BAB II

VIRTUAL PRIVATE NETWORK

2.1. Pengenalan Virtual Private Network

Era globalisasi, telah memaksa semua komponen di dunia untuk berkembang, dan beradaptasi dengan perkembangan jaman. Di mana perkembangan tersebut didukung dengan perkembangan teknologi yang semakin maju, serta mempermudah kerja manusia. Pada jaman dahulu untuk mengirimkan pesan, surat menjadi metode utama yang digunakan pada saat itu. Waktu pengiriman yang dibutuhkan pun juga tergantung dari jarak surat itu dikirimkan. Namun pada saat ini, surat sudah mulai ditinggalkan. Penggunaan faksimili dan e-mail sudah mulai menggatikan surat. Pengiriman pesan pun tidak membutuhkan waktu yang lama, sehingga pekerjaan manusia menjadi lebih efisien.

Begitu pula pada dunia usaha. Berkembangnya sebuah perusahaan, merupakan sebuah tuntutan bagi perusahaan tersebut untuk bersaing pada era globalisasi. Perkembangan perusahaan dapat terjadi pada berbagai macam aspek, mulai dari perkembangan kualitatif, maupun kuantitatif. Perkembangan kualitatif lebih mengarah pada perkembangan kualitas perusahaan tersebut, seperti penggunaan teknologi informasi, maupun penggunaan mesin-mesin yang dapat membantu kerja manusia. Sedangkan perkembangan kualitatif mengarah pada pada kapasitas perusahaan tersebut, seperti menambah pabrik baru, atau kantor cabang baru.

Pada perkembangan-perkembangan tersebut, bukan berarti pabrik atau kantor cabang baru tersebut terlepas dari perusahaan. Cabang-cabang baru tersebut tetap harus dapat dipantau oleh kantor pusat, di mana semua manajemen dan kebijakan ditentukan oleh kantor pusat. Oleh karena itu, dibutuhkan sarana komunikasi bagi kantor pusat dan kantor cabang.

Dalam komunikasi yang dilakukan oleh kantor pusat dan cabang tersebut, diperlukan adanya jaminan keamanan. Karena informasi yang dikirimkan,

mungkin berisi data-data yang sifatnya rahasia dan berdampak pada keberadaan perusahaan. Sehingga jika data tersebut tidak sengaja jatuh ke tangan perusahaan lain, dapat berdampak buruk pada perusahaan.

Internet merupakan sebuah solusi komunikasi. Namun keamanan Internet sedikit dipertanyakan, karena tidak ada yang tahu secara pasti apa yang terjadi pada data saat dikirimkan melalui Internet. Sehingga sangat mungkin sekali, bahwa data yang dikirimkan, dapat disadap oleh pihak-pihak yang tidak bertanggung jawab.

Sehingga untuk memenuhi kebutuhan komunikasi yang aman, terdapat beberapa pilihan solusi antara lain:

- Leased Line
- Dial Up
- Frame Relay
- Asynchronous Transfer Mode (ATM)

Dari solusi-solusi tersebut, komunikasi yang diberikan memberikan jaringan keamanan yang mumpuni. Namun, biaya yang dikeluarkan dalam penggunaan solusi tersebut cukup besar, terutama untuk pembangunan infrastruktur. Sehingga timbul sebuah tuntutan baru selain komunikasi dan keamanan, yakni biaya.

Internet merupakan sebuah solusi komunikasi dengan biaya yang dapat dikatakan cukup terjangkau. Oleh karena itu, untuk membentuk sebuah komunikasi yang aman dan terjangkau, timbullah sebuah konsep yang bernama Virtual Private Network.

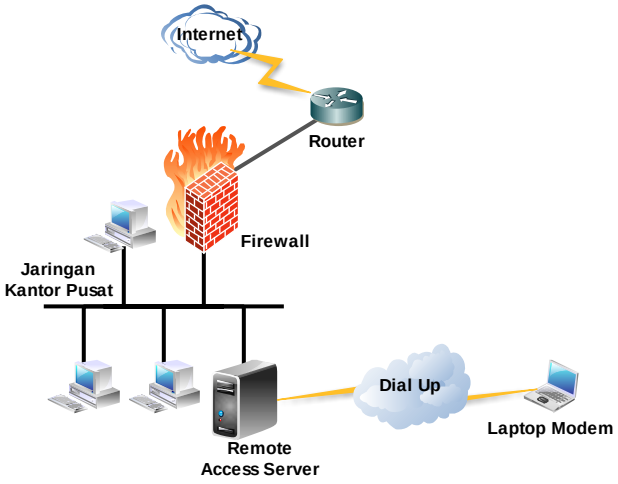
Virtual Private Network terdiri dari tiga kata, yaitu Virtual, Private, dan Network. Dari ketiga kata tersebut, dapat disimpulkan arti dan fungsi dari VPN, yaitu Jaringan Pribadi Virtual. Kata “private” memberikan arti kerahasiaan, di mana data yang dikirimkan bersifat rahasia dan tidak boleh diketahui oleh pihak lain yang tidak berkepentingan. Sedangkan tambahan kata “virtual”, memberikan arti maya, atau bukan sesungguhnya. Dikatakan bukan sesungguhnya, karena data rahasia tersebut ternyata dilewatkan pada jaringan umum yang sifatnya tidak

aman. Pada konteks ini, jaringan umum, atau jaringan tidak aman yang dimaksud adalah Internet. Karena melalui Internet, selalu ada kemungkinan bahwa data telah dimodifikasi.

Virtual Private Network adalah fasilitas yang memungkinkan koneksi jarak jauh (remote access) yang aman dengan memanfaatkan jaringan Internet untuk melakukan akses menuju jaringan yang dituju.

Sebelum teknologi Virtual Private Network ada, akses remotemenuju jaringan lokal dilakukan dengan menggunakan fasilitas *dial-up remote access*. Dengan fasilitas ini, pada jaringan lokal yang akan diakses, harus disediakan sebuah remote access server yang dapat dihubungkan dengan modem melalui jaringan telepon biasa, langsung dari perangkat komputer ataupun laptop pengguna. Demikian pula pada perangkat komputer atau laptop pengguna tersebut, harus sudah terpasang remote access client.

Koneksi dial-up dari modem pada perangkat komputer ataupun laptop pengguna ini akan langsung menuju modem pada remote access server, seperti tampak pada Gambar 2.1.

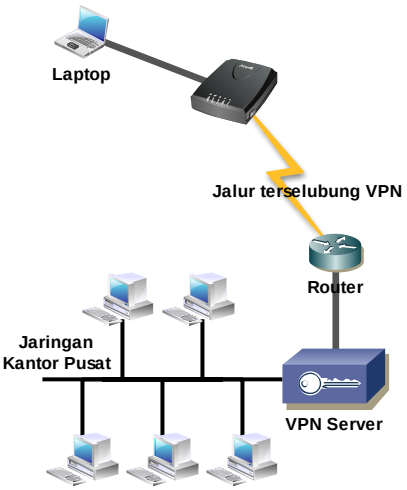


Gambar 2.1
Remote Access Dial-Up

Biaya yang diperlukan dalam penggunaan fasilitas Remote Access Dial-Up ini cukup besar, terlebih jika koneksi dilakukan dari luar negeri, karena menggunakan Sambungan Langsung Internasional atau SLI. Selain itu koneksi yang diberikan juga cukup lambat apabila dibandingkan dengan koneksi

broadband lainnya, misalnya dengan koneksi Asymmetric Digital Subscriber Line atau ADSL.

Virtual Private Network menggunakan jaringan Internet, sehingga koneksi dengan jaringan VPN dapat dilakukan dengan koneksi Internet yang disediakan oleh Internet Service Provider. Adapun ilustrasinya dapat digambarkan seperti Gambar 2.2.



Gambar 2.2
Jaringan dengan VPN

Penggunaan VPN menjadi sangat populer saat ini, karena VPN memberikan jaringan keamanan yang hampir sama dengan jaringan pribadi. Dengan menggunakan VPN Client Software pada perangkat komputer atau laptop pengguna, maka pengguna dapat memiliki akses menuju jaringan yang dituju dengan fasilitas yang diberikan oleh Virtual Private Network melalui jaringan Internet yang sudah tersedia di mana saja. Saat ini, biaya yang diperlukan untuk memperoleh koneksi Internet sudah cukup terjangkau, sehingga faktor ini menjadi faktor utama beralihnya penggunaan Dial-Up menuju Virtual Private Network.

Namun dengan kemudahan ini, bukan berarti koneksi yang diberikan oleh Internet menjadi suatu solusi yang aman, karena informasi-informasi yang dikirimkan melalui jaringan Internet dapat disadap oleh pengguna-pengguna yang lainnya, karena Internet merupakan jaringan umum atau publik yang dipakai bersama-sama oleh banyak orang, seperti layaknya jalan umum.

Penggunaan Virtual Private Network memberikan jaminan keamanan yang tinggi karena koneksi dengan Virtual Private Network dilakukan dengan perangkat yang menerapkan metode autentikasi untuk memberikan kejelasan identitas kepada pengguna, serta menerapkan metode enkripsi pada data yang dikirimkan melalui jaringan Virtual Private Network yang menggunakan jaringan publik.

Sesuai dengan kebutuhan, tersedia beberapa metode enkripsi dan autentikasi yang dapat digunakan dalam implementasi Virtual Private Network, seperti Internet Protocol Security (IPsec), Internet Key Exchange (IKE), dan Internet Security Association and Key Management Protocol (ISAKMP). Sehingga komunikasi antara VPN Client dan VPN Server yang melalui jaringan publik tersebut seakan-akan menjadi jalur pribadi yang tidak dapat disadap oleh pengguna lain yang tidak berkepentingan. Oleh sebab itu, jalur penghubung tersebut disebut dengan jaringan virtual, karena jalur pribadi tersebut, sebenarnya bukan jalur pribadi yang sebenarnya, melainkan hanya sebuah jaringan publik.

Virtual Private Network merupakan salah satu solusi dengan berbakai macam metode dan PKI (Public Key Infrastructure), yang memungkinkan sebuah instansi atu perusahaan melakukan pengiriman data secara aman melalui Internet.

Virtual Private Network merupakan sebuah jaringan pribadi yang dibuat melalui pembuatan terowongan (tunneling) melalui jaringan umum atau publik, yang secara umum adalah melalui Internet. Tanpa menggunakan jaringan khusus, Virtual Private Network menggunakan koneksi virtual yang disalurkan melaluiInternet dari pusat menuju titik yang berjarak jauh (remote site). Virtual Private Network yang petama kali diimplementasikan murni terowongan IP, tanpa mengimplementasikan auntentikasi dan enkripsi terhadap sebuah data. Sebagai contoh, Generic Routing Encapsulation (GRE) yang merupakan tunneling protocol yang dikembangkan oleh Cisco yang dapat merangkum berbagai jenis protokol Network Layer paket di dalam terowongan IP. Proses ini menciptakan sebuah hubungan antar titik (point-to-point) secara virtual menuju router pada remote points melalui sebuah IP antar jaringan. Contoh yang lain dari Virtual Private Network yang tidak memberikan keamanan tambahan secara otomatis

adalah Frame Relay, ATM PVC, dan jaringan Multiprotocol Label Switching (MPLS).

Cakupan sebuah Virtual Private Network adalah di mana akses komunikasi secara ketat dikontrol dalam memberikan ijin pada sebuah titik akses untuk bergabung pada Virtual Private Network tersebut. Kerahasiaan (confidentiality) diperoleh dengan memberikan proses enkripsi pada trafik dalam Virtual Private Network tersebut. Saat ini, implementasi keamanan Virtual Private Network dengan menggunakan proses enkripsi sudah setara dengan konsep jaringan pribadi (private).

Virtual Private Network memberikan beberapa keuntungan, yaitu:

- **Hemat Biaya**

  Virtual Private Network memungkinkan sebuah organisasi atau perusahaan untuk menggunakan biaya secara efektif melalui pihak ketiga, dalam hal ini koneksi Internet yang menghubungkan pusat dengan remote point. Virtual Private Network mengurangi biaya yang dibutuhkan untuk membentuk hubungan Wide Area Network yang relatif cukup mahal. Di samping itu, dengan munculnya teknologi hemat biaya serta bandwith tinggi, seperti DSL (Digital Subscriber Line), organisasi atau perusahaan dapat menggunakan Virtual Private Network untuk mengurangi biaya konektivitas yang mereka butuhkan, sekaligus meningkatkan bandwith koneksi remote.

- **Keamanan**

  Virtual Private Network memberikan tingkat keamanan tertinggi dengan menggunakan algoritma enkripsi yang rumit dan protokol autentikasi yang mampu melindungi data dari akses dari pihak pihak yang tidak berkepentingan dan tidak bertanggungjawab .

- **Skalabilitas**

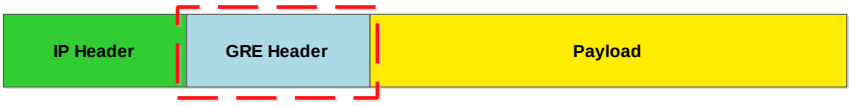
  Virtual Private Network memungkinkan organisasi atau perusahaan untuk menggunakan infrastruktur Internet yang ada di dalam ISP (Internet Service Provider) beserta perangkatnya. Dengan kemampuan ini, maka dapat mempermudah perusahaan untuk melakukan perluasan jaringan,

seperti menambahkan sebuah pengguna baru, sehingga organisasi atau perusahaan dapat meningkatkan kapasitas yang signifikan tanpa menambah infrastruktur yang signifikan.

- **Kompatibel dengan teknologi broadband yang ada**

  Virtual Private Network memungkinkan pekerja yang selalu berpindah-pindah tempat (mobile workers) untuk bekerja dengan cekatan tanpa harus kembali ke kantor pusat dengan memanfaatkan koneksi broadband untuk mendapatkan akses menuju jaringan pusat perusahaan mereka. Selain itu, hal ini juga memberikan fleksibilitas dan efisiensi yang signifikan kepada para pekerja tersebut. Kecepatan tinggi yang diberikan oleh koneksi broadband memberikan solusi hemat untuk menghubungkan pekerja dengan kantor pusat.

