PEMBANGUNAN JARINGAN VPN DI BADAN PENDAPATAN DAERAH (BAPENDA) PROVINSI JAWA BARAT

Rizki Agusti Ghofur[1], Iskandar Ikbal, S.T., M.Kom[2]

Program Studi Teknik Informatika
Fakultas Teknik dan Ilmu Komputer. Universitas Komputer Indonesia
Jl. Dipatiukur No 112-116 Bandung. 40132
E-mail : rizkiagusti@gmail.com[1] , iskandar.ikbal@email.unikom.ac.id[2]

ABSTRAK

Penelitian ini berjudul "Pembangunan Jaringan VPN di Badan Pendapatan Daerah (BAPENDA) Provinsi Jawa Barat". Tujuan penelitian ini adalah untuk memaksimalkan akses aplikasi Sistem Informasi Kearsipan (SIMKA) dan meminimalisir eksploitasi terhadap server SIMKA. Metode pengembangan sistem yang digunakan dalam penelitian ini adalah metode PPDIOO, dengan melakukan analisis terhadap masalah jaringan yang terjadi ditemukan masalah berupa, sulitnya mengakses aplikasi dikarenakan *bandwith* internet digunakan kepentingan diluar pekerjaan dan Masih mudahnya aplikasi Sistem Informasi Kearsipan (SIMKA) BAPENDA JABAR diakses secara umum yang bisa mengakibatkan eksploitasi terhadap aplikasi dan jaringan. Berdasarkan permasalahan yang terjadi dibuatlah jaringan VPN unutuk aplikasi Sistem Informasi Kearsipan (SIMKA) dengan menggunkan *protocol* PPTP. Beberapa tahapan dalam membangun jaringan VPN diantaranya Konfigurasi Profile, Konfigurasi PPTP Server, Konfigurasi Akun, Konfigurasi Filter Rules TCP PPTP In, Konfigurasi Filter Rules GRE PPTP Out, Konfigurasi Filter Rules GRE PPTP In, Konfigurasi Filter Rules GRE PPTP Out dan Konfigurasi Filter Rules GRE PPTP Forward. Hasil penelitian menunjukan bahwa, dengan dibuatnya jaringan VPN untuk aplikasi Sistem Informasi Kearsipan (SIMKA) dengan menggunkan *protocol* PPTP, dapat memaksimalkan akses aplikasi Sistem Informasi Kearsipan (SIMKA) dan meminimalisir eksploitasi terhadap *server* SIMKA.

Kata kunci : Eksploitasi, PPDIOO, PPTP, Server, VPN.

1. PENDAHULUAN

Badan Pendapatan Daerah Provinsi Jawa Barat (BAPENDA JABAR) merupakan organisasi perangkat daerah yang memiliki fungsi diantaranaya penyelenggaraan pendapatan dan pelayanan umum, meliputi kesekretariatan, perencanaan dan pengembangan pajak, non pajak, pengendalian dan pembinaan. BAPENDA JABAR mengelola kearsipan yang berkaitan dengan perpajakan diantaranya Pajak Kendaraan Bermotor (PKB) dan Bea Balik Nama Kendaraan Bermotor (BBNKB) di seluruh Jawa Barat, BAPENDA JABAR memiliki 34 Cabang Pelayanan Pendapatan Daerah (CPPD) di setiap Kota dan Kabupaten untuk melayani masyarakat dalam hal Perpajakan Kendaran Bermotor (PKB).

Berdasarkan wawancara dengan bapak Asep Kamil Husni S.Sos saat ini BAPENDA JABAR memiliki sistem aplikasi yang menangani kearsipan PKB DAN BBNKB yaitu Sistem Informasi Kearsipan (SIMKA), namun dari hasil observasi di lapangan dan wawancara dengan bapak Asep Kamil Husni S.Sos ditemukan beberapa kendala yang dialami, diantaranya tidak stabilnya jaringan yang digunakan sehingga sulit membuka aplikasi SIMKA, dikarenakan masih banyaknya pegawai menggunakan layanan *internet* diluar pekerjaan yang mengakibatkan tidak tercapainya target pelaporan arsip PKB dan BBNKB, terbukti berdasarkan data Daftar Rekaputilasi Hasil Evaluasi Alih Media Arsip Kendaran Bermotor Provinsi Jawa Barat dari bulan januari sampai maret 2018 terdapat hanya 11 cabang yang memenuhi target dan 23 cabang tidak memenuhi target pelaporan arsip.

