ISSN 2338 - 1434

Jurnal Teknologi Informasi

Fakultas Ilmu Komputer dan Manajemen
Universitas Sains dan Teknologi Jayapura

JTI

Vol. 5 No. 2 Oktober 2017

Fakultas Ilmu Komputer dan Manajemen (FIKOM)
Universitas Sains dan Teknologi Jayapura (USTJ)
Jl. Raya Sentani Padang Bulan Abepura 99351 – Padang Bulan – Jayapura – Papua
Telp. (0967) – 581659, 582449

ISSN 2338 - 1434

JURNAL TEKNOLOGI INFORMASI

Volume: 5 Nomor: 2 Oktober 2017

Alamat Redaksi:

Fakultas Ilmu Komputer dan Manajemen (FIKOM)
Universitas Sains dan Teknologi Jayapura (USTJ)
Jl. Raya Sentani Padang Bulan Abepura 99351 – Jayapura – Papua
Telp. (0967) 581659, Fax. (0967) 583259
e-mail: p3ai_ustj@yahoo.co.id laman: http://ejurnal.ustj-jayapura.com

Jurnal Teknologi Informasi (JTI) merupakan Jurnal Ilmiah untuk mengembangkan ilmu dan pengetahuan di Bidang Teknologi Informasi, diterbitkan oleh Fakultas Ilmu Komputer dan Manajemen (FIKOM) bekerjasama dengan Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LP2M) Universitas Sains dan Teknologi Jayapura (USTJ).

ISSN 2338 – 1434

JURNAL TEKNOLOGI INFORMASI

Volume: 5 Nomor: 2 Oktober 2017

DAFTAR ISI

Call for Paper

Jurnal Teknologi Informasi (JTI) mengundang para Dosen Peneliti, Pengkaji, Praktisi, dan Pemerhati di bidang Teknologi Informasi untuk mengirimkan paper ke JTI.

Topik-topik yang diterima meliputi bidang-bidang (namun tidak terbatas pada):

1. Rekayasa Perangkat Lunak
2. Data Wirehouse dan Data Mining
3. Teknologi Multimedia
4. Mobile Computing
5. Parallel / Distributed Computing
6. Kecerdasan Buatan (*Artificial Intelligent*)
7. Grafika Komputer
8. Virtual Reality

Petunjuk Penulisan Naskah

1. Jurnal Teknologi Informasi diterbitkan 2 (dua) kali dalam 1 (satu) tahun, yaitu pada **Bulan April** dan **Oktober**.
2. Naskah dapat berupa hasil penelitian/kajian, aplikasi teori, desain dan tulisan ilmiah lainnya dalam bidang Teknologi Informasi yang ditulis dalam Bahasa Indonesia atau Bahasa Inggris, serta belum pernah diterbitkan atau tidak sedang diajukan ke jurnal/media publikasi lain.
3. Format penulisan:
   a. Judul ditulis menggunakan huruf capital ukuran 14, nama (para) penulis ditulis lengkap tanpa mencantumkan gelar yang disertai dengan keterangan institusi tempat penulis bekerja dan alamat korespondensi (alamat instansi dan/atau email). Dilengkapi dengan abstrak maksimum 200 kata (satu spasi) dengan 3-5 kata kunci yang dicetak miring.
   b. Naskah ditulis menggunakan kertas ukuran A4, jarak satu spasi, huruf Arial 10, jumlah halaman 8-15 (termasuk lampiran) dengan urutan penulisan: Abstrak, Pendahuluan (di dalamnya menjelaskan latar belakang, permasalahan, tujuan, metode penelitian), Tinjauan Pustaka, Hasil dan Pembahasan dan Penutup (berisi kesimpulan dan saran), dan Daftar Pustaka
   c. Daftar Pustaka ditulis urut abjad tanpa nomor urut dengan tata cara penulisan: Nama Pengarang, Tahun, Judul Buku/Jurnal, Penerbit, Kota tempat Penerbit
4. Redaksi berhak mengedit redaksional paper yang diterima tanpa mengubah arti. Paper yang tidak memenuhi syarat akan dikembalikan jika disertai perangko balasan.
5. Naskah dikirimkan ke redaksi dalam bentuk *hardcopy* dan *softcopy* dengan mencantumkan alamat pengirim dan nomor telepon/HP.
6. Untuk proses seleksi paper, maka untuk penerbitan Bulan April, batas akhir penerimaan paper adalah awal Bulan Maret, sedangkan untuk penerbitan Bulan Oktober, paper diterima pada awal Bulan September.

Membangun Jaringan Komunikasi Lokal Menggunakan Virtual Private Network (VPN)

Yuliana Kolyaan[(1)], Muriani[(2)], Roberto Corputty[(3)]
mariasalimubun@gmail.com, muriani1979@gmail.com, roberto@unmus.ac.id

Fakultas Teknik
Universitas Musamus Merauke

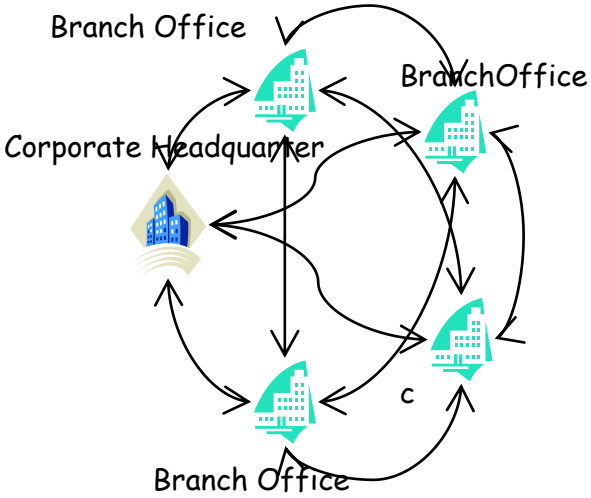
Abstraksi - *Virtual Private Network (VPN) sendiri merupakan sebuah teknologi komunikasi yang memungkinkan adanya koneksi dari dan ke jaringan publik serta menggunakannya bagaikan menggunakan jaringan lokal dan juga bahkan bergabung dengan jaringan lokal itu sendiri. Teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan publik yang sudah ada yaitu internet. Pada VPN sendiri terdapat beberapa protokol yang dapat digunakan, antara lain PPTP, L2TP, IPSec, SOCKS, CIPE yang diharapkan dapat membuat koneksi semakin membaik dari sisi kulitaspemanfaatannya.*

Kata Kunci: ***VPN, Protokol, Jaringan, Koneksi***

1. Pendahuluan

A. Latar belakang

Virtual Private Network (VPN) sendiri merupakan sebuah teknologi komunikasi yang memungkinkan adanya koneksi dari dan ke jaringan publik serta menggunakannya bagaikan menggunakan jaringan lokal dan juga bahkan bergabung dengan jaringan lokal itu sendiri. Dengan menggunakan jaringan publik ini, maka user dapat mengakses fitur-fitur yang ada di dalam jaringan lokalnya, mendapatkan hak dan pengaturan yang sama bagaikan secara fisik kita berada di tempat dimana jaringan lokal itu berada. Hal yang perlu diingat adalah sebuah private network haruslah berada dalam kondisi diutamakan dan terjaga kerahasiaannya. Keamanan data dan ketertutupan transfer data dari akses ilegal serta skalabilitas jaringan menjadi standar utama dalam Virtual Private Network ini.Virtual private network (VPN) ini juga berkembang pada saat perusahaan besar memperluas jaringan bisnisnya, namun mereka tetap dapat menghubungkan jaringan lokal (private) antar kantor cabang dengan perusahaan mitra kerjanya yang berada di tempat yang jauh. Perusahaan juga ingin memberikan fasilitas kepada pegawainya (yang memiliki hak akses) yang ingin terhubung ke jaringan lokal milik perusahaan di manapun mereka berada. Implementasi jaringan tersebut dapat dilakukan dengan menggunakan leased line.



