

# **Optimalisasi Interkoneksi *Virtual Private Network* (Vpn) Dengan Menggunakan *Hardware Based* dan *Iix* (Indonesia *Internet Exchange*) Sebagai Alternatif Jaringan Skala Luas (Wan)**

Deris Stiawan & Dian Palupi Rini

Jurusan Sistem Komputer  
Fakultas Ilmu Komputer  
Universitas Sriwijaya  
[deris@ilkom.unsri.ac.id](mailto:deris@ilkom.unsri.ac.id),

Jurusan Teknik Informatika  
Fakultas Ilmu Komputer  
Universitas Sriwijaya  
[azzahra@yahoo.com](mailto:azzahra@yahoo.com)

## *Abstrak*

*Virtual Private Network (VPN) salah satu solusi yang bisa digunakan untuk interkoneksi jaringan skala luas (WAN), saat ini banyak para provider telcom menawarkan solusi VPN sebagai komunikasi data perusahaan bisnis untuk interkoneksi ke kantor-kantor cabangnya. Indonesia Internet Exchange (IIX) yang menginterkoneksi semua penyedia jasa internet (ISP) di Indonesia dalam satu jaringan yang terpusat secara lokal. Solusi interkoneksi VPN dapat menggunakan hardware based yang mempunyai kelebihan dibandingkan software based. Solusi VPN dan penggunaan Interkoneksi IIX dapat menjawab interkoneksi secara lokal ke jaringan intranet dengan aman namun melalui jaringan yang bisa diakses dengan mudah dan murah seperti jaringan Internet. IIX lebih murah dan bisa dioptimalkan pengalaman routingsnya selama digunakan untuk diwilayah layanan Indonesia. IIX akan memperpendek lompatan paket data, memperkecil latency waktu, dan meningkatkan penggunaan traffic content di Indonesia.*

*Kata Kunci :VPN, Perangkat Keras, ISP*

## *Abstract*

*Virtual Private Network ( VPN) one of a solution which can be used for the interconnections wide area network ( WAN), in this time a lot of all provider telco offer the solution VPN as communications of data of business company for the interconnections of to its office of branch. Indonesia of Internet Exchange ( IIX) which interconnection all Internet Service Provider (ISP) in indonesian in one network which centrally locally. VPN solution can use the hardware based having excess compared to by software based. Solution of VPN and use of IIX Interconnections can reply the locally Interconnection to network intranet safely. IIX efficient in routing address during used for the region of Indonesia service. IIX will*

- 
1. Deris Setiawan, S.Kom, M.T Assisten Ahli Fakultas Ilmu Komputer
  2. Dian Palupi Rini, S.Si, M.Kom Asisten Ahli Fakultas Ilmu Komputer

*cut short the jumping movement of data packet, reduced latency time, and improve the use of traffic content in Indonesia.*

**Kata kunci : Virtual Private Network, VPN, IIX, Hardware Based**

## 1. PENDAHULUAN

### 1.1 Latar Belakang

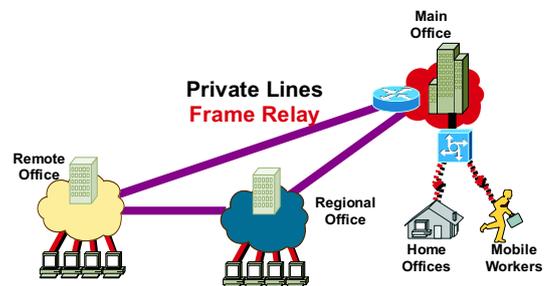
Jaringan komunikasi data yang terintegrasi saat ini sudah menjadi kebutuhan utama bagi sebuah institusi atau perusahaan bisnis, terutama perusahaan yang mempunyai banyak cabang di lokasi geografis yang berbeda dan juga untuk perusahaan yang kegiatan perkantornya menuntut seorang pegawai tidak hanya *behind the desk* saja, namun juga harus *mobile*. Oleh karena itu kemudahan untuk akses data antar kantor atau kekantor sangat diperlukan dimanapun dan kapanpun pegawai tersebut berada.

Kegiatan untuk komunikasi data langsung ke server suatu kantor, memerlukan suatu teknologi hardware dan dukungan teknis yang rumit sehingga hal ini akan menyebabkan pembiayaan menjadi mahal. Padahal kebutuhan koneksi data berupa sistem informasi yang terintegrasi saat ini sangat tinggi, dari sistem teknologi client server biasa sampai dengan implementasi sistem seperti *ERP*, *Supply Chain*, *CRM*, *E-business* dan sebagainya. Namun tidak semua perusahaan mempunyai anggaran yang banyak terutama untuk membiayai komunikasi data seperti sewa sirkuit, bandwidth dan biaya perbulan lainnya dari sebuah provider.

