I. Pengertian VPN

Virtual Private Network atau **VPN** adalah suatu jaringan pribadi yang dibuat dengan menggunakan jaringan publik, atau dengan kata lain menciptakan suatu WAN yang sebenarnya terpisah baik secara fisikal maupun geografis sehingga secara logika membentuk satu netwok tunggal, paket data yang mengalir antar site maupun dari user yang melakukan remote akses akan mengalami enkripsi dan authentikasi sehingga menjamin keamanan, integritas dan validitas data. Perlu penerapan teknologi tertentu agar walaupun menggunakan medium yang umum, tetapi traffic (lalu lintas) antar remote-site tidak dapat disadap dengan mudah, juga tidak memungkinkan pihak lain untuk menyusupkan traffic yang tidak semestinya ke dalam remote-site.

VPN (Virtual Private Network) merupakan suatu cara untuk membuat sebuah jaringan bersifat "*private*" dan aman dengan menggunakan jaringan publik misalnya internet. ***VPN*** dapat mengirim data antara dua komputer yang melewati jaringan publik sehingga seolah-olah terhubung secara ***point to point***. ***Data dienkapsulasi (dibungkus)*** dengan header yang berisi informasi ***routing*** untuk mendapatkan koneksi ***point to point*** sehingga data dapat melewati jaringan publik dan dapat mencapai akhir tujuan. Sedangkan untuk mendapatkan koneksi bersifat ***private***, data yang dikirimkan harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi. Proses ***enkapsulasi*** data sering disebut "***tunneling***".

Anda dapat mengakses server kantor melalui ***VPN*** dimana saja, entah itu dirumah atau dijalan secara aman meskipun anda menggunakan infrastruktur jaringan internet dalam penggunaannya. Menurut pandangan user, koneksi ***VPN*** merupakan koneksi point to point antara user computer dengan server korporasi dan data terkirim di atas jaringan ***"dedicated,"*** padahal tidak demikian kenyataannya.

VPN yang dipecah menjadi 4 kategori:

1. Trusted VPN : Seorang pelanggan "terpercaya" sirkuit disewakan penyedia layanan dan digunakan untuk berkomunikasi tanpa gangguan.. Meskipun "dipercaya" itu tidak dijamin.
2. Secure VPN : Dengan keamanan menjadi lebih dari sebuah isu bagi pengguna, enkripsi dan dekripsi digunakan pada kedua ujungnya untuk menjaga informasi yang dilewatkan ke sana kemari. Hal ini menjamin keamanan yang diperlukan untuk memenuhi perusahaan, pelanggan, dan penyedia.
3. Hybrid VPN : Sebuah campuran dari VPN yang aman dan terpercaya. Seorang pelanggan mengontrol bagian yang dilindungi dari VPN sedangkan penyedia, seperti ISP, menjamin aspek terpercaya.
4. Provider-provisioned VPN : VPN yang dikelola oleh penyedia layanan.

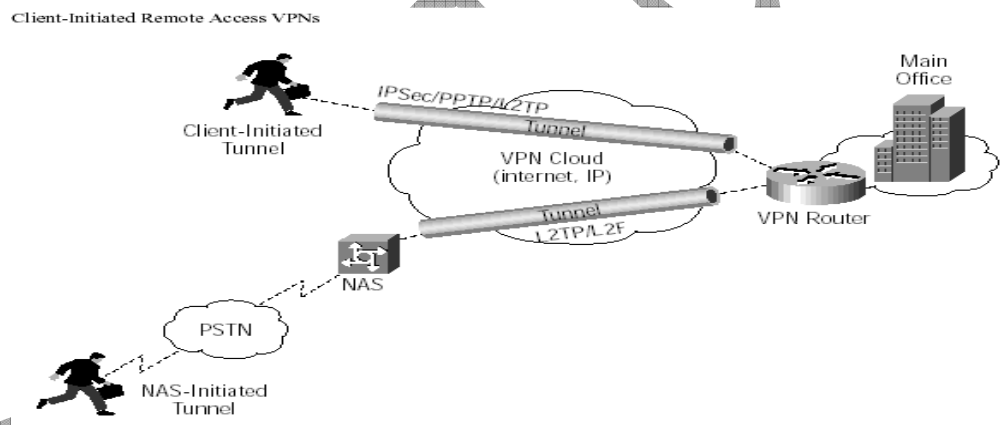
II. Jenis-jenis VPN

A. Remote access VPN

Remote akses VPN (virtual private network) memungkinkan kita mengakses resources corporate kita dengan cara yang aman dengan cara membuat suatu tunneling melalui Internet. Dengan melimpahnya jaringan internet termasuk Internet yang diakses dari Smart-phone, Blacknerry dan sebagainya belakangan ini, ditambah dengan technology VPN sekarang ini, memungkinkan suatu organisasi melebarkan sayap jaringan nya kepada setiap individu, dimanapun dan kapanpun dengan cara yang sangat murah dan tentunya sangat mengedepankan keamanan.