Berdasarkan observasi di lapangan dan wawancara dengan bapak Asep Kamil Husni S.Sos, saat ini Aplikasi SIMKA diakses oleh 34 cabang dengan akses internet *public* yang mengakibatkan eksploitasi yang mengarah langsung terhadap server, terbukti berdasarkan data pada tanggal 4 maret 2018 terjadi eksploitasi 317 *brute force* terhadap server SIMKA dan berdasarkan data hasil teknik sniffing menggunkan *tools wireshark*, masih mudahnya aplikasi SIMKA tereksploitasi hal ini dapat mengancam data maka dari itu dibutuhkan juga akan jaringan yang dapat melindungi data, dengan keamanan yang terjamin dikarenakan arsip merupakan aset yang berharaga dan termasuk kekayaan negara yang tertuang pada Undang-Undang Republik Indonesia Nomer 43 Tahun 2009 Tentang Kearsipan.

Untuk mengatasi masalah keamanan data dalam komunikasi pada jaringan umum (*public network* / *internet*) serta pengotimalan distribusi paket data, *Virtual Private Network* (VPN) dapat menjadi

solusi. Beberapa penelitian mengenai *Virtual Private Network* (VPN) telah dilakukan sebelumnya. Penelitian yang telah dilakukan oleh Heru Supriyono, Jisnu Adi Widjaya, dan Agus Supardi dengan judul "Penerapan Jaringan *Virtual Private Network* Untuk Keamanan Komunikasi Data Bagi Pt. Mega Tirta Alami", menghasilkan penelitian yang memfokuskan keamanan data . [6] Dalam penelitian lain yang dilakukan oleh Dhio Saputra dengan judul "Implementasi *Virtual Private Network* Pada Sistem Informasi Pengelolaan Keuangan Daerah Pemerintah Provinsi Riau", menghasilkan penelitian yang memfokuskan keamanan data dan pembatasan pengaksesan jaringan.[7]

Berdasarkan latar belakang masalah diatas maka penulis bermaksud mengambil topik tugas akhir ini dengan judul "**PEMBANGUNAN JARINGAN VPN DI BADAN PENDAPATAN DAERAH (BAPENDA) PROVINSI JAWA BARAT**".

Tujuan yang diharapkan akan dicapai dalam penelitian ini adalah:

1. Memaksimalkan akses Aplikasi SIMKA.
2. Meminimalisir eksploitasi terhadap Server SIMKA.

2. ISI PENELITIAN

2.1 Landasan Teori

2.1.1 Jaringan Komputer

Sejarah *network* atau jaringan komputer berawal dari *time-sharing networks*, yaitu "rangkaian" terminal yang terhubung dengan komputer sentral yang disebut mainframe. Contoh *time-sharing networks* adalah IBM's *system network architacture* (SNA) dan *digital network architacture.*
Kemudian komputer berskala kecil yang disebut *Personal Computer* atau PC mulai menggeser komputer-komputer mainframe.[13]

2.1.2 Topologi

LAN berkaitan dengan area *network* yang terbatas. Umumnya sebuah LAN dapat dikembangkan untuk mendukung kecepatan transfer data sangat tinggi. Ada 4 topologi dasar LAN (yang kadangkala digunkan juga unutk MAN, WAN, dan Internet) yaitu Bus, Ring, Start, Mesh.[15]

2.1.2 Internet

Istilah internet berasal dari kata *internetworking*. *Internetworking* sendiri bisa diartikan sebagai *network* dari *network*, yang berarti kumpulan dari arti jaringan-jaringan yang menghubungkan komputer dari sistem yang berbeda-beda. Jadi secara singkat dapat dikatakan bahwa internet adalah gabungan beberapa jenis jaringan komputer yang saling terkoneksi dan terhubung satu dengan yang lainnya.[13]

2.1.3 IP *Address*

IP *address* dibentuk oleh sekumpulan bilangan biner sepanjang 32 bit, yang dibagi atas 4 bagian. Setiap bagian panjangnya 8 bit. IP *address* merupkan pengenalan dari setiap *host* pada jaringan Internet. Artinya tidak diperbolehkan adanya *host* lain (yang tergabung ke internet) menggunakan IP *address* yang sama.[13]

2.1.3 VPN

Virtual Private Network (VPN) ialah sebuah teknologi jaringan komputer yang dipergunkan unutk menghubungkan dari beberapa *Local Area Network* yang lokasinya dipisahkan secara geografis menjadi sebuah LAN virtual.

VPN menggunakan media komunikasi publik (seperti internet) untuk menghubungkan area yang berjauhan. Data yang melalui jaringan publik akan dienkripsi sehingga terjamin keamanannya dan pengguna lain tidak dapat melihat isinya.

