KEAMANAN JARINGAN

1. Membatasi Akses ke Jaringan

A. Membuat tingkatan akses :

Pembatasan-pembatasan dapat dilakukan sehingga memperkecil peluang penembusan oleh pemakai yang tak diotorisasi, misalnya :

- Pembatasan login. Login hanya diperbolehkan :
  - Pada terminal tertentu.
  - Hanya ada waktu dan hari tertentu.
  - Pembatasan dengan call-back (Login dapat dilakukan siapapun. Bila telah sukses login, sistem segera memutuskan koneksi dan memanggil nomor telepon yang telah disepakati, Penyusup tidak dapat menghubungi lewat sembarang saluran telepon, tapi hanya pada saluran telepon tertentu).
- Pembatasan jumlah usaha login.
  - Login dibatasi sampai tiga kali dan segera dikunci dan diberitahu ke administrator.
  - Semua login direkam dan sistem operasi melaporkan informasi-informasi berikut :
    - Waktu, yaitu waktu pemakai login.
    - Terminal, yaitu terminal dimana pemakai login.
- Tingkat akses yang diizinkan (read / write / execute / all)

B. Mekanisme kendali akses :

Masalah identifikasi pemakai ketika login disebut otentifikasi pemakai (user authentication). Kebanyakan metode otentifikasi didasarkan pada tiga cara, yaitu :

1. Sesuatu yang diketahui pemakai, misalnya :
   - Password.
   - Kombinasi kunci.
   - Nama kecil ibu mertua.
   - Dan sebagainya.

2. Sesuatu yang dimiliki pemakai, misalnya :
   - Badge.
   - Kartu identitas.
   - Kunci.
   - Dan sebagainya.

3. Sesuatu mengenai (ciri) pemakai, misalnya :
   - Sidik jari.
   - Sidik suara.
   - Foto.
   - Tanda tangan.

C. Waspada terhadap Rekayasa sosial :

1. Mengaku sebagi eksekutif yang tidak berhasil mengakses, menghubungi administrator via telepon/fax.
2. Mengaku sebagai administrator yang perlu mendiagnosa masalah network, menghubungi end user via email/fax/surat.
3. Mengaku sebagai petugas keamanan e-commerce, menghubungi customer yang telah bertransaksi untuk mengulang kembali transaksinya di form yang disediakan olehnya.

4. pencurian surat, password.
5. penyuapan, kekerasan.

D. Membedakan Sumber daya internal dan Eksternal :

Memanfaatkan teknologi firewall yang memisahkan network internal dengan network eksternal dengan rule tertentu.

E. Sistem Otentikasi User :

Def : adalah proses penentuan identitas dari seseorang yang sebenarnya, hal ini diperlukan untuk menjaga keutuhan (integrity) dan keamanan (security) data, pada proses ini seseorang harus dibuktikan siapa dirinya sebelum menggunakan layanan akses.

Upaya untuk lebih mengamankan proteksi password, antara lain :

1. Salting.
   Menambahkan string pendek ke string password yang diberikan pemakai sehingga mencapai panjang password tertentu.
2. One time password.
   - Pemakai harus mengganti password secara teratur. Upaya ini membatasi peluang password telah diketahui atau dicoba-coba pemakai lain.
   - Bentuk ekstrim pendekatan ini adalah one time password, yaitu pemakai mendapat satu buku berisi daftar password. Setiap kali pemakai login, pemakai menggunakan password berikutnya yang terdapat di daftar password.
   - Dengan one time password, pemakai direpotkan keharusan menjaga agar buku passwordnya jangan sampai dicuri.
3. Satu daftar panjang pertanyaan dan jawaban.
   - Variasi terhadap password adalah mengharuskan pemakai memberi satu daftar pertanyaan panjang dan jawabannya. Pertanyaan-pertanyaan dan jawabannya dipilih pemakai sehingga pemakai mudah mengingatnya dan tak perlu menuliskan di kertas.
   - Pertanyaan berikut dapat dipakai, misalnya :
     - Siapa mertua abang ipar Badru ?
     - Apa yang diajarkan Pak Harun waktu SD ?
     - Di jalan apa pertama kali ditemukan simanis ?
   - Pada saat login, komputer memilih salah satu dari pertanyaan-pertanyaan secara acak, menanyakan ke pemakai dan memeriksa jawaban yang diberikan.
4. Tantangan tanggapan (chalenge response).
   - Pemakai diberi kebebasan memilih suatu algoritma, misalnya x3.
   - Ketika pemakai login, komputer menuliskan di layar angka 3. Dalam kasus ini pemakai mengetik angka 27. Algoritma dapat berbeda di pagi, sore, dan hari berbeda, dari terminal berbeda, dan seterusnya.

