BAB X
KEAMANANAN DALAM JARINGAN

10.1 Membatasi Akses ke Jaringan

[17]**Membuat tingkatan akses :**

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

a. 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).
b. 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)

10.2 Mekanisme kendali akses

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

a. Sesuatu yang diketahui pemakai, misalnya : Password,Kombinasi kunci,Nama kecil ibu mertua, Dan sebagainya.
b. Sesuatu yang dimiliki pemakai, misalnya : Badge,Kartu identitas,Kunci, Dan sebagainya.
c. Sesuatu mengenai (ciri) pemakai, misalnya : Sidik jari,Sidik suara,Foto,Tanda tangan.

10.3 Waspada terhadap Rekayasa sosial

Kewaspadaan yang harus di perhatikan pada rekayasa social, yaitu :

a. Mengaku sebagi eksekutif yang tidak berhasil mengakses, menghubungi administrator via telepon/fax.
b. Mengaku sebagai administrator yang perlu mendiagnosa masalah network,menghubungi end user via email/fax/surat.
c. Mengaku sebagai petugas keamanan e-commerce,menghubungi customer yang telah bertransaksi untuk mengulang kembali transaksinya di form yang disediakan olehnya.
d. pencurian surat, password.
e. penyuapan, kekerasan.

10.4 Membedakan Sumber daya internal dan Eksternal

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

Sistem Otentikasi User :

Defenisi : 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.

10.5 Upaya untuk lebih mengamankan proteksi password, antara lain :

a. Salting : Menambahkan string pendek ke string password yang diberikan pemakai sehingga mencapai panjang password tertentu.
b. 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.
c. 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.
d. Pada saat login, komputer memilih salah satu dari pertanyaan-pertanyaan secara acak, menanyakan ke pemakai dan memeriksa jawaban yang diberikan. 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 :

a. 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.
b. S/key (Bellcore) : System software yang membentuk one time password (OTP) berdasarkan informasi login terkhir dengan aturan random tertentu.
c. Password Authentication Protocol (PAP) : Protokol dua arah untuk PPP (Point to point Protocol). Peer mengirim pasangan user id dan password, authenticator menyetujuinya.
d. 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.
e. 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.
f. 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).

10.6 Melindungi Aset Organisasi

Secara Administratif\Fisik

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

Secara Teknis

- 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.

10.7 Virtual Private

Network atau VPN adalah suatu jaringan pribadi yang dibuat dengan menggunakan jaringan publik, atau dengan kata lain menciptakan suatu WAN yang sebenarnya terpisah baik secara fisikal maupun geografis sehingga secaralogikal membentuk satu netwok tunggal, paket data yang mengalir antar site maupun dari user yang melakukan remoteakses akan mengalami enkripsi dan authentikasi sehingga menjamin keamanan, integritas dan validitas data.

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, dan news, sedangkan user C hanya boleh mengakses . 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.

10.8 Keuntungan Firewall

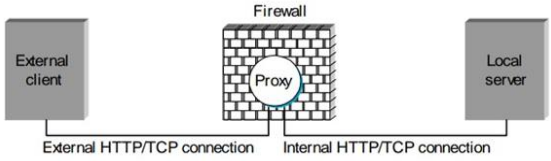
Firewall merupakan fokus dari segala keputusan sekuritas. Hal ini disebabkan karena Firewall merupakan satu titik tempat keluar masuknya trafik internet pada suatu jaringan.

Keuntungan pada firewall yaitu :

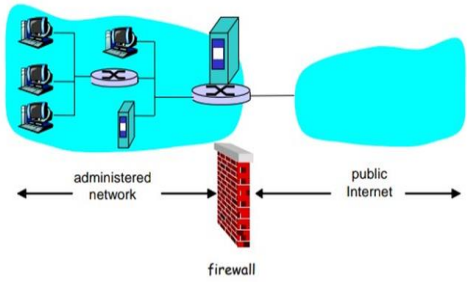
1. Firewall dapat menerapkan suatu kebijaksanaan sekuritas. Banyak sekali service - service yang digunakan di Internet. Tidak semua service tersebut aman digunakan, oleh karenanya Firewall dapat berfungsi sebagai penjaga untuk mengawasi service - service mana yang dapat digunakan untuk menuju dan meninggalkan suatu network.
2. 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.
3. 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.