Selama ini penggunaan teknologi wide area network (WAN) menjadi salah satu solusi banyak perusahaan untuk komunikasi data. WAN adalah jaringan

komunikasi yang meliputi area geografis yang luas dan biasanya menggunakan fasilitas dari transmisi provider, seperti perusahaan telpon atau lainnya. Infrastruktur inilah yang nantinya menjadi penghubung antara kantor pusat ke cabang-cabang dan *telecommuters*. Namun ada beberapa hal yang harus diperhatikan dalam memilih solusi Infrastruktur jaringan komunikasi ini, diantaranya : Bandwidth, Teknologi, Skalability, Support IP Based, Easy Configuration & maintenance, Low Cost dan Security.

Menurut hasil penelitian dari infonetics dikatakan bahwa saat ini penggunaan Interkoneksi WAN meningkat 58 % pada kuartal pertama tahun 2007 dan kuartal pertama tahun 2008.



**Gambar 1. Topology Classic WAN**  
(sumber cisco.com)

Pada gambar 1 terlihat topology yang dahulu digunakan untuk mengkoneksikan banyak kantor cabang dan para pegawai yang mobile menggunakan infrastruktur penyedia jasa leased line, Frame relay, Dial-up atau menggunakan ATM, namun

karana ketidakseimbangan antara tingginya biaya yang harus dikeluarkan dengan rendahnya aspek teknisnya seperti bandwidth, protocol, interface, lastmiles, coverage area, jarak dan lain-lain, maka solusi WAN klasik ini mulai ditinggalkan.

Pertumbuhan jaringan internet di Indonesia, sekalipun masih dalam tahap awal dan belum memasyarakat seperti halnya di negara-negara maju, menunjukkan trend yang sangat positif. Potensi penggunaannya yang begitu besar dari penduduk Indonesia yang pada saat ini (Juli 1997) berjumlah sekitar 200 juta jiwa tidak dapat diabaikan begitu saja.

Koneksi ke internet dilakukan dengan menghubungkan suatu perangkat komunikasi ke *Internet Service Provider* (ISP), sedangkan ISP akan terkoneksi ke *Network Access Provider* (NAP) dan NAP terkoneksi ke jaringan tulang punggung (backbone) dunia yang terhubung lewat kabel Fiber Optic bawah laut, jaringan nirkabel atau jaringan komunikasi satelite. Perkumpulan *Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)* membuat interkoneksi peering nasional agar pengalaman routing di Internet menjadi lebih cepat dan tidak membuang traffic internet ke Internet global / internasional. Interkoneksi ini disebut **IIX** atau **Indonesia Internet Exchange**, yang menghubungkan semua ISP (*internet Service Provider*), NAP (*Network Access Provider*) dan Telco lainnya kedalam jaringan yang terpusat dan saling terhubung. Interkoneksi IIX ini berujung di Gedung Cyber Jl. Kuningan Barat No 8 Jakarta. Jadi dengan interkoneksi peering ini maka koneksi antara ISP atau NAP di Indonesia tidak perlu pengalaman atau routing ke luar negeri lagi.

Solusi VPN dan penggunaan Interkoneksi IIX, dapat menjadi satu alternatif interkoneksi, dimana bisa terkoneksi secara lokal ke jaringan intranet kantor dengan aman namun melalui jaringan yang bisa diakses dengan mudah seperti jaringan Internet, dengan menggunakan interkoneksi jaringan IIX yang cenderung lebih murah dan bisa dioptimalkan pengalaman routingsnya selama digunakan untuk diwilayah layanan Indonesia. IIX akan memperpendek lompatan paket data, memperkecil latency waktu, dan meningkatkan penggunaan traffic content di Indonesia.

Kegunaan yang paling besar saat ini menggunakan traffic IIX adalah pengembang *content games* lokal atau pengembang games dunia yang meletakkan servernya di jaringan IIX. Akibatnya banyak para pengusaha warnet berlomba untuk terkoneksi ke jaringan IIX ini. Padahal optimalisasi jaringan IIX dapat dilakukan dengan memanfaatkan untuk interkoneksi lain, yang salah satunya dapat melewati dan mengintegrasikan perusahaan-perusahaan atau institusi bisnis ke kantor-lantor cabang lainnya.