Gambar 1. VPN dangan Leased Linebeberapa Branch Office

Namun biaya yang dibutuhkan untuk membangun infrastuktur jaringan yang luas menggunakan leased line sangat besar. Di sisi lain perusahaan ingin mengoptimalkan biaya untuk membangun jaringan mereka yang luas, oleh karena itu VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan publik yang sudah ada yaitu internet. Pada VPN sendiri terdapat beberapa protokol yang dapat digunakan, antara lain :

1. Point-to-point tunneling protocol (PPTP).
2. Layer-2 forwarding (L2F)
3. IP security protocol (IPSec).
4. PtP tunneling protocol (L2TP).

Protokol PPTP merupakan protokol awal yang dibangun oleh Microsoft. Selain menjadi dasar dari pengembangan protokol VPN selanjutnya, PPTP juga terdapat pada berbagai versi Windows, diberikan sejak Windows 95 dirilis. VPN dengan Protokol tersebut juga menawarkan solusi biaya yang murahSerta IPSec sudah menjadi standar dalam implementasi VPN karena cocok untuk lingkungan IP dibandingkan dengan PPTP, L2F, dan L2TP yang lebih cocok digunakan dalam multi protokol yang bukan dalam lingkungan IP seperti NetBEUI, IPX, dan Appletalk. Selain itu enkripsi, otentifikasi, dan manajemen kunci sudah menjadi bagian yang integral dalam IPSec.

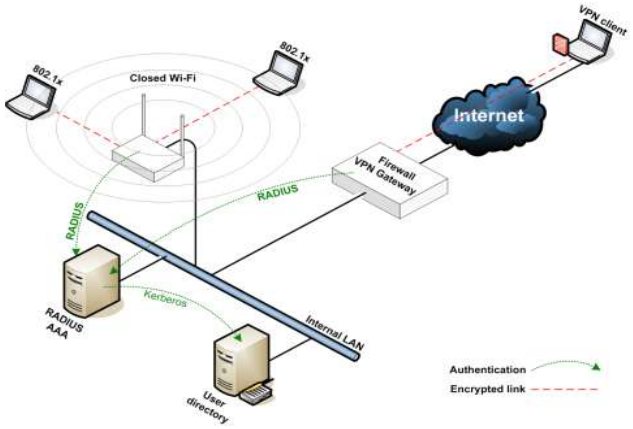
2. Dasar Teori

A. Virtual Private Network

Virtual Private Network (VPN) adalah sebuah teknologi komunikasi yang memungkinkan untuk dapat terkoneksi ke jaringan publik dan menggunakannya untuk dapat bergabung dengan jaringan lokal.

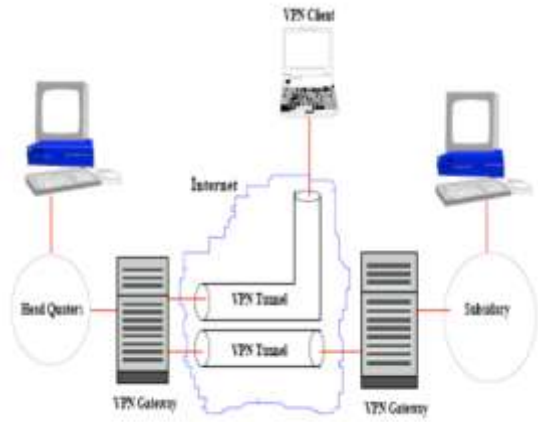
VPN (Virtual Private Network) merupakan jaringan pribadi dan tidak diakses untuk umum. Jaringan pribadi ini menggunakan internet untuk menghubungkan antar remote-site dengan aman. VPN beroperasi pada topologi yang rumit dari jaringan point to point. Fungsi dari VPN adalah untuk memberikan hubungan yang aman antara jaringan pribadi yang terhubung melalui internet. Ada 2 kata disini yang digaris bawahi yaitu :

1. Virtual Network
   Merupakan jaringan yang bersifat virtual. Tidak ada koneksi yang jaringan yang bersifat rill antara 2 titik yang saling berhubungan.
2. Private Network
   Merupakan jaringan yang terbentuk ini bersifat private (pribadi) sehingga tidak semua orang bisa akses. Datanya pun terenkripsi meskipun melalui jaringan public.



Gambar 2. Jaringan Virtual Private Network

Jadi, VPN merupakan salah satu cara aman untuk dapat mengakses Local Area Network (LAN) yang menggunakan internet atau jaringan umum untuk dapat melakukan transmisi data paket secara private dan terenkripsi. Dengan cara tersebut maka akan didapatkan hak dan pengaturan yang sama seperti halnya berada di dalam kantor atau LAN itu sendiri, walaupun sebenarnya menggunakan jaringan milik publik.

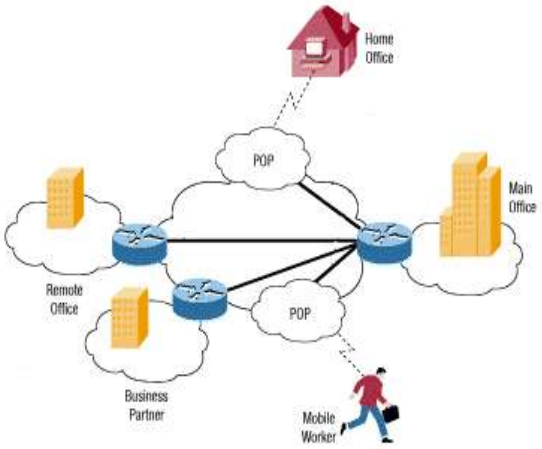


Gambar 3. Network to Network dan hostto host

VPN dapat terjadi antara dua end-system atau dua komputer atau antara dua atau lebih jaringan yang berbeda. VPN dapat dibentuk dengan menggunakan teknologi tunneling dan enkripsi. Koneksi VPN juga dapat terjadi pada semua layerpada protocol OSI, sehinggakomunikasi menggunakan VPN dapat digunakan untuk berbagai keperluan. Dengan demikian, VPN juga dapat dikategorikan sebagai infrastruktur WAN alterbatif untuk mendapatkan koneksi point-to-point pribadi antara pengirim dan penerima. Dan dapat dilakukan dengan menggunakan media apa saja, tanpa perlu media leased line atau frame relay.