Dengan kata lain, Virtual Private Network menghubungkan dua buah titik melalui jaringan publik untuk membentuk sebuah koneksi logis. Koneksi logis (logical connection) dapat dibuat di layer 2 atau layer 3 OSI (Open Systems Interconnection). Berdasarkan koneksi logis ini, teknologi Virtual Private Network ini dapat diklasifikasikan secara luas menjadi Layer 2 VPN dan Layer 3 VPN. Tidak ada perbedaan dalam pembentukan koneksi antara titik pada Layer 2 maupun Layer 3, yaitu dengan cara menambahkan sebuah header pengiriman di depan payload untuk mendapatkan situs tujuan.



Gambar 2.3
Header Pengiriman

Contoh umum Layer 3 VPN adalah GRE, MPLS, dan IPsec. Layer 3 VPN bisa berarti koneksi point-to-point seperti GRE dan IPsec, ataupun koneksi any-to-any menggunakan MPLS.

Generic Routing Encapsulation (GRE) pada awalnya dikembangkan oleh Cisco, dan kemudian distandarisasi sebagai RFC 1701. Header IP untuk

pengiriman GRE didefinisikan dalam RFC 1702. Sebuah tunnel GRE yang terbentuk antara dua buah titik dapat disebut sebagai Virtual Private Network, karena data pribadi antara kedua titik tersebut diselundupkan dalam sebuah header pengiriman GRE.

Setelah dipelopori oleh Cisco, MPLS (Multiprotocol Label Switching) yang awalnya dikenal sebagai Tag Switching dan kemudian distandarisasi oleh IETF (Internet Engineering Task Force) menjadi MPLS. ISP menjadi semakin gencar dalam menawarkan layanan Virtual Private Network MPLS kepada pelanggannya. Virtual Private Network MPLS menggunakan label untuk menyelundupkan data asli atau payload untuk membentuk Virtual Private Network.

Perlindungan terhadap keamanan data diberikan dengan melakukan enkripsi pada data yang bersangkutan. Hal ini dilakukan untuk mencegah penyadapan dari pihak-pihak yang tidak bekepentingan dan tidak bertanggungjawab. Proses enkripsi diperoleh dengan pendirian perangkat enkripsi pada masing-masing titik atau situs. IPsec merupakan seperangkat protokol yang dikembangkan dengan dukungan dari IETF untuk memperoleh layanan jaringan yang aman melalui jaringan IP packet switched. Internet merupakan jaringan IP packet switched yang paling sering ditemui, karena itu, sebuah Virtual Private Network IPsec yang digunakan melalui jaringan umum Internet dapat memberikan penghematan biaya secara signifikan untuk sebuah perusahaan dibandingkan dengan jalur sewaan (leased-line).

IPsec memungkinkan autentikasi, integritas, kontrol akses, dan kerahasiaan terhadap data yang dikirimkan. Dengan IPsec, pertukaran informasi antara situs remote dapat dienkripsi dan diverifikasi. Kedua titik remote dapat menggunakan IPsec sebagai protokol keamanannya.

2.2. Topologi Virtual Private Network

Berdasarkan cara koneksinya, Virtual Private Network dapat dibagi menjadi dua tipe:

- Site to Site VPN

  Site to Site VPN terbentuk ketika perangkat koneksi pada kedua pihak koneksi Virtual Private Network saling mengetahui aakan adanya koneksi di antara kedua pihak. Virtual Private Network ini bersifat statis, dalam artian selalu terhubung dan host internal tidak mengetahui tentang adanya Virtual Private Network. Frame Relay, ATM, GRE, dan VPN MPLS adalah contoh site-to-site VPN.

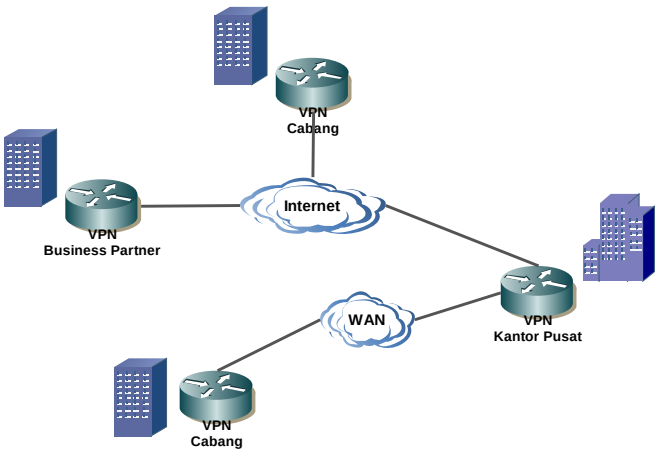
- Remote User VPN

  Sebuah remote access VPN terbentuk ketika informasi VPN tidak lagi diatur secara statis, tetapi memungkinkan untuk berubah secara dinamis, dan dapat diubah-ubah statusnya, aktif atau non-aktif. Hal ini menguntungkan pekerjaan telecommuter yang memerlukan akses Virtual Private Network menuju jaringan perusahaannya melalui Internet. Telecommuter tidak perlu melakukan koneksi Virtual Private Network sepanjang waktu. Komputer yang dimiliki oleh telecommuter bertanggung jawab untuk membangun koneksi Virtual Private Network. Informasi yang diperlukan untuk membuat koneksi Virtual Private Network, seperti alamat IP dari telecommuter tersebut, berubah secara dinamis sesuai dengan posisi lokasi dari telecommuter tersebut.

2.2.1. Site to Site Virtual Private Network

Site-to-site VPN merupakan perluasan dari sebuah jaringan Wide Area Network. Site-to-site VPN menghubungkan seluruh jaringan satu sama lain. Virtual Private Network dengan tipe site-to-site ini, membuat jalur yang aman dan tetap antar titik, misalnya komunikasi antara kantor pusat dengan kantor cabang melalui Internet seperti pada Gambar 2.3.

Kedua belah pihak baik kantor pusat maupun kantor cabang harus memiliki perangkat-perangkat pendukung Virtual Private Network untuk membangun jaringan Virtual Private Network tersebut.



Gambar 2.4
Site to Site Virtual Private Network

Di masa lalu, leased line atau koneksi Frame Relay digunakan sebagai penghubung beberapa situs, namun karena saat ini banya perusahaan yang menggunakan koneksi Internet, kedua koneksi tersebut dapat digantikan dengan site-to-site Virtual Private Network.

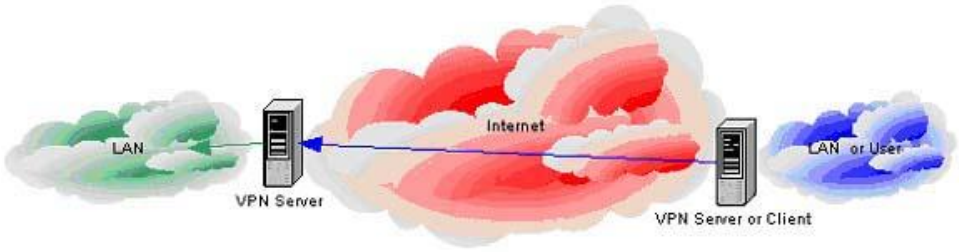
Pada sebuah site-to-site VPN, host mengirim dan menerima trafik TCP/IP seperti biasa melalui sebuah gateway atau gerbangVPN. Gateway VPN bertanggung jawab untuk melakukan proses enkapsulasi dan enkripsi terhadap trafik data yang akan keluar dari sebuah situs dan mengirimkannya melalui tunnel Virtual Private Network melewati Internet menuju gateway VPN situs tujuan. Setelah diterima, gateway VPN yang dituju melucuti header, dan melakukan dekripsi terhadap isi data, kemudian meneruskan paket data tersebut menuju host tujuan yang ada dalam jaringan lokalnya.

Terdapat beberapa jenis site-to-site VPN, antara lain:

- Point-to-Point Tunneling Protocol
- Layer 2 Tunneling Protocol
- Internet Protocol Security
- Multi Protocol Label Switching

2.2.1.1. Point-to-Point Tunneling Protocol

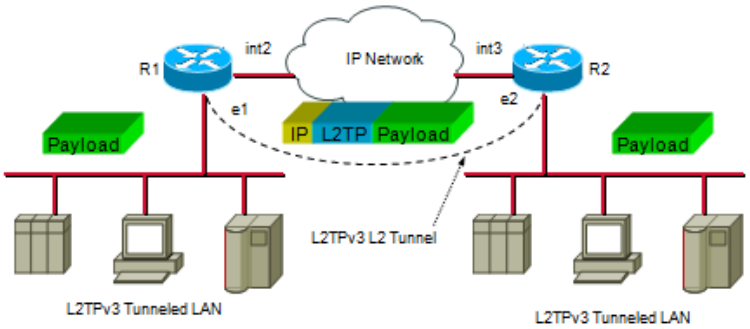
Point-to-Point Tunneling Protocol (PPTP) merupakan perluasan dari *Point-to-Point Protocol* (PPP). Service tunneling disediakan oleh PPTP dan diharapkan untuk bekerja pada bagian atas layer IP. PPP dimodifikasi sedemikian sehingga dapat memenuhi kebutuhan untuk koneksi VPN, yakni point-to-point tunnel. PPTP lebih aman daripada konelsi LAN to LAN. PPTP sudah memenuhi syarat untuk menjadi salah satu jenis VPN, yakni dengan adanya komponen enkapsulasi dan enkripsi.



Gambar 2.5
Topologi PPTP

2.2.1.2. Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) adalah protokol tunneling yang digunakan untuk mendukung VPN atau biasanya merupakan bagian dari pelayanan yang disediakan oleh ISP. L2TP tidak menyediakan enkripsi atau kerahasiaan dengan sendirinya, hal ini tergantung pada protokol enkripsi yang melalui terowongan itu sendiri.



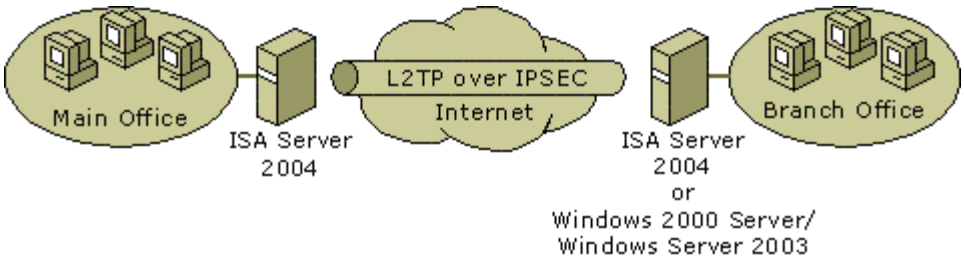
Gambar 2.6
L2TPv3

L2TP diperkenalkan pada tahun 1999 sebagai standard RFC 2661. L2TP berasal dari penggabungan Layer 2 Forwarding Protocol (L2F) yang dikembangkan oleh Cisco dan Point-to-Point Tunneling Protocol PPTP. Pada tahun 2005, diperkenalkan L2TPv3 sebagai standar RFC 3931. L2TPv3 menyediakan fitur keamanan tambahan, dengan enkapsulasi yang ditingkatkan, serta kemampuan untuk mengemas data lebih dari sekedar PPP melalui IP.

2.2.1.3. Internet Protocol Security (IPsec)

IPsec diaplikasikan dalam rangka menutupi kekurangan dari L2TP, di mana L2TP tidak memberikan jaminan keamanan terhadap data. Metode ini sering disebut sebagai L2TP/IPsec, dan didefinisikan dalam RFC 3193. Berikut ini proses mendirikan IPsec:

1. Negosiasi IPsec *Security Association*, dengan menggunakan proposal Internet Key Exchange (IKE).
2. Pembentukan Encapsulating Security Payload (ESP) dalam mode transport.
3. Negosiasi pembentukan tunnel L2TP di antara di antara peer yang berhubungan. Sering disebut dengan tunnel IPsec.

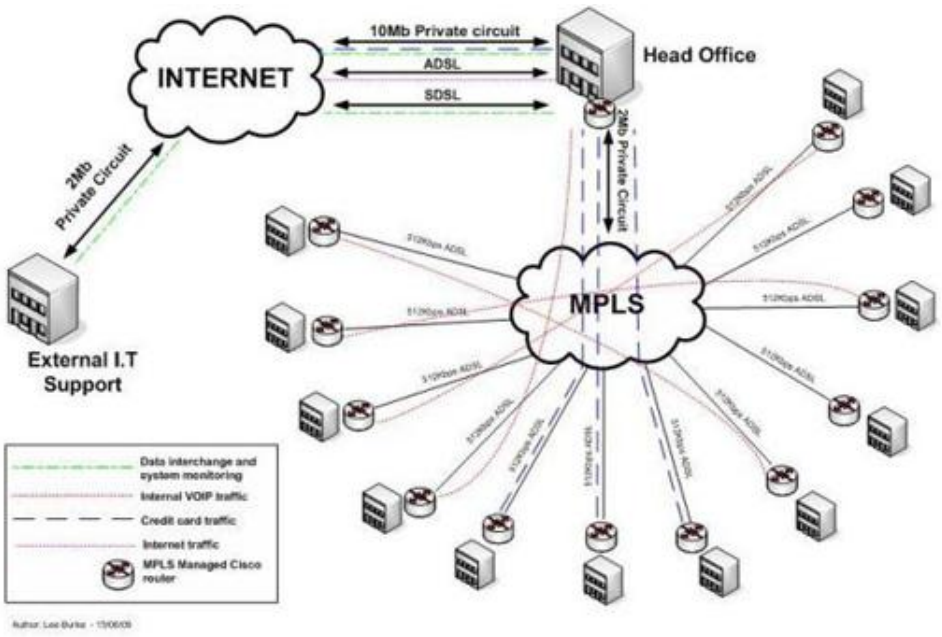


Gambar 2.7
L2TP over IPsec

2.2.1.4. Multi Protocol Label Switching (MPLS)

Multi Protocol Label Switching (MPLS), merupakan sebuah solusi sempurna bagi sebuah perusahaan untuk meningkatkan komunikasi antar cabang dengan jumlah cabang yang banyak. MPLS merupakan sebuah layanan setara dengan leased-line yang ditujukan untuk perusahaan yang membutuhkan jaringan

yang kokoh, di mana kebutuhan akan bandwith, baik *upload* maupun *download* sangat diperlukan.