## 1.2 Tujuan Penelitian

Tujuan dari penelitian ini adalah menganalisa dan kajian optimalisasi interkoneksi jaringan skala luas (WAN) dengan menggunakan VPN memanfaatkan interkoneksi IIX.

## 1.3 Manfaat Penelitian

Manfaat dari penelitian ini adalah memberikan gambaran tentang alternatif lain yang dapat menjadi solusi untuk interkoneksi jaringan skala luas (WAN).

#### 1.4 Metode Penelitian

Langkah – langkah yang dilakukan dalam penelitian ini adalah sebagai berikut :

1. Analisa kebutuhan jaringan WAN pada sebuah perusahaan melalui studi pustaka dan literatur.
2. Perancangan dan alternatif solusi
3. Evaluasi hasil

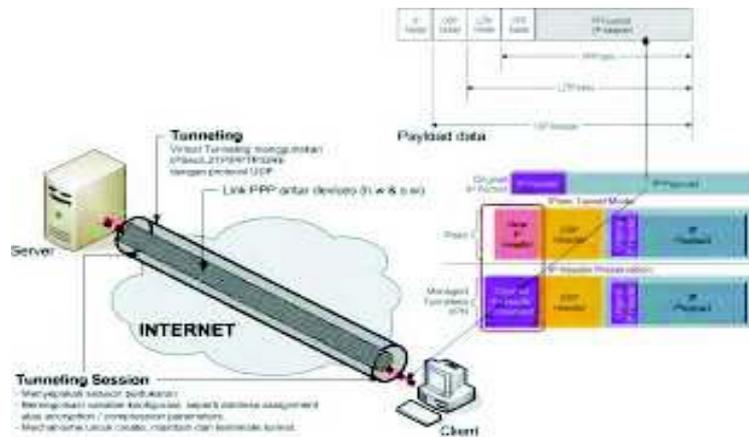
## 2. TINJAUAN PUSTAKA

### 2.1 Interkoneksi

Internet, adalah sebuah sistem yang besar dan banyak yang menghubungkan jutaan

sistem dan terdiri dari *multi-protocol*, berbagai macam media, jaringan global dunia yang dahulu dikembangkan oleh Departemen Pertahanan Amerika Serikat yang dikenal dengan ARPAnet, namun karena Internet adalah jaringan public maka bersifat open dan saat ini masalah keamanan menjadi sangat krusial terutama informasi-informasi penting yang lewat di Internet dapat disadap oleh orang lain.

Perkembangan teknologi Internet saat ini sangat cepat melebihi perkembangan teknologi radio dan televisi.



Gambar 2. Skema Tunneling & Encapsulations VPN

Jaringan Internet adalah kumpulan jaringan di dunia yang menghubungkan jutaan komputer perusahaan, badan pemerintahan, institusi pendidikan, dan perorangan, dengan internet pengguna mendapatkan akses untuk memperoleh informasi global dan komunikasi sistem (Shelly, *Discovering Computer*, 62)

Pertumbuhan jaringan internet di Indonesia, sekalipun masih dalam tahap awal dan belum memasyarakat seperti halnya di negara-negara maju, menunjukkan trend yang sangat positif. Potensi penggunaanya yang begitu besar dari penduduk Indonesia yang pada saat

ini (Juli 1997) berjumlah sekitar 200 juta jiwa tidak dapat diabaikan begitu saja.

Untuk mengembangkan pasar yang besar ini, salah satu prasyarat adalah dibentuknya suatu interkoneksi nasional antar penyelenggara jasa internet (PJI) di Indonesia, sehingga pelanggan dari satu PJI dapat dengan mudah dan murah berkomunikasi dengan pelanggan PJI yang lain yang berada di Indonesia. IIX dibentuk oleh APJII yang awalnya bersifat amal dan sukarela dengan maksud menyatukan trafik antar Internet Service Provider (ISP) di Indonesia sehingga tidak perlu transit ke luar negeri. ([www.iix.net.id/?do=latar-tujuan](http://www.iix.net.id/?do=latar-tujuan))

IIX dibuat untuk peering ISP-ISP dan NAP yang ada di Indonesia Tujuannya adalah membentuk jaringan interkoneksi nasional yang memiliki kemampuan dan fasilitas yang sesuai dengan kebutuhan yang ada, untuk digunakan oleh setiap ISP yang memiliki ijin beroperasi di Indonesia. ISP yang tersambung ke IIX tanpa biaya bandwidth, hanya biaya link fisik seperti serat optik, wireless atau leased line, yang berbeda-beda. Cukup murah bagi ISP yang berada di Jakarta tetapi mahal bagi ISP yang ada di luar Jakarta, apalagi di luar Jawa, karena biaya link fisiknya saja jauh lebih mahal daripada link internasional termasuk kapasitas bandwidth langsung melalui satelit ke luar negeri.