VPN telah menjadi suatu solusi logical kepada koneksi remote akses dengan alasan-alasan berikut ini:

- VPN bisa memberikan komunikasi yang aman dengan hak akses yang bisa di sesesuaikan menurut individu masing-masing user, seperti untuk karyawan, kontraktor, atau business partner.
- Menaikkan produktivitas karyawan dengan cara melebarkan jaringan dan applikasi corporate ke rumah-rumah atau ke mana saja ada jaringan internet
- Mengurangi biaya komunikasi dan menaikkan fleksibilitas



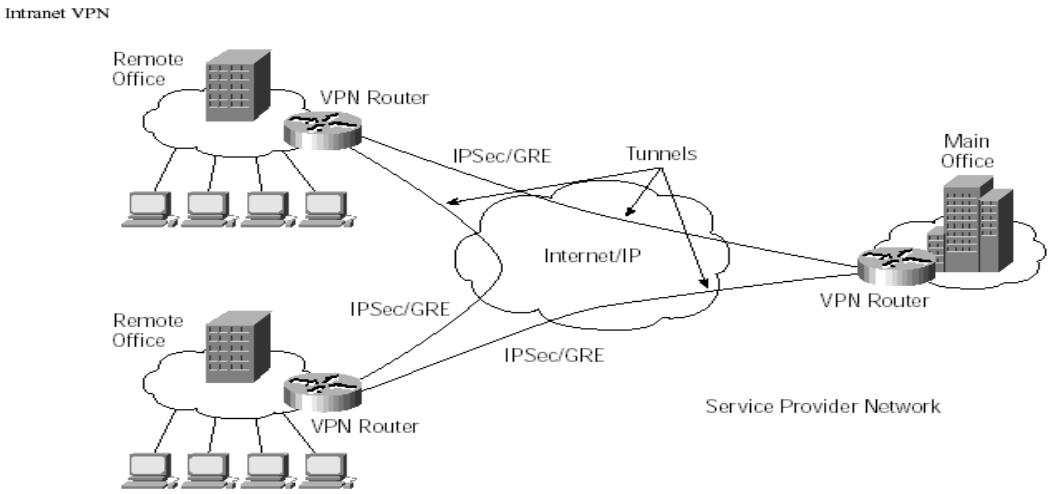
Gbr 1 Remote Access VPN

B. Intranet VPN

Konsep dari Intranet adalah menyediakan sirkuit virtual antara kantor-kantor organisasi melalui Internet. Mereka dibangun menggunakan Internet, penyedia layanan IP, Frame Relay, atau jaringan ATM. Infrastruktur WAN IP menggunakan IPSec atau GRE untuk membuat terowongan lalu lintas aman di jaringanManfaat dari VPN intranet meliputi:

- Mengurangi bandwidth WAN biaya, efisien penggunaan bandwidth WAN
- Fleksibel topologi

- Menghindari kemacetan dengan menggunakan lalu lintas manajemen bandwidth shaping