Gambar 2.8
Multi Protocol Label Switching

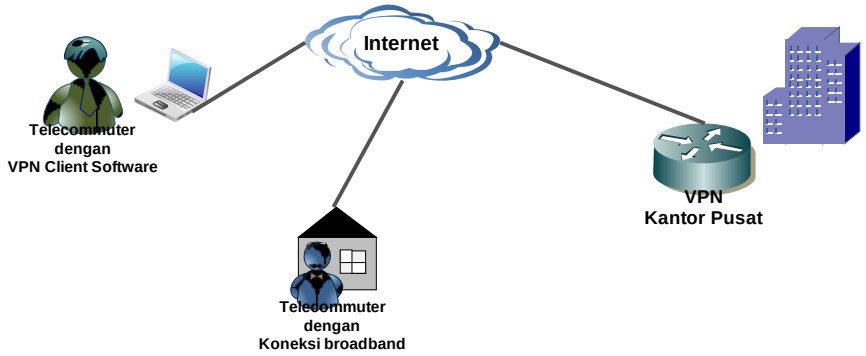
2.2.2. Remote Access Virtual Private Network

Remote Access VPN merupakan evolusi dari circuit-switching networks, seperti layanan telepon pada umumnya, ISDN. Remote Access VPN mendukung arsitektur client-server, di mana VPN Client (Remote Host) membutuhkan akses yang terjamin keamanannya menuju jaringan perusahaan melalui perangkat VPN Server.

Di masa lalu, remote user diimplementasikan dengan menggunakan jaringan Dial-Up dan ISDN. Dengan munculnya Virtual Private Network, seorang telecommuter hanya membutuhkan akses Internet yang biasanya merupakan koneksi broadband, untuk berkomunikasi dengan kantor pusat.

Pada Remote Access VPN, setiap host umumnya memiliki VPN Client Software. Setiap kali host akan mengirimkan data melewati VPN, VPN Client Software akan melakukan enkapsulasi dan enkripsi pada data tersebut, sebelum

mengirimkannya melalui Internet menuju Gateway VPN di ujung lainnya. Setelah data diterima, Gateway VPN bertugas sama seperti pada site-to-site VPN.



Gambar 2.9
Remote Access Virtual Private Network

Cisco IOS SSL VPN merupakan sebuah teknologi yang menyediakan koneksi Remote Access dari lokasi mana saja yang dapat dijangkau oleh jaringan Internet, dengan menggunakan browser dan enkripsi SSL. SSL VPN menyediakan fleksibilitas untuk mendukung akses yang terjamin keamanannya untuk semua user, tanpa memperhatikan di mana host mendirikan koneksi. SSL VPN yang ada pada saat ini memberikan tiga mode akses SSL VPN, yaitu clientless, thin client, dan full client. SSL VPN memungkinkan user untuk mengakses halaman web dan web services. Termasuk akses data, mengirim dan menerima email, dan menjalankan aplikasi berbasis TCP tanpa menggunakan software VPN client IPsec. Ketika kebutuhan akses dari suatu aplikasi terlalu sederhana, dalam arti hanya pada akses beberapa services atau server, SSL VPN tidak membutuhkan client software pada ujung yang yang lainnya. Kemampuan ini memungkinkan perusahaan untuk memperluas keamanan jaringan mereka dengan membatasi hak akses bagi pengguna yang berwenang saja.

SSL VPN sesuai untuk kelompok user yang memerlukan kontrol akses per aplikasi atau per server, bahkan akses dari komputer lain yang bukan milik perusahaan. Dalam beberapa kasus, IPsec dan SSL VPN saling mengimbangi satu sama lain karena masalah yang dihadapi juga berbeda. Pendekatan komplementer memungkinkan sebuah perangkat untuk mengatasi semua remote access yang

dibutuhkan oleh user. Manfaat utama dari SSL VPN adalah kompatibilitasnya dengan Dynamyc Multipoint VPN (DMVPN), Cisco IOS Firewall, IPsec, Intrussion Prevention System (IPS), Cisco Easy VPN, dan Network Address Translation (NAT).

2.3. Generic Routing Encapsulation (GRE) VPN

Generic Routing Encapsulation (GRE) merupakan sebuah tunneling protocol yang didefinisikan pada RFC 1702 dan RFC 2784. Pada awalnya, protokol ini dikembangkan oleh Cisco Systems untuk membuat hubungan point-to-point antar router Cisco yang jaraknya berjauhan melalui sebuah IP Internetwork.

Gambar 2.10
GRE Tunneling Protocol

GRE mendukung multiprotocol tunneling, yang membuatnya dapat melakukan enkapsulasi terhadap beberapa jenis paket protokol di dalam sebuah IP tunnel. Fungsi multi protokol ini diperoleh dengan penambahan header GRE di antara payload dengan header IP tunneling. IP tunneling dengan menggunakan GRE memungkinkan perluasan jaringan dengan cara menghubungkan multiprotocol subnetwork melalui sebuah backbone tunggal. Di samping itu, GRE juga mendukung IP multicast tunneling. Routing protocol yang digunakan sepanjang tunnel memungkinkan terjadinya pertukaran informasi routing dalam virtual network secara dinamis.

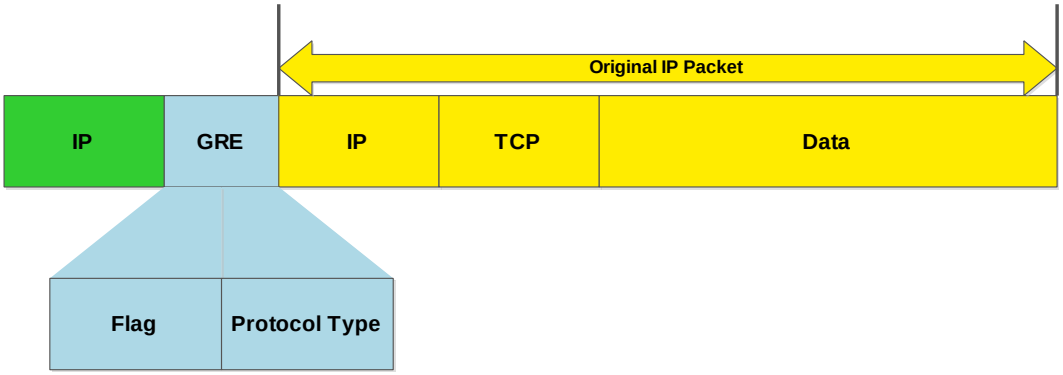
Tunnel GRE ini tidak memiliki status. Setiap ujung dari tunnel menyimpan informasi tentang status ketersediaan dari ujung yang lainnya. Fitur ini membantu

penyedia layanan atau service provider (SP) terhadap pengguna yang tidak mempedulikan arsitektur tunneling internal di ujung service provider. Selain itu, pengguna akhirnya memiliki fleksibilitas untuk melakukan konfigurasi terhadap IP arsitektur mereka, dengan tetap mempertahankan koneksi. Hal ini yang kemudian sebuah hubungan point-to-point virtual antar router melalui IP Internetwork. GRE tidak mencakup mekanisme keamanan yang kuat untuk melindungi muatannya.

2.3.1. Konfigurasi Site-to-Site GRE Tunnel

GRE melakukan proses enkapsulasi terhadap paket IP yang asli dengan sebuah header IP standar dan header GRE. Sebuah header GRE paling tidak memiliki 2 byte kolom wajib (mandatory field):

- GRE Flag
- Tipe Protokol



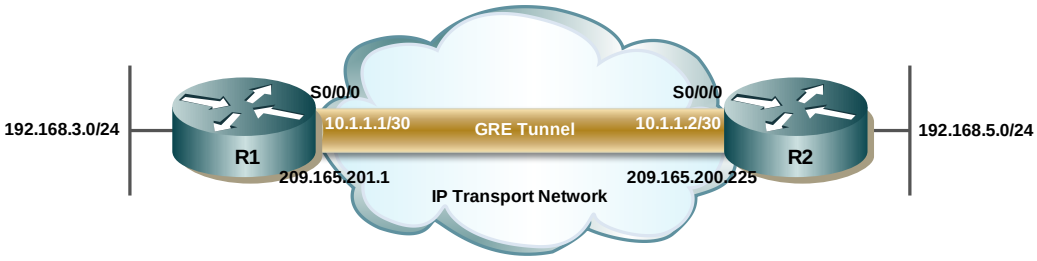
Gambar 2.11
Proses Enkapsulasi GRE

GRE menggunakan kolom tipe protokol untuk mendukung enkapsulasi dari protokol Layer 3 OSI. Header GRE, ditambahkan dengan header IPtunneling, memberikan setidaknya 24 bytes header tambahan untuk paket data yang akan dilewatkan pada tunnel.

Terdapat 5 tahap dalam konfigurasi Site-toSite GRE Tunnel pada router Cisco:

1. Buat sebuah tunnel interface
2. Berikan alamat IP pada tunnel tersebut

3. Identifikasi tunnel source
4. Identifikasi tunnel destination
5. Lakukan konfigurasi protokol GRE



Gambar 2.12
Konfigurasi GRE Tunnel

Jika diimplementasikan seperti Gambar 2.6, maka konfigurasi IOS pada masing masing router dapat dijabarkan seperti potongan program di bawah ini.

Listing2.1Konfigurasi GRE Router 1

```
1 :   R1(config)# interface tunnel 0
2 :   R1(config-if)# ip address 10.1.1.1 255.255.255.0
3 :   R1(config-if)# tunnel source serial 0/0/0
4 :   R1(config-if)# tunnel destination 209.165.200.225
5 :   R1(config-if)# tunnel mode gre ip
6 :   R1(config-if)#
```

Listing2.2Konfigurasi GRE Router 2

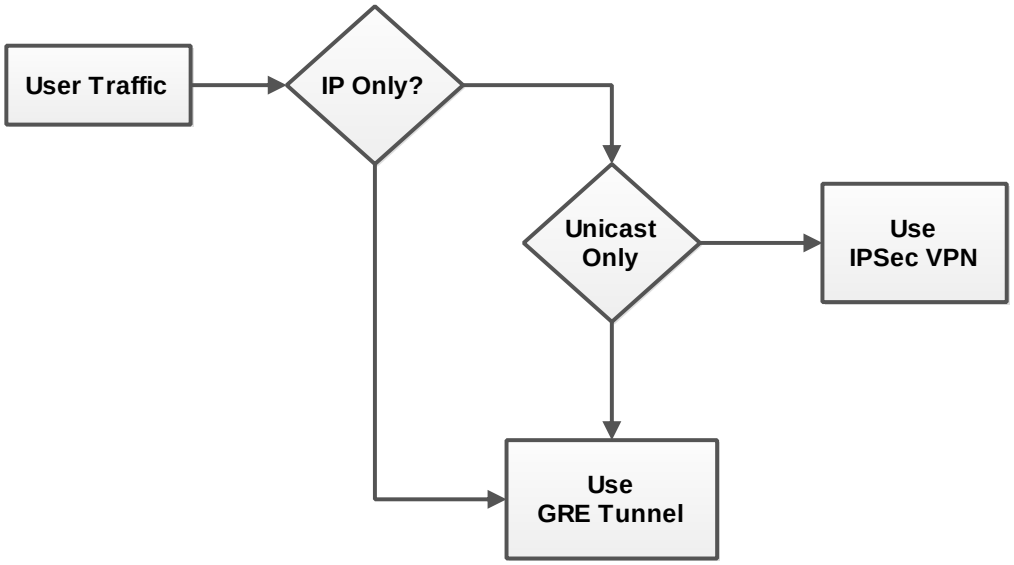
```
1 :   R1(config)# interface tunnel 0
2 :   R1(config-if)# ip address 10.1.1.2 255.255.255.0
3 :   R1(config-if)# tunnel source serial 0/0/0
4 :   R1(config-if)# tunnel destination 209.165.201.1
5 :   R1(config-if)# tunnel mode gre ip
6 :   R1(config-if)#
```

Status GRE akan menjadi up dan protokolnya menjadi up apabila:

- Tunnel source dan destination telah dikonfigurasi
- Tunnel destination ada dalam tabel routing
- GRE keepalives diterima (jika digunakan)
- GRE merupakan tunnel mode default

Kelebihan dari GRE adalah dapat digunakan untuk tunnel non-IP traffic melalui IP network. Tidak seperti IPsec, yang hanya dapat mendukung

komunikasi unicast, GRE mendukung multicast dan broadcast melalui hubungan tunnel tersebut. Sehingga, GRE secara tidak langsung mendukung protokol routing.



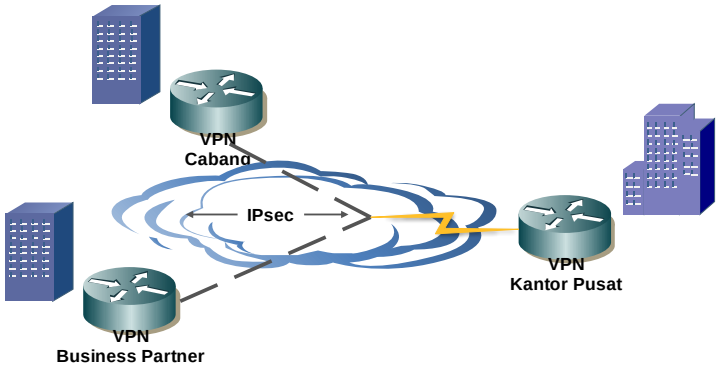
Gambar 2.13
Diagram GRE atau IPsec

GRE tidak menyediakan proses enkripsi. Jika keamanan dibutuhkan, maka teknologi IPsecmenjadi sebuah solusi.

2.4. Pengenalan Internet Protocol Security (IPsec)

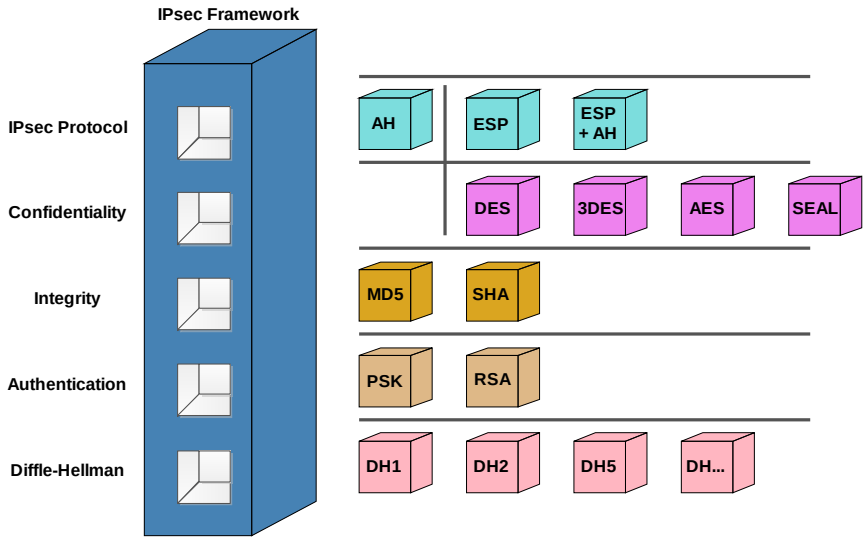
IPsec merupakan sebuah standar IETF (RFC 2401-2412) yang mendefinisikan bagaimana VPN dapat diatur menggunakan protokol pengalamatan IP atau IP addressing protocol.