Saat ini VPN banyak digunakan oleh perusahan besar, lembaga pendidikan, dan isntansi pemerintahan. Biaya untuk VPN jauh lebih murah dibandingkan biaya untuk *leased line*. Biasayanya VPN digunakan oleh perusahaan untuk menghubungkan kantor pusat dan kantor cabang. [13]

2.1.3 PPTP

Virtual Private Network (VPN) merupakan teknologi jaringan komputer yang digunkan unutk menggabungkan beberapa LAN yang lokasinya dipisahkan secara geografis (berjauhan) menjadi sebuah LAN virtual, PPTP merupakan protokol jaringan yang dikembangkan oleh Microsoft dan Cisco yang memungkinkan pengamanan transfer data dari *remoteclient* ke *server* pribadi instansi dengan membuat sebuah VPN melalui TCP/IP. [13]

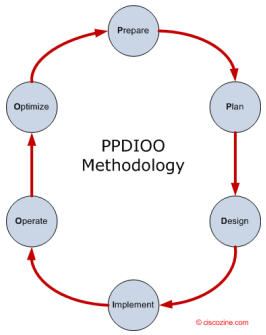
2.1.3 Firewall

Firewall atau tembok-api adalah sebuah sistem jaringan yang di desain untuk mengontrol transmisi data dimana firewall dapat mengijinkan atau memblok paket data yang masuk atau keluar berdasarkan kerentanan keamananya.[10]

Firewall dapat menyeleksi paket yang melaluinya, berdasarkan aturan atau *rules* yang dibuat oleh *admin*. Jadi, handal tidaknya sebuah *firewall* pada akhirnya sangat dipengaruhi oleh kemampuan/skill *admin* dalam membuat *rules*.[15]

2.2 Metodeologi Penelitian

Metode penelitian ini menggunakan metode *Prepare, Plan, Design, Implement, Operate, and Optimize* (PPDIOO) *Network Lifecycle* seperti pada Gambar 1 yang terdiri dari beberapa tahap, yaitu.



Gambar 1. Metode PPDIOO

1. *Prepare*
   Dalam model pengembangan sistem PPDIOO fase pertama dimulai dari fase *prepare*. Pada fase ini Menetapkan kebutuhan organisasi/institusi, strategi pengembangan jaringan, mengusulkan sebuah konsep arsitektur jaringan dengan mengidentifikasi pemanfaatan teknologi yang dapat memberikan dukungan rancangan hingga implementasi arsitektur terbaik.

2. *Plan*
   Untuk tahap selanjutnya adalah tahap *plan* yaitu Melibatkan identifikasi persyaratan jaringan awal berdasarkan sasaran, fasilitas, kebutuhan pengguna, dan sebagainya.

3. *Design*
   Dalam tahapan *design* merupakan dilakukannya perancangan berdasarkan analisis yang telah dikerjakan.

4. *Implement*
   Tahap selanjutnya adalah tahap implementasi, pada tahap ini dilakukannya penerapan berdasarkan analisis dan perancangan VPN.

5. *Operate*
   Dalam tahap ini adalah proses pengujian, dalam melakukan pengujian menggunakan parameter yang ditentukan terhadap VPN dan sejumlah komponen pendukung agar dipastikan sudah berjalan dengan baik dan benar dan sudah menjawab permasalahan yang telah dirumuskan.

6. *Optimize*
   Tahap ini merupakan tahap evaluasi dari sistem yang sudah berjalan agar sistem dapat berjalan dengan baik.

2.3 Hasil dan Pembahasan

2.3.1 Persiapan(*Prepare*)

Prepare merupakan tindakan untuk mengetahui dan memahami lebih jauh tentang objek yang akan diteliti. Tahapan ini menguraikan proses analisis implementasi dan perancangan VPN (*Virtual Private Network*) menggunakan Router Mikrotik. Sebelum dilakukan implementasi dan perancangan sistem, terlebih dahulu dilaksanakan analisis kebutuhan pokok sistem yang akan dibangun.

2.3.2 Perencanaan (*Plan*)

Plan merupakan suatu tahapan perencanaan yang bertujuan untuk mengetahui dan mengamati apa saja yang terlibat dalam suatu sistem. *Plan* bertujuan untuk mendapatkan pemahaman secara keseluruhan tentang sistem yang akan dibangun berdasarkan masukan dari pihak-pihak luar dan juga pengalaman analisis yang berkepentingan dengan sistem tersebut.