([http://id.wikipedia.org/wiki/Indonesia\\_Internet\\_Exchange](http://id.wikipedia.org/wiki/Indonesia_Internet_Exchange))

*Virtual Private Network (VPN)* memungkinkan dibentuk interkoneksi network melalui jaringan internet dengan protocol tunneling agar terbentuk koneksi secara private. (James E Goldman, *Applied Data Communications*, 624). *Virtual Private Network (VPN)* sebuah session yang di authentication dan lajur

komunikasi yang dienkripsi melalui jaringan publik seperti Internet, dimana VPN hanya memproteksi session komunikasi antara dua domain. (Chris Brenton, *Mastering Network Security*, 321).

Saat ini ada beberapa jenis peralatan VPN yang ada di pasaran dunia, dengan banyaknya produk VPN akan menyulitkan dalam menentukan peralatan yang tepat yang akan digunakan, *Hardware Based VPN* adalah suatu perangkat alternatif dari *router based* yang berfungsi sebagai perangkat keras yang menangani mekanisme *routing* dan *network addressing*, *VPN tunneling protocol*, Enkripsi, *Bandwidth management*, Layanan otentikasi, *Accounting*, Kompresi data, Fungsi *Firewall*, dan Koneksitas dengan *VPN client*

## 2.2 Virtual Private Network (VPN)

Dengan perkembangan interkoneksi Internet yang semakin luas dan turunnya harga bandwidth yang signifikan di Indonesia, maka Teknologi komunikasi data yang menggunakan interkoneksi Internet adalah suatu pilihan yang tepat. VPN merupakan sebuah jaringan *private* yang menghubungkan satu *node* jaringan ke *node* jaringan lainnya dengan menggunakan jaringan Internet. Data yang dilewatkan akan *diencapsulation* (dibungkus) dan dienkripsi, supaya data tersebut terjamin kerahasiaannya.

Peningkatan penggunaan koneksi VPN dari tahun ke tahun sangat signifikan karena mudahnya infrastruktur yang dibutuhkan serta mudahnya dalam instalasi, maka koneksi ini lebih efisien dibandingkan dengan metode WAN.

Ada beberapa alasan mengapa saat ini penggunaan perusahaan banyak membangun solusi VPN, diantaranya ;

1. Menekan biaya interkoneksi
2. Memperluas interkoneksi ke user yang selama ini susah dijangkau
3. Dapat mengirimkan aplikasi-aplikasi baru berbasis Internet Protocol
4. Fleksibel dalam pemilihan topology
5. Skalabilitas Network terjaga
6. Meningkatkan tingkat Security

Mengapa aman, karena Sistem keamanan di VPN menggunakan beberapa lapisan, seperti pada Gambar 2 sebelumnya dapat dijabarkan beberapa metode keamanan VPN, diantaranya ;

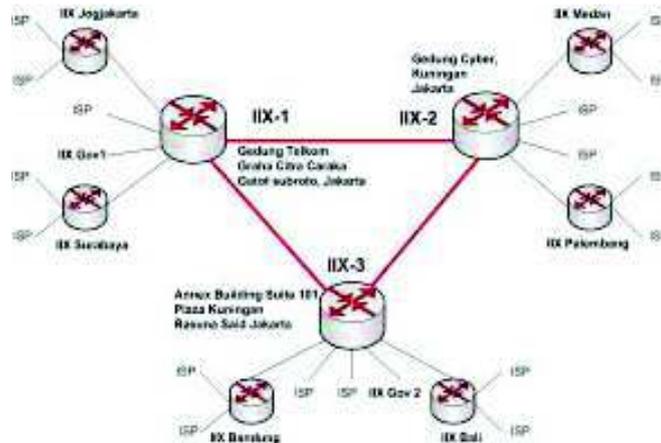
1. **Metode tunneling** (terowongan), membuat terowongan virtual diatas jaringan publik menggunakan protocol seperti *Point to Point Protocol* (PPTP), *Layer 2 Tunneling Protocol* (L2TP), *Generic Routing Encapsulation* (GRE) atau *IP Sec*. PPTP dan L2TP adalah layer 2 tunneling protocol. keduanya melakukan pembungkusan *payload* pada frame *Point to Point Protocol* (PPP) untuk di lewatkan pada jaringan. IP Sec berada di layer 3 yang menggunakan packet, yang akan melakukan pembungkusan IP header sebelum dikirim ke jaringan.
2. **Metode Enkrpsi** untuk *Encapsulations* (membungkus) paket data yang lewat di dalam *tunneling*, dimana data akan dienkripsi pada saat dilewatkan. Data disini akan dirubah dengan metode algoritma *cripthography* tertentu seperti DES, 3DES, atau AES