Gbr 2 Intranet VPN

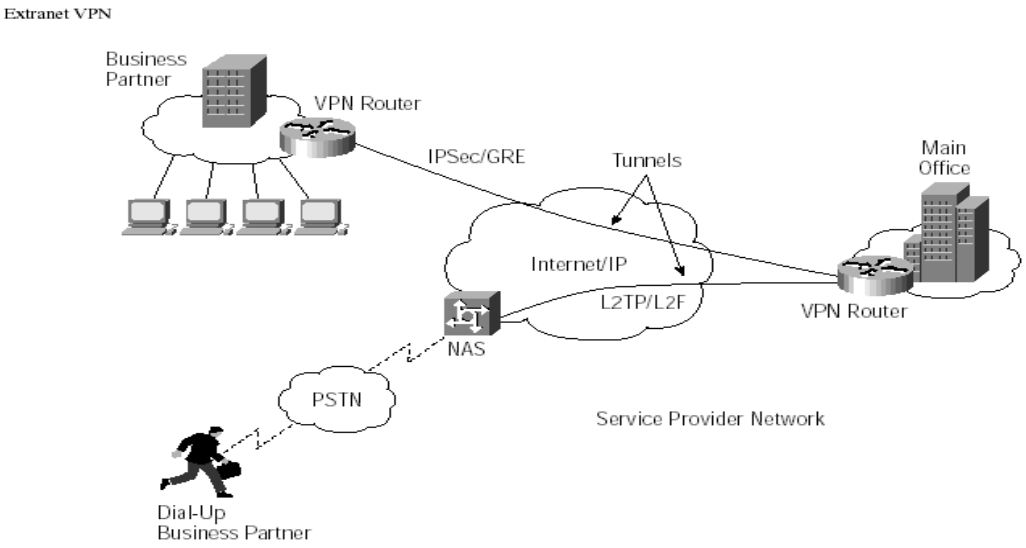
Contoh Kasus:

Menghubungkan kantor pusat dan seluruh kantor cabang melalui infrastruktur jaringan publik menggunakan IP security (IPSec) atau Generic Route Encryption (GRE) untuk memberikan keamanan pada tunnel yang dipakai. Dengan menggabungkan service dari provider seperti mekanisme Quality of Service (QoS), manajemen bandwidth Weighted Fair Queuing (WFQ) dan penggunaan Commited Access Rate (CAR) di router peusahaan, akan memberikan penggunaan bandwidth WAN yang efisien dan throughput yang bisa dipercaya. Keuntungan dari Intranet VPN adalah pengurangan biaya bandwidth di WAN, kemudahan penggabungan kantor cabang baru dan adanya link redundancy WAN pada service provider.

C. Extranet VPN

Extranet adalah sebuah jaringan komputer yang memungkinkan akses dikendalikan dari luar, untuk bisnis tertentu atau tujuan pendidikan.. Extranet dapat dilihat sebagai perpanjangan dari sebuah perusahaan intranet yang diperluas ke pengguna di luar perusahaan, biasanya mitra, vendor, dan pemasok. Ini juga telah digambarkan sebagai "keadaan pikiran" di mana Internet dianggap sebagai cara untuk melakukan bisnis dengan set yang dipilih perusahaan lain (business-to-business , B2B), di isolasi dari semua pengguna Internet lainnya. In contrast, business-to-consumer (B2C) models involve known servers of one or more companies, communicating with previously unknown consumer users. Sebaliknya, bisnis-ke-konsumen (B2C) model melibatkan server diketahui dari satu atau lebih perusahaan, berkomunikasi dengan pengguna konsumen yang sebelumnya tidak diketahui. An extranet is like a DMZ in that it provides access to needed services for channel partners, without granting access to an organization's entire network. Sebuah extranet adalah seperti

DMZ dalam hal ini menyediakan akses ke layanan yang dibutuhkan untuk mitra saluran, tanpa memberikan akses ke seluruh jaringan organisasi.



Gbr 3 Extranet VPN

Contoh kasusnya:

Menghubungkan ke perusahaan partner dan supplier membutuhkan biaya yang tinggi dan tingkat kesulitan yang tinggi pula. Selain itu, dibutuhkan sering terjadi masalah dengan kompatibilitas device yang digunakan tiap perusahaan. Extranet VPN menghubungkan pelanggan, supplier dan partner melalui jaringan telekomunikasi publik dengan menggunakan saluran khusus. Pelayanan yang disediakan sama dengan pelayanan jika menggunakan jaringan pribadi, sehingga pengguna seperti menggunakan intranet dari perusahaan tersebut. Extranet menggunakan arsitektur dan protokol yang sama dengan yang digunakan pada Access VPN dan Intranet VPN.

III. Kriteria yang harus dipenuhi VPN

A. User Authentication

VPN harus mampu mengklarifikasi identitas klien serta membatasi hak akses user sesuai dengan otoritasnya. VPN juga dituntut mampu memantau aktifitas klien tentang masalah waktu, kapan, di mana dan berapa lama seorang klien mengakses jaringan serta jenis resource yang diaksesnya.