1. Analisis Masalah

Badan Pendapatan Daerah Provinsi Jawa Barat (BAPENDA JABAR) beralamat di Jl. Soekarno Hatta No.528, Sekejati, Buahbatu, Kota Bandung, Jawa Barat. BAPENDA JABAR merupakan organisasi perangkat daerah yang memiliki fungsi diantaranaya penyelenggaraan pendapatan dan pelayanan umum, meliputi kesekretariatan, perencanaan dan pengembangan pajak, non pajak, pengendalian dan pembinaan. BAPENDA JABAR mengelola kearsipan yang berkaitan dengan perpajakan diantaranya Pajak Kendaraan Bermotor (PKB) dan Bea Balik Nama Kendaraan Bermotor (BBNKB) dan memiliki 34 CPPD di setiap Kabupaten dan Kota diseluruh Jawa Barat. BAPENDA JABAR memiliki sistem aplikasi yang menangani kearsipan PKB DAN BBNKB yaitu Sistem Informasi Kearsipan (SIMKA) namun ditemukan beberapa kendala yang dialami diantaranya tidak stabilnya jaringan yang digunakan sehingga sulit membuka aplikasi SIMKA, dikarenakan masih banyaknya pegawai menggunakan layanan *internet* diluar pekerjaan yang mengakibatkan tidak tercapainya target pelaporan arsip PKB dan BBNKB. Aplikasi SIMKA diakses oleh 34 cabang dengan akses internet *public* yang mengakibatkan eksploitasi yang mengarah langsung terhadap *server* hal ini dapat mengancam data. Adapun kendala yang terjadi berdasarkan paparan diatas adalah sebagai berikut

a. Sulitnya mengakses aplikasi dikarenakan *bandwith* internet digunakan kepentingan diluar pekerjaan.
b. Masih mudahnya aplikasi Sistem Informasi Kearsipan (SIMKA) BAPENDA JABAR diakses secara umum yang bisa mengakibatkan eksploitasi terhadap aplikasi dan jaringan.

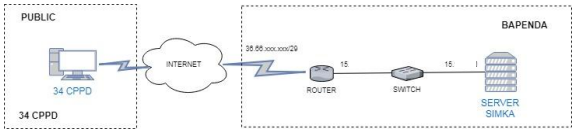
2. Analisis Jaringan

Analisis jaringan yang akan dibahas pada bagian ini meliputi Analisis Topologi Jaringan, Analisis *Subnetting*, Analisis *Internet Protocol*.

a. Analisis Topologi Jaringan

Berikut ini adalah topologi jaringan aplikasi SIMKA (Sistem Informasi Kearsipan) yang sedang berjalan di Badan Pendapatan Daerah Provinsi Jawa

Barat. Berikut topologi jaringan SIMKA pada Gambar 2.



Gambar 2. Sekema Jaringan Sekarang

b. Analisis *Subnetting*

Analisis *subnetting* adalah menganalisis teknik memecah suatu jaringan besar menjadi jaringan yang lebih kecil dengan cara mengorbankan *bit Host* ID pada *subnet mask* untuk dijadikan *network* ID baru. Teknik *subnetting* yang digunakan pada aplikasi SIMKA di (BAPENDA) Provinsi Jawa Barat. dapat dilihat pada Tabel 1.

Tabel 1. Analisis Subnetting

IP	Keterangan
36.66.xxx.xxx/29	Sebagai IP Publik
15.xxx.xxx.0/24	Sebagai Subnet digunakan Server

c. Analisis *Internet Protocol*

Dalam penelitian ini, analisis IP (*Internet Protocol*) pada aplikasi SIMKA di (BAPENDA) Provinsi Jawa Barat akan dibagi menjadi beberapa bagian yaitu IP *Public* dan IP *Private* yang digunakan oleh Badan Pendapatan Daerah (BAPENDA) Provinsi Jawa Barat. Dapat dilihat pada Tabel 2 dan 3.

Tabel 2. IP Public

Keterangan	IP
Address	36.66.xxx.xxx
Netmask	255.255.255.248
Keterangan	IP
Wildcard	0.0.0.7
Network	36.66.xxx.xxx
Broadcast	36.66.xxx.xxx
HostMin	36.66.xxx.xxx
HostMax	36.66.xxx.xxx

Tabel 3. IP Private

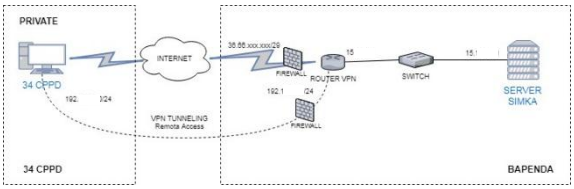
Keterangan	IP
Address	15.xxx.xxx.xxx
Netmask	255.255.255.0
Wildcard	0.0.0.255
Network	15.xxx.xxx.xxx
Broadcast	15.xxx.xxx.xxx
HostMin	15.xxx.xxx.xxx
HostMax	15.xxx.xxx.xxx
Server	15.xxx.xxx.xxx

2.3.3 Perancangan (*Design*)

Perancangan adalah suatu proses yang menggambarkan bagaimana suatu sistem dibangun untuk memenuhi kebutuhan pada fase analisis.