3. **Metode Otentikasi User**, karena banyak user yang akan mengakses dari banyak titik maka digunakan beberapa metode protocol otentikasi user tertentu, seperti *Remote Access Dial In User Services* (RADIUS) dan *Digital Certificates*.
4. **Integritas Data**, karena paket data yang dilewatkan di jaringan publik maka diperlukan penjaminan integritas data atau kepercayaan data apakah terjadi perubahan atau tidak. Metode VPN dapat menggunakan HMA C-MD5 atau HMA C-SHA1 untuk menjamin paket tidak dirubah pada saat pengiriman.

### 3. ALTERNATIF WAN VIA IIX

#### 3.1 Interkoneksi IIX

Sejak tahun 2000an disaat trend Internet di Indonesia booming dan makin banyaknya penyedia jasa internet, perkumpulan *Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)* membuat interkoneksi *peering* nasional agar pengalaman routing di Internet menjadi lebih cepat dan tidak membuang traffic internet ke Internet global / internasional. Interkoneksi ini disebut **IIX** atau **Indonesia Internet Exchange**.



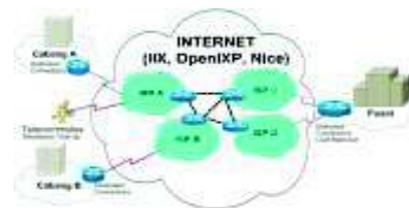
**Gambar 3. Design Topology IIX**

Interkoneksi IIX ini menghubungkan semua ISP (*Internet Service Provider*), NAP (*Network Access Provider*) dan Telco lainnya kedalam jaringan yang terpusat dan saling terhubung. Interkoneksi IIX ini berujung dan bertemu di Gedung Cyber Jl. Kuningan Barat No 8 Jakarta. Jadi dengan interkoneksi ini maka koneksi antara ISP atau NAP di Indonesia tidak perlu pengelamatan atau routing ke luar negeri lagi. Dari Gambar 3 topology gambar diatas dapat diterangkan ;

1. Koneksi backbone membentuk topology Ring antara IIX-1 dengan IIX-2 dan IIX-3 menggunakan kabel Fiber Optic (FO) dengan transfer data mencapai 1Gbps.
2. Koneksi dari IIX di jakarta ke IIX Wilayah di daerah-daerah menggunakan *leased channel*, atau *metro-e* dari NAP UPSTREAM yang disewa oleh para ISP di daerah tersebut.
3. Koneksi E-Gov untuk kepentingan Departemen DIKNAS, MILITER atau

pemerintahan lainnya dihubungkan ke core IIX via *leased channel* atau provider UPSTREAMnya.

Tujuan utama membuat simpul-simpul di daerah indonesia untuk mengumpulkan semua provider ISP di indonesia dan pengguna content lokal lainnya untuk terinterkoneksi ke IIX. Dari data yang didapat 50 % traffic berasal dari ISP dan kebanyakan untuk traffic bandwidth games. Hal ini sangat disayangkan dengan kemampuan jaringan IIX yang belum dapat dioptimalkan.



**Gambar 4. Perancangan Topology koneksi private via IIX**

### 3.1 Aspek Teknik IIX

Saat ini terdapat tiga node utama IIX yang terhubung dengan backbone Fiber Optic dan topology ring. Interkoneksi utama inilah yang menjadi backbone ke ISP, NAP yang ada diseluruh Indonesia baik yang berada di Jawa atau daerah-daerah lainnya. IIX juga saat ini di interkoneksi dengan jaringan pemerintahan seperti untuk keperluan militer dan pendidikan (INHERENT / JARDIKNAS).

Dari gambar 3 terlihat tiga tempat interkoneksi IIX ;

1. IIX 1 berada di Gedung Telkom Graha Citra Caraka, Jl. Jend. Gatot Subroto 52 dan direlokasi ke Gedung Arthatel
2. IIX-2 terletak di Gedung Cyber Jl. Kuningan Barat No. 8 Jakarta
3. IIX-3 berada di Annex Building Suite 101 AB Plaza Kuningan Jl. H.R. Rasuna Said Kav C 11 – 14 (<http://www.napinfo.net>)

## 4. PERANCANGAN VPN

### 4.4.1. Analisa Kebutuhan Jaringan WAN P Pada Sebuah Perusahaan

Ada beberapa solusi komunikasi VPN yang ditawarkan oleh provider telekomunikasi kepada perusahaan. Salah satunya adalah VPN IP dengan teknologi MPLS.