B. Address Management

VPN harus dapat mencantumkan addres klien pada intranet dan memastikan alamat/address tersebut tetap rahasia.

C. Data Encryption

Data yang melewati jaringan harus dibuat agar tidak dapat dibaca oleh pihak-pihak atau klien yang tidak berwenang.

D. Key Management

VPN harus mampu membuat dan memperbarui encryption key untuk server dan klien.

E. Multiprotocol Support

VPN harus mampu menangani berbagai macam protokol dalam jaringan publik seperti IP, IPX dan sebagainya.

IV. Komponen – Komponen VPN

Perusahaan perlu untuk menjaga VPN mereka aman dari gangguan dan pengguna yang tidak sah. Solusi VPN juga perlu memiliki Skalabilitas Platform - kemampuan untuk beradaptasi VPN untuk memenuhi persyaratan peningkatan mulai dari konfigurasi untuk kantor kecil perusahaan besar implementasi. Sebuah keputusan kunci perusahaan harus membuat sebelum memulai pelaksanaannya adalah untuk mempertimbangkan bagaimana VPN akan tumbuh untuk memenuhi kebutuhan jaringan perusahaan dan jika VPN akan kompatibel dengan jaringan

A. Protokol

1. Point-to-Point Tunneling Protocol (PPTP)

PPTP dikembangkan oleh Microsoft dan Cisco merupakan protokol jaringan yang memungkinkan pengamanan transfer data dari remote client ke server pribadi perusahaan dengan membuat sebuah VPN melalui TCP/IP (Snader, 2005). Teknologi jaringan PPTP merupakan pengembangan dari remote access Point-to-Point protocol yang dikeluarkan oleh Internet Engineering Task Force (IETF). PPTP merupakan protokol jaringan yang merubah paket PPP menjadi IP datagrams agar dapat ditransmisikan melalui intenet. PPTP juga dapat digunakan pada jaringan private LAN-to-LAN.

PPTP terdapat sejak dalam sistem operasi Windows NT server dan Windows NT Workstation versi 4.0. Komputer yang berjalan dengan sistem operasi tersebut dapat menggunakan protokol PPTP dengan aman untuk terhubung dengan private network sebagai klien dengan remote access melalui internet. PPTP juga dapat digunakan oleh komputer yang terhubung dengan LAN untuk membuat VPN melalui LAN.

Fasilitas utama dari penggunaan PPTP adalah dapat digunakannya public-switched telephone network (PSTNs) untuk membangun VPN. Pembangunan PPTP yang mudah dan berbiaya murah untuk digunakan

secara luas, menjadi solusi untuk remote users dan mobile users karena PPTP memberikan keamanan dan enkripsi komunikasi melalui PSTN ataupun internet.

2. Layer 2 Tunneling Protocol (L2TP)

L2TP adalah tunneling protocol yang memadukan dua buah tunneling protokol yaitu L2F (Layer 2 Forwarding) milik cisco dan PPTP milik Microsoft (Gupta, 2003). L2TP biasa digunakan dalam membuat Virtual Private Dial Network (VPDN) yang dapat bekerja membawa semua jenis protokol komunikasi didalamnya. Umunnya L2TP menggunakan port 1702 dengan protocol UDP untuk mengirimkan L2TP *encapsulated* PPP frames sebagai data yang di tunnel.Terdapat dua model tunnel yang dikenal (Lewis, 2006), yaitu *compulsory*dan *voluntary*. Perbedaan utama keduanya terletak pada *endpoint tunnel*-nya. Pada *compulsory tunnel*, ujung tunnel berada pada ISP, sedangkan pada *voluntary*ujung tunnel berada pada client remote.

3. IPsec (Internet Protokol Security)

IPSec merupakan suatu pengembangan dari protokol IP yang bertujuan untuk menyediakan keamanan pada suatu IP dan*layer* yang berada diatasnya (Carmouche, 2006). IPSec (*Internet Protocol Security*) merupakan salah satu mekanisme yang diimplementasikan pada *Virtual Private Network*. Paket IP tidak memiliki aspek *security*, maka hal ini akan memudahkan untuk mengetahui isi dari paket dan alamat IP itu sendiri. Sehingga tidak ada garansi bahwa menerima paket IP merupakan dari pengirim yang benar, kebenaran data ketika ditransmisikan. IPSecmerupakan metode yang memproteksi IP datagram ketika paket ditransmisikan pada *traffic*. IPSec berkerja pada*layer* tiga OSI yaitu *network layer* sehingga dapat mengamankan data dari *layer* yang berada atasnya. IPSec terdiri dari **dua buah *security* protokol (Carmouche, 2006) :**

- **AH (*Authentication Header*)** melakukan autentikasi datagram untuk mengidentifikasi pengirim data tersebut.
- **ESP (*Encapsulating Security Header*)** melakukan enkripsi dan layanan autentifikasi.