IPsec tidak terikat dengan metode enkripsi, autentikasi, algoritma keamanan, maupun teknologi penguncian tertentu. IPsec merupakan sebuah framework terbuka standar yang memperinci aturan-aturan yang dibutuhkan untuk keamanan komunikasinya. IPsec bergantung pada algoritma yang telah ada sebelumnya untuk mengimplementasikan enkripsi, autentikasi, dan pertukaran kunci atau key exchange.



Gambar 2.14
Topologi IPsec VPN

IPsec tidak terikat dengan metode enkripsi, autentikasi, algoritma keamanan, maupun teknologi penguncian tertentu. IPsec merupakan sebuah framework terbuka standar yang memperinci aturan-aturan yang dibutuhkan untuk keamanan komunikasinya. IPsec bergantung pada algoritma yang telah ada sebelumnya untuk mengimplementasikan enkripsi, autentikasi, dan pertukaran kunci atau key exchange.



Gambar 2.15
Framework IPsec

IPsec bekerja pada Network Layer (Layer 3 OSI), yang melindungi dan memberikan autentikasi paket IP antar perangkat IPsec yang berhubungan (peer). Sehingga, IPsec dapat melindungi hampir semua traffic aplikasi, karena perlindungan yang diberikan dapat melindungi dari layer 4 sampai layer 7 OSI.

Semua implementasi dari IPsec memiliki plaintext dari layer 3, sehingga nantinya tidak akan ada masalah dengan routing. Fungsi IPsec memiliki seluruh protokol layer 2, seperti Ethernet, ATM, Frame Relay, Synchronous Data Link Control (SDLC), dan High-Level Data Link Control (HDLC).

Framework IPsec terdiri dari lima bagian:

- Bagian pertama mewakili protokol IPsec. Terdapat dua buah pilihan protokol, antara ESP atau AH
- Bagian kedua mewakili tipe kerahasiaan yang akan diimplementasikan dengan menggunakan algoritma seperti DES, 3DES, AES, atau SEAL. Pilihan algoritma bergantung dari level keamanan yang diinginkan
- Bagian ketiga mewakili implementasi integritas yang diinginkan, antara SHA atau MD5
- Bagian keempat mewakili bagaimana kunci rahasia dibentuk, dengan menggunakan Pre-Shared Key atau RSA
- Bagian kelima mewakili grup algoritma DH (Diffie-Hellman). Terdapat 4 jenis algoritma DH yang dapat digunakan, yaitu DH Group 1 (DH1), DH Group 2 (DH2), DH Group 5 (DH5), dan DH Group 7 (DH7). Group DH dipilih berdasarkan kebutuhan spesifik.

IPsec menyediakan framework, dan administrator menentukan algoritma yang digunakan untuk mengimplementasikan keamanan jaringan. Dengan tidak mengikat IPsec dengan algoritma tertentu, memungkinkan bagi algoritma yang baru dan lebih baik untuk diimplementasikan tanpa menambal IPsec standar yang ada.

IPsec mampu mengamankan jalur di antara sepasang ganteway, sepasang host, maupun gateway dan host. Dengan menggunakan IPsec framework, IPsec menyediakan beberapa fungsi keamanan esensial:

- Kerahasiaan (Confidentiality)

  IPsec memastikan kerahasiaan data dengan menggunakan enkripsi
- Integritas / Keaslian (Integrity)

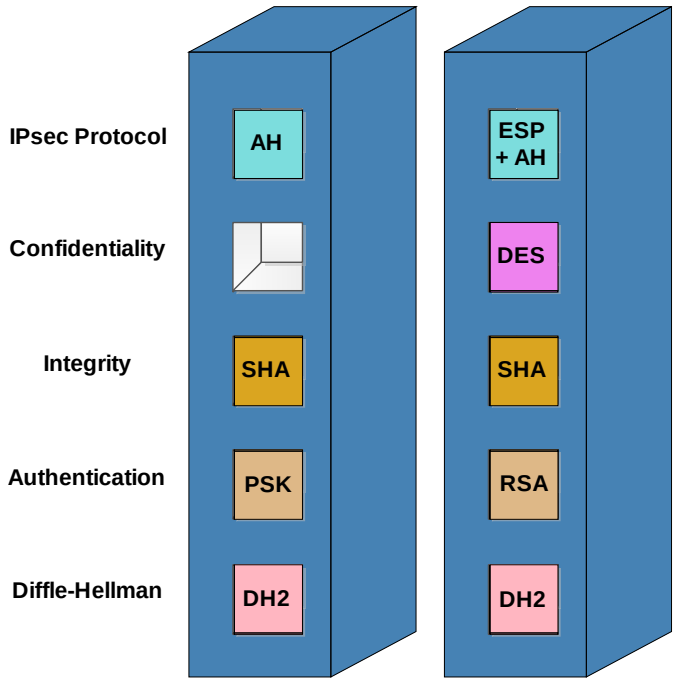
IPsec menjamin keaslian data yang tiba di tujuan tidak berubah dengan menggunakan algoritma hash seperti SHA dan MD5

- Autentikasi (Authentication)

  IPsec menggunakan Internet Key Exchange (IKE) untuk melakukan autentikasi terhadap pengguna dan perangkat yang mampu melakukan komunikasi secara bebas. IKE menggunakan beberapa tipe autentikasi, termasuk username dan password, one-time password, biometrics, pre-shared key (PSK), serta digital certificates.

- Security Key Exchange

IPsec menggunakan algoritma Diffie-Hellman (DH) untuk menyediakan metode pertukaran publik key kepada dua titik untuk menghasilkan sebuah secret key atau kunci rahasia.

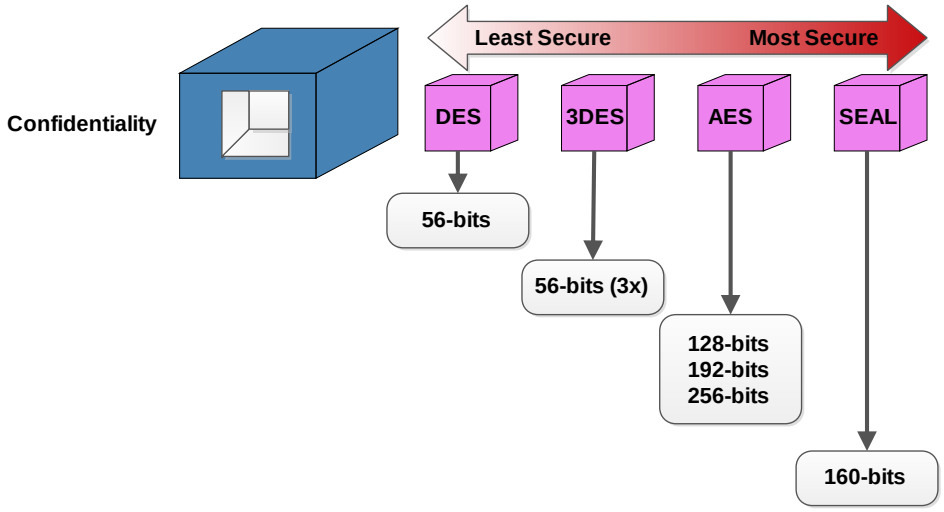


Gambar 2.16
Implementasi Framework IPsec

2.4.1. Kerahasiaan (Confidentiality)

Confidentiality diperoleh melalui enkripsi dari trafic saat trafic tersebut melewati jaringan VPN. Tingkat keamanannya, bergantung dari panjang kunci dan algoritma enkripsi yang digunakan. Jika seseorang mencoba untuk meretas

kunci dengan cara brute-force atau serangan brutal, jumlah kemungkinan untuk mencoba berbanding lurus dengan panjang kunci yang digunakan. Dan waktu yang dibutuhkan untuk memproses semua kemungkinan tersebut, bergantung dari kekuatan perangkat penyerang yang bersangkutan. Semakin pendek kunci, semakin mudah untuk dipecahkan. Sebuah kunci berukuran 64-bit, memerlukan waktu sekitar satu tahun untuk dipecahkan oleh sebuah komputer yang mutakhir. Sebuah kunci dengan ukuran 128-bit, memerlukan waktu setidaknya 10 pangkat 19 tahun untuk dipecahkan dengan komputer yang sama.



Gambar 2.17
Confidentiality Algorithm

Berikut ini adalah beberapa algoritma enkripsi dan panjang kunci yang digunakan dalam implementasi VPN:

- DES

  Menggunakan key berukuran 56-bit, yang memastikan enkripsi dengan kinerja yang tinggi. DES merupakan sebuah cryptosystem dengan kunci simetric atau simetric key.

- 3DES

  Merupakan varian dari DES 56-bit. 3DES menggunakan tiga kunci enkripsi 56-bit dari setiap blok 64-bit, yang menghasilkan kemampuan

enkripsi yang lebih tangguh dari DES. 3DES merupakan sebuah cryptosystem dengan kunci simetric atau simetric key.

- AES

  Memberikan keamanan yang lebih tangguh dibandingkan DES dan lebih efisien daripada 3DES. AES menawarkan tiga panjang kunci yang berbeda: 128-bit, 192-bit, dan 256-bit. AES merupakan sebuah cryptosystem dengan kunci simetric atau simetric key.

- Software-Optimized Encryption Algorithm (SEAL)

  Merupakan sebuah stream cipher yang dikembangkan pada 1993 oleh Phillip Rogaway dan Don Coppersmith, yang menggunakan kunci dengan ukuran 160-bit. SEAL merupakan sebuah cryptosystem dengan kunci simetric atau simetric key.

2.4.1.1. DES (Data Encryption Standard)

DES (Data Encryption Standard) biasanya beroperasi dalam modus blok. DES melakukan enkripsi data dalam blok 64-bit. Algoritma DES pada dasarnya mengaplikasikan operasi permutasi dan subtitusi terhadap bit data yang dikombinasikan dengan encryption key. Algoritma dan key yang sama digunakan untuk proses enkripsi dan dekripsi.

DES meiliki kunci dengan panjang tetap. Dari sebuah kunci dengan panjang 64-bit, yang digunakan untuk proses enkripsi hanya 56-bit saja. 8-bit yang tersisa digunakan sebagai parity. Least Significant Bit (LSB) dari setiap byte key digunakan untuk penanda parity ganjil.

Key DES selalu 56-bit panjangnya. Saat DES digunakan dalam enkripsi yang lebih lemah dari 40-bit key, encryption key adalah 40-bit rahasia, dan 16-bit yang dikenal, sehingga membuat panjang key menjadi 56-bit. Sehingga pada kasus ini, kekuatan key DES hanya sebatas 40-bit.

Selain menggunakan modus blok cipher, DES juga dapat menggunakan modus stream cipher. Untuk melakukan enkripsi atau dekripsi lebih dari 64-bit data, DES menggunakan dua modus blok cipher standard, Electronic Code Book (ECB) atau Cipher Block Chaining (CBC). Kedua mode cipher tersebut

menggunakan operasi logika XOR seperti yang didefinisikan pada tabel di bawah ini:

Tabel 2. 1
Operasi XOR

X	Y	X XOR Y
0	0	0
0	1	1
1	0	1
1	1	0

Terdapat beberapa hal yang harus dipertimbangkan saat melakukan pengamanan data menggunakan enkripsi DES:

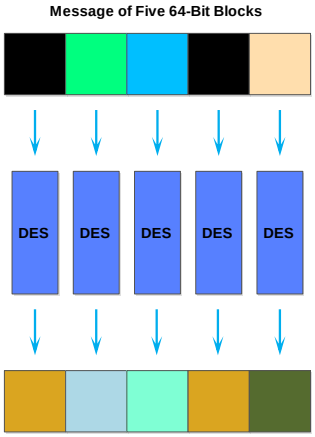
- Penggantian kunci secara berkala untuk mencegah serangan brute force
- Penggunaan jalur yang aman untuk mengirimkan DES key
- Pertimbangkan penggunaan DES pada mode CBC. Dengan CBC, enkripsi dari blok 64-bit bergantung pada blok sebelumnya.
- Uji coba key untuk menguji kekuatan dari key tersebut, sebelum menggunakan key tersebut. DES memiliki 4 key lemah, dan 12 key semi lemah. Karena terdapat 2^56 kemungkinan dari DES key, kemungkinan pemilihan sebuah kunci sangatlah kecil. Bagaimanapun, uji coba sangat disarankan.

Karena key yang digunakan cukup pendek, DES dianggap sebagai protokol yang baik untuk memberika perlindungan terhadap data pada waktu yang singkat. Untuk perlindungan yang lebih tangguh, terdapat algoritma 3DES yang memiliki jaminan keamanan lebih tinggi dari DES.

2.4.1.1.1. Block Cipher Mode

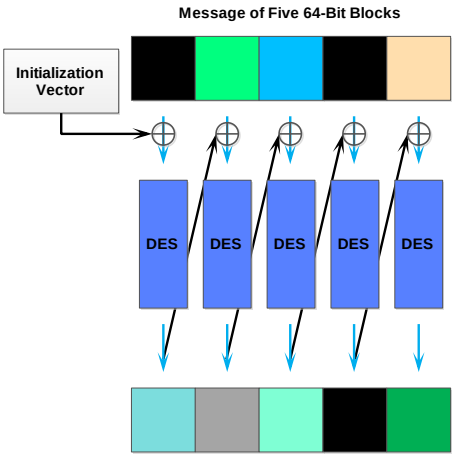
Mode ECB secara berurutan melakukan enkripsi setiap blok 64-bit plaintext menggunakan 56-bit key yang sama. Jika dua buah plaintext yang identik dienkripsi menggunakan key yang sama, blok ciphertext yang dihasilkan juga identik. Oleh karena itu seorang penyusup dapat mengidentifikasi traffic identik yang mengalir melalui sebuah jalur komunikasi. Penyusup bisa saja tanpa

mengetahui isi pesan yang dikirimkan, membuat sebuah pesan baru, kemudian melepaskan pesan tersebut kembali ke jalur pesan yang ditangkap tadi pada waktu yang berlainan, untuk memperoleh hak akses yang ilegal. Sebagai contoh, seorang penyusup secara tidak sengaja menangkap urutan login seseorang dengan hak istimewa administratif yang dilindungi olehDES-ECB, dan kemudian mengirimnya kembali. Untuk mengatasi resiko tersebut, diciptakanlah mode CBC.



