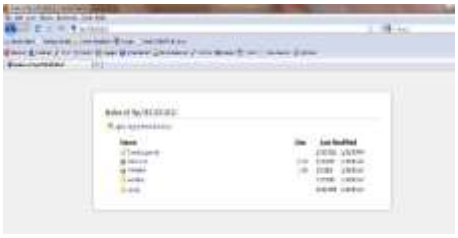


Gambar 7. Ping Client ke vpn server

Gambar 8 Hasil Scanning TCPDUMP

3. Pengujian Akses *Server* dimana *client* melakukan akses terhadap layanan yang terdapat pada *server,* seperti Web Server, FTP Server dan DNS Server.

Gambar 8. Pengujian Web Server



Gambar 9. ftp melalui web browser

4. Pengujian Keamanan yang berupa tes *port scanning* terhadap VPN *server*, memonitoring data dan analisis perbandingan datanya.

5. KESIMPULAN

Dengan menggunakan SSL VPN komunikasi jaringan private yang melewati jaringan public (Internet) akan lebih aman sehingga dapat merahasiakan transaksi pertukaran data milik pemerintah Kota Sukabumi terutama dalam pemanfaatan dan keamanan e-goverment.

Dengan menggunakan solusi VPN over Internet maka biaya untuk interkoneksi jaringan antar dinas dan kecamatan yang jarak geographisnya terpisah jauh lebih murah dalam implementasinya jika menggunakan layanan provider seperti VPN-IP, MPLS, leased line, dan lain-lain.

Pembangunan SSL VPN menjadi solusi untuk remote users dan mobile users karena SSL VPN memberikan keamanan dan enkripsi komunikasi melalui internet.

REFERENSI

[1] T. Rawles Philips E. Goldman James, *Applied Data Communications: A Business Oriented Approach*. Mishawaka, USA: Wiley, 2001:470.

[2] Hartono, D. Utomo dan E. Mulyanto, 2010. *"Electronic Government Pemberdayaan Pemerintahan Dan Potensi Desa Berbasis Web", J. Teknol. Inf.*, vol. 6, no. April, pp. 9–21.

[3] Ariyus, D. 2007. *Intrusion Detection System*. Andi Yogyakarta. Yogyakarta

[4] Sukmaaji, Anjik dan Rianto. 2008. "*Jaringan Komputer Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan"*. Yogyakarta: Andi.

[5] Schneier, Bruce. 1996. *"Applied Cryptography Second Edition: protocol, algorithm, and source code in C".* John Wiley and Son

[6] Hool, Kim. 2003. *OSI Defense in Depth to Increase Application Security.* SANS Security Essentials GSEC Practical Assignment v1.4b. SANS Institute.

[7] Frankel, Sheila and Friend's. 2008. *"Guide to SSL VPNs - Recommendations of the National Institute of Standards and Technology"*. NIST Special Publication 800-113.

[8] M. Feilner, 2006. "*OpenVPN: Building and Integrating Virtual Private Networks"*, Packt Publishing LTD, Birmingham.

[9] Goldman, James E And Rawles, Phillip. T. 2014. *"Applied Data Communications – A Bussiness-Oriented Approach"*. Wiley

[10] Andreas Kostoulas and Friend's. 2015. *"Connect street light control devices in a secure network".* Thesis. Halmstad University.

[11] Alex Yuasta1, Fazmah Arif Yulianto, S.T., M.T.2, Gandeva Bayu Satrya, S.T., M.T. 2014. *"Analisis Performansi Remote Access VPN Berbasis IPSec dan Berbasis SSL pada Jaringan IPv6"*

[12] Zhiyuan Fang, “E-Government in Digital Era : Concept , Practice, and Development,” *Int. J. Comput. Internet Manag.*, vol. 10, no. 2, pp. 1–22, 2002.

[13] Simar Preet Singh and Raman Maini, 2011. *“Comparison of data encryption algorithms*”. International Journal Computer Science and Communication Vol. 2, no. 1, pp. 125–127, 2011.

[14] B. Kang and M. Balintanas. 2009 *“Vulnerabilities of VPN using IPSec and Defensive Measures”* International Journal of Advanced Science and Technology, vol. 8. pp. 9–17.

[15] Kumar, N. Mahesh and Senthilkumar, 2013. *“Proposed Architecture For Implementing Privacy In Cloud Computing Using Grids an Virtual Private Network”*. International Journal of Technology Enhancement and Emerging Engineering Research, Vol. 1, Issue 3 ISSN 2347-4289