1. Perancangan Topologi Jaringan

Gambaran Topologi Pembangunan Jaringan VPN Di Badan Pendapatan Daerah (BAPENDA) Provinsi Jawa Barat. Berikut perancangan VPN secara global, akan diilustrasikan pada Gambar 3.



Gambar 3. Sekema Jaringan VPN

2. Perancangan VPN

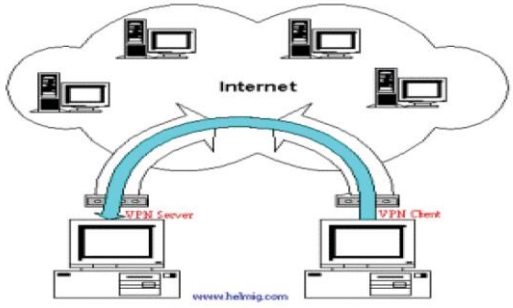
Dalam penelitian ini, perancangan VPN (*Virtual Private Network*) pada aplikasi SIMKA di (BAPENDA) Provinsi Jawa Barat akan dibagi menjadi beberapa bagian yaitu Jenis Implementasi dan Protokol yang digunakan oleh Badan Pendapatan Daerah (BAPENDA) Provinsi Jawa Barat.

a. Jenis Implementasi VPN

Dilihat dari jenis implementasi VPN yang ada, dalam penelitian ini termasuk dalam kategori *Remota Access* VPN.

b. Protokol Yang Digunakan VPN

Dalam penelitian ini protokol yang digunakan adalah *Point-to-Point Tunneling Protocol*. Komunikasi PPTP menggunkan protokol TCP port 1723, dan menggunkan IP Protokol 47 (GRE) untuk enkasulapsi paket datanya. PPTP mendukung *network security protocol* untuk keperluan otentikasi. Beberapa diantaranya yaitu PAP, CHAP, MSCHAP, MSCHAP2.



Gambar 4. Alur VPN PPTP Remota Access

4. Perancangan *Subnetting*

Badan Pendapatan Daerah (BAPENDA) Provinsi Jawa Barat juga mempunyai 34 cabang. Oleh karena itu, teknik *subnetting* digunakan untuk memudahkan pembagian jaringan VPN aplikasi SIMKA di

(BAPENDA) Provinsi Jawa Barat. dapat dilihat pada Tabel 4.

Tabel 4. Perancangan Subnetting

IP	Keterangan
36.66.xxx.xxx/29	Sebagai IP Publik
15.xxx.xxx.xxx/24	Sebagai Subnet digunakan Server
192.xxx.xxx.0/24	Sebagai Subnet Local Addres VPN
192.xxx.xxx.0/24	Sebagai Subnet Remote Address VPN

5. Perancangan IP(*Internet Protocol)*

Dalam penelitian ini, perancangan IP (*Internet Protocol*) pada aplikasi SIMKA di (BAPENDA) Provinsi Jawa Barat akan dibagi menjadi beberapa bagian yaitu IP *Public* dan IP *Private* yang digunakan oleh Badan Pendapatan Daerah (BAPENDA) Provinsi Jawa Barat.

a. IP *Public*

Perancangan IP *Public* yang digunakan pada aplikasi SIMKA di (BAPENDA) Provinsi Jawa Barat dapat dilihat pada Tabel 5.

Tabel 5. Perancangan IP Public

Keterangan	IP
Address	36.66.xxx.xxx
Netmask	255.255.255.248
Keterangan	IP
Wildcard	0.0.0.7
Network	36.66.xxx.xxx
Broadcast	36.66.xxx.xxx
HostMin	36.66.xxx.xxx
HostMax	36.66.xxx.xxx

b. IP *Private*

Perancangan IP *private* yang digunkan pada aplikasi SIMKA di (BAPENDA) Provinsi Jawa Barat dapat dilihat pada Tabel 6 , Tabel 7 dan Tabel 8.

Tabel 6. Perancangan IP Private Server

Keterangan	IP
Address	15.xxx.xxx.xxx
Netmask	255.255.255.0
Wildcard	0.0.0.255
Network	15.xxx.xxx.xxx
Broadcast	15.xxx.xxx.xxx
HostMin	15.xxx.xxx.xxx
HostMax	15.xxx.xxx.xxx
Server	15.xxx.xxx.xxx

Tabel 7. Perancangan IP Private Local Address VPN

Keterangan	IP
Address	192.xxx.xxx.0
Netmask	255.255.255.0
Wildcard	0.0.0.255
Network	192.xxx.xxx.xxx
Broadcast	192.xxx.xxx.xxx
HostMin	192.xxx.xxx.xxx
HostMax	192.xxx.xxx.xxx

