

IMPLEMENTASI DAN KONFIGURASI VPN SERVER MENGUNAKAN JUNIPER

Kurniawan¹, Tengku Musri, M.Kom², Lipantri Mashur Gultom, M.Kom³
Program Studi Teknik Informatika

Politeknik Negeri Bengkalis, Jl. Bathin Alam, Sei. Alam, Bengkalis
Wawan.webhost@gmail.com¹, musri@polbeng.ac.id², Lipantri@polbeng.ac.id³

Abstract

The internet network in Bengkalis district has been evenly distributed in every sub-district and offices in Bengkalis district. And one of them is at the population and civil registration office (DUKCAPIL). Currently the internet network in this office still uses Mikotik in daily work operations and for VPN Servers still using mikrotik, but over time the use of data and information is very high, causing several security problems in the network because that is to overcome these security problems need a VPN Server. Research and design of a VPN Server using Juniper and will be applied in the Bengkalis Regency Population and Civil Registry Office is a literature study, and a field survey to obtain valid data about the Civil Service Server.

Keywords: Juniper, VPN Server, Configuration

1. PENDAHULUAN

Perkembangan teknologi informasi telah membawa dampak dalam kehidupan. Sejak diketemukannya komputer pada tahun 1955, peradaban dunia telah memasuki era informasi. Teknologi informasi dengan komputer sebagai motor penggerak telah mengubah segalanya. Pemrosesan informasi berbasis komputer mulai dikenal orang dan hingga saat ini sudah banyak *software* yang dapat digunakan orang sebagai alat pengolah data untuk menghasilkan informasi. Perkembangan teknologi dan komunikasi setiap tahunnya sangat berkembang pesat dan sangat cepat tujuan untuk memberikan kemudahan untuk menghasilkan informasi yang dapat dipercaya, relevan, tepat waktu, lengkap, dapat dipahami, dan teruji. Perkembangan teknologi yang ada sekarang tidak terlepas dari jaringan komputer. Dimana kebutuhan jaringan tidak hanya untuk satu orang saja bahkan masyarakat luas pun sangat membutuhkan jaringan, selain itu jaringan menjadi salah satu kebutuhan instansi pemerintahan Bengkalis untuk memperlancar komunikasi dan informasi. Dengan adanya jaringan pertukaran informasi dan data menjadi lebih cepat. Karena perkembangan teknologi semakin pesat banyak protocol keamanan yang sudah dikembangkan namun, ada saja orang-orang atau kelompok tertentu yang dapat menembus keamanan jaringan sehingga berakibat pencurian data dan penyerangan terhadap server. Seperti di kantor dinas Kependudukan dan Catatan Sipil (DUKCAPIL) kabupaten Bengkalis, begitu banyak informasi yang bisa dicuri atau diserang oleh pihak yang tidak bertanggung jawab tentu saja itu sangat merugikan dinas capil. Oleh karena itu dibutuhkan sebuah cara atau metode yang dapat mengurangi bahkan mencegah pencurian atau peretasan informasi yang dilakukan pada jaringan internet. Virtual Private Network (VPN) merupakan salah satu cara untuk melindungi pertukaran data dan informasi yang diakses atau dilakukan melalui jaringan internet. Seperti menggunakan protocol Layer 2 Tunnel Protokol (L2TP) dapat membuat komunikasi antar beberapa pengguna melalui jaringan internet.

Sedangkan Jaringan internet di kabupaten Bengkalis ini sudah merata disetiap kecamatan dan dinas-dinas yang terdapat di kabupaten Bengkalis. Dan salah satunya di kantor dinas kependudukan dan catatan sipil , sebagai tempat untuk mengurus berbagai macam surat yang berhubungan dengan catatan