Contoh Produk Otentikasi User, antara lain :

1. Secureid ACE (Access Control Encryption)
   System token hardware seperti kartu kredit berdisplay, pemakai akan menginput nomor pin yang diketahui bersama, lalu memasukkan pascode bahwa dia pemilik token.

2. S/key (Bellcore)
   System software yang membentuk one time password (OTP) berdasarkan informasi loginterkhir dengan aturan random tertentu.

3. Password Authentication Protocol (PAP)

Protokol dua arah untuk PPP (Point to point Protocol). Peer mengirim pasangan user id dan password, authenticator menyetujuinya.

4. Challenge Handshake Authentication Protocol (CHAP)
   S/key pada PAP, protocol 3 arah, authenticator mengirim pesan tantangan ke peer, peer menghitung nilai lalu mengirimkan ke authenticator, authenticator menyetujui otentikasi jika jawabannya sama dengan nilai tadi.

5. Remote Authentication Dial-in User Service (RADIUS)
   Untuk hubungan dial-up, menggunakan network access server, dari suatu host yang menjadi client RADIUS, merupan system satu titik akses.

6. Terminal Access Controller Access Control System (TACACS)
   Protokol keamanan berbasis server dari CISCO System. Secury\ity Server terpusat dangan file password UNIX, database otentikasi, otorisasi dan akunting, fungsi digest (transmisi password yang tidak polos)

2. Melindungi Aset Organisasi

A.Secara Adminsistratif / fisik

- Rencana kemungkinan terhadap bencana
- Program penyaringan calon pegawai system informasi
- Program pelatihan user
- Kebijakan akses network

B. Secara Teknis

B.1. Penerapan Firewall

Istilah pada penerapan Firewall

- Host
  Suatu sistem komputer yang terhubung pada suatu network
- Bastion host
  Sistem komputer yang harus memiliki tingkat sekuritas yang tinggi karena sistem ini rawan sekali terhadap serangan hacker dan cracker, karena biasanya mesin ini diekspos ke network luar (Internet) dan merupakan titik kontak utama para user dari internal network.
- Packet Filtering
  Aksi dari suatu devais untuk mengatur secara selektif alur data yang melintasi suatu network. Packet filter dapat memblok atau memperbolehkan suatu paket data yang melintasi network tersebut sesuai dengan kebijaksanaan alur data yang digunakan (security policy).
- Perimeter network
  Suatu network tambahan yang terdapat di antara network yang dilindungi dengan network eksternal, untuk menyediakan layer tambahan dari suatu sistem security. Perimeter network juga sering disebut dengan DMZ (De-Millitarized Zone).

Keuntungan Firewall :

- Firewall merupakan fokus dari segala keputusan sekuritas. Hal ini disebabkan karena Firewall merupakan satu titik tempat keluar masuknya trafik internet pada suatu jaringan.
- Firewall dapat menerapkan suatu kebijaksanaan sekuritas. Banyak sekali service-service yang digunakan di Internet. Tidak semua service tersebut aman digunakan, oleh

karenanya Firewall dapat berfungsi sebagai penjaga untuk mengawasi service-service mana yang dapat digunakan untuk menuju dan meninggalkan suatu network.

- Firewall dapat mencatat segala aktivitas yang berkaitan dengan alur data secara efisien. Semua trafik yang melalui Firewall dapat diamati dan dicatat segala aktivitas yang berkenaan dengan alur data tersebut. Dengan demikian Network Administrator dapat segera mengetahui jika terdapat aktivitas-aktivitas yang berusaha untuk menyerang internal network mereka.
- Firewall dapat digunakan untuk membatasi pengunaan sumberdaya informasi. Mesin yang menggunakan Firewall merupakan mesin yang terhubung pada beberapa network yang berbeda, sehingga kita dapat membatasi network mana saja yang dapat mengakses suatu service yang terdapat pada network lainnya.

Kelemahan Firewall :

- Firewall tidak dapat melindungi network dari serangan koneksi yang tidak melewatinya (terdapat pintu lain menuju network tersebut).
- Firewall tidak dapat melindungi dari serangan dengan metoda baru yang belum dikenal oleh Firewall.
- Firewall tidak dapat melindungi dari serangan virus.