3. Fungsi Utama Teknologi VPN

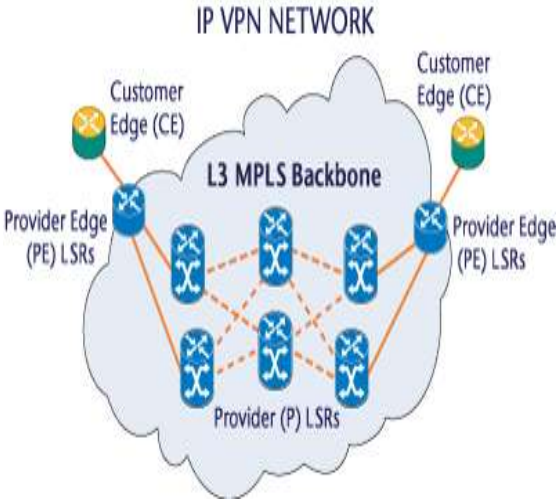
Teknologi VPN menyediakan tiga fungsi utama untuk penggunaannya. Ketiga fungsi utama tersebut antara lain sebagai berikut.Confidentially (Kerahasiaan)Dengan digunakannnya jaringan publik yang rawan pencurian data, maka teknologi VPN menggunakan sistem kerja dengan cara mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi tersebut, maka kerahasiaan data dapat lebih terjaga. Walaupun ada pihak yang dapat menyadap data yang melewati internet bahkan jalur VPN itu sendiri, namun belum tentu dapat membaca data tersebut, karena data tersebut telah teracak. Dengan menerapkan sistem enkripsi, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data dengan mudah.Data Intergrity (Keutuhan data)Ketika melewati jaringan internet, sebenarnya data telah berjalan sangat jauh melintasi berbagai negara. Pada saat perjalanan tersebut, berbagai gangguan dapat terjadi terhadap isinya, baik hilang, rusak, ataupun dimanipulasi oleh orang yang tidak seharusnya. Pada VPN terdapat teknologi yang dapat menjaga keutuhan data mulai dari data dikirim hingga data sampai di tempat tujuan.



Gambar 4. Fungsi FPN Pada Jaringan

4. Origin Authentication (Autentikasi sumber)

Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi dari sumber datanya. Kemudian, alamat sumber data tersebut akan disetujui apabila proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima berasal dari sumber yang seharusnya.
Tidak ada data yang dipalsukan atau dikirim oleh pihak-pihak lain.Non-repudiation Yaitu mencegah dua perusahaan dari menyangkal bahwa mereka telah mengirim atau menerima sebuah file mengakomodasi Perubahan.



Gambar 5. Network VPN mengunakan MPLS

5. Kendali akses

Menentukan siapa yang diberikan akses ke sebuah sistem atau jaringan, sebagaimana informasi apa dan seberapa banyak seseorang dapat menerima.

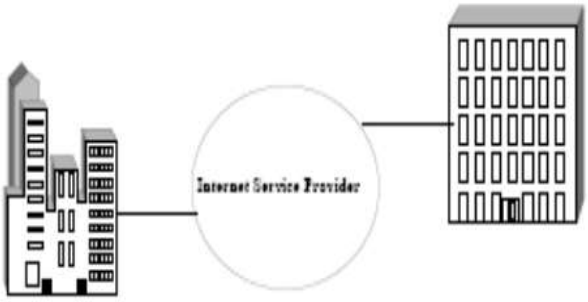
6. Perangkat VPN

Pada dasarnya, semua perangkat komputer yang dilengkapi dengan fasilitas pengalamatan IP dan diinstal dengan aplikasi pembuat tunnel dan algoritma enkripsi dan dekripsi, dapat dibangun komunikasi VPN di dalamnya. Komunikasi VPN dengan tunneling dan enkripsi ini dapat dibangun antara sebuah router dengan router yang lain, antara sebuah router dengan beberapa router, antara PC dengan server VPN concentrator, antara router atau PC dengan firewall berkemampuan VPN, dan masih banyak lagi.

7. Teknologi Tunneling

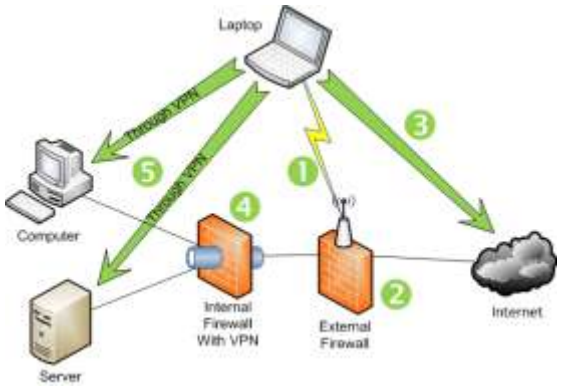
Teknologi tunneling merupakan teknologi yang bertugas untuk manangani dan menyediakan koneksi point-to-point dari sumber ke tujuannya. Disebut tunnel karena koneksi point-to-point tersebut sebenarnya terbentuk dengan melintasi jaringa umum, namun koneksi tersbut tidak mempedulikan paket-paket data milik orang lainyang sama-sama melintasi jaringan umum tersebut, tetapi koneksi tersebut hanya

melayani transportasi data dari pembuatnya.Hal ini sama dengan seperti penggunaan jalur busway yang pada dasarnya menggunakan jalan raya, tetapi dia membuat jalur sendiri untuk dapat dilalui bus khusus. Koneksi point-to-point ini sesungguhnya tidak benar-benar ada, namun data yang dihantarkannya terlihat seperti benar-benar melewati koneksi pribadi yang bersifat point-to-point.



Gambar 6.Koneksi VPN melalui Internet Publik

Teknologi ini dapat dibuat di atas jaringan dengan pengaturan IP Addressing dan IP Routing yang sudah matang. Maksudnya, antara sumber tunnel dengan tujuan tunnel telah dapat saling berkomunikasi melalui jaringan dengan pengalamatan IP. Apabila komunikasi antara sumber dan tujuan dari tunnel tidak dapat berjalan dengan baik, maka tunnel tersebut tidak akan terbentuk dan VPN pun tidak dapat dibangun.Apabila tunnel tersebut telah terbentuk, maka koneksi point-to-point palsu tersebut dapat langsung digunakan untuk mengirim dan menerima data. Namun, di dalam teknologi VPN, tunnel tidak dibiarkan begitu saja tanpa diberikan sistem keamanan tambahan. Tunnel dilengkapi dengan sebuah sistem enkripsi untuk menjaga data-data yang melewati tunnel tersebut. Proses enkripsi inilah yang menjadikan teknologi VPN menjadi mana dan bersifat pribadi.Teknologi Enkripsi Teknologi enkripsi menjamin data yang berlalu-lalang di dalam tunnel tidak dapat dibaca dengan mudah oleh orang lain yang bukan merupakan komputer tujuannya. Semakin banyak data yang lewat di dalam tunnel yang terbuka di jaringan publik, maka teknologi enkripsi ini semakin dibutuhkan. Enkripsi akan mengubah informasi yang ada dalam tunnel tersebut menjadi sebuah ciphertext atau teks yang dikacaukan dan tidak ada artinya sama sekali apabila dibaca secara langsung. Untuk dapat membuatnya kembali memiliki arti atau dapat dibaca, maka dibutuhkan proses dekripsi. Proses dekripsi terjadi pada ujung-ujung dari hubungan VPN. Pada kedua ujung ini telah menyepakati sebuah algoritma yang aka digunakan untuk melakukan proses enkripsi dan dekripsinya. Dengan demikian, data yang dikirim aman sampai tempat tujuan, karena orang lain di luar tunnel tidak memiliki algoritma untuk membuka data tersebut.