sipil seperti akta kelahiran, E-KTP dan lain sebagainya. Karena itu dibutuhkan sebuah VPN server untuk mengamankan pertukaran data dan digunakan sebuah alat yaitu Juniper Firewall sebagai VPN Servernya, yang di implementasi dikantor tersebut. Tujuan dari penelitian ini adalah Mengimplementasikan VPN Server L2TP agar bisa akses jaringan dan komputer kantor dinas dari mana saja selama terhubung internet. Mengimplementasikan VPN Server L2TP di Juniper Firewall. Mencegah penyusupan dari pihak luar dengan menggunakan vpn server L2TP. Manfaat yang didapat dalam penelitian ini adalah diharapkan bisa memberikan sebuah revolusi dalam hal kemananan server dan data yang berada di server Dinas Kependudukan dan Catatan Sipil Kabupaten Bengkalis dan dapat dimanfaatkan sebagaimana semestinya.

2. TINJAUAN PUSTAKA

- a. Ayu,dkk (2020) dalam penelitiannya pada perancangan jaringan *Virtual Private Network* berbasis *IP SECURITY* menggunakan *Router Mikrotik*. Perancangan jaringan *VPN* dengan memanfaatkan *IPsec* dapat membuat jaringan *VPN* menjadi lebih aman hal ini di disebabkan oleh tingkat keamanan yang lebih baik dari adanya enkripsi data pada fasilitas yang diberikan oleh *IPsec*, maka dengan demikian jaringan *VPN* dapat berjalan dengan baik.
- b. Varianto dan Badrul (2015) dalam penelitiannya pada implementasi *virtual network* dan *proxy server* menggunakan *clear os* pada PT.VALDO INTERNATIONAL. Salah satu cara untuk membangun keamanan komunikasi data dalam jaringan internet adalah dengan menggunakan jaringan *Virtual Private Network (VPN)*. Teknologi *Virtual Private Network (VPN)* memungkinkan setiap user dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada.
- c. Permana, Widiyasono, dan Rahmatulloh (2020) dalam penelitiannya pada perbandingan algoritma pada *Virtual Private Network IPSEC* terhadap kecepatan data transfer. Algoritma yang paling lambat dalam melakukan transfer data pada *VPN* adalah *AES 192*. Algoritma tersebut kalah pada file ke-0 dengan kecepatan *12,008 seconds* serta dengan rasio *34,78%* lebih lambat, pada file ke-2 dengan kecepatan *75,019 seconds* serta dengan rasio *27,89%* lebih lambat, pada proses *download* dan pada file ke-4 dengan kecepatan *36,237 seconds* serta dengan rasio *18,37%* lebih lambat. Sedangkan pada proses *upload* *AES 192* kalah pada file ke-0 dengan kecepatan *12,423 seconds* serta dengan rasio *35,89%* lebih lambat, file ke-2 dengan kecepatan *76,345 seconds* serta dengan rasio *22,68%* lebih lambat dan pada file ke-4 dengan kecepatan *37,398 seconds* serta dengan rasio *21,83%* lebih lambat.
- d. Supendar (2016) dalam penelitiannya pada Implementasi Remote Site Pada *Virtual Private Network* Berbasis *Mikrotik* Dengan menggunakan *VPN* dapat mempermudah dan efeisiensi waktu dalam pertukarandata hanya dengan mengaktifkan *VPN client*. *VPN* dengan protokol *PPTP* terbukti memberikankeamanan pada data dan konektivitas jaringan. Hal ini ditunjukkan pada saat *VPN client* melakukan *log in* ke *VPN server* akan terdapat autentikasi *username* dan *password*, terdapat juga enkapsulasi dan enkripsi data serta integritas data yang telah terbukti pada simulasinya.

Alat yang digunakan dalam proses perancangan *VPN Server* menggunakan *juniper* adalah perangkat keras. Adapun perangkat kerasnya adalah:

1. Komputer digunakan sebagai client dan juga sebagai operator yang bertugas mengakses server, dan juga digunakan untuk melakukan konfigurasi ke Juniper.



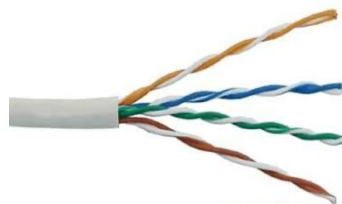
Gambar 2.1 Komputer.