IPSec menggunakan dua buah protokol berbeda untuk menyediakan pengamanan data yaitu AH dan ESP keduanya dapat dikombinasikan ataupun berdiri sendiri. IPSec memberikan layanan *security* pada *level* IP dengan memungkinkan suatu *system* memilih protokol *security* yang dibutuhkan, algoritma yang digunakan untuk layanan, dan menempatkan kunci kirptografi yang dibutuhkan unutk menyediakan layanan. Dua buah protokol yang digunakan untuk memberikan layanan kemanan yaitu autentikasi protokol yang ditunjuk pada *header* protokol yaitu **AH (*Authentication Header*)** dan sebuah protokol yang mengkombinasikan enkripsi dan autentikasi yang ditunjuk oleh *header* paket untuk format tersebut yaitu **ESP (*Encapsulating Security Payload*).**

B. Security

1. Enkripsi

Sebuah virtual private network adalah hanya sebagai baik sebagai kemampuan enkripsi. Enkripsi adalah proses pengkodean data sehingga hanya komputer dengan decoder yang tepat akan dapat membaca dan menggunakannyaAnda bisa menggunakan enkripsi untuk melindungi file di komputer Anda atau e-mail Anda kirim ke teman atau kolega.

2. Key

Sebuah **kunci enkripsi** memberitahu komputer apa perhitungan untuk melakukan pada data dalam rangka untuk mengenkripsi atau mendekripsi itu. Bentuk yang paling umum dari enkripsi symmetric-key enkripsi atau enkripsi public-key:

- Dalam **symmetric-key enkripsi,** semua komputer (atau pengguna) berbagi kunci yang sama digunakan baik untuk mengenkripsi dan mendekripsi pesan.
- Dalam **enkripsi public-key,** setiap komputer (atau user) memiliki sepasang kunci publik-swastaSatu komputer menggunakan kunci pribadi untuk mengenkripsi pesan, dan komputer lain menggunakan kunci publik yang sesuai untuk mendekripsi pesan itu.

3. Authentication

Proses mengidentifikasi komputer dan manusia atau user yang memulai VPN Connection. Metode otentikasi dapat dilakukan dengan protocol. Hal ini diperlukan untuk memverifikasi identitas pengguna yang mencoba untuk mengakses sumber daya dari jaringan perusahaan sebelum mereka diberikan akses. Otentikasi pengguna juga menentukan tingkat akses, data diambil atau dilihat oleh pengguna, dan izin hibah untuk daerah-daerah tertentu dari sumber daya dari perusahaan.

C. Appliances

Firewall parameter bertugas memonitor lalu lintas jaringan penyeberangan, dan melindungi perusahaan dari akses yang tidak sah. Organisasi harus merancang jaringan yang memiliki firewall di tempat pada setiap koneksi jaringan antara organisasi dan internet. Dua jenis yang umum digunakan firewall paket-tingkat firewall dan aplikasi-tingkat firewall.

Packet-level firewall memeriksa sumber dan alamat tujuan dari setiap paket yang mencoba untuk melewati jaringan. Packet-level firewall hanya memungkinkan pengguna dalam dan keluar dari jaringan organisasi hanya jika pengguna memiliki paket diterima dengan sumber dan alamat tujuan