Gambar 2.18
ECB

Pada mode CBC, setiap 64-bit plaintext dilakui dengan operasi XOR dengan ciphertext hasil dari block cipher sebelumnya, dan kemudian dienkripsi dengan menggunakan DES key. Enkripsi setiap blok bergantung dari blok sebelumnya. Enkripsi dari blok 64-bit plaintext yang sama dapat menghasilkan blok ciphertext yang berbeda.



Gambar 2.19
CBC

Mode CBC dapat mencegah serangan-serangan tertentu, tetapi tidak dapat membantu melawan cryptanalysis tingkat tinggi atau serangan brute-force.

2.4.1.1.2. Stream Cipher Mode

Untuk melakukan enkripsi atau dekripsi lebih dari 64-bit data, DES menggunakan dua mode stream cipher:

- Cipher Feedback (CFB)

  Hampir sama dengan CBC, dapat melakukan proses enkripsi berapapun jumlah bitnya, termasuk bit tunggal maupun karakter tunggal.
- Output Feedback

  Menghasilkan blok keystream, yang kemudian dioperasikan XOR dengan blok plaintext untuk memperoleh ciphertext.

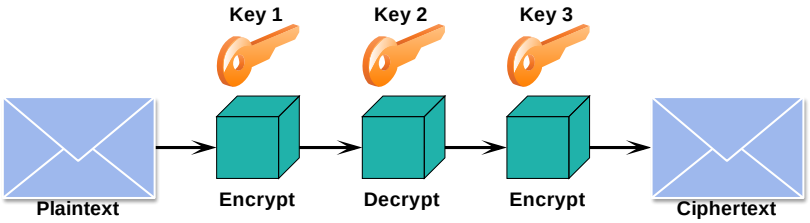
Pada mode stream cipher, cipher menggunakan ciphertext sebelumnya dan secret key untuk menghasilkan sebuah pseudo-random stream of bits, yang hanya bisa dihasilkan oleh secret key. Untuk melakukan enkripsi, data dioperasikan XOR engan pseudo-random stram bit demi bitnya, atau kadang-kadang byte demi byte, untuk menghasilkan ciphertext. Prosedur dekripsinya berjalan sama. Penerima menghasilkan random stream yang sama dengan menggunakan secret key, dan kemudian melakukan operasi XOR terhadap ciphertext dan pseudo-random stream untuk memperoleh plaintext.

2.4.1.2. 3DES (Triple DES)

Dengan perkembangan kemapuan proses perangkat komputer, DES 56-bit yang asli menjadi terlalu dangkal dan mudah untuk dipecahkan oleh penyusup dengan kemampuan yang mumpuni. Salah satu cara untuk memperkuat pertahanannya adalah dengan meningkatkan panjang DES key, tanpa mengubah algoritma yang dianalisa baik tersebut, dengan menggunakan algoritma yang sama dengan kunci yang berbeda beberapa kali berturut-turut.

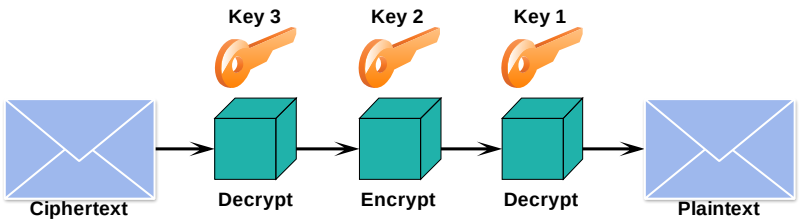
Teknik penerapan DES tiga kali berturut-turut ke blok plaintext disebut 3DES. Saat ini, serangan brute force pada 3DES dianggap tidak layak karena algoritma dasar telah diuji dengan baik di lapangan selama 35 tahun.

3DES menggunakan sebuah metode yang disebut dengan 3DES-Encrypt-Decrypt-Encrypt (3DES-EDE) untuk melakukan enkripsi plaintext. Pertama, plaintext dienkripsi dengan key 56-bit pertama, yang disebut dengan K1. Kemudian, data didekripsi dengan key 56-bit kedua, yang disubut dengan K2. Terakhir, data dienkripsi lagi menggunakan key 56-bit yang ketiga, yang disebut dengan K3.



Gambar 2.20
Enkripsi 3DES

Prosedur 3DES-EDE lebih efektif untuk meningkatkan level keamanan dari sekedar melakukan enkripsi data tiga kali dengan tiga key yang berbeda. Enkripsi data tiga kali berturut-turut dengan key 56-bit yang berbeda setara dengan kekuatan key 58-bit. Di sisi lain, prosedur 3DES-EDE menyediakan enkripsi dengan panjang key efektif 168-bit. Dalam beberapa kasus, jika key K1 dan K3 sama maka enkripsi dianggap kurang aman, karena kekuatannya hanya sebatas 112-bit.



Gambar 2.21
Dekripsi 3DES

Untuk melakukan dekripsi terhadap ciphertext, metode kebalikan dari 3DES-EDE digunakan. Pertama, ciphertxt didekripsi menggunakan K3.

Selanjutnya dienkripsi menggunakan K2. Dan yang terakhir, data didekripsi dengan menggunakan K1.

Meskipun 3DES dikatakan sangat aman, namun sumber daya yang dibutuhkan sangatlah besar. Oleh karena itu dikembangkan enkripsi AES, yang tingkat keamanannya setingkat dengan 3DES, namun prosesnya lebih cepat.

2.4.1.3. AES (Advanced Encryption Standard)

Selama bertahun-tahun, akhirnya DES dinyatakan kadaluarsa. Pada 1997, inisiatif AES diumumkan, dan publik diundang untuk mengusulkan skema enkripsi pengganti DES. Setelah proses standarisasi selama lima tahun, di mana 15 desain bersaing dan dievaluasi, U.S National Institute of Standards and Technology (NIST) memilih blok cipher Rijndael sebagai algoritma AES.

Cipher Rijndael yang dikembangkan oleh Joan Daemen dan Vincent Rijmen, menggunakan panjang blok dan panjang key yang bervariasi. Rijndael merupakan blok cipher yang diiterasi, yang berarti bahwa blok masukan awal dan kunci cipher menjalani beberapa siklus transformasi sebelum menghasilkan output. Algoritma ini dapat beroperasi pada panjang blok yang bervariasi dengan menggunakan panjang key yang bervariasi. Sebuah kunci sepanjang 128-bit, 192-bit, atau 256-bit dapat digunakan untuk melakukan enkripsi terhadap blok data yang memiliki panjang 128-bit, 192-bit, maupun 256-bit dengan 9 kemungkinan kombinasi dari panjang key dan blok tersebut.

Impelmentasi Rijndael yang diterima AES hanya berisi beberapa kemampuan dari algoritma Rijndael. Algoritma ini ditulis sehingga panjang blok atau panjang key, bahkan keduanya dengan mudah dapat diperpanjang dalam kelipatan 32-bit, dan sistem dirancang untuk diimplementasikan dalam berbagai jenis perangkat.

Algoritma AES telah dianalisa secara mendalam, dan saat ini digunakan di seluruh dunia. Meskipun belum terbukti digunakan dalam kegunaan sehari-hari seperti DES, AES dengan algoritma Rijndael terbukti lebih efisien. Dapat digunakan pada lingkungan sistem dengan high-troughput, latency rendah, terutama saat 3DES tidak sanggup beroperasi dengan throughput dan latency

suatu sistem. AES diharapkan untuk memperoleh kepercayaan setelah beberapa waktu dan bertahan dalam penyerangan.

2.4.1.4. SEAL (Software-Optimized Encryption Algorithm)

Software-Optimized Encryption Algorithm merupakan sebuah algoritma enkripsi alternatif untuk perangkat lunak berbasis DES, 3DES, dan AES. SEAl didesain oleh Phillip Rogaway dan Don Coppersmith pada tahun 1993. SEAL merupakan stream cipher yang menggunakan key 160-bit. Karena merupakan stream cipher, data dienkripsi secara berkelanjutan, sehingga prosesnya lebih cepat daripada blok cipher. Namun, SEAL memiliki tahap inisialisasi yang lebih lama, di mana satu set tabel besar dibuat dengan menggunakan SHA.

SEAL memberikan dampak yang lebih rendah terhadap CPU dibandingkan dengan perangkat lunak berbasis algoritma. SEAL sudah dapat digunakan pada Cisco IOS Software Release 12.3(7)T.

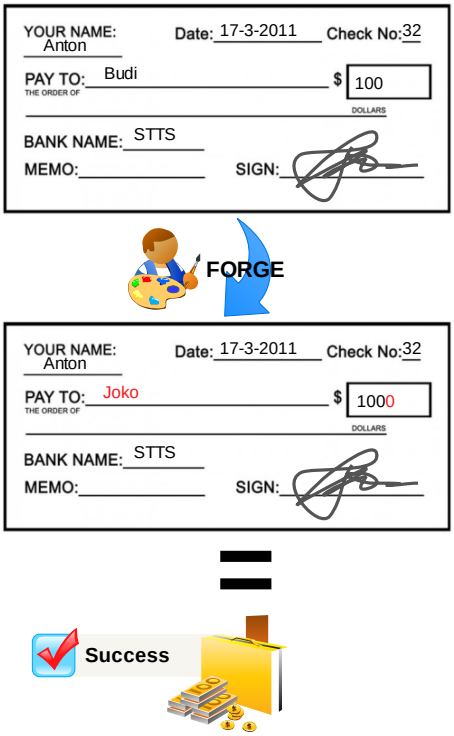
2.4.2. Keaslian (Integrity)

Fungsi yang sangat penting berikutnya, pada VPN adalah data integrity atau keaslian data.Misalnya terdapat sebuah cek senilai $100 yang tertulis untuk Budi dari Anton. Lalu cek dikirimkan menuju alamat Budi, namu pada saat pengiriman, cek tersebut dicuri oleh seorang pencuri. Si pencuri mengubah nama penerima, serta jumlah uangnya. Jika kualitas pemalsuan yang dilakukan oleh pencuri tersebut mendekati aslinya, maka pencuri tersebut bisa sukses menipu bank.

Skenario ini dapat berlaku juga pada VPN, karena data juga diangkut melalui jaringan umum atau publik. Sangat berpotensi sekali bahwa data tersebut dapat dicuri dan dimodifikasi isinya oleh bihak-pihak yang tidak bertanggung jawab. Sebuah metode untuk membuktikan keaslian data ini diperlukan untuk menjamin keaslian isi dari suatu data yang dikirimkan melalui jaringan publik. Algoritma integrity mampu memberikan jaminan tersebut.

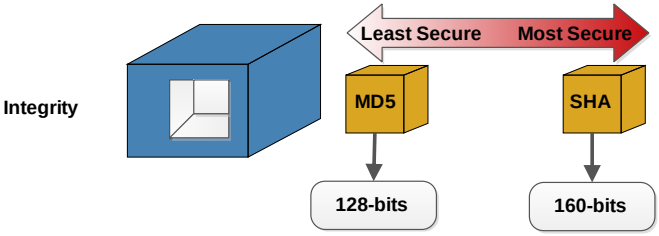
Hashed Message Authentication Codes (HMAC), merupakan sebuah algoritma integrity yang menjamin integritas dari sebuah data menggunakan nilai

hash. Pada perangkat lokal, data pesan dan sebuah shared-secret key diproses menggunakan algoritma hash, yang kemudian menghasilkan nilai hash. Nilai ini ditambahkan ke dalam pesan, dan kemudian pesan dikirimkan melalui jaringan.



Gambar 2.22
Forged Data

Pada ujung jaringan yang lain, di sisi penerima, nilai hash dari data pesan yang diterima akan dihitung ulang, dan dicocokkan hasilnya dengan nilai hash yang dikirimkan oleh pengirim pesan tersebut. Jika hasilnya sama, maka integritas data pesan tersebut sudah terverifikasi. Namun, jika tidak cocok, maka artinya pesan tersebut sudah tidak asli, atau sudah berubah dalam perjalanannya, sehingga data pesan tersebut tidak valid.



Gambar 2.23
Integrity Algorithm

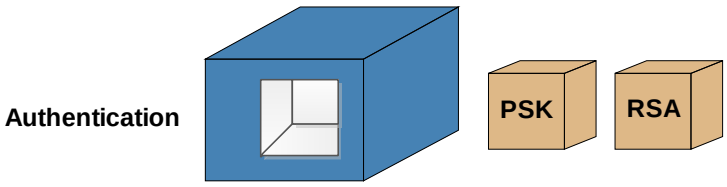
Terdapat dua jenis algoritma HMAC yang sering digunakan:

- HMAC-Message Digest 5 (HMAC-MD5)
  Menggunakan sebuah shared-secret key sepanjang 128-bit. Panjang pesan dan 128-bit shared-secret key dikombinasikan dan diproses menggunakan algoritma HMAC-MD5. Hasilnya berupa hash berukuran 128-bit.
- HMAC-Secure Hash Algorithm 1 (HMAC-SHA-1)
  Menggunakan sebuah shared-secret key sepanjang 160-bit. Panjang pesan dan 160-bit shared-secret key dikombinasikan dan diproses menggunakan algoritma HMAC-MD5. Hasilnya berupa hash berukuran 160-bit.

HMAC-SHA-1 dianggap sebagai kriptografi yang lebih tangguh daripada HMAC-MD5. Sangat dianjurkan untuk menggunakan HMAC-SHA-1 apabila membutuhkan keamanan yang sedikit ketat.

2.4.3. Autentikasi (Authentication)

Saat melakukan komunikasi bisnis melalui jarak jauh, sangat perlu untuk mengetahui siapa yang ada di ujung telepon, fax, maupun email. Hal yang sama juga terjadi pada VPN. Perangkat pada ujung lain VPN juga harus disahkan, sebelum jalur komunikasi dianggap aman.