10.9 Kelemahan Firewall :

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



Gambar 10.1 Contoh Proxy firewall



Gambar 10.2 Contoh kerja firewall

10.10 Tipe *Firewall*

1. Packet Filter

Jenis firewall yang pertama ini merupakan jenis yang paling *simple*. Firewall yang satu ini merupakan sebuah computer yang dibekali dengan dua buah Network Interface Card (NIC) yang mana fungsinya menyaring berbagai paket yang masuk. Umumnya, perangkat ini dikenal dengan packet-filtering router.

2. Circuit Level Gateway

Jenis berikutnya yaitu Circuit Level Gateway. Jenis ini umumnya baerupa komponen suatu proxy server. Tidak hanya itu, firewall tersebut beroperasi dalam level yang memang lebih tinggi pada model referensi OSI ketimbang jenis Packet Filter Firewall. Firewall ini tepatnya bekerja pada lapisan sesi (*session layer*). Adapun modifikasi dari jenis firewall ini cukup berguna bagi siapa saja yang ingin menyembunyikan informasi yang berkaitan dengan jaringan terproteksi, meskipun firewall jenis ini tak melakukan penyaringan atas beragam paket individual dalam suatu koneksi.

3. Application Level

Jenis selanjutnya kita kenal dengan Application Level Firewall yang mana jenis ini dapat disebut sebagai Application Level Gateway atau application proxy. Penggunaan firewall ini akan mengakibatkan tidak dibolehkannya paket untuk masuk melewati firewall tersebut secara langsung. Namun demikian,

aplikasi proxy pada suatu computer yang mengaktifkan firewall akan mengalihkan permintaan tersebut pada layanan yang ada dalam jaringan privat. Kemudian meneruskan respons permintaan tersebut ke computer atau PC yang pertama kail membuat permintaan dimana letaknya berada di jaringan publik.

4. Network Address Translation (NAT)

Disingkat dengan NAT, jenis firewall yang satu ini menyediakan proteksi secara otomatis terhadap system di balik firewall. Pasalnya, Firewall berjenis NAT ini hanya mengizinkan koneksi dari computer yang letaknya di balik firewall. Sementara itu, tujuan NAT firewall yaitu melakukan multiplexing pada lalu lintas jaringan internal lalu menyampaikannya ke jaringan semacam WAN, MAN ataupun jaringan Internet yang memang lebih luas jaringannya. Hal ini membuat paket tersebut seolah-olah berasal dari sebuah IP address. Di samping itu, NAT membuat tabel yang berisikan informasi tentang koneksi yang dijumpai oleh firewall. Fungsi dari tabel ini yaitu memetakan alamat suatu jaringan internal ke eksternalnya. Adapun kemampuan dalam meletakkan seluruh jaringan di balik IP address berdasarkan pada pemetaan port-port NAT firewall.

5. Stateful Firewall

Jenis Firewall yang satu ini dikenal sebagai sebuah firewall dengan fungsinya dalam menggabungkan berbagai keunggulan yang biasanya ditawarkan oleh firewall berjenis packet filtering, Proxy dan Circuit Level dalam suatu system. Firewall jenis ini dapat melakukan filtering pada lalu lintas atas dasar karakteristik paket, sebagaimana halnya filtering berjenis packet filtering serta memiliki pengecekan pada sesi koneksi guna meyakinkan kalau sesi koneksi tersebut diizinkan.

6. Virtual Firewall

Yang perlu juga anda ketahui yaitu adanya virtual firewall dimana nama virtual tersebut adalah sebutan yang dialamatkan pada firewall logis tertentu yang berada dalam suat perangkat fisik (seperti computer maupun perangkat firewall yang lain). Pengaturan dari firewall ini memperbolehkan beberapa network untuk dapat diproteksi oleh firewall yang memiliki keunikan dimana fungsinya menjalankan kebijakan keamanan system yang tentunya unik juga, cukup dengan memanfaatkan sebuah perangkat. Dengan memanfaatkan firewall tersebut, sebuah ISP atau *Internet Service Provider* dapat menghadirkan layanan firewall untuk para pelanggannya agar lalu lintas dari jaringan mereka akan selalu aman, yaitu hanya dengan memfungsikan sebuah perangkat. Tentunya, ini akan menjadi langkah penghematan biaya (efisiensi) yang signifikan, walaupun firewall jenis yang satu ini hanya ditemukan pada firewall yang berasal dari kelas atas, misalnya Cisco PIX 535.