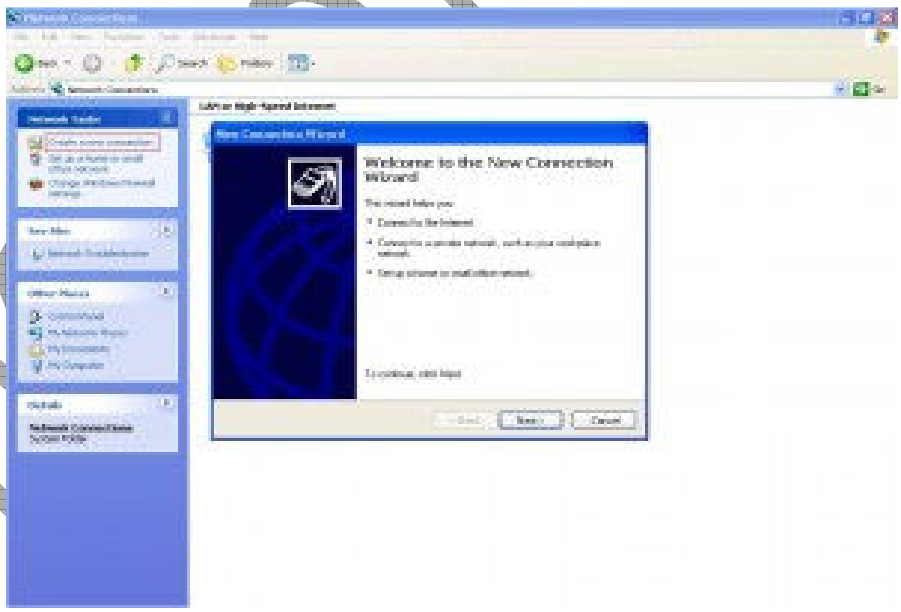
koresponden. Paket tersebut akan diperiksa secara individual melalui port TCP mereka ID dan alamat IP, sehingga tahu di mana paket pos. Kerugian dari paket-level firewall adalah bahwa hal itu tidak memeriksa isi paket, atau mengapa mereka sedang dikirim, dan sumber daya yang tidak cacat yang tersedia untuk semua pengguna.

Aplikasi-level firewall bertindak sebagai komputer host antara jaringan organisasi dan Internet. Pengguna yang ingin mengakses jaringan organisasi pertama harus log in ke aplikasi firewall-tingkat dan hanya mengizinkan informasi yang mereka berwenang untukKeuntungan untuk menggunakan aplikasi-level firewall adalah: pengguna akses kontrol tingkat, dan tingkat sumber daya otorisasi. Hanya sumber daya yang berwenang dapat diakses. Sebaliknya, pengguna akan harus ingat set ekstra password ketika mereka mencoba untuk login melalui Internet.

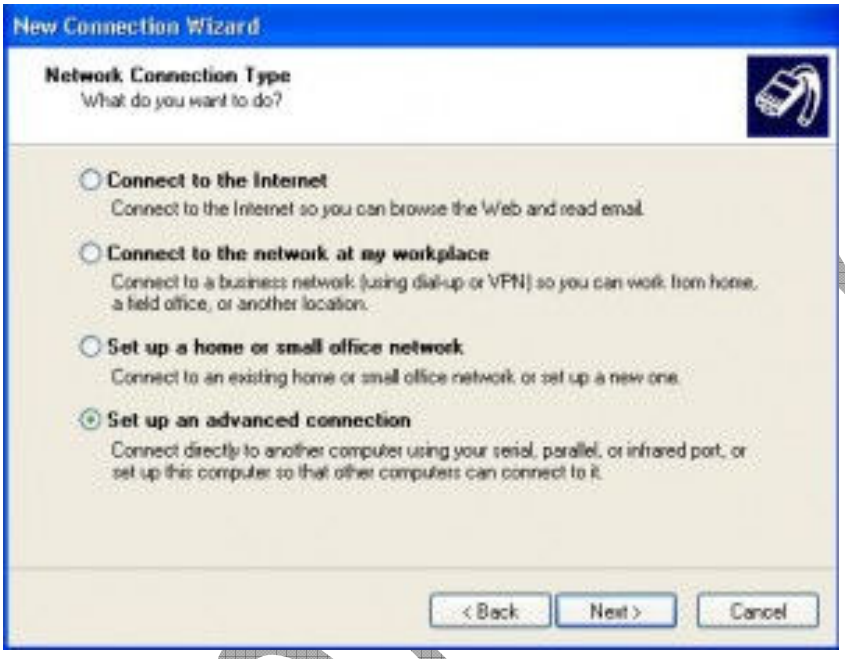
V. Langkah Sederhana Membangun VPN Pada Windows XP

Cara membangun VPN server pada windows XP, Yang di butuhkan yaitu (tidak mutlak) 2 NIC (network interface card) salah satunya akan digunakan untuk komunikasi antara komputer yang berstatus sebagai VPN server dan VPN client.