Gambar 2.24
Authentication Algorithm

Pada abad pertengahan, sebuah segel berfungsi untuk menjamin keaslian dokumen. Di jaman modern ini, sebuah dokumen disahkan dengan cara ditandatangani, kemudian disegel dan ditandatangani oleh notaris. Di era elektronik, dokumen ditandatangani menggunakan kunci yang terencripsi secara pribadi yang sering disebut dengan digital signature. Sebuah signature,

diautentikasi dengan cara mendeskripsikan signature tersebut dengan kunci publik yang dimiliki oleh pengirim.

Terdapat dua buah metode yang digunakan untuk melakukan autentikasi pada suatu peer:

- Pre-shared Key (PSK)

  Sebuah nilai pre-shared key (dibagikan sebelumnya) dimasukkan kepada masing masing peer secara manual, dan digunakan untuk melakukan autentikasi terhadap setiap peer. Pada masing-masing ujung, PSK dikombinasikan dengan informasi lain untuk membentuk sebuah kunci autentikasi. Setiap peer harus memastikan identitas peer yang lain sebelum tunnel yang dibangun dinyatakan aman. Pre-shared Key mudah untuk dikonfigurasi secara manual, namun tidak untuk skala yang besar, karena setiap peer IPsec harus dikonfigurasi setiap saat ada peer yang baru yang akan ikut berhubungan.

- RSA Signatures

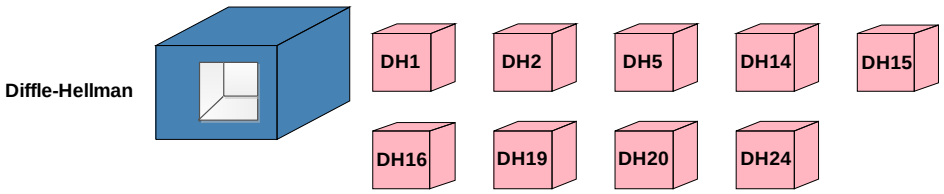
  Pertukaran digital certificates merupakan proses autentikasi dari peer-peer yang ada. Perangkat lokal melakukan enkripsi terhadap hash yang diperoleh. Hasil enkripsi hash tersebut kemudian dilampirkan menuju pesan dan dikirimkan menuju ujung yang lain, sehingga bertindak selayaknya tanda tangan atau signature. Pada ujung lainnya, hash terenkripsi yang diterima didekripsi dengan menggunakanpublik key dari ujung lokalnya. Jika hasil dekripsi sesuai dengan hasil hash yang dihitung ulang, maka tanda tangan atau signature tersebut dinyatakan asli. Setiap peer harus melakukan autentikasi terhadapujung yang lain sebelum tunnel dinyatakan aman.

Terdapat sebuah cara yang tidak umum, atau jarang digunakan untuk melakukan autentikasi, yaitu dengan menggunakan RSA-encrypted nonces. Nonce adalah nomor acak yang dihasilkan oleh peer. RSA-encrypted nonces menggunakan RSA untuk melakukan enkripsi terhadap nilai nonce dan nilai-nilai

yang lainnya. Untuk menggunakan metode ini, public key dari kedua peer harus ada pada peer yang lain, sebelum pesan ketiga dan keempat dari pertukaran IKE dapat dicapai. Karena itu, publik key harus diberikan secara manual menuju peer yang lain sebagai bagian dari proses konfigurasi.

2.4.4. Secure Key Exchange

Algoritma enkripsi seperti DES, 3DES, dan AES, serta MD5 dan SHA-1 memerlukan sebuah shared-secret key yang simetris untuk melakukan enkripsi dan dekripsi. Email, kurir, maupun kiriman semalam dapat digunakan untuk mengirim shared-secret key kepada para admin dari setiap perangkat. Namun, metode paling mudah untuk mendistribusikan shared-secret key tersebut adalah dengan menggunakan metode public key exchange.



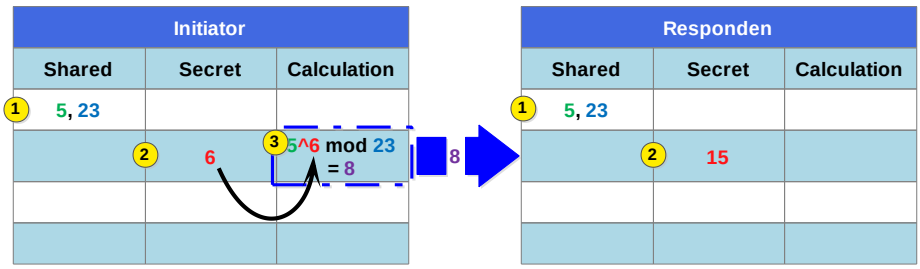
Gambar 2.25
Diffie-Hellman Algorithm

Diffie Hellman (DH) key agreement, merupakan sebuah metode public key exchange yang menyediakan media bagi kedua peer untuk membuat sebuah secret key yang hanya diketahui oleh kedua pihak, meskipun kedua pihak tersebut melakukan komunikasi melalui saluran yang dikatakan tidak aman.

Berikut ini sebuah ilustrasi untuk memahami komunikasi DH:

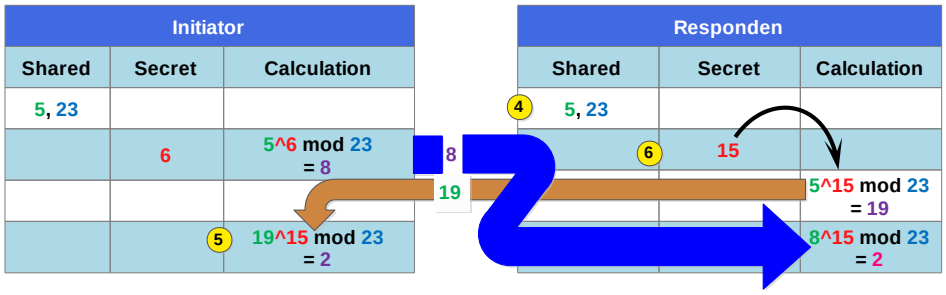
1. Untuk memulai perthkaran DH, inisiator dan responden harus menyepakati dua buah angka yang bersifat terbuka. Angka pertama disebut dengan “g”, adalah angka dasar (generator). Angka kedua disebut “p”, merupakan bilangan prima yang akan digunakan sebagai modulus. Kedua angka ini biasanya bersifat publik dan diperoleh melalui tabel yang sudah diketahui nilainya sebelumnya. Biasanya “g” adalah angka kecil, misalnya 2,3,4,atau 5, dan “p” adalah bilangan prima yang lebih besar.

2. Inisiator membuat sebuah nomor rahasia "X_a", dan responden membuat nomor rahasianya "X_b".
3. Berdasarkan "g", "p", dan "X_a", inisiator menghitung sebuah nilai publik "Y_a" menggunakan algoritma DH, lalu mengirimkannya menuju responden.



Gambar 2.26
Tahap 1-3 DH

4. Responden juga menghitung nilai publiknya "Y_b" berdasakan "g", "p", dan "X_b", dan mengirimkannya menuju inisiator. Kedua nilai ini tidak sama.
5. Inisiator melakukan operasi algoritma DH yang kedua dengan menggunakan nilai publik responden (Y_b)
6. Responden juga melakukan operasi algoritma DH yang kedua dengan menggunakan nilai publik inisiator (Y_a)
7. Hasilnya, inisiator dan responden memperoleh nilai yang sama "Z". angka yang baru ini merupakan key rahasia bersama antara inisiator dan responden yang dapat digunakan oleh algoritma enkripsi yang digunakan oleh keduanya.



Gambar 2.27
Tahap 4-6 DH

Variasi dari DH key exchange ditetapkan sebagai DH groups. Terdapat beberapa jenis DH groups:

- DH groups 1,2, dan 5

  Mendukung eksponen di atas sebuah modulus utama dengan ukuran kunci masing-masing 768-bit, 1024-bit, dan 1536-bit. Kelompok ini tidak dianjurkan untuk digunakan setelah tahun 2012.
- DH groups 14,15, dan 16

  Menggunakan ukuran kunci masing-masing 2048-bit, 3072-bit, dan 4096-bit, dan hanya direkomendasi untuk digunakan sampai tahun 2030.
- DH groups 19,20, dan 24

  Mendukung Elliptical Curve Cryptography (ECC), yang mengurangi waktu yang diperlukan untuk menghasilkan sebuah kunci. Dengan ukuran kunci masing-masing 256-bit, 384-bit, dan 2048-bit. DH group 24 lebih sering dipilih untuk penggunaan jangka panjang.
- IOS Cisco versi terbaru mendukung DH groups yang lebih rumit.

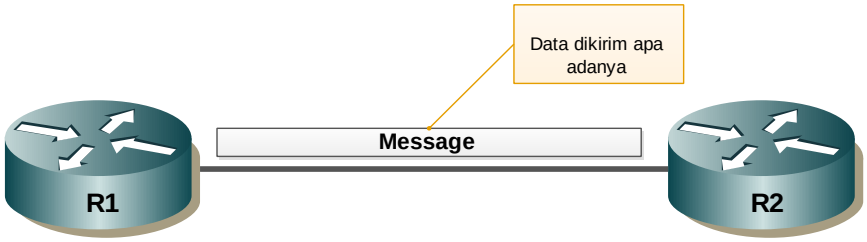
DH groups yang dipilih harus cukup tangguh (memiliki cukup bit) untuk melindungi kunci IPsec selama proses negosiasi. Sebagai contoh, DH group 1 cukup tangguh untuk hanya mendukung enkripsi DES dan 3DES, tetapi tidak untuk AES. Selapa proses pembangunan tunnel, peer-peer VPN berunding untuk menentukan DH groups yang akan digunakan.

2.5. Protokol Keamanan IPsec

IPsec merupakan framework dengan standar terbuka. IPsec merinci pesan guna mengamankan jalur komunikasi, namu tetap bergantung pada algoritma yang sudah ada. Dua buah kerangka utama dari protokol IPsec ini adalah protokol AH dan ESP. Protokol IPsec merupakan blok pertama dari framework IPsec. Pemilihan AH atau ESP, menentukan ketersediaan blok framework yang selanjutnya:

- Authentication Header (AH)

  AH merupakan IP protocol 51, adalah protokol yang sesuai untuk digunakan saat kerahasiaan tidak dibutuhkan atau tidak diijinkan. AH menyediakan autentikasi dan integritas data kepada paket IP yang melewati dua buah sistem.

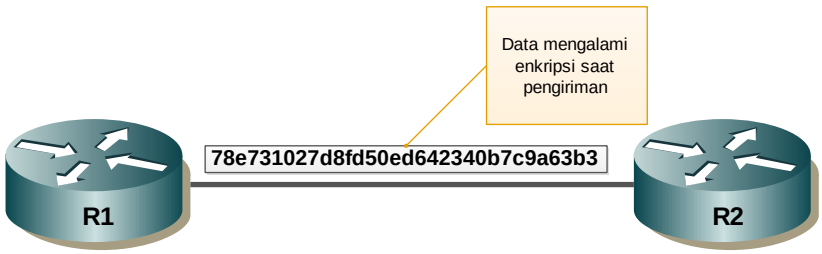


Gambar 2.28
Authentication Header

AH memastikan asal-usul data baik pada R1 maupun R2 dan melakukan verifikasi terhadap keaslian selama proses transmit data tersebut. AH tidak memberikan fasilitas kerahasiaan atau confidentiality dari paket yang dikirimkan. Semua teks yang diangkut tidak mengalami enkripsi sama sekali. Jika protokol AH digunakan tanpa ada protokol pengaman lainnya, maka perlindungan yang diberikan dikategorikan lemah.

- Encapsulating Security Payload (ESP)

  ESP yang merupakan IP protocol 50, mampu menyediakan kerahasiaan atau confidentiality dan autentikasi. ESP menyediakan confidentiality dengan cara melakukan enkripsi pada paket IP. Proses enkripsi paket IP menyembunyikan isi data payload, identitas pengirim dan tujuan. ESP menyediakan autentikasi untuk paket IP yang asli, dan header ESP.



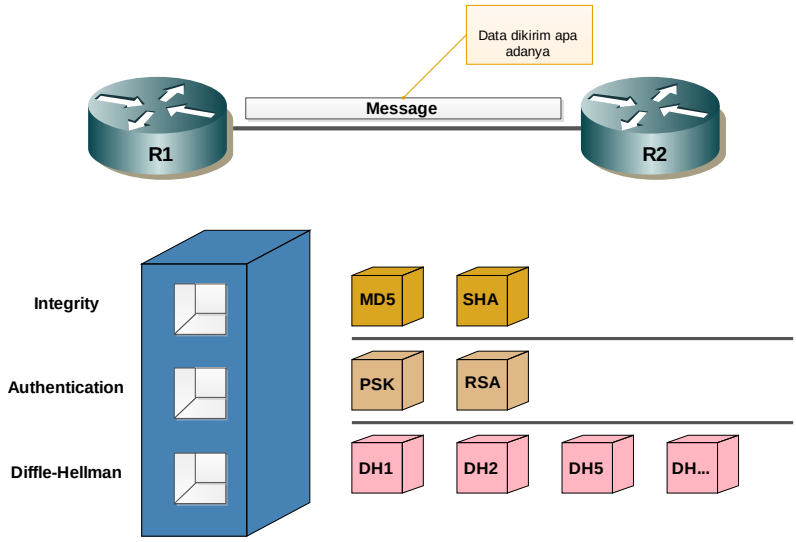
Gambar 2.29
Encapsulating Security Payload

Autentikasi yang diberikan mencakup data asli dan integritas data. Meskipun enkripsi dan autentikasi merupakan opsional, paling tidak harus digunakan salah satu dalam ESP.

2.5.1. Authentication Header (AH)

AH memperoleh fungsi autentikasi dengan menerapkan fungsi keyed one-way hash terhadap paket untuk membuat hash atau message digest. Hash tersebut dikombinasikan dengan teks dan kemudian dikirimkan. Penerima mendeteksi perubahan yang terjadi pada setiap bagian dari paket selama proses pengiriman dengan melakukan fungsi one-way hash yang sama pada paket yang diterima dan kemudian membandingkannya dengan nilai pesan yang sudah dipersiapkan sebelumnya oleh pengirim. Fakta bahwa one-way hash melibatkan sebuah shared-secret key di antara dua sistem, membuktikan adanya jaminan autentikasi.

