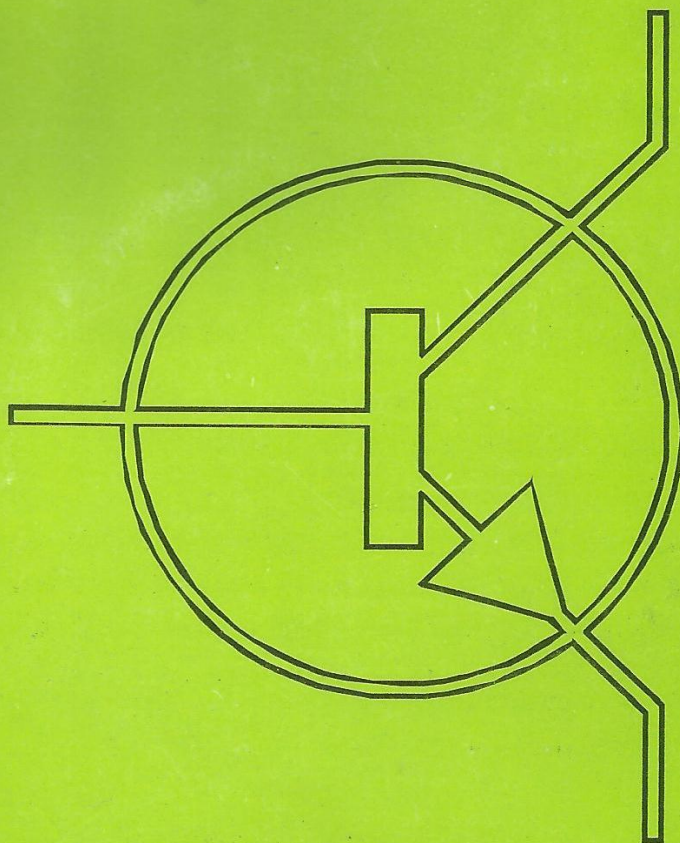


JURNAL TEKNIK ELEKTRO

Vol. 1. No. 2, September 2001

ISSN 1411-8890

Emitor



Emitor

Vol. 1

No. 2

Halaman
60-127

Teknik Elektro UMS
September 2001

ISSN 1411-8890

Emitor

Jurnal Teknik Elektro

Volume1, Nomor 02, September 2001

ISSN 1411-8890

Daftar Isi

Telepon Internet

Agus Suhari

60-69

Kegagalan Minyak Transformator sebagai Bahan Isolasi Cair

Agus Supardi

70-78

Jaringan Syaraf Tiruan untuk Analisis Komponen Utama

Achmad Hidayatno

79-87

Analisa Implementasi Teknologi ADSL untuk Pengiriman Data

Endah Sudarmilah

88-95

Uji Keputihan dan Uji Rerata Nol untuk Verifikasi Derau Putih dengan Rarate Nol

Husni Thamrin

96-102

Sifat Dielektrik Bahan Isolasi Resin Epoksi *Bisphenol A* untuk Isolator Tegangan Tinggi

Jatmiko

103-109

WLAN : Solusi Ber-Internet Saat Ini

Muhammad Kusban

110-119

Manajemen Keamanan Sistem Informasi

Bambang Hari Purwoto

120-127



UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS TEKNIK

Jl. A. Yani Pabelan Kartasura Tromol Pos 1 Surakarta 57102 Telp. (0271) 717417 Ext. 212, 213, 225, 253 Fax. (0271) 715448
E-mail : teknik@ums.ac.id. Website : <http://www.ums.ac.id>

**SURAT PENGALIHAN
PUBLIKASI**

Nomor : 122/A.2-VIII/FT/III/2015

Yang bertanda tangan dibawah ini :

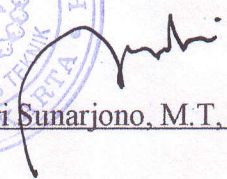
Nama : Ir. Sri Sunarjono, M.T, PhD

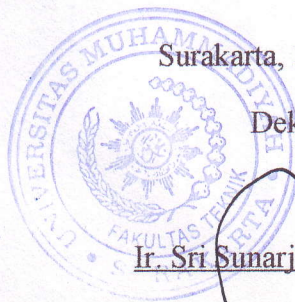
Jabatan : Dekan Fakultas Teknik

Menyatakan persetujuan pengalihan hak unggah publikasi Kepada Lembaga Pengembangan Publikasi Ilmiah Universitas Muhammadiyah Surakarta atas artikel berjudul "Manajemen Keamanan System Informasi" yang ditulis oleh Bambang Hari Purwoto, NIDN : 0628036803, Dosen program Studi/Fakultas Teknik Elektro/Teknik Universitas Muhammadiyah Surakarta dalam jurnal ilmiah Emitor Vol. 1 No. 2 September 2001.