Gambar7. Akses VPN

8. Jenis implementasi VPN

1. Remote Access VPN

Pada umumnya implementasi VPN terdiri dari 2 macam. Pertama adalah remote access VPN, dan yang kedua adalah site-to-site VPN. Remote access yang biasa juga disebut virtual private dial-up network (VPDN), menghubungkan antara pengguna yang mobile dengan local area network (LAN).

Jenis VPN ini digunakan oleh pegawai perusahaan yang ingin terhubung ke jaringan khusus perusahaannya dari berbagai lokasi yang jauh (remote) dari perusahaannya. Biasanya perusahaan yang ingin membuat jaringan VPN tipe ini akan bekerjasama dengan enterprise service provider (ESP). ESP akan memberikan suatu network

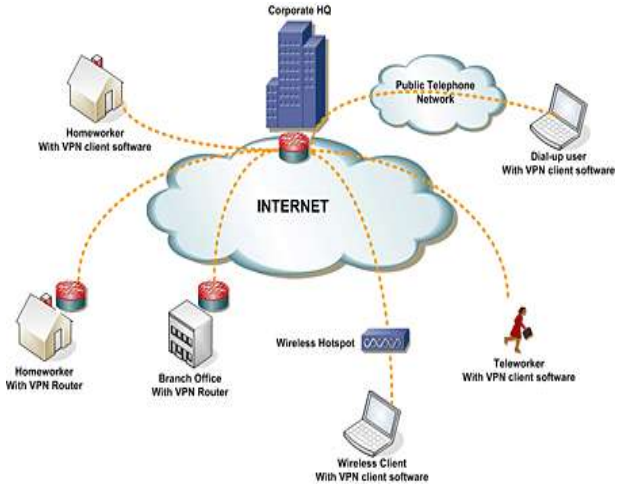
access server (NAS) bagi perusahaan tersebut. ESP juga akan menyediakan software klien untuk komputer-komputer yang digunakan pegawai perusahaan tersebut.
Untuk mengakses jaringan lokal perusahaan, pegawai tersebut harus terhubung ke NAS dengan men-dial nomor telepon yang sudah ditentukan. Kemudian dengan menggunakan sotware klien, pegawai tersebut dapat terhubung ke jaringan lokal perusahaan.
Perusahaan yang memiliki pegawai yang ada di lapangan dalam jumlah besar dapat menggunakan remote access VPN untuk membangun WAN. VPN tipe ini akan memberikan keamanan, dengan mengenkripsi koneksi antara jaringan lokal perusahaan dengan pegawainya yang ada di lapangan. Pihak ketiga yang melakukan enkripsi ini adalah ISP
.

2. Site-to-site VPN

Jenis implementasi VPN yang kedua adalah site-to-site VPN. Implementasi jenis ini menghubungkan antara 2 kantor atau lebih yang letaknya berjauhan, baik kantor yang dimiliki perusahaan itu sendiri maupun kantor perusahaan mitra kerjanya. VPN yang digunakan untuk menghubungkan suatu perusahaan dengan perusahaan lain (misalnya mitra kerja, supplier atau pelanggan) disebut ekstranet. Sedangkan bila VPN digunakan untuk menghubungkan kantor pusat dengan kantor cabang, implementasi ini termasuk jenis intranet site-to-site VPN.
Ada empat buah protocol yang biasa dan sering digunakan dalam pengimplementasian VPN(Virtual Private Network).

1. Ipsec (Ip Security Protocol)
2. Layer-2 Forwarding
3. Layer-2 Tunneling Protocol (L2TP)
4. Point to Point Tunneling Protocol

Secara umum ada empat komponen dalam VPN internet: jaringan internet, security gateways, security policy, dan key management. Jaringan internet menyediakan infrastruktur komunikasi data untuk VPN. Security gateways berdiri antara jaringan public dan private, mencegah intrusi yang tidak berhak kedalam jaringan private. Security gateways juga menyediakan layanan tunneling dan enkripsi data sebelum ditransmisikan ke jaringan public. Secara detail security gateway untuk VPN meliputi kategori: router, firewall, hardware khusus
VPN yang terintegrasi, dan perangkat lunak VPN.



Gambar 8. Topologi Jaaringan VPN

9. Komponen VPN

Agar terjalinnya sebuah ikatan koneksi antara kedua titik jaringan menggunakan VPN, maka diperlukan beberapa komponen diantaranya :

1. Koneksi Internet

Sudah jelas, kata "virtual" dalam VPN berarti koneksi jaringan privat secara "tidak langsung", yang artinya VPN membutuhkan media internet agar dapat diaplikasikan. Jika ada sebuah private network antar dua lokasi tanpa melalui internet, hal itu disebut dengan leased line network.

2. IP Publik

IP Publik ini wajib diterapkan pada VPN Server agar dapat dikenali oleh client-nya melalui internet.

3. VPN Server

Sebuah VPN tidak dapat dilakukan tanpa adanya penyedia layanan VPN. VPN Server ini yang menerima koneksi privat dari suatu jaringan lain atau suatu client secara personal. VPN Server dapat diimplementasikan pada sebuah kantor.

4. VPN Account

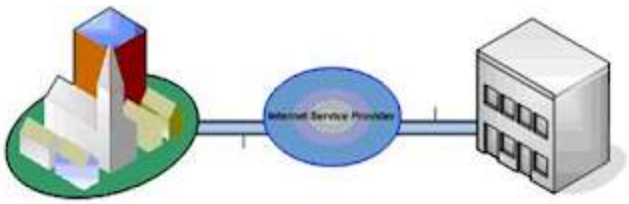
Agar koneksi VPN dapat terjalin pasti membutuhkan autentikasi user dan password dari client-nya agar koneksi menjadi aman. VPN account ini dibuat pada VPN Server. Pada beberapa metode VPN juga diterapkan sistem keamanan yang lebih ketat seperti penggunaan certificate dan otorisasi user.

5. VPN Client

Seperti yang sudah disinggung di atas, ada 2 macam client yang dapat terkoneksi dengan VPN yaitu perangkat personal secara langsung (komputer/laptop/smartphone), dan sebuah jaringan lokal lainnya. Untuk perangkat personal, dibutuhkan software VPN Client seperti OpenVPN Client, PPTP Client Windows, dll. Tetapi jika client-nya adalah sebuah jaringan lokal lain seperti kantor, harus dipasang sebuah dedicated VPN Client yang biasanya diimplementasikan pada router/server firewall kantor tersebut.

10. Jenis-jenis VPN berdasarkan Koneksi/Topologi

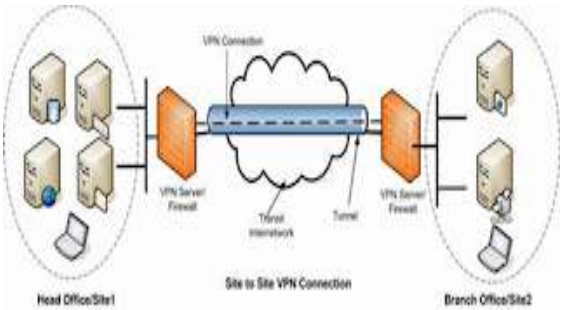
1. Jaringan Privat melalui ISP



Gambar 8. Jaringan Privat melalui ISP

VPN dengan konsep ini merupakan sebuah layanan yang disediakan oleh Internet Service Provider bagi perusahaan-perusahaan besar yang ingin menghubungkan kantor pusat dengan cabang-cabangnya melalui koneksi privat yang aman. VPN jenis ini biasanya menggunakan konsep MPLS dengan BGP Routing. Meskipun tidak secara langsung melalui internet (hanya melalui jaringan ISP), VPN ini tidak termasuk leased line karena ada peran ISP yang membuat saluran "tidak langsung" antar jaringan perusahaan tersebut, tetapi juga dapat melakukan routing menuju internet. VPN dengan konsep ini memakan biaya yang lebih besar namun dengan keamanan yang sangat tangguh.