Dari Gambar 4 diatas dapat dijelaskan sebagai berikut ;

1. Kebutuhan interkoneksi untuk menghubungkan beberapa kantor cabang dan telecommuters yang berada di wilayah Indonesia.

2. Kebutuhan perusahaan untuk terkoneksi secara lokal melalui jaringan interkoneksi.
3. Koneksi di Kantor Pusat menggunakan koneksi *dedicated*, koneksi *dedicated* terkoneksi ke dua ISP yang berbeda **backbone upstreamnya** agar bisa mengoptimalkan *load balancing* yang akan dikonfigurasi. Load Balancing dibutuhkan agar tingkat layanan terjaga dan terjamin, sedangkan Bandwidtnya dibutuhkan lebih besar dari bandwidth yang di kantor cabang.
4. Di setiap kantor cabang dapat menggunakan koneksi *dedicated* atau koneksi *broadband*, yang mana pointing ip addressnya *point-to-point* ke ip publik atau mesin Domain Name Server (DNS) yang berada di kantor pusat.
5. Para pekerja rumah secara remote dan mobile (telecommuters) dapat terkoneksi secara langsung ke server kantor pusat dengan menggunakan VPN Client software yang juga di pointing ip addressnya *point-to-point* ke ip publik atau mesin Domain Name Server (DNS) yang berada di kantor pusat via koneksi broadband.

### 4.2 Perancangan Jaringan VPN dengan menggunakan interkoneksi IIX

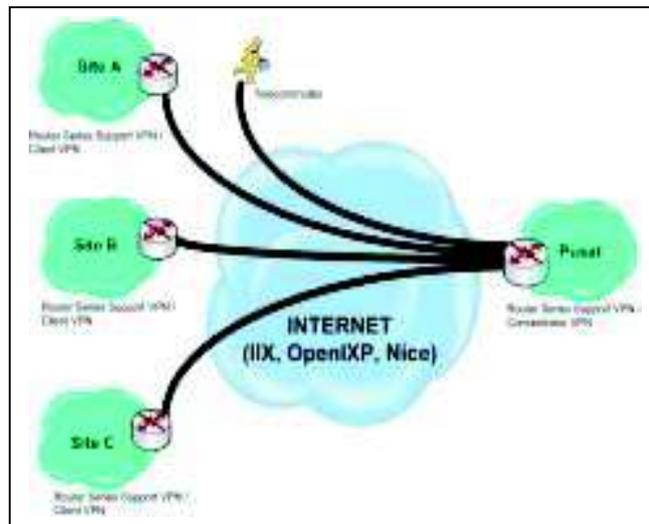
Penggunaan sistem VPN dengan IIX bisa menggunakan suatu perangkat hardware khusus produksi vendor tertentu yang dibuat untuk melakukan proses komunikasi lewat jaringan Internet, sistem ini sering disebut sebagai solusi hardware based.

Kelebihan utama dari sistem *hardware based* ini adalah sistem keamanan, kinerja, fleksibel, dan kontrol manajemen serta

dapat di koneksikan dengan infrastruktur jaringan lainnya seperti sistem keamanan atau kualitas layanan yang sudah ada untuk memperkuat fungsi VPN tersebut. Dengan memilih perangkat yang tepat maka komunikasi data dengan VPN dapat juga mengintegrasikan komunikasi suara melalui metode **IP Telephony**. Maksudnya perangkat VPN ini juga dapat

mendukung protocol untuk komunikasi suara, konsep yang dikenal sebagai **AVVID** (*Architecture Voice, Video and Integrated Data*) untuk mengoptimalkan koneksi dalam jaringan

### 4.3 Solusi Hardware Router / Concentrator



**Gambar 5. Design Topology Interkoneksi private via IIX**

Solusi ini menggunakan sebuah perangkat router series tertentu, router yang sudah mensupport protocol VPN dapat langsung dikonfigurasi baik disisi pusat atau disisi kantor cabang, intinya yang membangun “koneksi” antara dua titik atau lebih secara simultan dilakukan oleh router tersebut. Ciri router bisa mensupport VPN adalah dengan disediakannya perintah *Tunneling encapsulation* VPN didalam sistemnya. Pada gambar 5 semua node router di setiap kantor cabang terkoneksi secara point-to-point ke router yang berada di kantor pusat melewati jaringan IIX.