7. Transparent Firewall

Di antara jenis-jenis firewall yang telah disebutkan sebelumnya, jangan pernah lupakan jenis yang terakhir, yaitu Transparent Firewall. Jenis ini bisa juga disebut dengan bridging firewall yang mana bukanlah merupakan firewall murni, akan tetapi hanya sebuah turunan atas satateful firewall. Transparent

firewall melakukan apa saja yang dapat dilakukan oleh firewall jenis packet filtering, sebagaimana halnya stateful firewall serta tak Nampak oleh pengguna. Maka dari itu jenis firewall yang satu ini bernama Transparent Firewall.

10.11 Application Gateway

1. Proxy

Istilah umum pada teknik jaringan yaitu proses yang berada antara client dan server proses. proxy yang berjalan dalam komputer yang menjalankan firewall akan meneruskan permintaan tersebut kepada layanan yang tersedia dalam jaringan privat dan kemudian meneruskan respons dari permintaan tersebut kepada komputer yang membuat permintaan pertama kali yang terletak dalam jaringan publik yang tidak aman.

a. Dari sisi client : proxy mewakili server, Application Level Firewall juga umumnya mengharuskan beberapa konfigurasi yang diberlakukan pada pengguna untuk mengizinkan mesin klien agar dapat berfungsi. Sebagai contoh, jika sebuah proxy FTP dikonfigurasikan di atas sebuah application layer gateway, proxy tersebut dapat dikonfigurasikan untuk mengizinlan beberapa perintah FTP, dan menolak beberapa perintah lainnya.
b. Dari sisi server : proxy mewakili client , Jenis ini paling sering di implementasikan pada proxy SMTP sehingga mereka dapat menerima surat elektronik dari luar (tanpa menampakkan alamat e-mail internal), lalu meneruskan e-mail tersebut kepada e-mail server dalam jaringan.
c. Umumnya proxy : terkait dengan konteks aplikasi. yang umumnya juga merupakan komponen dari sebuah proxy server. Firewall ini tidak mengizinkan paket yang datang untuk melewati firewall secara langsung. Tetapi, aplikasi proxy yang berjalan dalam komputer yang menjalankan firewall akan meneruskan permintaan tersebut kepada layanan yang tersedia dalam jaringan privat dan kemudian meneruskan respons dari permintaan tersebut kepada komputer yang membuat permintaan pertama kali yang terletak dalam jaringan publik yang tidak aman.
d. Security : Proxy dapat menerap kan(enforce) kebijakan keamanan dalam memberi kan services dari suatu aplikasi , Tetapi, karena adanya pemrosesan yang lebih rumit, firewall jenis ini mengharuskan komputer yang dikonfigurasikan sebagai application gateway memiliki spesifikasi yang tinggi, dan tentu saja jauh lebih lambat dibandingkan dengan packet-filter firewall.

10.12 Cont. Proxy

1. proxy SOCKS (kaus kaki) :

PSOCKS proxy server adalah server proxy generik. SOCKS adalah pintu gerbang sirkuit-tingkat bagian bawah adalah David Koblas dikembangkan pada tahun 1990, sejak itu telah standar terbuka sebagai standar Internet RFC. Socks tidak diwajibkan untuk mengikuti sistem operasi tertentu, platform aplikasi, proxy Socks dan proxy aplikasi-lapisan, HTTP proxy lapisan yang berbeda, proxy Socks hanya melewati paket data yang tidak peduli apa jenis protokol aplikasi (seperti FTP, HTTP dan permintaan NNTP) . Oleh karena itu, aplikasi proxy Socks proxy lapisan dari yang lain lebih cepat. Hal ini biasanya

terkait dengan 1080 port server proxy. Jika Anda berada di jaringan perusahaan atau jaringan kampus, harus melalui firewall atau melalui server proxy untuk mengakses Internet mungkin perlu untuk menggunakan SOCKS. Secara umum, untuk pengguna dial-up tidak perlu menggunakannya. Catatan, ketika browsing web proxy server sering menggunakan proxy http khusus, SOCKS itu berbeda. Oleh karena itu, Anda dapat mengunjungi situs web tidak berarti Anda selalu dapat mengakses internet melalui SOCKS. Umumnya digunakan firewall, atau SOCKS proxy dukungan perangkat lunak. HTTP Proxy yaitu menerima dan menolak user melalui HTTP / TCP.
Contoh kebijakan keamanan dalam proxy, yaitu:

1. Kebijakan membatasi akses ke direktory tertentu di web server untuk user tertentu / remote site.
2. Menggunakan filter port 80, tidak efektif karena melakukan blok pada keseluruhan akses.

Soal

1. Jelas kan apa yang dimaksud dengan VPN?
2. Sebutkan apa Keuntungan dari Firewall ?