2. Juniper digunakan untuk mensetting VPN Server, bahkan banyak lagi fitur yang terdapat di Juniper ini, seperti keamanan dan lain sebagainya. Juniper digunakan yaitu Juniper SSG 20. Dengan beberapa fitur yang dipakai seperti VPN IKE, L2TP dan lain sebagainya, dan disini memakai Fitur L2TP untuk VPN Servernya.



Gambar 2.2 Juniper

3. Kabel UTP UTP berguna untuk mendukung konektivitas berbagai perangkat. UTP merupakan jenis kabel yang paling umum yang sering digunakan di dalam jaringan lokal (LAN). Kabel UTP merupakan salah satu perangkat keras komputer berupa kabel yang digunakan sebagai penghubung atau transmisi data pada sebuah jaringan.



Gambar 2.3 Kabel UTP.

4. *Connector* (RG 45) berfungsi sebagai penghubung kabel *ethernet* yang biasanya dipakai untuk jaringan. Konektor tersebut biasanya mempunyai ujung kabel UTP atau *unshielded twisted pair* yang mampu menghubungkannya ke pemancar penerima atau transceiver.



Gambar 2.4 connector rg45.

5. Server di Dinas Capil memiliki fungsi yaitu menyimpan data-data penduduk seperti data kelahiran, KTP dan data-data mengenai penduduk.



Gambar 2.5 Server.

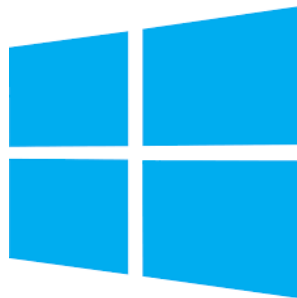
2.2.12 Software

6. menggunakan web browser untuk mengakses juniper dengan memasukkan *IP Address* ke web browsernya kita bisa mengakses Router Juniper dengan menggunakan sistem GUI.



Gambar 2.6 logo google firefox.

7. Windows sebagai system operasi yang dipakai oleh komputer *client*, *operator*, atau sebagai *Server*. Dengan Operasi sistem Windows baik windows 7 maupun windows 8.



Gambar 2.7 Windows.

METODE PENELITIAN

Data yang digunakan dalam proses perancangan VPN Server menggunakan Juniper adalah jurnal atau penelitian sebelumnya yang dilakukan peneliti sebelumnya yang digunakan sebagai referensi dalam penelitian ini. Kemudian penulis harus mengetahui sistem

Dalam perancangan VPN Server menggunakan Juniper digunakan alat dan bahan untuk mendukung berjalannya perancangan perancangan VPN Server menggunakan Juniper adalah perangkat keras dan perangkat lunak.

Spesifikasi perangkat keras yang digunakan adalah :

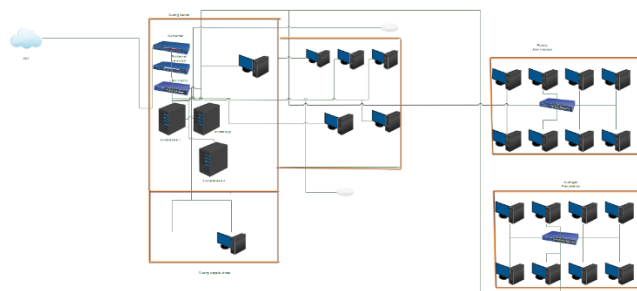
Laptop dengan spesifikasi prosesor intel(R) Celeron(R) 1000 CPU@ 1,80GHz (2 CPUs), ~1,8GHz, (RAM) 4,00 GB berfungsi untuk melakukan konfigurasi. Perancangan sistem merupakan tahapan setelah melakukan analisis sistem, mendapatkan gambaran dengan jelas tentang apa yang peneliti kerjakan, dan bagaimana membentuk sistem tersebut dan bagaimana sistem yang akan diajukan oleh peneliti.