Pilihan klasifikasi desain Firewall :

1. Packet Filtering

   Sistem paket *filtering* atau sering juga disebut dengan *screening router* adalah *router* yang melakukan routing paket antara internal dan eksternal *network* secara selektif sesuai dengan *security policy* yang digunakan pada *network* tersebut. Informasi yang digunakan untuk menyeleksi paket-paket tersebut adalah:

   - IP address asal
   - IP address tujuan
   - Protocol (TCP, UDP, atau ICMP)
   - Port TCP atau UDP asal
   - Port TCP atau UDP tujuan

   Beberapa contoh routing paket selektif yang dilakukan oleh *Screening Router* :

   - Semua koneksi dari luar sistem yang menuju internal *network* diblokade kecuali untuk koneksi SMTP
   - Memperbolehkan *service* email dan FTP, tetapi memblok *service-service* berbahaya seperti TFTP, X Window, RPC dan ‘r’ *service* (rlogin, rsh, rcp, dan lain-lain).

   Selain memiliki keuntungan tertentu di antaranya aplikasi *screening router* ini dapat bersifat transparan dan implementasinya relatif lebih murah dibandingkan metode *firewall* yang lain, sistem paket *filtering* ini memiliki beberapa kekurangan yakni : tingkat *security*nya masih rendah, masih memungkinkan adanya IP Spoofing, tidak ada *screening* pada layer-layer di atas *network* layer.

2. Application Level Gateway (Proxy Services)

   Proxy service merupakan aplikasi spesifik atau program server yang dijalankan pada mesin *Firewall*, program ini mengambil *user request* untuk Internet *service* (seperti FTP, telnet, HTTP) dan meneruskannya (bergantung pada *security policy*) ke *host* yang dituju. Dengan kata lain adalah *proxy* merupakan perantara antara internal *network* dengan eksternal *network* (Internet).

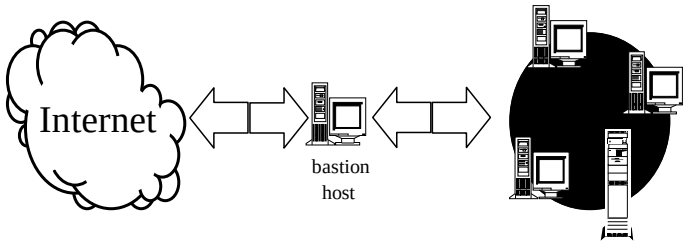
   Pada sisi ekternal hanya dikenal mesin *proxy* tersebut, sedangkan mesin-mesin yang berada di balik mesin *proxy* tersebut tidak terlihat. Akibatnya sistem *proxy* ini kurang transparan terhadap *user* yang ada di dalam

Sistem *Proxy* ini efektif hanya jika pada konjungsi antara internal dan eksternal *network* terdapat mekanisme yang tidak memperbolehkan kedua *network* tersebut terlibat dalam komunikasi langsung.
Keuntungan yang dimiliki oleh sistem *proxy* ini adalah tingkat sekuritasnya lebih baik daripada *screening router*, deteksi paket yang dilakukan sampai pada layer aplikasi. Sedangkan kekurangan dari sistem ini adalah perfomansinya lebih rendah daripada *screening router* karena terjadi penambahan *header* pada paket yang dikirim, aplikasi yang di-*support* oleh *proxy* ini terbatas, serta sistem ini kurang transparan.

Arsitektur dasar firewall :

- Arsitektur dengan dual-homed host (kadang kadang dikenal juga sebagai *dual homed gateway*/ DHG)

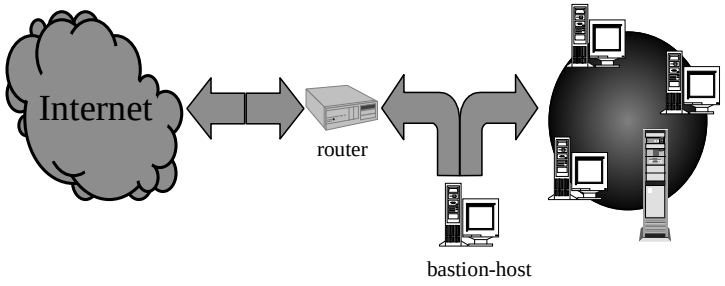
  Sistem DHG menggunakan sebuah komputer dengan (paling sedikit) dua network-interface. Interface pertama dihubungkan dengan jaringan internal dan yang lainnya dengan Internet. Dual-homed host nya sendiri berfungsi sebagai bastion host (front terdepan, bagian terpenting dalam firewall).