Surakarta, 10 Maret 2015

Dekan


Ir. Sri Sunarjono, M.T, Ph.D



MANAJEMEN KEAMANAN SISTEM INFORMASI

Bambang Hari Purwoto
Teknik Elektro Fakultas Teknik UMS
Jl. A. Yani Tromol Pos 1 Kartasura, Surakarta

ABSTRAK

Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin. Keamanan sistem informasi meliputi: keamanan yang bersifat fisik (physical security), keamanan yang berhubungan dengan orang (personel), keamanan dari data dan media serta teknik komunikasi (communication) dan keamanan dalam operasi.

Kata Kunci : Keamanan sistem informasi, firewall, IDS (*intruder detection system*), VPN (*virtual private networks*)

PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayangnya masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan. Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "information-based society". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial

(perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi. Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh diakses oleh orang-orang tertentu. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang dapat diterima.

Ada beberapa macam teori yang digunakan untuk pengamanan sistem informasi. Antara lain : kriptografi, enkripsi dan dekripsi (baik dengan menggunakan *private-key* maupun dengan menggunakan *public-key*).

Kriptografi (*Cryptography*)

Kriptografi merupakan ilmu dan seni untuk menjaga pesan agar aman. “*Crypto*” berarti “*secret*” (rahasia) dan “*graphy*” berarti “*writing*” (tulisan). Para pelaku atau praktisi kriptografi disebut *cryptographers*. Sebuah algoritma kriptografik (*cryptographic algorithm*), disebut **cipher**, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat.

Enkripsi (*Encryption*)

Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah “*encipher*”.

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (untuk kasus *private key cryptography*) atau dengan kunci yang berbeda (untuk kasus *public key cryptography*). Secara matematis, proses atau fungsi enkripsi (*E*) dapat dituliskan sebagai:

$$E(M) = C \quad (1)$$

dimana: *M* adalah *plaintext (message)* dan *C* adalah *ciphertext*.

Proses atau fungsi dekripsi (*D*) dapat dituliskan sebagai:

$$D(C) = M \quad (2)$$

dimana: *M* adalah *plaintext (message)* dan *C* adalah *ciphertext*.

Dekripsi (*Decryption*)

Deskripsi adalah proses kebalikan dari enkripsi, untuk mengubah *ciphertext* menjadi *plaintext*. Menurut ISO 7498-2, terminologi yang lebih tepat untuk proses ini adalah “*decipher*”. *Cryptanalysis* adalah seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci. *Cryptanalyst* adalah pelaku atau praktisi yang menjalankan *cryptanalysis*. *Cryptology* merupakan gabungan dari *cryptography* dan *cryptanalysis*.

ELEMEN DARI ENKRIPSI

Algoritma dari Enkripsi dan Dekripsi

Algoritma dari enkripsi adalah fungsi-fungsi yang digunakan untuk melakukan fungsi enkripsi dan dekripsi. Algoritma yang digunakan menentukan kekuatan dari enkripsi, dan ini biasanya dibuktikan dengan basis matematika. Berdasarkan cara memroses teks (*plaintext*), cipher dapat dikategorikan menjadi dua jenis : *block cipher* and *stream cipher*. *Block cipher* bekerja dengan memroses data secara blok, dimana beberapa karakter/data digabungkan menjadi satu blok. Setiap proses satu blok menghasilkan keluaran satu blok juga. Sementara itu *stream cipher* bekerja memroses masukan (karakter atau data) secara terus menerus dan menghasilkan data pada saat yang bersamaan.