Estimasi yang dibutuhkan untuk solusi ini adalah ;

Kantor pusat	
Jenis Koneksi	Dedicated CIR 1:1
Bandwidth	2 x minimal 1024 kbps
Jenis Perangkat	Router series support VPN(series yang lebih tinggi dari kantor cabang)
Routing	Static ke cabang with load balancing
Management	Firewall dan QoS Bandwidth akses

Kantor Cabang	
Jenis Koneksi	Dedicated CIR 1:1
Bandwidth	minimal 512 kbps
Jenis Perangkat	Router series support VPN
Routing	Static ke pusat
Management	Firewall dan QoS Bandwidth akses

Contoh series router ternama yang mensupport VPN adalah 7000 series, 3600 series, 2600 series, 1700 series dan SOHO 900 series / 800 series. Terdapat juga VPN Module yang bisa digunakan di series tertentu dan mempunyai features tambahan seperti IOS plus Firewall IPsec dan Dual 10/100 Mbps. Sedangkan contoh series router lainnya seperti Passport series 200, 1750, 2700, dan 5000.

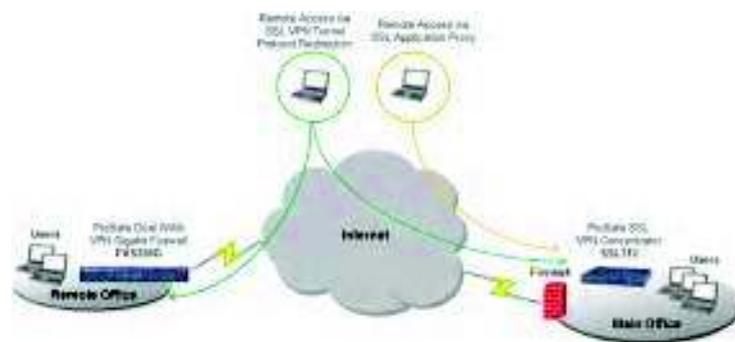
Kelebihan utama dari sistem ini adalah di tingkat kehandalan dan jaminan layanan yang diberikan, karena memang suatu perangkat yang dibuat untuk melakukan fungsi pengalaman.

#### 4.4 Solusi Server based produk SOHO/SMB

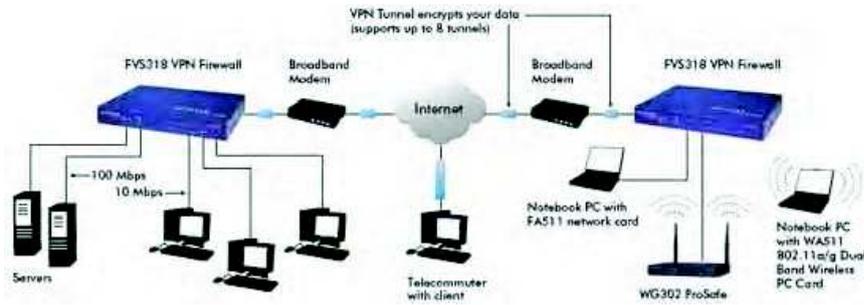
Solusi tepat untuk perusahaan *Small Office Home Office* (SOHO) atau *Small Medium Business* (SMB), di beberapa contoh studi kasus perusahaan bisnis di Indonesia yang menggunakan solusi ini adalah sistem maskapai penerbangan, travel dan perusahaan *retailed* menggunakan sistem yang dibangun dengan “backbone” solusi dari vendor SOHO/SMB.

Perangkat ini juga bisa digunakan sebagai “router broadband” untuk melakukan NAT, dan beberapa feature firewall sederhana. Rata-rata produk dari vendor ini dapat melakukan 200 koneksi dedicated VPN tunnels secara simultan dengan fungsi mendukung metode IP Sec / IKESA.

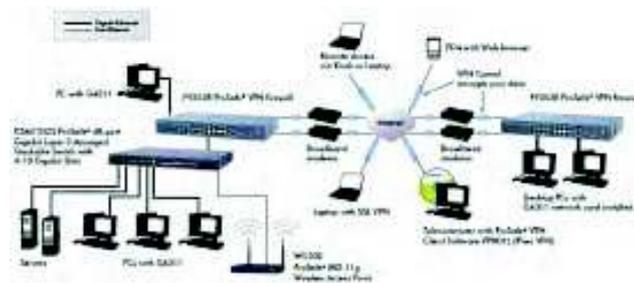
Pada gambar 6 sampai gambar 8 dibawah adalah contoh dari topology dan produk vendor SOHO/SMB yang menawarkan solusi hardware based.