Arsitektur dengan dual-homed host

- screened-host (*screened host gateway*/ SHG)

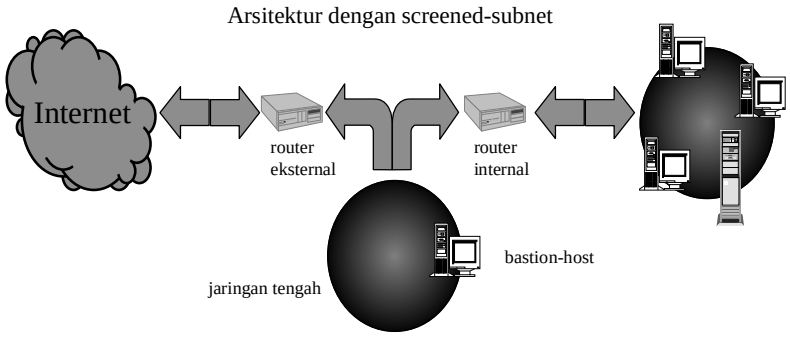
  Pada topologi SHG, fungsi firewall dilakukan oleh sebuah screening-router dan bastion host. Router ini dikonfigurasi sedemikian sehingga akan menolak semua trafik kecuali yang ditujukan ke bastion host, sedangkan pada trafik internal tidak dilakukan pembatasan. Dengan cara ini setiap client servis pada jaringan internal dapat menggunakan fasilitas komunikasi standard dengan Internet tanpa harus melalui proxy.



Arsitektur dengan screened-host

- screened subnet (*screened subnet gateway*/ SSG).

Firewall dengan arsitektur screened-subnet menggunakan dua screening-router dan jaringan tengah (*perimeter network*) antara kedua router tersebut, dimana ditempatkan bastion host. Kelebihan susunan ini akan terlihat pada waktu optimasi penempatan server.



B.2. Penerapan Virtual Privat Network (VPN)

Defenisi VPN

Virtual Private Network atau Jaringan Pribadi Maya sesungguhnya sama dengan Jaringan Pribadi (Private Network/PN) pada umumnya, di mana satu jaringan komputer suatu lembaga atau perusahaan di suatu daerah atau negara terhubung dengan jaringan komputer dari satu grup perusahaan yang sama di daerah atau negara lain. Perbedaannya hanyalah pada media penghubung antar jaringan. Kalau pada PN, media penghubungnya masih merupakan milik perusahaan/grup itu sendiri, dalam VPN, media penghubungnya adalah jaringan publik seperti Internet.

Dalam VPN, karena media penghubung antar jaringannya adalah jaringan publik, diperlukan pengamanan dan pembatasan-pembatasan. Pengamanan diperlukan untuk menjaga agar tidak sebarang orang dari jaringan publik dapat masuk ke jaringan pribadi. Yang dikecualikan hanyalah orang-orang yang terdaftar atau terotentifikasi terlebih dahulu yang dapat masuk ke jaringan pribadi. Pembatasan diperlukan untuk menjaga agar tidak semua orang atau user dari jaringan pribadi dapat mengakses jaringan publik (internet).

Cara membentuk VPN

1. Tunnelling

Sesuai dengan arti tunnel atau lorong, dalam membentuk suatu VPN ini dibuat suatu tunnel di dalam jaringan publik untuk menghubungkan antara jaringan yang satu dan jaringan lain dari suatu grup atau perusahaan.yang ingin membangun VPN tersebut. Seluruh komunikasi data antarjaringan pribadi akan melalui tunnel ini, sehingga orang atau user dari jaringan publik yang tidak memiliki izin untuk masuk tidak akan mampu untuk menyadap, mengacak atau mencuri data yang melintasi tunnel ini. Ada beberapa metode tunelling yang umum dipakai, di antaranya:

- IPX To IP Tunnelling, atau
- PPP To IP Tunnelling

IPX To IP tunnelling biasa digunakan dalam jaringan VPN Novell Netware. Jadi dua jaringan Novell yang terpisah akan tetap dapat saling melakukan komunikasi data melalui jaringan publik Internet melalui tunnel ini tanpa kuatir akan adanya gangguan pihak ke-3 yang ingin mengganggu atau mencuri data. Pada IPX To IP tunnelling, paket data dengan protokol IPX (standar protokol Novell) akan dibungkus (encapsulated) terlebih dahulu oleh protokol IP (standar protokol Internet) sehingga dapat melalui tunnel ini pada jaringan publik Internet. Sama halnya untuk PPP To IP tunnelling, di mana PPP protokol diencapsulated oleh IP protokol.

Saat ini beberapa vendor hardware router seperti Cisco, Shiva, Bay Networks sudah menambahkan kemampuan VPN dengan teknologi tunnelling pada hardware mereka.