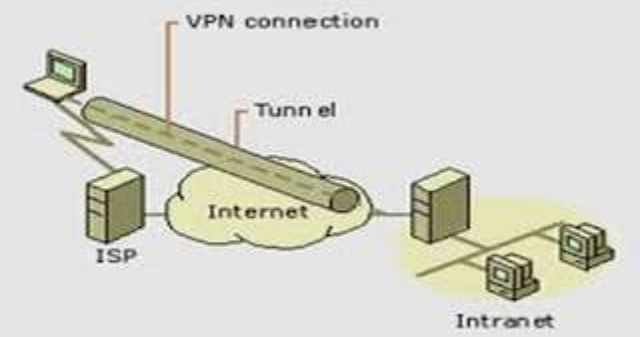
2. VPN Site to Site



Gambar 9. VPN Site to Site

VPN jenis ini menghubungkan kedua jaringan lokal, misalnya kantor pusat dengan kantor cabang. Bedanya, VPN SIte to Site tidak memerlukan peran ISP dalam implementasinya. Semua konfigurasi dapat dilakukan oleh pelaku/vendor IT pada jaringan tersebut. Pada satu site dibuatkan sebuah dedicated VPN Server dan di site lain dibuatkan sebuah dedicated VPN Client sehingga kedua jaringan lokal ini dapat saling terhubung melalui jaringan private. Koneksi "tunneling" VPN ini melalui internet, tidak hanya melalui ISP saja. VPN ini memakan biaya yang murah dengan keamanan yang disesuaikan dengan protokol VPN yang digunakan (PPTP/L2TP/lainnya).

3. Road Warrior



Gambar 10. Road Warrior

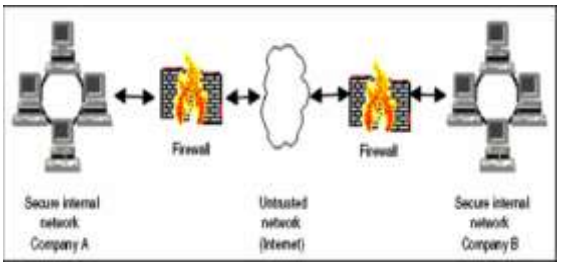
Road Warrior di sini berarti koneksi VPN yang menghubungkan perangkat personal (PC/Laptop/Smartphone) dengan suatu jaringan lokal melalui internet dengan menggunakan VPN. Ibaratnya Si "Ksatria Jalanan" yang menyendiri ini menempuh sebuah "terowongan" untuk mencapai "suatu lokasi". Misalnya kita memiliki smartphone dengan koneksi internet dari provider telekomunikasi dan memiliki software VPN Client, dapat mengakses resource jaringan kantor kita dari mana saja. Keren kan? That is The Road Warrior.
Layanan VPN jenis ini bisa juga dikombinasikan dengan VPN Site to Site sehingga tidak hanya antar jaringan lokal saja, tetapi juga dapat menghubungkan dengan perangkat personal.

12. Metode pengamanan jaringan VPN

Seperti telah dijelaskan sebelumnya, teknologi jaringan VPN menggunakan internet sebagai media transmisi data ke tempat yang dituju. Oleh karena itu pengamanan transmisi data melalui internet menjadi hal yang sangat substansial untuk diperhatikan agar diperoleh komunikasi yang aman.Beberapa metode pengamanan data yang dapat dilakukan pada teknologi jaringan VPN antara lain dengan menggunakan :

1. Firewall

Firewall merupakan sekumpulan komponen yang diletakkan antara dua jaringan. Komponen tersebut terdiri dari komputer, *router* yang dirancang sebagai buffer antara jaringan publik dan jaringan internal (*private*). Fungsi dari *firewall* adalah untuk membatasi akses ke jaringan `internal yang terhubung ke jaringan publik (misal internet). Akses ke jaringan tersebut hanya diperbolehkan bagi orang-orang yang memiliki autorisasi terhadap jaringan tersebut. Arsitektur *firewall* dapat dilihat pada gambar 11



Gambar 11. Arsitektur *firewall*

Pada saat ini terdapat dua jenis metode *firewall* yang umum digunakan yaitu

1. ***Packet filtering router***

Packet filtering router merupakan *router* yang dirancang untuk menjaga koneksi dari jaringan luar ke beberapa layanan yang tidak dibuka, menjaga koneksi jaringan internal dengan internet. *Firewall* ini menerapkan beberapa aturan untuk memfilter paket yang akan masuk dan keluar jaringan.Parameter-parameter yang digunakan untuk memfilter suatu paket adalah protokol, port atau alamat sumber paket, dan port atau alamat tujuan paket. Aturan terhadap paket yang ada di *router* mendefinisikan jenis koneksi yang diperbolehkan dan koneksi yang dilarang. *Packet filter* dapat digunakan untuk memfilter paket berdasarkan tipenya, apakah paket TCP, UDP atau ICMP.

Jika suatu aturan pada *firewall* telah terpenuhi, aturan tersebut akan langsung dijalankan. Peraturan yang diterapkan pada *firewall* dapat berupa memblok paket yang masuk atau yang akan dikirim, meneruskan paket dari atau ke luar sistem internal, atau aturan tersebut dapat pula berisi perintah untuk mengirim pesan ICMP ke tempat asal. Hanya perturan yang pertama kali terpenuhi saja yang akan dilaksanakan oleh *firewall* karena proses penyesuaian aturan dengan parameter paket dilakukan secara berurutan. Oleh karena itu aturan yang dituliskan pada *firewall* biasa disebut sebagai aturan rantai (*rule chain*).kemudahan dan keamanan dalam membuat aturan paket pada router, sebaiknya aturan yang didefinisikan pada *router* adalah dengan menuliskan aturan paket yang boleh diterima dan dikirim. Paket yang tidak memenuhi aturan itu tidak akan diteruskan oleh *router*.

Packet filtering biasanya terjadi pada level jaringan dan protokol transpor. Jika port-port tertentu pada NetBIOS tidak di-*enable*, maka permintaan komunikasi pada port-port tersebut akan diblok, sehingga sistem akan aman dari serangan internet.

Beberapa keuntungan menggunakan *packet filtering router* adalah,

a. arsitekturnya yang sederhana
b. transparansi terhadap *user*, karena setiap *user* dapat mengetahui apakah suatu paket yang diterima atau dikirm akan diteruskan *firewall*
c. proses memfilter berlangsung dengan cepat

Meskipun memiliki beberapa keuntungan, *packet filtering router* juga memiliki beberapa kekurangan yaitu,

a. kesulitan dalam menerapkan aturan filter pada *router*
b. kurangnya sistem autentikasi terhadap *router*

Beberapa kelemahan di atas dapat menyebabkan serangan terhadap sistem yang dijaga menggunakan *packet filtering router*. Beberapa kemungkinan serangan yang dapat menyerang *packet filtering router* adalah *IP address spoofing*, dan *source routing attacks*.