Gambar 6. Solusi hardware based VPN



Gambar 7. Solusi hardware based VPN



Gambar 8. Solusi hardware based VPN

Mungkin sistem mixed atau campuran yang dikombinasikan perangkat router atau concentrator khusus yang dipasang di sisi kantor pusat dan penggunaan solusi SOHO/SMB digunakan sebagai solusi kantor cabang atau telecommuters adalah solusi yang bijak. Namun tingkat kompatibilitas pasti sangat menjadi perhatian utama.

## 5. KESIMPULAN

Tulisan ini diharapkan dapat memberikan gambaran tentang alternatif interkoneksi jaringan skala luas (WAN) yaitu interkoneksi dengan menggunakan teknologi VPN dengan memanfaatkan interkoneksi IIX.

Dengan menggunakan jaringan IIX maka dapat mereduksi biaya sewa layanan bandwidth yang selama ini menjadi solusi

perusahaan bisnis. Interkoneksi *Indonesia Internet Exchange* (IIX) sangat efektif untuk menghubungkan traffic data yang interkoneksinya berada di Indonesia, karena dengan IIX dapat meningkatkan kinerja jaringan karena latency yang kecil dan dapat mengoptimalkan pengelematan di router kita. IIX dapat menjadi solusi tepat bagi para perusahaan bisnis yang mempunyai banyak kantor cabang di Indonesia

VPN saat ini berkembang pesat dikarenakan faktor efektifitas dan efisien bari dari sisi teknis dan bisnis, ditunjang dengan semakin beragamnya solusi yang ditawarkan oleh para vendor-vendor pembuat solusi jaringan komputer. VPN dapat mengintegrasikan jaringan melewati jaringan publik dengan aman.

Solusi VPN dengan menggunakan hardware based sangat tepat untuk

mendapatkan performa dan kehandalan interkoneksi yang dibangun, karena proses *encapsulations*, *enkripsi* dan *tunneling* dilakukan diperangkainya bukan di sebuah sistem operasi.

## 6. DAFTAR PUSTAKA

- Archer Kevin, Core James, Cothen Chuck, Davis Roger, White B. Gregory, Ph.D, Dicenso David, Goog J, Travis, William E. Dwayne, 2001, "Voice and Data Security", Sams Publishing., USA., 14-15 pp.
- Dicson Kevin.,1999, "The ABCs Of VPNs",Packet Magazine Cisco System., Third Editions 2002,USA., 50-55 pp.
- David Barry, 2002, "VPN Management", Third Edition 2002, Packet Magazine Cisco System., USA., 57-60 pp.
- Chris Brenton, Sybex Network, 1996., "Mastering Network Security",USA.
- James E Goldman, Phillip T Rawless, "Applied Data Communications", 2001 .,John Wiley & Sons, Inc.,USA
- Marilee Ford, H. Kim Lew, Steve Spanier, Tim Stevenson, 1997, Internetworking Techlogies Handbook, Cisco Network Press, USA \_\_\_\_\_, 2003, "VPN with windows 2003", Whitepaper Microsoft,USA, [www.technet.microsoft.com/en-us/network/bb545442.aspx](http://www.technet.microsoft.com/en-us/network/bb545442.aspx).
- Shelly Cashman Vermaat, *Discovering Computer*, Salemba Infotek, Jakarta, 2007
- Steve Spanier, Tim Stevenson, Marilee Ford, 1997., "Internetworking Technologies Handbook", Cisco Press., USA, \_\_\_\_\_,2002., "Virtual Private Network : An Overview", Whitepaper Microsoft .,USA., <<http://www.microsoft.com/docs/vpnoverview>> \_\_\_\_\_,2002. [http://www.byteandswitch.com/document.asp?doc\\_id=161113&WT.svl=wire2\\_6](http://www.byteandswitch.com/document.asp?doc_id=161113&WT.svl=wire2_6) \_\_\_\_\_, <http://www.iix.net.id/?do=latar-tujuan> \_\_\_\_\_,2008 [http://id.wikipedia.org/wiki/Indonesia\\_Internet\\_Exchange](http://id.wikipedia.org/wiki/Indonesia_Internet_Exchange)) \_\_\_\_\_,2008, <http://www.napinfo.net>