Fungsi AH diterapkan terhadap keseluruhan paket, kecuali untuk field header IP yang dapat berubah karena kebutuhan transportasi. Sebagai contoh, time to live (TTL) merubakan bagian yang diubah oleh router yang disinggahi sepanjang jalur transportasi.



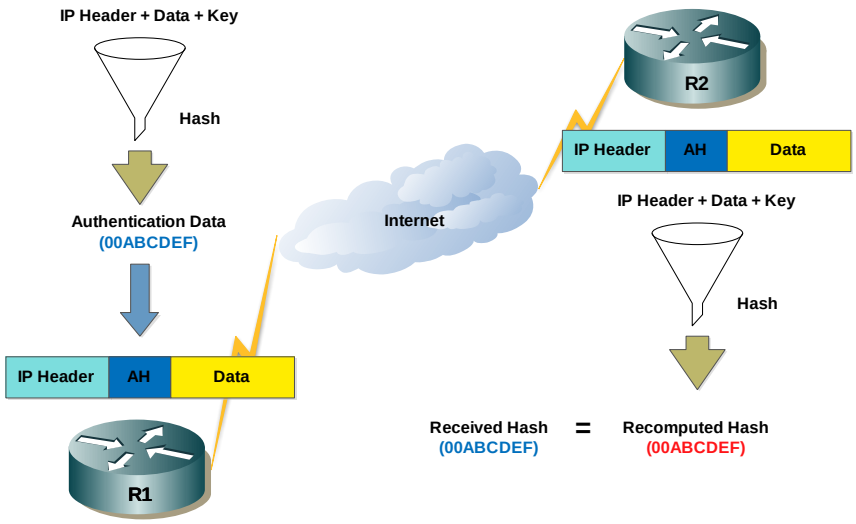
Gambar 2.30
Protokol AH

Proses AH yang terjadi adalah:

1. IP Header dan payload data hash menggunakan shared-secret key

2. Hash membuat sebuah header AH baru, yang kemudian dimasukkan ke dalam paket yang asli.
3. Paket yang baru dikirimkan menuju router IPsec di ujung penerima
4. Router di ujung penerima melakukan hash terhadap header IP dan muatan data yang diterima dengan menggunakan shared-secret key, membongkar hash yang ada pada header AH, dan membandingkan kedua hash tersebut.

Hasil perbandingan kedua hash tersebut harus sama persis. Jika satu bit saja dalam paket yang diterima berubah, maka hasil output hash akan berbeda dengan hash yang berada pada AH header.



Gambar 2.31
AH Authentication and Integrity

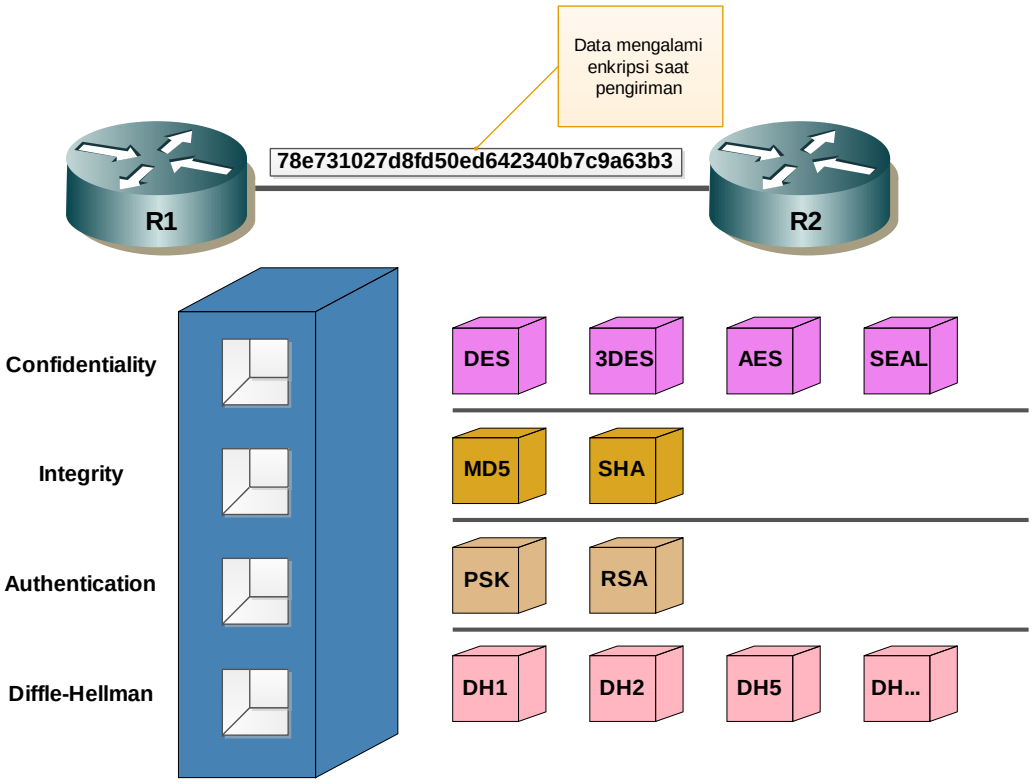
AH mendukung algoritma HMAC-MD5 dan HMAC-SHA-1. AH dapat menemui masalah apabila berhadapan dengan Network Address Translation (NAT).

2.5.2. Encapsulating Security Payload (ESP)

ESP menyediakan kerahasiaan atau confidentiality dengan melakukan enkripsi terhadap payload. Dengan ini, ESP mendukung beberapa algoritma enkripsi simetris. Apabila ESP dipilih sebagai protokol IPsec, maka sebuah algoritma enkripsi wajib dipilih. Algoritma standar IPsec adalah DES 56-bit.

Perangkat Cisco juga mendukung penggunaan 3DES, AES, dan SEAL untuk proses enkripsi yang lebih tangguh.

ESP juga mampu memberikan integritas dan autentikasi. Pertama, payload akan dienkripsi. Selanjutnya, hasil enkripsi payload tersebut diproses dengan menggunakan algoritma hash, HMAC-MD5 atau HMAC-SHA-1. Hash tersebut memberikan autentikasi dan integritas data pada payload.



Gambar 2.32
Protokol ESP

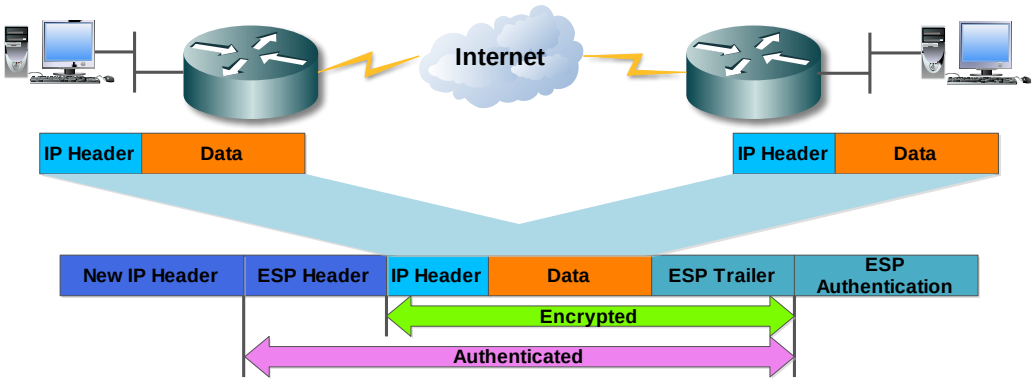
Secara opsional, juga dapat memberikan anti-replay protection. Anti-replay protection melakukan verifikasi bahwa setiap paket bersifat unik dantidak terduplikasi. Perlindungan ini menjamin agar hacker tidak mampu menyadap dan mengubah isi dari data lalu mengembalikannya ke dalam alur perjalanan data. Anti-replay bekerja dengan melacak urutan paket dan menggunakan sliding window pada ujung penerima. Ketika sebuah koneksi dibangun di antara asal dan tujuan, nilai counter mereka diberi nilai nol. Setiap sebuah paket terkirim, sebuah nomor urutan ditambahkan pada paket oleh pengirim. Penerima menggunakan

sliding window untuk memastikan nomor urut sesuai dengan yang diperkirakan. Penerima melakukan verifikasi akan nomor urut pada paket yang diterima tidak diduplikasi dan telah benar urutannya. Saat penerima mendeteksi adanya urutan yang tidak lazim, misalnya penerima menerima paket kedua dengan nomor urut satu, maka sebuah pesan error akan dikirimkan, dan paket tersebut akan dibuang, dan peristiwa tersebut akan dicatat pada log.

Anti-replay biasanya digunakan pada protokol ESP, namun juga didukung penggunaannya pada protokol AH.

Dengan menggunakan ESP, data asli akan terlindung dengan baik, karena seluruh blok mulai dari IP datagram yang asli dan blok ESP dienkripsi. Dengan menggunakan autentikasi ESP, IP datagram yang terenkripsi beserta blok header ESP, ikut termasuk kedalam proses hashing. Selanjutnya, sebuah IP header yang baru dilampirkan pada payload yang sudah ter-autentikasi. Alamat IP yang baru digunakan untuk mengarahkan paket melewati Internet.

Pada saat autentikasi dan enkripsi digunakan, proses enkripsi akan dijalankan terlebih dahulu. Hal ini dilakukan untuk mempercepat proses transfer, di mana pada perangkat penerima terdapat anti-replay protection, sehingga apabila data terlambat akan ditolak oleh perangkat penerima. Sebelum melakukan dekripsi terhadap paket yang diterima, perangkat penerima dapat melakukan autentikasi terhadap paket yang masuk tersebut. Dengan melakukan ini, perangkat penerima dapat segera mendeteksi masalah dengan cepat dan mengurangi potensi serangan Denial of Service (DoS).



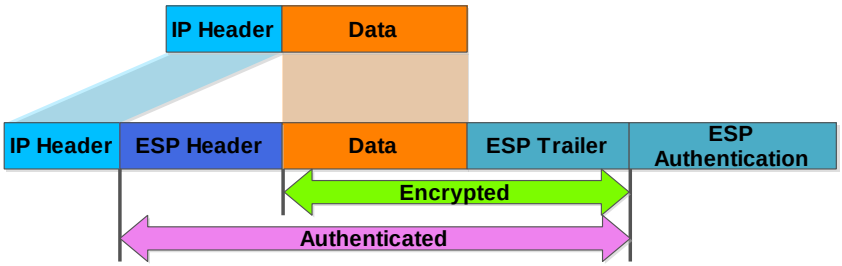
Gambar 2.33
Autentikasi dan Enkripsi ESP

2.6. Mode Protokol IPsec

ESP dan AH dapat diaplikasikan pada paket IP pada dua mode yang berbeda, yakni transport mode dan tunnel mode.

2.6.1. Transport Mode

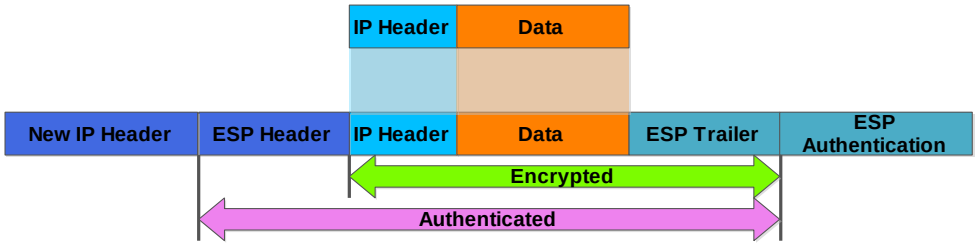
Pada mode transport, keamanan hanya disediakan pada layer transport pada OSI model dan layer-layer di atasnya. Mode transport memberikan proteksi terhadap payload dari paket namun tetap membiarkan IP asli apa adanya. IP asli tersebut digunakan untuk mengarahkan paket melalui Internet.



Gambar 2.34
Transport Mode

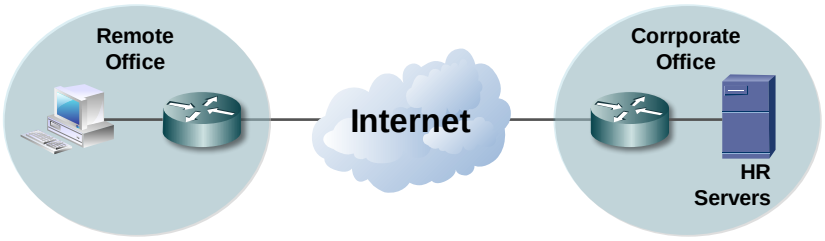
Mode transport ESP digunakan di antara host-host yang berkomunikasi. Mode transport bekerja dengan baik bersama GRE, karena GRE menyembunyikan alamat IP perangkat tujuan dengan menambahkan IP miliknya.

2.6.2. Tunnel Mode



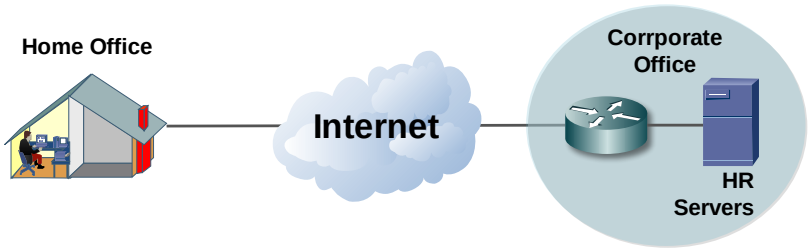
Gambar 2.35
Tunnel Mode

Mode tunnel menyediakan keamanan kepada keseluruhan paket IP. Paket IP yang asli, dienkripsi dan kemudian diselubungkan pada paket IP yang lain. Peristiwa ini disebut IP-in-IP encryption. Alamat IP yang berada di bagian luar, digunakan untuk mengarahkan paket melalui Internet.



Gambar 2.36
Gateway-to-Gateway IPsec

Terowongan atau tunnel ESP digunakan antara sebuah host dan security gateway, atau di antara dua buah security gateway. Aplikasi gateway-to-gateway lebih dipilih untuk digunakan, daripada mengaplikasikan IPsec pada semua komputer klien yang terhubung dengan kantor pusat, lebih mudah apabila mengalikasikan IP-to-IP encryption and encapsulation pada security gateway.