Tabel 8. Perancangan IP Private Remote Address VPN

Keterangan	IP
Address	192.xxx.xxx.xxx
Netmask	255.255.255.0
Wildcard	0.0.0.255
Network	192.xxx.xxx.xxx
Broadcast	192.xxx.xxx.xxx
HostMin	192.xxx.xxx.xxx
HostMax	192.xxx.xxx.xxx

6. Perancangan *Firewall*

Firewall berfungsi meningkatkan keamanan jaringan dengan cara menentukan paket data apa saja yang bisa masuk maupun keluar dari jaringan tersebut. Untuk menentukan paket mana yang akan diterima (*accept*) atau dibuang (*drop*), *firewall* akan memerikasa *header* dari sebuah IP paket.

Untuk memberi keamanan yang lebih dari VPN maka dibuatlah *Filter Rule*, sebagai berikut.

a. Membangun *Filter Rules* Jalur Tunnel PPTP

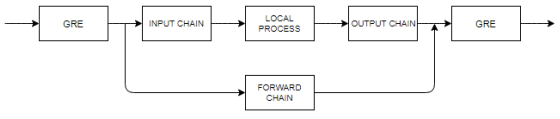
Dalam tahap ini dibentuk sebuah jalur tunnel protokol PPTP yaitu port 1723 dan prtokol TCP. Dimana terbentuknya *tunnel private* didalam jaringan *public* antara *client* dan *server*.



Gambar 5. Alur Firewall Tunnel PPTP

b. Membangun Filter Rules Enkripsi dan encapsulation pada paket data

Dalam tahap ini dilakukanya enkripsi dan *encapsulation* pada paket data di dalam *tunnel* yang terbentuk antara *server* dengan *client* ataupun *client* dengan *server* dengan menggunkan protokol GRE.



Gambar 6. Alur Firewall Enkripsi dan Encapsulation

c. Menampilkan Pesan *Request Timed Out.*

Filter rules ini memblok paket data dengan prtokol ICMP yang berasal dari WAN masuk ke *router* dan menampilkan pesan *Request Timed Out* kepada pengirim paket.



Gambar 7. Filter Rules Drop ICMP WAN

2.3.4 Implementasi (*Implementation*)

Implementasi sistem jaringan merupakan tahapan penerjemahan perancangan jaringan berdasarkan hasil analisis serta penerapan kebutuhan pada keadaan yang sebenarnya.

1. Implementasi Konfigurasi VPN dan Firewall

Konfigurasi VPN dilakukan dengan menggunakan mikrotik, mikrotik yang digunakan adalah routerboard 2011uias-rm, dimana Konfigurasi VPN menggunkan Winbox sebagai software remote. Berikut implementasi konfigurasi VPN dan *firewall* pada mikrotik routerboard 2011uias-rm dapat dilihat pada Tabel 9.

Tabel 9. Implementasi Konfigurasi VPN dan Firewall

Nama	**Keterangan**
Konfigurasi Profile	Konfigurasi profile digunakan untuk membuat set DNS.
Konfigurasi PPTP Server	Konfigurasi PPTP Server digunakan untuk membuat VPN menggunkan protocol PPTP.
Konfigurasi Akun	Konfigurasi Akun digunakan untuk membuat username dan password bagi user pengguna VPN.
Konfigurasi Filter Rules TCP PPTP In	Konfigurasi Filter Rules TCP PPTP In digunakan untuk mengizinkan paket data yang masuk kedalam router berupa paket TCP yang mengunkan port 1723.
Konfigurasi Filter Rules GRE PPTP Out	Konfigurasi Filter Rules TCP PPTP Out digunakan untuk mengizinkan paket data yang keluar dari router berupa protokol TCP.
Konfigurasi Filter Rules GRE PPTP In	Konfigurasi Filter Rules GRE PPTP In digunakan untuk mengizinkan paket data yang masuk kedalam router berupa Protokol GRE.
Konfigurasi Filter Rules GRE PPTP Out	Konfigurasi Filter Rules GRE PPTP Out digunakan untuk mengizinkan paket data yang keluar dari router berupa Protokol GRE.
Konfigurasi Filter Rules GRE PPTP Forward	Konfigurasi Filter Rules GRE PPTP Forward digunakan untuk mengawasi paket data yang melalui router berupa Protokol GRE.
Konfigurasi Filter Rules ICMP	Konfigurasi Filter Rules ICMP digunakan untuk memblok paket data yang menuju router berupa Protokol ICMP.
Konfigurasi Filter Rules Drop Access	Konfigurasi Filter Rules Drop Access digunakan untuk memblok paket data yang menuju router.
Konfigurasi NAT Masqurade Server	Konfigurasi NAT Masqurade Server digunakan untuk memberi akses internet terhadap server.
Konfigurasi NAT Masqurade	Konfigurasi NAT Masqurade VPN digunakan untuk mengarahkan seluruh akses terhadap ppp.
Konfigurasi WEB Proxy HTTP	Konfigurasi WEB Proxy HTTP digunakan untuk mengarahkan seluruh akses port 80 ke port 3192.
Konfigurasi WEB Proxy HTTPS	Konfigurasi WEB Proxy HTTPS digunakan untuk mengarahkan seluruh akses port 443 ke port 3192.
Konfigurasi DNS Proxy UDP	Konfigurasi DNS Proxy UDP digunakan untuk mengarahkan seluruh akses protokol UDP dengan port 53 ke DNS Lokal.
Konfigurasi DNS Proxy TCP	Konfigurasi DNS Proxy TCP digunakan untuk mengarahkan seluruh akses protokol TCP dengan port 53 ke DNS Lokal.