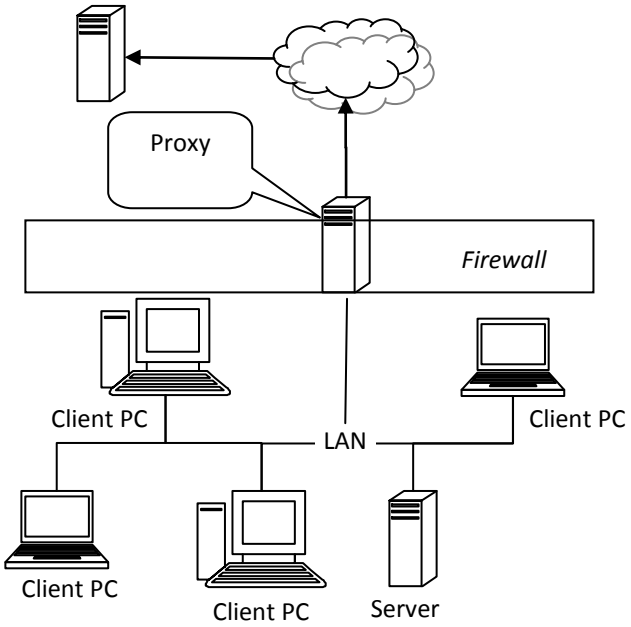
IP address spoofing merupakan teknik yang digunakan penyusup untuk mendapatkan akses ke komputer tertentu. Sang penyusup mengirim pesan ke komputer yang dituju menggunakan alamat IP seolah-olah pesan tersebut berasal dari komputer yang memiliki akses. Untuk melakukan *IP address spoofing*, sang penyusup harus memperoleh alamat IP yang memiliki hak akses. Kemudian penyusup tersebut harus memodifikasi *header* paket yang akan dikirim sehingga seolah-olah paket tersebut berasal dari komputer yang memiliki hak akses.*Source routing attacks* merupakan teknik untuk mengendalikan jalur transmisi suatu paket pada suatu jaringan. Paket yang dikirim melalui TCP/IP tidak akan memperdulikan jalur yang akan dilaluinya ke alamat IP yang dituju. Setiap paket yang dikirim dari titik A ke titik B dapat melalui jalur yang berbeda. Jalur pengiriman paket melalui TCP/IP sangat tergantung dari *traffic* di jaringan, kemampuan *router*, dan faktor lainnya.Pengirim paket menggunakan teknik *source routing* dapat menentukan rute yang dilalui paket menuju alamat yang dituju. Jika rute yang diinginkan tidak bias dilalui, maka paket akan terhenti dan tidak akan terkirim ke alamt tujuan. Jika paket yang dikirim sampai ke alamat yang dituju dan penerima membalas paket ke pengirim, paket tersebut akan dikirim melalui rute yang sama.

Teknik *source routing* pada beberapa kasus merupakan aktivitas yang legal. Misalnya, teknik ini dapat digunakan untuk menemukan alamat IP *router* pada jaringan.Namun teknik ini memiliki potensi untuk disalahgunakan. Teknik ini dapat digunakan orang-orang yang jahat untuk mempelajari seluk beluk jaringan yang akan diserang. Paket data akan mengandung informasi tentang jalur dan mesin mana saja yang telah dilaluinya. Para penyerang dapat mengirimkan data ke jaringan untuk mengmpulkan informasi tentang topologi jaringannya. Jika *source routing* berhasil dilakukan, mereka dapat menyelidiki topologi jaringan secara efektif dengan mengirimkan sejumlah paket ke bagian jaringan tertentu.Teknik *source routing* juga memungkinkan terjadinya beberapa penyerangan. Sebagai contoh, penyerang tidak dapat menyerang perusahaan A karena perusahaan

tersebut menggunakan *firewall* yang tangguh. Namun perusahaan B yang tidak memiliki *firewall* dapat berhubungan dengan perusahaan A tanpa melalui *firewall*. *Source routing* memungkinkan penyerang mengirim paket ke perusahaan A tanpa melewati *firewall* melalui perusahaan B.

2. *Proxy server*

Jenis implementasi *firewall* yang lain adalah *proxy server*. *Proxy server* merupakanJenis implementasi *firewall* yang lain adalah *proxy server*. *Proxy server* merupakan *firewall* yang dibuat secara *software* untuk memfilter paket, baik yang masuk ke jaringan internal, maupun paket yang keluar jaringan. Arsitektur *firewall* jenis ini dapat dilihat pada gambar 12



Gambar 12. Arsitektur *proxy server*

Software proxy server dijalankan pada bagian *host routing* yang berada di antara jaringan internal dan internet. Fungsi utama *proxy server* adalah untuk meneruskan koneksi aplikasi yang telah diinisiasi dari jaringan internal ke internet. Sedangkan permintaan koneksi aplikasi ke internet yang belum diinisiasi tidak akan dilayani dan akan dihentikan. Oleh karena itu *proxy sever* juga disebut sebagai *application-level gateway*.Semua koneksi dari dan ke internet akan diproses di *proxy server*. Kemudian *proxy server* akan membentuk koneksi yang telah diinisiasi. Jika koneksi berhasil, *proxy server* akan menerima data dari alamat yang dituju dan me-*relay* data tersebut ke jaringan internal. Begitu juga sebaliknya, permintaan koneksi dari internet akan diproses di *proxy server*. Jika koneksi diizinkan, *proxy server* akan membentuk koneksi ke jaringan internal. Oleh karena itu *proxy server* berperan sebagai relay trafik pada level aplikasi.

Proxy server ada yang menggunakan cache untuk proses koneksinya. Penggunaan cache akan mempercepat proses koneksi karena pada cache disimpan informasi alamat yang pernah dikunjungi. Sehingga penggunaan cache akan menghemat *bandwidth* internet. Apa bila *Proxy server* yang tidak menggunakan cache akan menurukan performa jaringan. Meskipun demikian, *proxy server* tanpa cache memiliki tingkat kemanan yang lebih baik daripada *proxy server* dengan cache.Beberapa keunggulan *proxy server* :

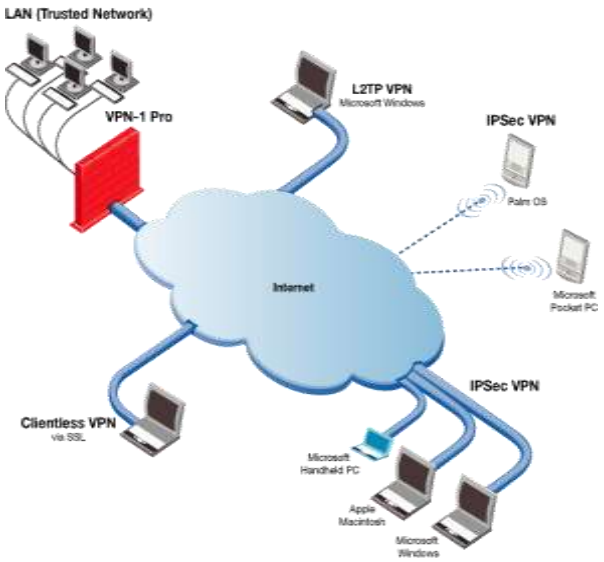
a. memiliki keamanan yang lebih baik dan lebih fleksibel daripada *packet filtering router*.
b. hanya perlu memeriksa beberapa aplikasi yang diizinkan
c. mudah untuk memeriksa trafik yang masuk ke jaringan internal

Proxy server juga memiliki kekurangan yaitu dibutuhkan proses koneksi tambahan karena *proxy server* bertindak sebagai titik sambungan. Kombinasi antara *packet filtering router* dan *proxy server* akan memberikan keamanan jaringan yang baik dan fleksibel.