Perancangan sistem adalah suatu fase dimana *IP* diperlukan suatu keahlian perancangan untuk elemen-elemen komputer yang menggunakan sistem yaitu pemilihan dan program komputer untuk sistem baru.

Pertama dengan mengalisa sistem yang sedang di dinas, dimana VPN Servernya menggunakan router utama jadi mulai dari routing, firewall, dhcp dan lain-lain ditugaskan di router utama dan router kedua, sehingga memberatkan routernya.

Analisa Sistem yang sedang berjalan.

Menurut hasil analisa sistem dari VPN Server yang gunakan dapat dilihat dari gambar 3.1

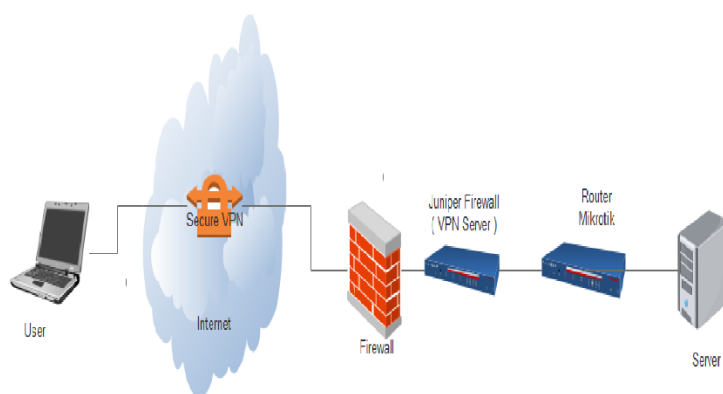


Gambar 3.1 Topologi Sebelum

Dari topologi diatas sistem sebelumnya memakai Mikrotik sebagai VPN Servernya, dimana menggunakan router Mikrotik sebagai VPN Servernya, yang sudah terhubung di dinas Kependudukan dan Catatan Sipil Kabupaten Bengkalis.dengan menggunakan Router

Mikrotik sebagai router utama mendapatkan *IP Address* dan akses jaringan dari ISP dan membagikan jaringan ke router kedua. kemudian dari router kedua membagi jaringan ke Switch yang terhubung ke ruangan-ruangan yang terdapat di kantor dinas capil. Disini VPN Servernya menggunakan Mikrotik router board, dan VPN Server yang menggunakan Mikrotik ini masih bisa dibobol Servernya walaupun operator mengakses menggunakan VPN Server yang sudah diterapkan di kantor dinas.

Cara kerja dari perancangan yang akan dibuat disetting menggunakan *Web browser*. dari web browser masuk ke sistem Juniper firewallnya dengan masuk ke sistemnya, kemudian merubah *IP Address* yang terhubung ke Internet dengan *IP Publik* yang diberikan oleh pihak admin, kemudian di konfigurasinya VPN Servernya, lalu dipasang di Sever Capil dari router utama menuju ke Juniper Firewall sebagai keamanannya kemudian dilanjutkan ke internet. Dengan mengkonfigurasi disisi client dan disisi Servernya, seperti memberi hak akses serta kunci untuk masuk secara aman dari internet dengan menggunakan *IP Publik* masuk ke sistem keamanan melewati Juniper nya terlebih dahulu kemudian data nya dilanjutkan menuju Router utama dan akhirnya dilanjutkan ke jaringan kantor, di Juniper VPN Sever yang di konfigurasi pada bagian menu VPN lalu kita bisa memilih VPN yang akan kita konfigurasi, seperti Layer 2 Tunnel Protokol (L2TP) sebagai VPN Servernya. Setelah itu disisi clientnya pun di konfigurasi dengan jenis VPN yang sama serta memasukkan username dan password yang telah diberikan oleh vpn Servernya. Sehingga yang sudah terdaftar di Juniper nya yang bisa memakai VPN Servernya, seperti mengakses jaringan kantor seperti mengakses webServer atau database Server, jadi hanya yang diberikan hak akses yang bisa masuk atau mengakses ke jaringan lokal dinas capil. Ketika akan mau masuk kedalam jaringan lokal kantor maka yang diminta adalah username dan password jika sesuai dengan yang ada pada Juniper maka user boleh lewat sedangkan yang tidak memilikinya tidak masuk, walaupun dengan cara memasukkan *IP Address* publik yang terdapat pada Juniper nya. Setelah itu baru dilanjutkan ke router utama sebelum ke Server.