Kunci yang Digunakan dan Panjangnya Kunci

Kekuatan dari penyandian bergantung kepada kunci yang digunakan. Beberapa algoritma enkripsi memiliki kelemahan pada kunci yang digunakan. Untuk itu, kunci yang lemah tersebut tidak boleh

digunakan. Selain itu, panjangnya kunci yang biasanya dalam ukuran *bit*, juga menentukan kekuatan dari enkripsi. Kunci yang lebih panjang biasanya lebih aman dari kunci yang pendek. Jadi enkripsi dengan menggunakan kunci 128-bit lebih sukar dipecahkan dengan algoritma enkripsi yang sama tetapi dengan kunci 56-bit. Semakin panjang sebuah kunci, semakin besar *keyspace* yang harus dijalani untuk mencari kunci dengan cara *brute force attack* atau coba-coba karena *keyspace* yang harus dilihat merupakan pangkat dari bilangan 2. Jadi kunci 128-bit memiliki *keyspace* 2128, sedangkan kunci 56-bit memiliki *keyspace* 256. Artinya semakin lama kunci baru bisa ketahuan.

Plaintext

Plaintext adalah pesan atau informasi yang akan dikirimkan dalam format yang mudah dibaca atau dalam bentuk aslinya.

Ciphertext

Ciphertext adalah informasi yang sudah dienkripsi. Algoritma yang digunakan dalam enkripsi atau dekripsi bergantung kepada beberapa aspek. Salah satu aspek yang cukup penting adalah sifat algoritma yang digunakan. Apabila kekuatan dari sebuah algoritma sangat tergantung kepada pengetahuan (tahu atau tidaknya) orang terhadap algoritma yang digunakan, maka algoritma tersebut disebut "restricted algorithm". Apabila algoritma tersebut bocor atau ketahuan oleh orang banyak, maka pesan-pesan dapat terbaca. Tentunya hal ini masih bergantung kepada adanya kriptografer yang baik. Jika tidak ada yang tahu, maka sistem tersebut dapat dianggap aman (meskipun semu).

Meskipun kurang aman, metoda pengamanan dengan *restricted algorithm*

ini cukup banyak digunakan karena mudah implementasinya dan tidak perlu diuji secara mendalam.

PUBLIC-KEY CRYPTOGRAPHY LAWAN SYMMETRIC CRYPTOGRAPHY

Perbedaan prinsip dan penggunaan *public-key cryptography* dan *symmetric cryptography* membutuhkan diskusi tersendiri. Pada *symmetric cryptography*, satu kunci yang sama digunakan untuk melakukan enkripsi dan dekripsi. Pada sistem *public-key cryptography*, enkripsi dan dekripsi menggunakan kunci yang berbeda.

Sejak dikembangkannya *public-key cryptography*, selalu timbul pertanyaan mana yang lebih baik. Para pakar kriptografi mengatakan bahwa keduanya tidak dapat dibandingkan karena mereka memecahkan masalah dalam domain yang berbeda.

Symmetric cryptography merupakan hal yang terbaik untuk mengenkripsi data. Kecepatannya dan keamanan akan *choosenciphertext attack* merupakan kelebihanannya. Sementara itu *public-key cryptography* dapat melakukan hal-hal lain lebih baik daripada *symmetric cryptography*, misalnya dalam hal key management.

Untuk lebih meningkatkan keamanan sistem informasi, proteksi dapat ditambahkan. Proteksi ini dapat berupa filter (secara umum) dan yang lebih spesifik seperti firewall, IDS (Intruder Detection System), VPN (Virtual Private Networks) dan lain sebagainya. Filter dapat digunakan untuk memfilter e-mail, informasi, akses, atau bahkan dalam level packet. Sebagai contoh, di sistem UNIX ada paket program "*tcpwrapper*" yang dapat digunakan untuk membatasi akses kepada servis atau

aplikasi tertentu. Misalnya, servis untuk "telnet" dapat dibatasi untuk sistem yang memiliki nomor IP tertentu, atau memiliki domain tertentu.

FIREWALL

Firewall merupakan sebuah perangkat yang diletakkan antara Internet dengan jaringan internal. Informasi yang keluar atau masuk harus melalui firewall ini.

Tujuan utama dari firewall adalah untuk menjaga (*prevent*) agar akses (kedalam maupun ke luar) dari orang yang tidak berwenang (*unauthorized access*) tidak dapat dilakukan. Konfigurasi dari firewall bergantung kepada kebijaksanaan (*policy*) dari organisasi yang bersangkutan, yang dapat dibagi menjadi dua jenis:

- apa-apa yang tidak diperbolehkan secara eksplisit dianggap tidak diperbolehkan (*prohibited*)
- apa-apa yang tidak dilarang secara eksplisit dianggap diperbolehkan (*permitted*)

Firewall bekerja dengan mengamati paket IP (Internet Protocol) yang melewatinya. Berdasarkan konfigurasi dari firewall maka akses dapat diatur berdasarkan IP address, port, dan arah informasi.