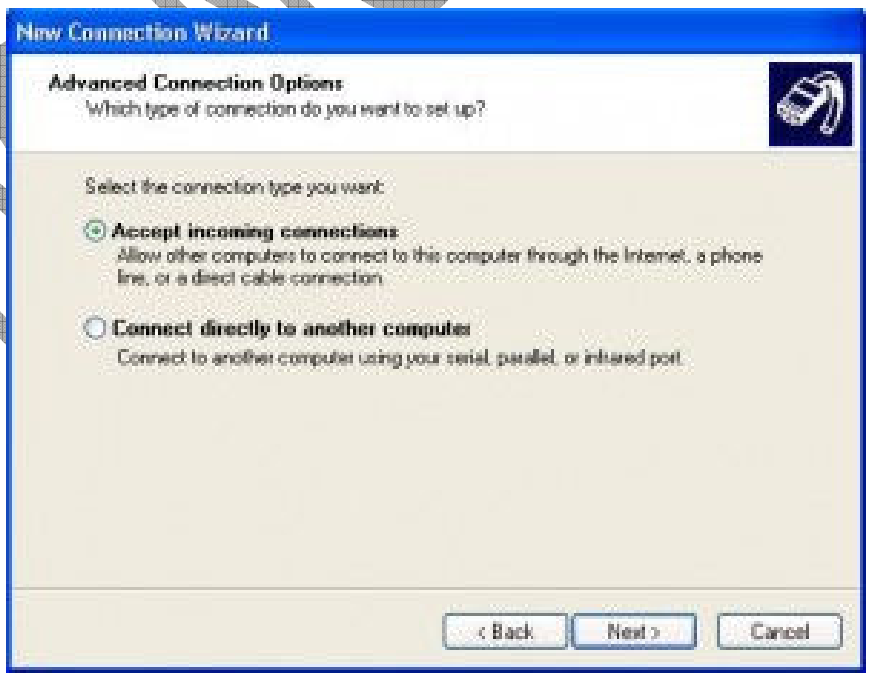
A. Start -> Control Panel -> Network Connections -> Create a New Connection



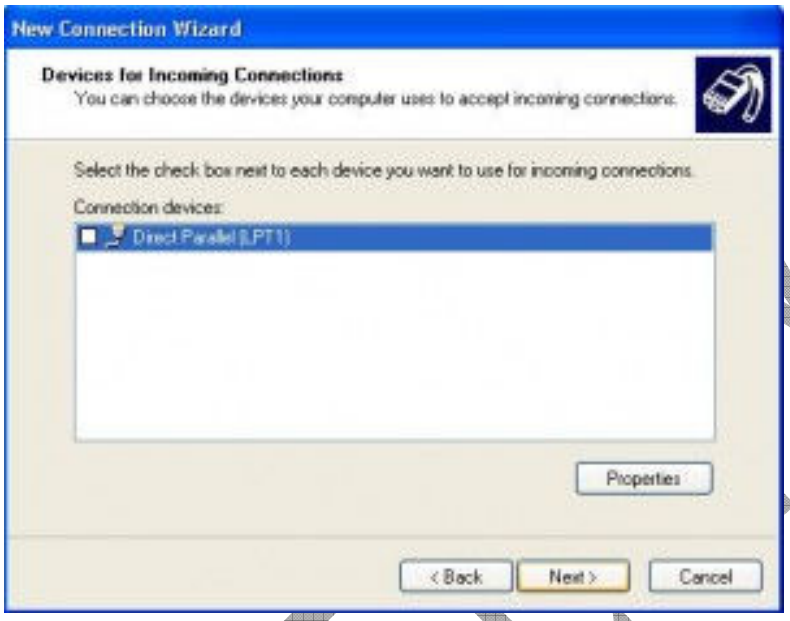
B. **Klik Next -> Pilih** "Set up an advanced connection"