Gambar 3.3 Topologi VPN Server.

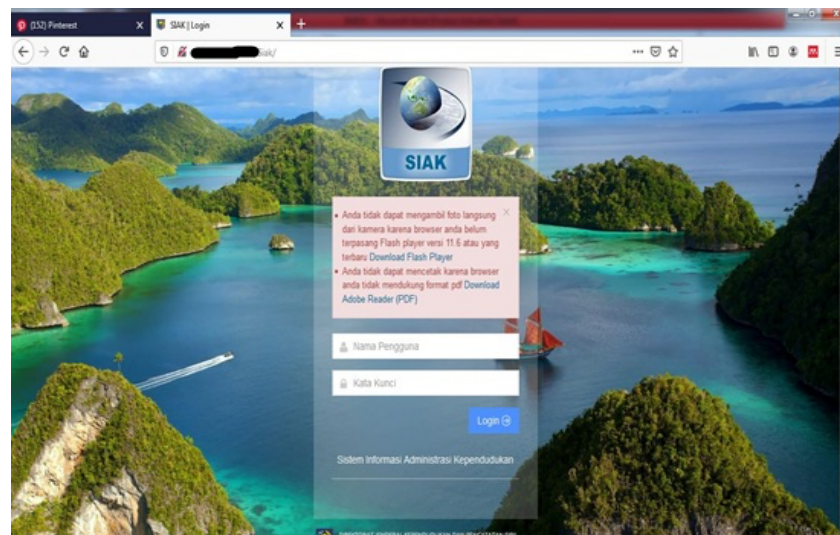
HASIL PENELITIAN DAN PEMBAHASAN

Hasil Implementasi ini adalah sebuah VPN Server yang akan diterapkan di Server dinas Kependudukan dan Catatan Sipil Kabupaten Bengkalis. Sistem ini dibuat agar dapat membantu pihak admin dalam mengelola Server baik dalam mengontrol Server maupun memantau Server jika sedang

berada diluar kantor. Dengan menggunakan VPN Server ini ip dari Server dapat dijadikan ip private sehingga pihak luar tidak bisa menggunakan ip sembarangan untuk mengakses server.

Dalam proses implementasi ini dilakukannya pengujian dengan 2 device yang berbeda yaitu pc/laptop dan mobile, dengan cara mengkonfigurasi di sisi client seperti memasukkan nama VPN lalu jenis VPN serta username dan password yang telah di berikan oleh pihak admin jaringan kepada user yang berhak menerimanya, dengan begitu kita bisa melihat apakah user tersebut sudah bisa menggunakan VPN Server yang berada di dinas Capil.

Untuk mengetahui hasil dari implementasi vpn server menggunakan juniper di Dinas Kependudukan dan Catatan Sipil Kabupaten Bengkalis yaitu dengan cara mengkonfigurasi dibagian *client* sehingga *client* dapat mengakses jaringan kantor seperti database ataupun *website* yang hanya bisa diakses secara lokal. Dengan cara memasukkan *username* dan *password* yang telah diberikan oleh pihak admin dan memasukkannya di sisi *client* apa bila *username* dan *password* sudah dimasukkan maka kita dapat mengakses jaringan kantor seperti *website* yang hanya bisa diakses secara lokal seperti dibawah ini:



Gambar 11 mengakses webserver.

Hasil dari implementasi dari VPN Server ini adalah dapat mengakses jaringan lokal kantor menggunakan internet. Dengan memasukkan ip publik kita dapat membuka *webserver* kantor dinas Capil.