Gambar 2.37
Remote Access IPsec

Mode Tunnel ESP digunakan pada IPsec remote application. Sebuah kantor rumahan belum tentu memiliki router untuk melakukan enkapsulasi dan enkripsi ala IPsec. Pada kasus ini, sebuah IPsec client software yang berjalan pada komputer, melakukan enkapsulasi dan enkripsi IPsec. Pada kantor pusat, router penerima membongkar dan mendekripsi isi paket yang sudah diterima.

Proses VPN melibatkan pemilihan dan penerapan beberapa parameter.

2.7. Internet Key Exchange

VPN IPsec melakukan negosiasi terhadap parameter pertukaran kunci atau key exchange, menetapkan shared key, meng-sutentikasi peer, dan melakukan negosiasi terhadap parameter enkripsi. Parameter yang dinegosiasikan di antara dua buah perangkat disebut dengan security association (SA).

Security Association merupakan sebuah fondasi dari IPsec. Security association disimpan dalam sebuah SA database (SADB), yang dibangun oleh setiap perangkat. Sebuah VPN memiliki catatan SA yang mendefinisikan parameter enkripsi IPsec sebagaimana catatan SA mendefinisikan parameter key exchange.

Semua jenis kriptografi, termasuk Caesar cipher, Vigenere cipher, mesin Enigma, hingga algoritma enkripsi modern, harus berurusan dengan masalah manajemen kunci. DH digunakan untuk membuat shared secret key. Namun, IPsec menggunakan protokol Internet Key Exchange (IKE) untuk membentuk proses pertukaran kunci.

IKE tidak mengirimkan kunci secara terang-terangan melalui jaringan. IKE melakukan kalkulasi terhadap shared key berdasarkan pertukaran dari sekumpulan paket. Proses ini mencegah pihak ketiga untuk mendekripsi shared key, bahkan ketika pihak ketiga menangkap semua pertukaran data yang digunakan untuk melakukan kalkulasi perhitungan kunci.

IKE terletak pada lapisan UDP, dan menggunakan UDP port 500 untuk melakukan pertukaran informasi IKE di antara security gateway. Paket UDP port 500 harus diberi hak akses pada setiap IP interface yang terlibat pada hubungan antar security gateway.

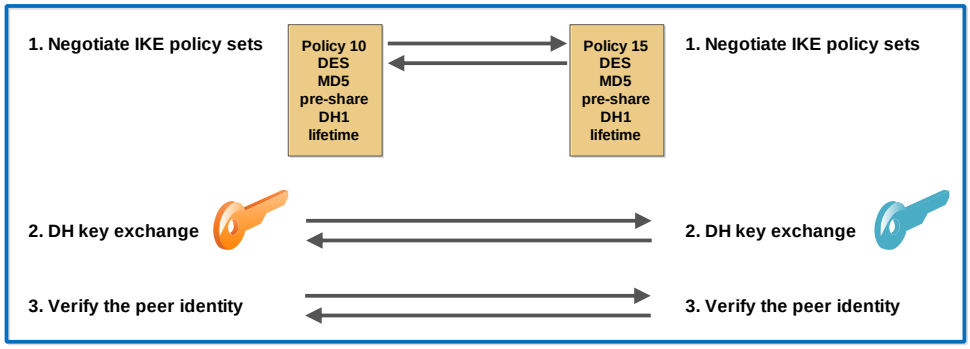
IKE didefinisikan pada RFC 2409. IKE merukapan protokol hibrid, yang menggabungkan Internet Security Association dan Key Management Protocol (ISAKMP) dan Oakley, dan metode pertukaran Skeme Key. ISAKMP mendefinisikan format pesan, mekanisme dari sebiah key-exchange, dan proses negosiasi guna membangun SA untuk kepentingan IPsec. ISAKMP tidak mendefinisikan pengelolaan, maupun pembagian key di antara dua buah peer IPsec. Oakley dan Skeme memiliki lima kelompok kunci yang telah didefinisikan. Dari pengelompokan ini, router Cisco mendukung kelompok 1 (768-bit key), kelompok 2 (1024-bit key), dan kelompok 5 (1536-bit key).

Alternatif penggunaan IKE adalah dengan melakukan konfigurasi secara manual semua parameter yang diperlukan untuk membuat koneksi IPsec yang aman. Proses ini menjadi tidak praktis karena tidak memiliki tolak ukur.

Untuk membangun sebuah jalur komunikasi yang aman di antara dua buah titik, protokol IKE melakukan dua tahapan:

- Tahap 1

  Dua buah peer IPsec melakukan proses negosiasi awal dari SA. Tujuan utama tahap 1 adalah mengegosiasikan IKE policy sets, melakukan autentikasi terhadap peer, dan membuat jalur aman di antara kedua peer tersebut.



Gambar 2.38
Pertukaran IKE Tahap 1

- Tahap 2

  SA dinegosiasikan oleh proses ISAKMP dari IKE atas nama IPsec. Proses ini berjalan dengan singkat.

Gambar 2.39
Pertukaran IKE Tahap 2

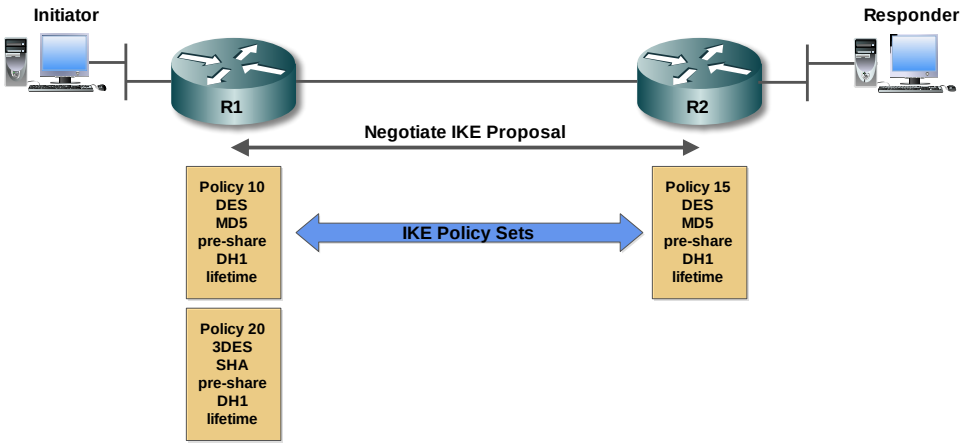
Pada tahap 1, set transformasi, metode hash, dan parameter yang lainnya ditentukan. Sebuah session IKE dimulai oleh router (inisiator) dengan mengirim sebuah proposal menuju router yang lain (responden). Proposal dikirim oleh inisiator yang mendefinisikan protokol enkripsi dan autentikasi yang dapat diterima, berapa lama key harus berstatus aktif, dan apakah perfect forward secrecy (FPS) harus dilakukan. PFS merupakan properti yang menyatakan bahwa key yang digunakan untuk melindungi data tidak digunakan untuk memperoleh key yang lainnya. PFS memastikan bahwa jika salah satu key terganggu, maka key sebelum dan berikutnya akan tetap aman.

Pada pertukaran IKE Tahap 1, terjadi tiga pertukaran:

- Pertukaran pertama

  Pertukaran pertama yang terjadi antara inisiator dengan responden adalah penetapan kebijakan keamanan dasar atau basic security policy. Peer bernegosiasi dan menyetujui algoritma dan hash yang digunakan untuk mengamankan komunikasi IKE. Negosiasi tidak dilakukan secara individu, protokol dikelompokkan ke dalam set-set, yang disebut dengan IKE policy sets. IKE policy sets adalah yang pertama kali dipertukarkan.

  Pertama, inisiator mengirimkan proposal skema enkripsi dan autentikasi yang akan digunakan. Responden mencari policy ISAKMP yang cocok. Responden memilih proposal yang paling cocok untuk situasi keaman dan kemudian mengembalikan proposal tersebut menuju inisiator. Jika ditemukan kecocokan antara policy dari kedua peer tersebut, maka IKE tahap 1 dilanjutkan, jika tidak tunnel akan dibubarkan.



Gambar 2.40
Negosiasi IKE Policy

Jumlah policy set hanya perlu merujuk pada sebuah perangkat VPN. Jumlah policy set tidak harus seseuai dengan dua peer VPN yang berbeda. Dalam point-to-point application, setiap ujung hanya membutuhkan IKE policy set tunggal untuk didefinisikan. Dalam situasi percabangan, situs pusat memerlukan beberapa IKE policy set untuk memenuhi kebutuhan dari peer-peer yang lain.

- Pertukaran kedua

  Pertukaran yang kedua melibatkan proses pembuatan dan pertukaran DH public key di antara dua ujung yang berhubungan. DH memungkinkan dua buah pihak yang tidak memiliki pengetahuan sebelumnya satu sama lain untuk membentuk sebuah shared secret key melalui jalur yang tidak aman.

  Dua buah peer tersebut menjalankan protokol DH key exchange untuk memperoleh bahan-bahan yang diperlukan untuk memebntuk key dengan berbagai macam algoritma hash dan enkripsi yang sebelumnya sudah disepakati bersama. Dengan algoritma DH, setiap peer menghasilkan shared secret key tanpa benar-benar bertukar secara rahasia. Semua negosiasi yang terjadi berikutnya akan dienkripsi dengan menggunakan kunci DH yang sudah dihasilkan bersama sebelumnya.

- Pertukaran ketiga

  Perangkat di setiap ujung harus melakukan autentikasi perangkat di ujung lainnya sebelum jalur komunikasi dinyatakan aman. Pertukaran terakhir dari IKE tahap 1 melakukan autentikasi terhadap peer yang lain.

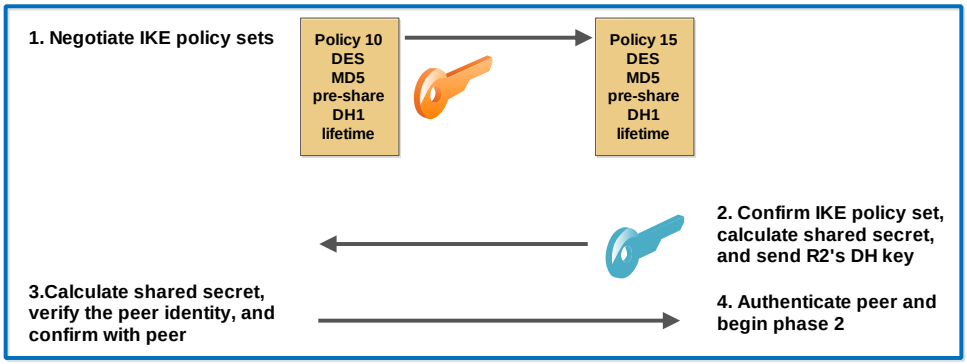
  Inisiator dan responden melakukan autentikasi satusama lain menggunakan salah satu dari tiga metode autentikasi di bawah ini:

  - PSK
  - RSA Signature
  - RSA Encrypted Nonce

  Tahap pertama negosiasi SA berjalan dua arah, di mana data dapat dikirim dan diterima menggunakan key enkripsi yang sama. Meskipun aliran data negosiasi SA di antara dua buah peer IPsec sedikit terganggu, sangat kecil kemungkinan key untuk didekripsi.

Peristiwa terjadinya tiga buah pertukaran dari IKE tahap 1 disebut dengan modus utama. Hasil dari modus utama adalah jalur komunikasi yang aman untuk pertukaran berikutnya antara kedua peer.

Modus aggresif merupakan sebuah pilihan yang ditujukan untuk IKE tahap 1. Modus agresif ini bekerja lebih cepat dari modus utama, karena jumlah pertukaran yang terjadi lebih sedikit. Modus agresif mempersingkat proses negosiasi SA IKE menjadi satu pertukaran dengan tiga paket, sementara modus utama memerlukan tiga pertukaran dengan enam paket.



Gambar 2.41
Modus Agresif IKE Tahap 1

Modus agresif mencakup:

- Paket pertama

  Paket inisiator yang berisi semua kebutuhan untuk proses negosiasi SA pada pesan pertama, termasuk DH public key.

- Paket kedua

  Responden merespon dengan parameter yang diterima, informasi autentikasi, dan DH public key.

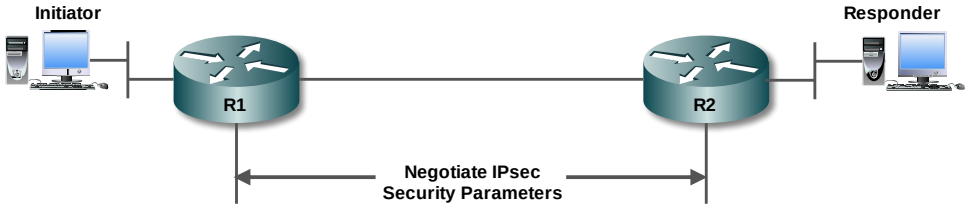
- Paket ketiga

  Inisiator mengirimkan konfirmasi bahwa informasi tersebut sudah diterima.

Proses modus agresif berjalan lebih singkat. Identitas inisiator dan responden lewat dalam bentuk teks biasa. Setelah SA IKE terbentuk, tahap kedua dimulai.

Tujuan tahap 2 dari IKE adalah untuk melakukan negosiasi terhadap parameter keamanan IPsec yang akan digunakan untuk mengamankan tunnel IPsec. Tahap 2 IKE disebut dengan modus singkat dan hanya dapat terjadi

setelahIKE sudah membangun terowongan atau tunnel yang aman pada tahap 1. SA mlakukan negosiasi melalui proses ISAKMP dari IKE atas nama IPsec, yang memerlukan kunci enkripsi untuk pelaksanaannya. Modus singkat melakukan negosiasi SA tahap 2 IKE. Pada tahap ini, SA yang digunakan oleh IPsec tidak terarah, oleh karena itu, pertukaran kunci terpisah diperlukan untuk setiap aliran data.



Gambar 2.42
Modus Singkat IKE Tahap 2

IKE tahap 2 melakukan fungsi-fungsi berikut ini:

- Melakukan negosiasi terhadap parameter keamanan IPsec, yang dikenal dengan IPsec transform sets
- Menetapkan IPsec SA
- Melakukan negosiasi ulang secara berkala untuk menjamin kepastian keamanan
- Melakukan additional DH exchange (optional)

Modus singkat juga melakukan negosiasi ulang IPsec SA yang baru apabila umur IPsec SA sudah kadaluarsa. Pada dasarnya, modus singkat melakukan proses refresh terhadap bahan-bahan pembentuk key yang menciptakan shared secret key yang didasarkan pada bahan-bahan pembentuk key dari pertukaran DH tahap 1.