BAB 9:
VIRTUAL PRIVATE NETWORK

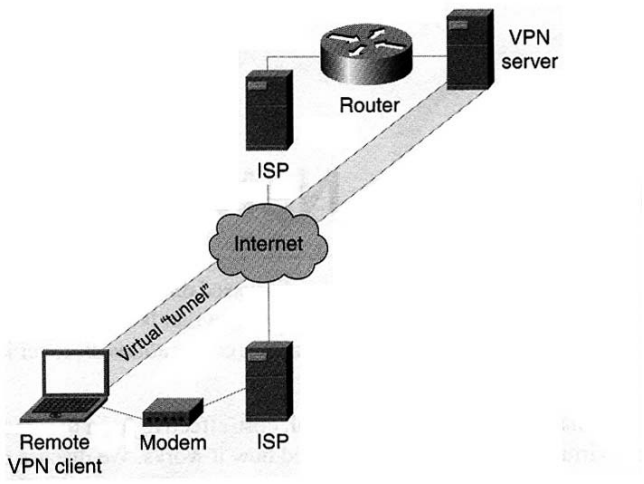
Sumber: Debra Littlejohn Shinder, *Computer Networking Essentials*, Cisco Press, Indianapolis, 2001.

Apakah VPN itu?

Virtual Networking: menciptakan 'tunnel' dalam jaringan yang tidak harus *direct*. Sebuah 'terowongan' diciptakan melalui public network seperti Internet. Jadi seolah-olah ada hubungan *point-to-point* dengan data yang dienkapsulasi.

Private Networking: Data yang dikirimkan terenkripsi, sehingga tetap rahasia meskipun melalui public network.

Figure 16-1 *A VPN connection creates a tunnel through a public network such as the Internet.*



Cara Kerja

VPN bisa bekerja dengan cara:

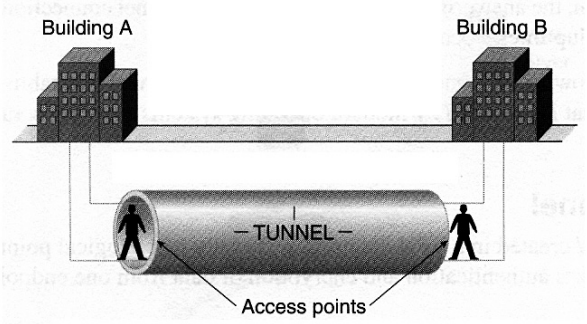
- dial-up
- bagian dari router-to-router

Digging the Tunnel

Tunnel dalam VPN sebenarnya hanya logical point-to-point connection dengan otentikasi dan enkripsi. Analoginya adalah kalau sebuah organisasi/perusahaan punya kantor di 2 gedung yang berbeda. Nah, untuk orang/informasi bergerak dari satu kantor ke kantor lainnya, bisa melalui:

- kaki lima atau jalan umum
- menggali lubang di bawah tanah (analog dengan VPN).

Figure 16-2 *A tunnel offers a private way to get people and data from one point to another.*



Proses Enkapsulasi

Paket lama dibungkus dalam paket baru. Alamat ujung tujuan terowongan (*tunnel endpoints)* diletakkan di destination address paket baru, yang disebut dengan *encapsulation header.* Tujuan akhir tetap ada pada header paket lama yang dibungkus (encapsulated). Saat sampai di endpoint, kapsul dibuka, dan paket lama dikirimkan ke tujuan akhirnya.

Enkapsulasi dapat dilakukan pada lapisan jaringan yang berbeda.

Layer 2 Tunneling

VPN paling sering menggunakan lapisan data link, misalnya:

- Point-to-Point Tunneling Protocol (PPTP) dari Microsoft.
- Contoh yang lain adalah Layer 2 Forwarding (L2F) dari Cisco yang bisa bekerja pada jaringan ATM dan Frame Relay. L2F didukung oleh Internetwork Operating System yang didukung oleh router-router Cisco.
- Yang terbaru adalah Layer 2 Tunneling Protocol (L2TP) yang mengkombinasikan elemen dari PPTP dan L2F.