KESIMPULAN DAN SARAN

Berdasarkan hasil implementasi dan konfigurasi vpn server menggunakan Juniper, dapat disimpulkan dari implementasi ini bahwa telah berhasil dilakukan di server dinas Capil dengan mengakses jaringan lokal yang berada di kantor dinas Capil menggunakan jaringan internet melalui perangkat *mobile*

phone dan juga *computer*. Sehingga pihak bersangkutan dapat mengambil data sewaktu-waktu dibutuhkan.

Adapun saran penulis mengenai implementasi dan konfigurasi vpn server menggunakan juniper ini adalah diharapkan kedepannya untuk peneliti selanjutnya bisa menambahkan beberapa fitur yang mungkin penulis belum bisa penuhi seperti melakukan pengujian dari sisi keamanannya dan juga dari sisi *bandwidth* yang digunakan di kantor dinas capil. Karena maraknya dari pihak yang tidak bertanggung jawab yang ingin merusak server maka dari itu diharapkan kepada peneliti selanjutnya untuk menambahkan fitur keamanan agar server dan data di dinas capil lebih aman.

DAFTAR PUSTAKA

- Ayu Purnama Sari, Sulistiyono, dan Naga Kemala, (2020). “ perancangan jaringan *Virtual Private Network* berbasis *IP SECURITY* menggunakan *Router Mikrotik*”. Jurnal PROSISKO Vol. 7 No.2. September 2020
- Eka Varianto dan Mohammad Badrul, (2015). “ implementasi *virtual network* dan proxy server menggunakan *clear os* pada PT.VALDO INTERNATIONAL”. VOL. 1 NO. 1 FEBRUARI 2015.
- Supendar (2016). “dalam penelitiannya pada Implementasi Remote Site Pada Virtual Private Network Berbasis Mikrotik” BINA INSANI ICT JOURNAL, Vol. 3, No.1, Juni 2016, 85 – 98.
- Permana, Widiyasono, dan Rahmatulloh (2020). “ perbandingan algoritma pada *Virtual Private Network IPSEC* terhadap kecepatan data transfer”. *Jurnal Sistem Informasi, Volume 9, Nomor 2, Mei 2020 : 259–273*.
- Dahnial (2019).”analisa perbandingan *Quality of servive* antara PPTP dan L2TP pada *Virtual private network* berbasis Router Mikrotik”. JURNAL ILMIAH INFORMATIKA GLOBAL VOLUME 10 No. 02 Desember 2019.
- Kaseger Arthur Farly, Xaverius B. N. Najoan dan Arie S. M. Lumenta (2017).” Perancangan dan Implementasi VPN Server dengan menggunakan protocol SSTP (*Secure Socket Tunneling Protokol*) studi kasus kampus Universitas Sam Ratulangi”. E-Journal Teknik Informatika Vol 11, No.1 (2017) Tekno.
- Rachmawan dan prihanto , ST.,M.Kom (2018) Perbandingan Protokol L2TP dan PPTP untuk membangun Jaringan Intranet Diatas VPN”. Jurnal Manajemen Informatika, Volume 8 Nomor 02 Tahun 2018, 53-57.
- Ikhwan dan Amalina (2017). “ Analisa Jaringan VPN Menggunakan PPTP dan L2TP”. *Jurnal Infotel Vol.9 No.3 Agustus 2017*.
- Larasati, Rizal, dan Nugroho (2015). “ Implementasi Remote Desktop Melalui VPN Berbasis IPsec pada Smarthphone dengan menggunakan Vyatta OS”. Jurnal Teknologi Informasi Vol. 2, No. 2, Mei 2015
- Supriyanto dan Suharyanto (2019). “ Perancangan jaringan VPN Menggunakan metode Point To Point Tunneling Protokol”. Jurnal Teknik Komputer, Vol V No.2 Agustus 2019 P-ISSN 2442-2436, E-ISSN: 2550-0120