2. *IPSec*

IPSec merupakan singkatan dari IP *security*. IPSec merupakan suatu protokol yang digunakan untuk melakukan pertukaran paket pada layer IP secara aman. IPSec

menyediakan dua jenis mode enkripsi, yaitu mode transport dan mode tunnel. Mode transport akan mengkripsi bagian data (*payload*) masing-masing paket tanpa mengubah *header* paket tersebut. Algoritma yang digunakan untuk mengenkripsi data adalah algoritma kriptografi simetris. IPSec mode ini menggunakan sub-protokol yang disebut sebagai *encapsulated security payload (*ESP).Pada mode tunnel, data dan *header* paket yang akan dikirim dilakukan komputasi menggunakan teknik *checksum* kriptografi dan mengubah bagian *header* paket IP menggunakan fungsi *hasing* yang aman. Paket ini akan ditambahkan *header* baru yang mengandung nilai *hash* agar informasi yang ada pada paket biasa diautentikasi di bagian penerima. Mode ini seolah-olah membuat "terowongan" khusus pada jaringan publik yang hanya dapat diakses oleh orang-orang tertentu. Contoh diagram penggunaan IPSec untuk menghasikan komunikasi yang aman menggunakan jaringan publik ditunjukkan pada gambar



Gambar 13. implementasi IPSec

Pada gambar 13 di atas jaringan privat jaringan #1 menggunakan IP privat, begitu juga dengan jaringan privat #2. Sedangkan kedua *gateway* menggunakan IP publik yang bisa diakses dari mana saja. Untuk dapat melakukan perintah ping dari jaringan internal #1 ke jaringan internal #2, ada beberapa tahapan yang harus dilalui.

Pertama, setiap paket yang akan dikirim ke IP 192.168.2.1 harus dibungkus ke dalam paket lain sehingga *header* IP yang muncul adalah IP A.B.C.D. Kemudian paket ini akan dikirim ke IP W.X.Y.Z melalui *gateway* dengan *header* IP yang menyatakan seolah-olah paket berasal dari IP A.B.C.D. Proses ini disebut sebagai proses enkapsulasi paket.

Kedua, *gateway* harus mengetahui jalan untuk mencapai IP 192.168.2.1. dengan kata lain, *gateway* harus mengarahkan paket ke IP 192.168.2.1.

Ketiga, paket yang tiba di IP W.X.Y.Z harus di ekstraksi (*unencapsulated*) sehingga diperoleh paket yang sebenarnya dan dikirim ke alamat IP 192.168.2.1.

Proses seperti ini membuat jalur khusus ("terowongan") antara dua jaringan. Dua ujung jalur ini berada di alamat IP A.B.C.D dan W.X.Y.Z. Jalur ini harus diberikan aturan yang mengizinkan alamat IP mana saja yang boleh melalui "terowongan" ini. Apabila koneksi telah terbentuk, perintah ping 192.168.2.1 yang dilakukan di komputer dengan IP 192.168.1.1 akan mendapat balasan (*reply*).

3.AAA Server

AAA server, singkatan dari *authentication*, *authorization* dan *accounting*, merupakan program server yang bertugas untuk menangani permintaan akses ke suatu komputer dengan menyediakan proses autentikasi, otorisasi dan akunting (AAA). AAA merupakan cara yang cerdas untuk mengendalikan akses ke suatu komputer, menerapkan kebijakan, memeriksa penggunaan komputer dan menyediakan informasi yang diperlukan untuk keperluan tagihan (pembayaran). Kompinasi proses ini sangat efektif untuk menyediakan manajemen dan keamanan jaringan.Proses pertama yang dilakukan adalah autentikasi, yaitu proses untuk mengidentifikasi pengguna. Proses ini bekerja berdasarkan kenyataan bahwa setiap pengguna memiliki beberapa kriteria yang unik untuk masing-

masing pengguna. Biasanya proses ini dilakukan dengan meminta pengguna untuk memasukkan *user name* dan *password*-nya. Jika masukan pengguna sesuai dengan data yang ada di database, pengguna tersebut berhak mengakses komputer atau jaringan. Namun bila masukan ini gagal, pengguna tersebut tidak bisa mengakses komputer atau jaringa tersebut.Setelah proses autentikasi, setiap pengguna harus memiliki otorisasi untuk melakukan tugaas-tugas tertentu. Sebagai contoh, setelah pengguna tersebut masuk ke jaringan yang dituju, pengguna tersebut mencoba untuk memberikan beberapa perintah pada jaringan tersebut. Proses otorisasi akan menentukan apakah pengguna tersebut dapat memberikan perintah seperti yang diinginkan atau tidak. Sehingga otorisasi dapat didefinisikan sebagai proses untuk menerapkan kebijakan untuk menentukan aktivitas, sumber dan layanan apa saja yang dapat diperoleh suatu pengguna. Biasanya proses otorisasi juga dilakukan pada saat proses autentikasi.

Proses terakhir adalah akunting yang berfungsi untuk menghitung jumlah *resource* yang digunakan setiap pengguna pada saat akses dilakukan, diantaranya waktu yang digunakan, atau besarnya data yang dikirim atau diterima selama akses berlangsung. Proses ini dilakukan berdasarkan informasi yang ada pada catatan (*log*) masing-masing pengguna. Catatan ini dapat digunakan untuk mengendalikan otoritas masing-masing pengguna, analisis kecenderungan pengguna, mengamati pemanfaatan *resource*, dan perencanaan.

4. Enkripsi

Enkripsi merupakan teknik untuk mengamankan data yang dikirim dengan mengubah data tersebut ke dalam bentuk sandi-sandi yang hanya dimengerti oleh pihak pengirim dan pihak penerima data. Teknik enkripsi pada computer bedasarkan pada perkembangan ilmu kriptografi. Dahulu kriptografi banyak digunakanpada bidang militer. Tujuannya adalah untuk mengirimkan informasi rahasia ke tempat yang jauh. Namun saat ini enkripsi telah banyak digunakan untuk aplikasi-aplikasi seperti informasi kartu kredit, PIN (personal identity number), informasi tabungan di bank dan lain sebagainya. Enkripsi yang banyak digunakan saat ini adalah enkripsi kunci simetris dan enkripsi kunci publik.

1. **Kunci simetris**

Pada enkripsi menggunakan kunci simetris, setiap komputer memiliki kunci rahasia (kode) yang dapat digunakan untuk mengenkripsi informasi sebelum informasi tersebut dikirim ke komputer lain melalui jaringan. Kunci yang digunakan untuk mengenkripsi data sama dengan kunci yang digunakan untk mendekripsi data. Oleh karena itu, kunci tersebut harus dimiliki kedua komputer.