Layer 3 Tunneling

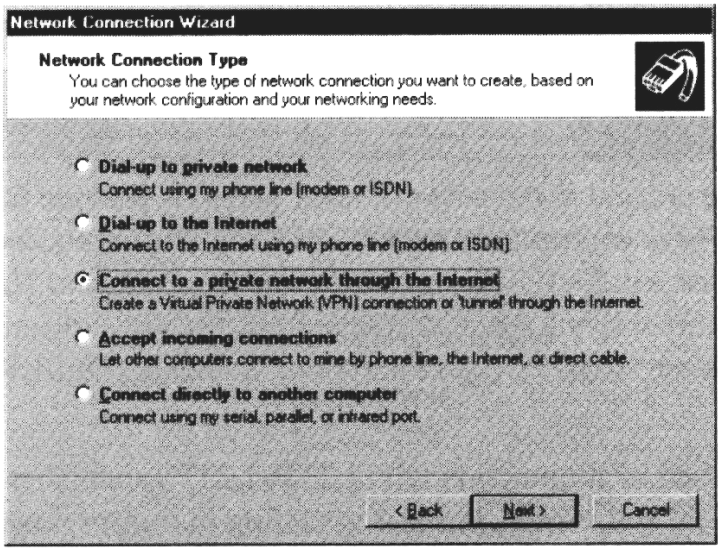
Tunneling dapat dibuat pula pada lapisan IP. Jadi paket IP dibungkus dalam IP Security (IPSec) dengan menggunakan pula IKE (Internet Key Exchange).

IPSec bisa dipergunakan dengan beberapa cara:

- transport mode: IPSec melakukan enkripsi, tetapi tunnel dibuat oleh L2TP. Perhatikan bahwa L2TP bisa juga mengenkapsulasi IPX (Internetwork Packet Exchange) dan jenis paket-paket layer 3 lainnya.
- tunneling mode: IPSec melakukan enkripsi dan tunneling-nya. Ini mungkin harus dilakukan jika router/gateway tidak mendukuk L2TP atau PPTP.

Dukungan Sistem Operasi

- Windows 9x, Windows NT: PPTP
- Windows 2000: L2TP, PPTP
- Linux: IPSec & SSH (Secure Shell)



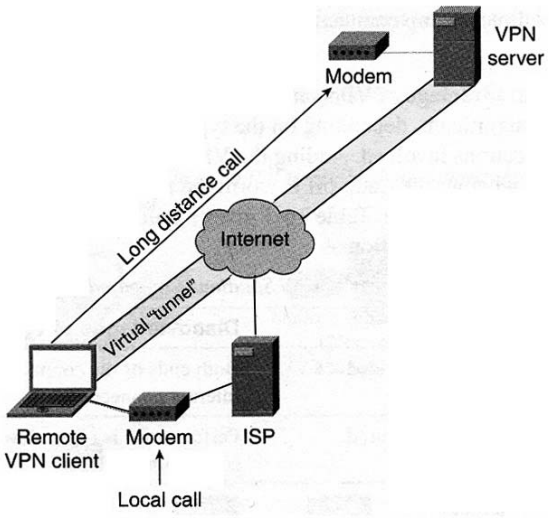
VPN pada Windows 2000

Alasan Penggunaan VPN

VPN vs Dial-up Networking:

Misalnya seorang pegawai yang *mobile* bertugas antarkota. Bisa saja pakai dial-up service, tetapi kalau dial-up antar kota, bisa mahal sekali.
Oleh karena itu menggunakan ISP lokal + VPN, untuk mengakses LAN perusahaan.

Using a VPN enables a user to dial in to a local ISP instead of making a long distance call to the corporate LAN.



Selain itu VPN juga akan mereduksi jumlah telephone line & modem bank yang perlu disediakan perusahaan. Perusahaan cukup menyediakan 1 koneksi saja ke Internet. Hal ini akan mereduksi cost dari perusahaan.