2.3.5 *Operate*

Operate merupakan hal terpenting yang bertujuan untuk menemukan kesalahan atau kekurangan pada sistem jaringan yang diuji. Pengujian sistem dimaksud untuk mengetahui kinerja sistem yang telah dibuat sesuai dengan tujuan perancangan sistem.

1. Pengujian Sistem

Pada tahap pengujian sistem VPN di Badan Pendapatan Daerah (BAPENDA) Provinsi Jawa Barat, akan diuji untuk menemukan kesalahan-kesalahan dan kekurangan-kekurangan pada jaringan yang dibangun. Untuk pengujian menggunkan pengujian *balckbox*.

a. Sekenario Pengujian

Pada skenario pengujian difokuskan pada kesesuaian perancangan dan performasi dari VPN. Skenario pengujian dapat dilihat pada Tabel 10.

Tabel 14. Sekenario Pengujian VPN

Nama Pengujian	Sekenrio Pengujian
Pengkoneksian VPN	Memilih tipe dial up koneksi VPN
	Memilih tipe koneksi VPN
	Mengisi alamat address dan nama dial up
	Memasukkan username dan password akun VPN
	Memanggil DNS Server pada browser berupa simka.local
Ping Server	Membuka command prompt
	Melakukan ping terhadap IP Server
	Melakukan ping terhadap DNS Server
	Melakukan ping terhdap DNS google
	Melakukan ping terhadap domain www.google.com
Ping Router	Membuka command prompt
	Melakukan ping terhadap IP address 36.66.xxx.xxx
Keamanan VPN	Membuka aplikasi simka
	Mengisi username dan password
	Melakukan login
	Melakukan input data
	Membaca proses aksi fungsi dengan aplikasi wireshark

b. Hasil Pengujian

Pengujian VPN di Badan Pendapatan Daerah (BAPENDA) Provinsi Jawa Barat terbagi menjadi beberapa tahapan, hasil pengujian VPN dapat dilihat pada Tabel 11.

Tabel 11. Sekenario Pengujian VPN

Nama Pengujian	**Sekenrio Pengujian**	**Hasil Yang Diharapkan**	Hasil Pengujian
Pengkoneksian VPN	Memilih tipe dial up koneksi VPN	Muncul tipe koneksi	[√] diterima [ ] ditolak
	Memilih tipe koneksi VPN	Muncul tampilan pengisian alamat address	[√] diterima [ ] ditolak
	Mengisi alamat address dan nama dial up	Muncul tampilan pengisian username dan password	[√] diterima [ ] ditolak
	Memasukkan username dan password akun VPN	Dapat terkoneksi tehadap VPN	[√] diterima [ ] ditolak
	Memanggil DNS Server pada browser berupa simka.local	Muncul tampilan login aplikasi simka	[√] diterima [ ] ditolak
Ping Server	Membuka command prompt	Muncul Command Prompt	[√] diterima [ ] ditolak
	Melakukan ping terhadap IP Server	Memunculkan tampilan reply	[√] diterima [ ] ditolak
	Melakukan ping terhadap DNS Server	Memunculkan tampilan reply	[√] diterima [ ] ditolak
	Melakukan ping terhdap DNS google	Memunculkan tampilan request time out	[√] diterima [ ] ditolak
	Melakukan ping terhadap domain www.google.com	Memunculkan tampilan tidak dapat meneumkan host	[√] diterima [ ] ditolak
Ping Router	Membuka command prompt	Muncul Command Prompt	[√] diterima [ ] ditolak
	Melakukan ping	Memunculkan	[√] diterima [ ] ditolak

	terhadap IP address 36.66.xxx.xxxx	tampilan request time out	
Keamanan VPN	Membuka aplikasi simka	Muncul tampilan login aplikasi simka	[√] diterima [ ] ditolak
	Mengisi username dan password	Muncul tampilan dashboard simka	[√] diterima [ ] ditolak
	Melakukan login	Dapat tersimpan data scan	[√] diterima [ ] ditolak
	Melakukan input data	Proses login dan input data scan dapat ter enkripsi	[√] diterima [ ] ditolak
	Membaca proses aksi fungsi dengan aplikasi wireshark	Hasil Yang Diharapkan	[√] diterima [ ] ditolak