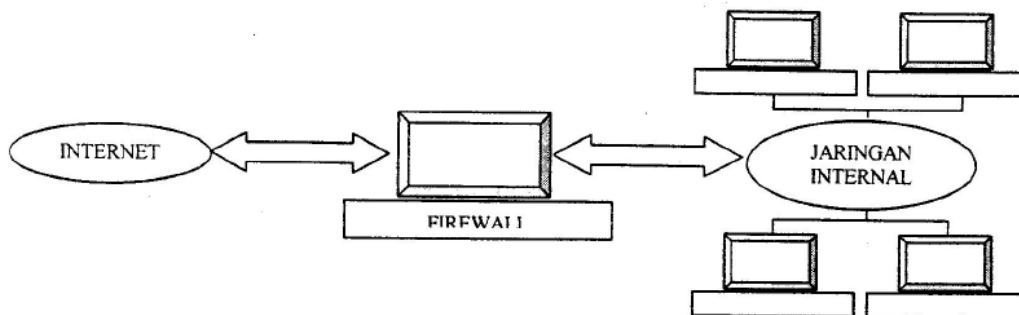
Detail dari konfigurasi bergantung kepada masing-masing firewall.

Firewall dapat berupa sebuah perangkat keras yang sudah dilengkapi dengan perangkat lunak tertentu, sehingga pemakai (*administrator*) tinggal melakukan konfigurasi dari firewall tersebut. Firewall juga dapat berupa perangkat lunak yang ditambahkan kepada sebuah server (baik UNIX maupun Windows NT), yang dikonfigurasi menjadi firewall.

Dalam hal ini, sebetulnya perangkat komputer dengan prosesor Intel 80486 sudah cukup untuk menjadi firewall yang sederhana.

Firewall biasanya melakukan dua fungsi; fungsi (IP) filtering dan fungsi proxy. Keduanya dapat dilakukan pada sebuah perangkat komputer (*device*) atau dilakukan secara terpisah. Beberapa perangkat lunak berbasis UNIX yang dapat digunakan untuk melakukan IP filtering antara lain :

- *ipfwadm*: merupakan standar dari sistem Linux yang dapat diaktifkan pada level kernel
- *ipchains*: versi baru dari Linux kernel packet filtering yang diharapkan dapat menggantikan fungsi *ipfwadm*.



Gambar 1. Firewall secara umum

Fungsi proxy dapat dilakukan oleh berbagai software tergantung kepada jenis proxy yang dibutuhkan, misalnya web proxy, rlogin proxy, ftp proxy dan seterusnya.

Di sisi client sering kali dibutuhkan software tertentu agar dapat menggunakan proxy server ini, seperti misalnya dengan menggunakan SOCKS.

Beberapa perangkat lunak berbasis UNIX untuk proxy antara lain:

- *Socks*: proxy server oleh NEC Network Systems Labs
- *Squid*: web proxy server

**PEMANTAU ADANYA SERANGAN
“INTRUDER DETECTION SYSTEM”
(IDS)**

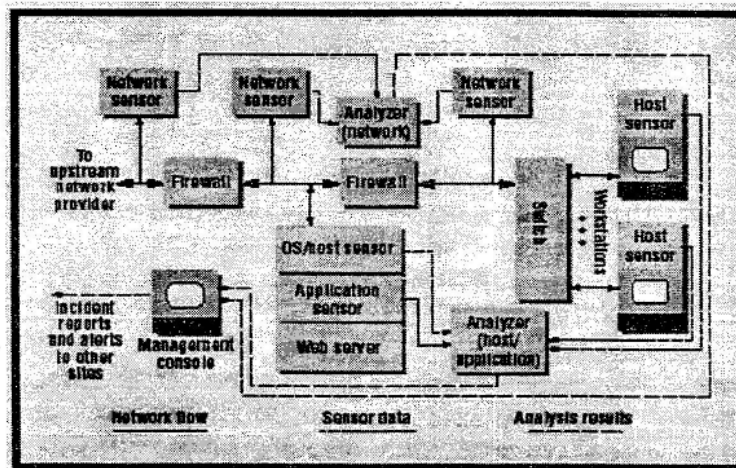
Sistem pemantau (*monitoring system*) digunakan untuk mengetahui adanya tamu tak diundang (*intruder*) atau adanya serangan (*attack*). Nama lain dari sistem ini adalah “*intruder detection system*” (IDS).