2. Firewall

Sebagaimana layaknya suatu dinding, Firewall akan bertindak sebagai pelindung atau pembatas terhadap orang-orang yang tidak berhak untuk mengakses jaringan kita. Umumnya dua jaringan yang terpisah yang menggunakan Firewall yang sejenis, atau seorang remote user yang terhubung ke jaringan dengan menggunakan software client yang terenkripsi akan membentuk suatu VPN, meskipun media penghubung dari kedua jaringan tersebut atau penghubung antara remote user dengan jaringan tersebut adalah jaringan publik seperti Internet.

Suatu jaringan yang terhubung ke Internet pasti memiliki IP address (alamat Internet) khusus untuk masing-masing komputer yang terhubung dalam jaringan tersebut. Apabila jaringan ini tidak terlindungi oleh tunnel atau firewall, IP address tadi akan dengan mudahnya dikenali atau dilacak oleh pihak-pihak yang tidak diinginkan. Akibatnya data yang terdapat dalam komputer yang terhubung ke jaringan tadi akan dapat dicuri atau diubah. Dengan adanya pelindung seperti firewall, kita bisa menyembunyikan (hide) address tadi sehingga tidak dapat dilacak oleh pihak-pihak yang tidak diinginkan.

Kemampuan firewall dalam penerapannya pada VPN

- IP Hiding/Mapping. Kemampuan ini mengakibatkan IP address dalam jaringan dipetakan atau ditranslasikan ke suatu IP address baru. Dengan demikian IP address dalam jaringan tidak akan dikenali di Internet.

- Privilege Limitation. Dengan kemampuan ini kita dapat membatasi para user dalam jaringan sesuai dengan otorisasi atau hak yang diberikan kepadanya. Misalnya, User A hanya boleh mengakses home page, user B boleh mengakses home page, e-mail dan news, sedangkan user C hanya boleh mengakses e-mail.

- Outside Limitation. Dengan kemampuan ini kita dapat membatasi para user dalam jaringan untuk hanya mengakses ke alamat-alamat tertentu di Internet di luar dari jaringan kita.

- Inside Limitation. Kadang-kadang kita masih memperbolehkan orang luar untuk mengakses informasi yang tersedia dalam salah satu komputer (misalnya Web Server) dalam jaringan kita. Selain itu, tidak diperbolehkan, atau memang sama sekali tidak dizinkan untuk mengakses seluruh komputer yang terhubung ke jaringan kita.

- Password and Encrypted Authentication. Beberapa user di luar jaringan memang diizinkan untuk masuk ke jaringan kita untuk mengakses data dan sebagainya, dengan terlebih dahulu harus memasukkan password khusus yang sudah terenkripsi.

3. Mengamankan saluran terbuka

Protokol TCP/IP merupakan protocol dalam set standar yang terbuka dalam pengiriman data, untuk itulah perlu dilakukan enkripsi dalam rangka penanganan keamanan data yang diterapkan pada protocol tersebut, yang meliputi :

A. Keamanan Panda lapisan Aplikasi

- SET (Secure Electronics Transaction)
  - Menentukan bagaimana transaksi mengalir antara pemakai, pedagang dan bank.
  - Menentukan fungsi keamanan : digital signature, hash dan enkripsi.
  - Produk dari Mastercard dan VISA International.

- Secure HTTP
  - Produk dari workgroup IETF, diimplementasikan pada webserver mulai 1995.
  - Menentukan mekanisme kriptografi standar untuk mengenkripsikan pengiriman data http

- Pretty Good Privacy (PGP)
  - Standarisasi RFC 1991
  - Membuat dan memastikan digital signature, mengenkripsi – deskripsi dan mengkompresi data.

- Secure MIME (S/MIME)
  - Standarisasi RFC 1521
  - MIME (Multipurpose Internet Mail Extension)
  - Menentukan cara menempelkan file untuk dikirim ke internet dengan menggunakan metode hirarki dalm pendefenisian user remi dan sertfikat digitalnya.

- Cybercash
  - Standarisasi RFC 1898
  - Memproses kartu kredit di internet dengan mengenkripsi dan menandatangani transaksi secara digital.

B. Keamanan dalam Lapisan Transport

- SSL (Secure Socket Layer)
  - Produk Netscape
  - Protocol yang menegoisasikan hubungan yang aman antara client dan server, dengan menggunakan kunci enkripsi 40-bit.

C. Keamanan dalam Lapisan Network

- IP security Protocol : melindungi protocol client IP pada network layer.
- IP Authentication header
- IP Encapsulating Security protocol
- Simple-key management for Internet protocol (SKIP)
- Internet security Association and key management protocol (ISAKMP)
- Internet key management protocol (IKMP)
- Sumber : www.ietf.org