Kunci harus dipastikan ada pada computer penerima. Artinya pengirim harus memberitahu kunci yang digunakan pada penerima melalui orang yang dipercaya. Selanjutnya informasi yang akan dikirim, dienkripsi menggunakan kunci tersebut. Sehingga penerima bisa mendekripsi, dan mendapatkan informasi yang diinginkan. Contoh sederhana kunci simetris mengganti huruf yang sebenarnya dengan 2 huruf di bawahnya. Misalnya “A” menjadi “C” dan “B” menjadi “D”. Kunci tersebut harus diketahui oleh penerima. Jika penerima tidak memiliki kunci, informasi tersebut tidak ada gunanya. Pada enkripsi ini, pihak penerima mengetahui kunci pihak pengirim.

2. **Kunci publik**

Enkripsi kunci publik menggunakan kombinasi kunci privat dan kunci publik. Kunci privat hanya diketahui oleh pihak pengirim informasi. Sedangkan kunci publik dikirim ke pihak penerima. Untuk mendekripsi informasi, pihak penerima harus menggunakan kunci public dan kunci privat miliknya. Kunci privat penerima berbeda dengan kunci privat pengirim, dan hanya penerima saja yang mengetahuinya.

Enkripsi kunci publik memerlukan perhitungan yang besar. Akibatnya sebagian besar sistem menggunakan kombinasi kunci public dan kunci simetri untuk proses enkripsi data. Pada saat dua komputer akan berkomunikasi secara aman, komputer A akan membuat kunci simetris dan dikirim ke komputer B menggunakan enkripsi kunci publik. Setelah itu kedua komputer dapat berkomunikasi menggunakan enkripsi kunci simetris. Setelah proses komunikasi tersebut selesai, kunci simetris untuk sesi tersebut dibuang. Jika kedua komputer ingin membentuk sesi komunikasi yang aman lagi, kunci simteris untuk sesi tersebut harus dibuat lagi. Dengan demikian setiap akan membentuk suatu sesi, kunci simetris baru akan dibuat.

Algoritma kunci publik dibuat berdasarkan algorima “hashing”. Kunci publik dibuat berdasarkan nilai “hash“ yang diperoleh. Ide dasar enkripsi kunci publik adalah perkalian dua bilangan prima yang menghasilkan bilangan prima yang baru. Contohnya diberikan pada tabel di bawah ini.

Tabel 1. Algoritma “hashing’

Angka masukan	Algoritma “hashing”	Nilai “hash”
10667	Masukan x 143	1525381

Angka masukan merepresentasikan ingormasi yang akan dikirim. Nilai “hash” merupakan representasi informasi yang telah dienkripsi. Dari hasil di atas dapat ditunjukkan bahwa nilai “hash” 1525381 sanga sulit untuk dicari faktor-faktor bilangan primanya kalau tidak memiliki kuncinya. Namun kalau kuncinya (pengali) diketahui, sangat mudah untuk mendapatkan informasi aslinya. Algoritma kunci publik yang sebenarnya jauh lebih rumit dari contoh ini. Contoh ini adalah ide dasar munculnya lagoritma kunci publik.Kunci publik umumnya menggunkan algoritma yang lebih kompleks, dan nilai “hash” yang sangat besar mencapai 40-bit atau bahkan 128-bit. Jika nilai “hash” dibangun menggunakan 128-bit, akan ada 2^{128} kombinasi yang muncul. Nyaris tidak mungkin untuk memecahkan enkripsi ini tanpa ada kuncinya.

3. Hasil dan Pembahasan

1. Virtual Private Network (VPN) dapat memberikan solusi bagi berbagai persoalan yang ada. Karena dengan adanya VPN, hubungan yang dilakukan antara kantor pusat dan cabang serta partner bisnis perusahaan lebih ekonomis. Selain itu koneksi dengan VPN tidak terbatas hanya pada hubungan antara kantor pusat dan cabang saja, tetapi VPN juga memberikan keuntungan lebih dengan memberikan security hubungan untuk pengguna yang berpindah- pindah.
2. IP VPN berbasis jaringan publik yang berjalan di platform IP sehingga pengiriman layanan lebih bersifat connectionless, dalam artian data terkirim begitu saja tanpa ada proses pembentukan jalur terlebih dahulu (connection setup). IP bertugas untuk menangani masalah-masalah pengiriman, juga menjadi tanggung jawab IP untuk menangani masalah pengenalandatagram atau reassembly datagram sebagai akibat langsung proses fragmentasi.

3. Penggunaan jaringan publik internet dalam layanan VPN menuntut jaminan security yang lebih baik dibandingkan dengan layanan internet yang biasa. Sharing infrastruktur jaringan publik untuk suatu hal yang namanya privat menuntut pengamanan-pengamanan tersendiri.
4. Dengan adanya jaminan security tersebut, pelanggan dapatmengirimkan dan mengakses informasi secara aman dan terlindung dari kemungkinan disusupi oleh pengakses yang tidak diinginkan.

4. Penutup

1. Kesimpulan

VPN merupakan layanan yang menyediakan komunikasi yang aman antara dua jaringan internal atau lebih melalui jaringan publik. Penggunaan VPN dapat menghemat biaya produksi bila dibandingkan dengan pembangunan jaringan khusus untuk menghubungkan tempat-tempat yang jauh.Meskipun demikian, keamanan pengiriman data menggunakan VPN harus diperhatikan. Beberapa teknik pengamanan yang telah dijelaskan dapat dipilih sesuai dengan kondisi dan keperluan masing-masing perusahaan. Setiap teknik pengamanan memiliki keunggulan dan kelemahan. Oleh karena itu perlu dipikirkan teknik mana yang akan diterapkan pada perusahaan agar memeproleh hasil yang efektif dan efisien.

2. Saran

VPN sebaiknya menggunakan tunnel mode dengan protokol ESP dan melakukan enkripsi, dan menggunakan pertukaran kunci secara otomatik untuk pengamanan maksimum pada transmisi data.

Bagi perusahaan yang ingin mengaplikasikan IPSec (VPN) perlu merumuskan terlebih dahulu dengan jelas mengenai fungsi dan tujuan keamanan transmisi data yang ingin dicapai, agar pemilihan perangkat keras, perangkat lunak, dan spesifikasi IPSec yang ada dapat memenuhi kriteria yang diinginkan perusahaan tersebut.

DAFTAR PUSTAKA

Aris Wendi-Ahmad SS Rahmadhan , MembangunVPN Linux Secara Cepat, Penerbit Yogya andi 2015

Aditya, A. Mahir Membuat Jaringan Komputer. Jakarta: Dunia Komputer, 2011

Nanang sadikin, Cara mudah dan murah membangun solusi VPN client acces diwindows server 2003. Gramedia Digital

Nial Mansfield, PRACTICAL TCP/IP Mendisain, Menggunakan, dan Trubleshooting Jaringan TCP/IP di Linux dan Windows, Jilid 2

Sofana, Iwan. 2009. Cisco CCNA dan Jaringan Komputer Edisi Revisi. Bandung: Informatika.

Thomas, Tom. Network Security First step. 2005. Penerbit Andi, Yogyakarta.

Thomas, Tom.. Computer Networking First step, 2005

Winarto, E., Zaki, A., & Community, S. , Membuat Sendiri Jaringan Komputer. Semarang: PT. Elex Media Komputindo, 2013.

http://www.ipsec-howto.org/ipsec-howto

www.cert.or.id/~budi/courses/Http://linto.jmn.net.id

www.budi.insan.co.id/courses/ec7010/dikmenjur