Sistem ini dapat memberitahu administrator melalui e-mail maupun

melalui mekanisme lain seperti melalui pager.

Gambar 2 mengilustrasikan struktur sistem dan *phenomenology sense*. pada perusahaan/instansi kecil dikonfigurasi dengan firewall untuk mengisolasi web server-nya. Konfigurasi komputer sebagai sensor jaringan mengekstrak paket yang mencurigakan dari tiga segmen jaringan utama dan meneruskannya ke suatu stasiun jaringan analisis spesifik. Web server dan workstation menjalankan software untuk melihat interaksi yang mencurigakan dengan sistem operasi dan melaporkannya ke stasiun host analisis yang spesifik. Web server melihat penyalahgunaan (*abuse*) seperti exploit CGI-bin yang spesifik untuk HTTP server. Analyzer melaporkan ke management console bahwa server tersebut sebagai user interface IDS. Management console memberikan tanda kepada administrasi perusahaan untuk melaporkan intrusi ke organisasi incident-response seperti pusat koordinasi CERT.

Ada berbagai cara untuk memantau adanya intruder. Ada yang sifatnya aktif



Gambar 2. Aplikasi IDS pada suatu sistem proteksi jaringan

dan pasif. IDS cara yang pasif misalnya dengan memonitor logfile. Contoh software IDS antara lain:

- *Autobuse*, mendeteksi probing dengan memonitor logfile.
- *Courtney* dan *portsentry*, mendeteksi probing (*port scanning*) dengan memonitor packet yang lalu lalang. *Portsentry* bahkan dapat memasukkan IP penyerang dalam filter *tcpwrapper* (langsung dimasukkan kedalam berkas */etc/hosts.deny*)
- *Shadow* dari SANS
- *Snort*, mendeteksi pola (*pattern*) pada paket yang lewat dan mengirimkan alert jika pola tersebut terdeteksi. Pola-pola atau *rules* disimpan dalam berkas yang disebut library yang dapat dikonfigurasi sesuai dengan kebutuhan.

VIRTUAL PRIVATE NETWORKS

VPN adalah suatu jalur (terowongan) yang melalui internet umum yang dibuat dengan tujuan mendapatkan layanan yang memungkinkan untuk dapat mengakses jaringan secara pribadi dari apa saja yang tersedia secara umum dari koneksi internet. Jalur ini dibuat oleh software pada mesin pengguna (user) yang disebut klien. Seorang klien menyediakan semua konektifitas yang diperlukan untuk 'bicara' ke mesin server kantor pada perusahaan atau instansi dimana mereka bekerja. Ketika suatu pengguna (user) dial ke Internet Server Provider milik mereka, tersedia sebuah koneksi antara komputer user dengan internet. Kemudian user dapat memulai suatu koneksi yang dibuat secara abstrak, suatu terowongan dari mesin user ke server. Seorang user dapat mengakses file, menjalankan aplikasi jaringan, transfer data dan file, dsb.

Melalui suatu proses yang disebut enkripsi, jalan aliran data antara user dan

jaringan perusahaan tetap dalam keadaan aman, Ada beberapa metode untuk membuat sebuah VPN.

Untuk kantor perusahaan atau instansi harus tersedia :