Keuntungan VPN terhadap *dial-up access*:

1. menghemat biaya interlokal
2. membutuhkan lebih sedikit saluran telepon di perusahaan
3. membutuhkan hardware yang lebih sedikit (seperti modem bank)

Kerugian VPN

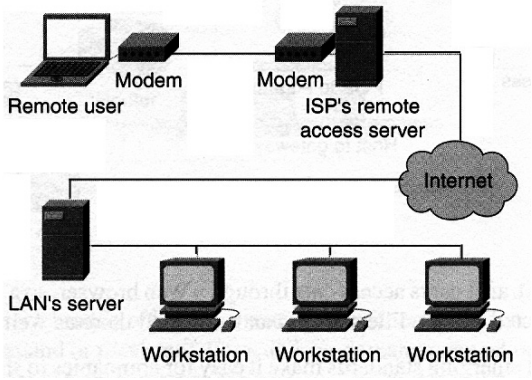
1. kedua endpoints dari VPN, koneksinya harus reliable. Sebagai contoh, kalau ISP di sisi client (sang telecommuter employee) tidak bisa diakses/di-dial, maka tentu VPN tidak bisa juga! Lain halnya kalau bisa dial-up service ke kantor.
2. Performance VPN bisa lebih lambat daripada dial-up service yang biasa tanpa VPN. Hal ini disebabkan karena ada proses tunneling dan enkripsi/dekripsi.

Skenario-skenario VPN

Remote Access VPN

1. Home user atau mobile user men-dial ke ISP
2. Setelah ada koneksi Internet, client menghubungkan diri ke remote access server yang telah dikonfigurasikan dengan VPN.
3. User diotentikasi, dan akses kemudian diizinkan.

The mobile or home user dials in to an ISP to establish an Internet connection, through which he tunnels to the private network.

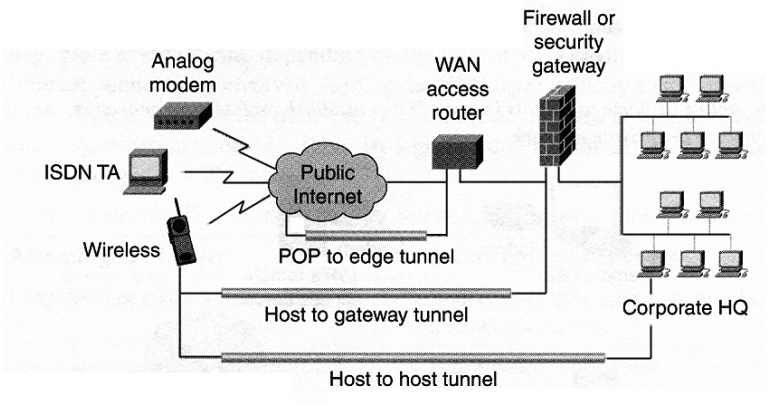


Virtual Private Extranets

Untuk menghubungkan diri partner, supplier atau customer, seperti dalam B2B e-commerce. Hal yang penting adalah melindungi LAN (intranet) dari akses yang mungkin merugikan dari luar. Oleh karena itu harus dilindungi oleh firewall.

Koneksi client ke intranet dengan VPN di perimeter network. Karena biasanya yang diakses adalah web server, maka web server juga ada di perimeter network.

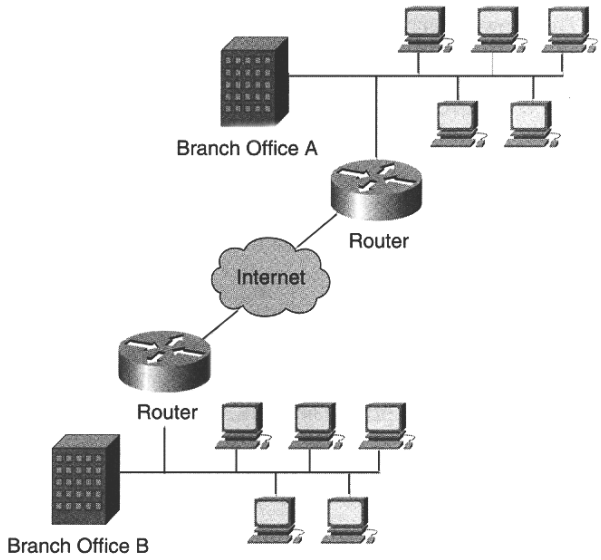
The internal network can be protected from outside access by the implementation of a firewall.