3. PENUTUP

Kesimpulan dan saran ini berisi hasil-hasil yang diperoleh setelah dilakukan analisis, desain, dan implementasi dari perancangan jaringan VPN yang dibangun dan telah dikembangkan, serta saran yang akan memberikan catatan penting dan kemungkinan perbaikan yang perlu dilakukan untuk pengembangan Jarinagan VPN selanjutnya.

3.1 Kesimpulan

Berdasarkan hasil pembahasan pada bab sebelumnya, kesimpulan yang didapat dari proses analisis, perancangan, dan implementasi Jaringan VPN adalah pembangunan jaringan VPN di Badan Pendapatan Daerah (BAPENDA) Provinsi Jawa Barat pada aplikasi SIMKA dapat membantu memaksimalkan akses aplikasi SIMKA dan dapat meminimalisir eksploitasi terhadap server SIMKA.

3.1 Saran

Adapaun saran Pada pembangunan jaringan VPN di BAPENDA JABAR adalah kedepanaya bisa menggunakan sistem yang dapat meremote komputer pada setiap cabang tanpa perlu ketempat cabang dan kedepanaya bisa menggunakan sistem yang lebih aman dan lebih maksimal dalam hal transmisi paket data.

DAFTAR PUSTAKA

[1] BAPENDA JABAR, *Sejarah BAPENDA*, https://bapenda.jabarprov.go.id/sejarah-bapenda, 9 April 2018 20.25

[2] BAPENDA JABAR, *Visi dan Misi*, https://bapenda.jabarprov.go.id/visi-dan-misi, 9 April 2018 20.30

[3] BAPENDA JABAR, *Program Kerja*, https://bapenda.jabarprov.go.id/program-kerja, 9 April 2018 20.40

[4] BAPENDA JABAR, *Tugas Pokok dan Fungsi*, https://bapenda.jabarprov.go.id/tugas-pokok-dan-fungsi, 9 April 2018 20.45

[5] BAPENDA JABAR, *Struktur Organisasi*, https://bapenda.jabarprov.go.id/struktur-organisasi, 9 April 2018 20.55

[6] Heru Supriyono, Jisnu Adi Wijaya dan Agus Supardi, "Penerapan Jaringan Virtual Private Network Untuk Keamanan Komunikasi Data Bagi Pt. Mega Tirta Alami," Universitas Muhammadiyah Surakarta, 2013.

[7] Dhio Saputra, "Implementasi Virtual Private Network Pada Sistem Informasi Pengelolaan Keuangan Daerah Pemerintah Provinsi Riau," Universitas Putra Indonesia YPTK Padang, 2016.

[8] Hendara Supendar, "Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik," AMIK BSI Jakarta, 2016.

[9] Prihatin Oktivasari , dan Andri Budhi Utomo, "Analisa Virtual Private Network Menggunakan Openvpn Dan Point To Point Tunneling Protocol," Politeknik Negeri Jakarta, 2016.

[10] Alfin Hikmaturokhman, Adnan Purwanto, dan Rendy Munadi, "Analisis Perancangan Dan Implementasi Firewall danTraffic Filtering Menggunakan Cisco Router," Pasca Sarjana IT Telkom Bandung, 2010.

[11] I Gusti Komang Oka Mardiyana, "Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali," STMIK STIKOM Bali, 2015.

[12] Yesi Mardiana, dan Julidian Sahputra, " Analisa Performansi Protokol TCP, UDP dan SCTP Pada Lalu Lintas Multimedia," Universitas Dehasen Bengkulu, 2017.

[13] I. Sofana, CISCO CCNA dan Jaringan Komputer, Bandung: Informatika Bandung, 2010.

[14] Balaji Sivasubramanian, Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) Network Lifecycle, http://www.ciscopress.com, 8 April 2018 20.30

[15] I. Sofana, Jaringan Komputer Berbasis Mikrotik, Bandung: Informatika Bandung, 2017.

[16] R. Towidjojo, MIKROTIK KUNG FU KITAB 2, Bandung : Jasakom, 2016.

[17] wirelessmode.net, *Memahami Winbox dan Fungsinya*, 25 Mei 2018 20.55