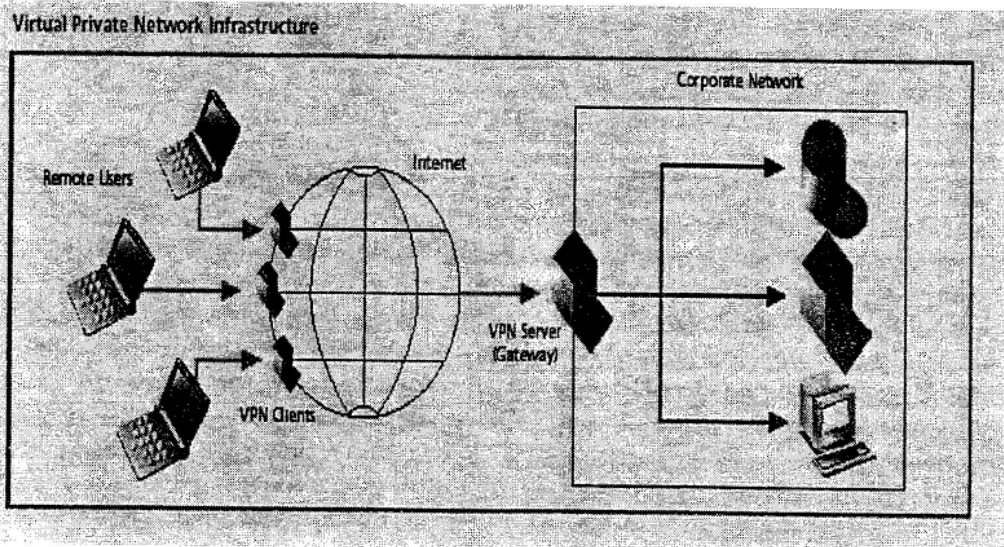
1. Sebuah server Windows NT dengan koneksi internet permanen, dan oleh karena itu IP address statis (tidak berubah). Koneksi yang tepat dan cepat diberikan oleh perusahaan seperti DSL, kabel, T1, T3, jalur yang disewa, (56-384kbps), atau ISDN. Semua ini adalah layanan yang tersedia melalui sebagian besar pada Internet Service Providers.
2. Sebuah firewall, Sebuah firewall terdiri dari sebuah hardware atau software cara penyelesaian yang menyaring data dari dunia luar didasarkan pada aturan yang dikonfigurasi oleh administrator atau installer.
3. Seorang user yang memiliki account, tidak hanya dapat mengakses data pada server, tapi memiliki hak untuk dapat menghubungi server tersebut. Account ini harus secara logic dikelompokkan dalam struktur pada perusahaan dan memberikan hak yang pantas untuk menyediakan sumber pada jaringan Logic, dan mudah untuk mengerti struktur username atau password, dengan password alphanumeric dan berbeda pada masing-masing user, dapat berubah secara sering dan teratur. Hal ini adalah penting untuk suksesnya keamanan Virtual Private Network dan harus dilakukan secara benar.
4. Memonitor secara konstant dan konsisten, termasuk update software antivirus, menambal keamanan, panjang sesi dan file yang diakses, memasukkan IP dari VPN dimana kita dapat mengontak address jaringan yang mengakses.

Pada sisi mobile user harus tersedia :

1. Sebuah komputer Windows dengan sebuah adapter Microsoft VPN yang diinstall. Hal ini merupakan aspek pada komponen jaringan yang telah tersedia dalam sistem operasi. Dikonfigurasi dengan informasi dan latihan yang disediakan oleh sistem administrator.
2. Account Internet Service Provider dikonfigurasi sebagaimana mestinya. Hal ini dapat account pribadi siapa saja dilayani oleh sebuah provider yang lain dari AOL, Prodigy, atau Direct Dial Service yang lain yang berbeda dari general internet. Ini juga didukung oleh perusahaan, kesatuan kebijakan dan anggaran yang ada pada perusahaan. Hal ini akan lebih baik jika

account konsumen yang cepat seperti DSL ISDN, atau kabel, tapi standar layanan dial up 56 K akan menyediakan fungsi yang dibutuhkan.

3. Mengerti proses dengan baik dan hak-hak yang diijinkan pada user. Keuntungan sebuah ISP untuk hubungan kecepatan tinggi untuk lokal POP. Kita hanya membayar untuk panggilan lokal dan akses ISP gratis, hal ini memberikan keuntungan relatif harga yang rendah akses layanan IP termasuk harga jarak sensitif bandwidth. Mengingat bahwa banyak ISP yang menawarkan struktur biaya rata-rata (flat), biaya akses telepon secara dramatis dapat dikurangi.



Gambar 3. Virtual private network

DAFTAR PUSTAKA

- Budi Rahardjo, 1997, *Keamanan Sistem Informasi: Beberapa Topik Keamanan di Internet*, Seminar Informasi Infrastruktur Nasional, ITB
- Richard H. Baker, 1995, *Network Security: how to plan for it and achieve it*, McGraw-Hill International
- Steven M. Bellovin, 1989, *Security Problems in TCP/IP Protocol Suite*, Computer Communication Review, Vol. 19, No. 2, pp. 32-48