VPN Connections Between Branch Offices

Disebut juga *gateway-to-gateway* atau *router-to-router configuration*. Routernya harus disetup sebagai VPN server dan client.
Software seperti vpnd (VPNdaemon) bisa dipergunakan untuk menghubungkan 2 LAN dengan Linux atau FreeBSD.

Figure 16-7 *A router-to-router VPN connects two branch offices.*



VPN Protocols

Tunneling Protocols

1. PPTP
   Dikembangkan oleh Microsoft dari PPP yang dipergunakan untuk remote access. Caranya:
   a. PPTP mengenkapsulasi frame yang bisa berisi IP, IPX atau NetBEUI dalam sebuah header Generic Routing Encapsulation (GRE). Tetapi PPTP

membungkus GRE dalam paket IP. Jadi PPTP membutuhkan IP untuk membuat tunnel-nya, tetapi isinya bisa apa saja.

b. Data aslinya dienkripsi dengan MPPE.

PPTP-linux adalah client software. Sedangkan yang server adalah PoPToP untuk Linux, Solaris dan FreeBSD.

2. L2F
   Dibuat Cisco tahun 1996. Bisa menggunakan ATM dan Frame Relay, dan tidak membutuhkan IP. L2F juga bisa menyediakan otentikasi untuk tunnel endpoints.

3. L2TP
   Dikembangkan oleh Microsoft dan Cisco. Bisa mengenkapsulasi data dalam IP, ATM, Frame Relay dan X.25.
   Keunggulan L2TP dibandingkan PPTP:
   - multiple tunnels between endpoints, sehingga bisa ada beberapa saluran yang memiliki perbedaan Quality of Service (QoS).
   - mendukung kompresi
   - bisa melakukan *tunnel authentication*
   - bisa bekerja pada jaringan non-IP seperti ATM dan Frame Relay.

4. IPSec
   Dalam *tunneling mode,* IP Sec bisa dipergunakan untuk mengenkapsulasi paket. IP Sec juga bisa dipergunakan untuk enkripsi dalam protokol tunneling lainnya.

   IPSec menggunakan 2 protokol
   - Authentication Header (AH): memungkinkan verifikasi identitas pengirim. AH juga memungkinkan pemeriksaan integritas dari pesan/informasi.
   - Encapsulating Security Payload (ESP): memungkinkan enkripsi informasi sehingga tetap rahasia. IP original dibungkus, dan outer IP header biasanya berisi gateway tujuan. Tetapi ESP tidak menjamin integrity dari outer IP header, oleh karena itu dipergunakan berbarengan dengan AH.

5. SSH dan SSH2
   Dikembangkan untuk membuat versi yang lebih aman dari rsh, rlogin dan rcp pada UNIX. SSH menggunakan enkripsi dengan public key seperti RSA. SSH bekerja pada *session layer* kalau merujuk pada OSI *reference model,* sehingga disebut *circuit-level VPN*. SSH membutuhkan login account.

6. CIPE
   Adalah driver kernel Linux untuk membuat secure tunnel anatara 2 IP subnet. Data dienkripsi pada lapisan *network layer* (OSI) sehingga di sebut low-level encryption. Oleh karena itu CIPE tidak memerlukan perubahan besar pada layer-layer di atasnya (termasuk aplikasi).

Encryption Protocols

- MPPE
- IPSec encryption: DES atau 3DES
- VPNd: Blowfish

- SSH: public key encryption

VPN Security

1. Authentication
   Proses mengidentifikasi komputer *dan* manusia/user yang memulai VPN connection. Metode otentikasi dapat dilakukan dengan protokol:
   - Extensible Authentication Protocol (EAP)
   - Challenge Handshake Authentication (CHAP)
   - MS-CHAP
   - Password Authentication Protocol (PAP)
   - Shiva-PAP

2. Authorization
   Menentukan apa yang boleh dan yang tidak boleh diakses seorang user.

3. Enkripsi

Masalah Performa VPN

Yang paling jadi masalah adalah performa Internet sendiri. Misalnya kadang-kadang bisa terjadi ISP tidak bisa diconnect, atau sedang ada heavy traffic di Internet (karena ada berita besar misalnya).
Kemudian adalah masalah kecepatan, dimana circuit-level VPN lebih lambat ketimbang network-level VPN.