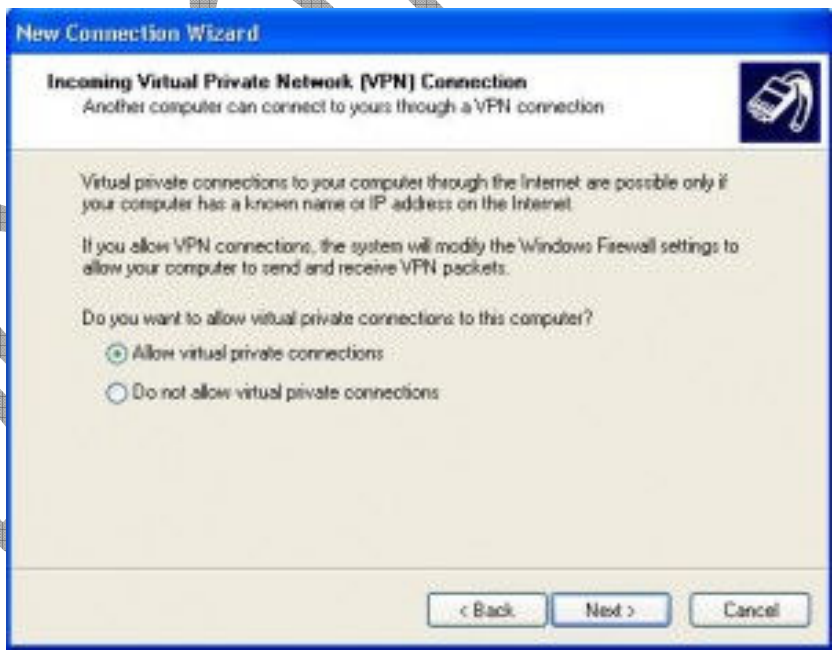
C. **Klik Next -> Pilih** "Accept incoming connections"



D. **Klik Next -> Kalau komputer/laptop kalian ada port LPT1 (printer) jangan di beri tanda centang, abaikan saja -> Klik Next**



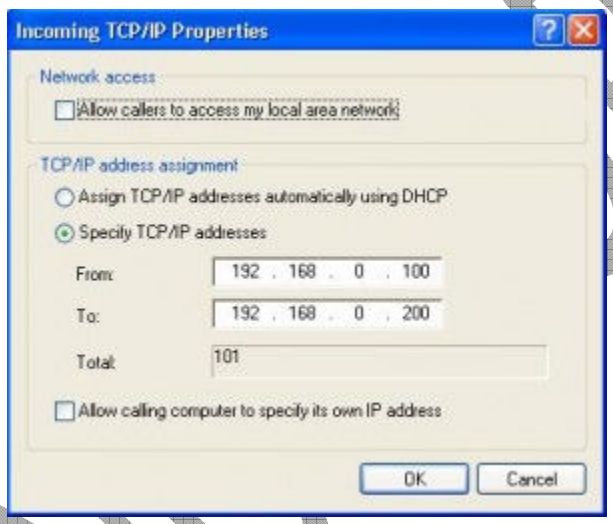
E. **Pilih "**Allow virtual private connections**" -> Klik Next**



F. **Pilih User yang kita perbolehkan untuk melakukan koneksi kedalam mesin, Bisa juga kita menambahkan User sendiri dengan klik tombol** "Add"

G. **Klik Next -> Pilih** "Internet Protocol (TCP/IP)" **-> Properties**

H. **Centang** "Allow callers to access my local area network" **(Jika memperbolehkan user mengakses lokal area network termasuk didalamnya share files/printers/device lainnya yang dishare) Kalau tidak memperbolehkan silahkan dihapus centangnya. Pilih** "Assign TCP/IP addresses automatically using DHCP" **Kalau menggunakan DHCP server (butuh program khusus karena XP tidak menyediakan DHCP server secara default). Pilih** "Specify TCP/IP addresses" **range (batasan) misalnya 192.168.0.1 sampai dengan 192.168.1.255 maka otomatis client terhubung akan mendapatkan IP dalam range tersebut selama available. Pilih** "Allow calling computer to specify it's own IP address" **Jika memperbolehkan user yang terhubung boleh merubah konfigurasi TCP/IP sendiri secara manual.**



i. Klik Next -> Klik Finish

Setelah konfigurasi benar pertanyaan klasik berikutnya pasti bagaimana cara menghubungkan client dengan server? Client bisa menggunakan program tambahan atau menggunakan default VPN client yang disediakan windows. Contohnya Telnet.

Kenapa saya tidak bisa terhubung? Pastikan username dan password semuanya benar, Jika anda berada dibelakang modem/firewall pastikan konfigurasinya benar, gunakan Port Mapping untuk mengarahkan jalur menuju komputer yang seharusnya, port standard PPTP adalah 1723.

VI. Kesimpulan

VII. Daftar Pustaka