

**Tugas EC7010
Keamanan Sistem Lanjut**

MANAJEMEN KEBIJAKAN KEAMANAN FIREWALL

Dosen: Ir. Budi Raharjo, M.Sc., Ph.D

oleh:
Joni Hariyanto
232 03 112



**Program Pasca Sarjana Jurusan Teknik Elektro
Bidang Khusus Teknologi Informasi
Institut Teknologi Bandung
2004**

ABSTRAK

Firewall merupakan suatu perangkat keamanan jaringan yang memperkenankan berbagai bagian ruas jaringan untuk melaksanakan komunikasi antara satu dengan yang lainnya sesuai dengan definisi kebijakan keamanan (security policy) yang telah diterapkan sebelumnya.

Firewalls peka terhadap kesalahan konfigurasi dan kegagalan untuk menerapkan kebijakan, sehingga diperlukan tambahan atau peningkatan keamanan lain. Oleh karena itu, konfigurasi dan administrasi firewall harus dilakukan secara hati-hati, sehingga organisasi seharusnya dapat bertahan dengan mengurangi kerapuhan (vulnerabilities) dan gangguan baru. Firewall merupakan garis pertahanan yang terdepan dari suatu organisasi, maka organisasi seharusnya menerapkan pertahanan ini dengan sungguh-sungguh untuk strategi keamanan departemennya, terkait dengan di lapisan-lapisan mana saja firewall dan sistem keamanan lainnya digunakan diseluruh jaringan. Yang paling penting, organisasi perlu bekerja keras untuk memelihara semua sistem di dalam cara mengamankan dan tidak semata-mata mengandalkan pada firewall untuk menghentikan ancaman keamanan. Organisasi memerlukan perencanaan backup untuk mengatasi kasus kegagalan firewall.

Tulisan ini mengandung informasi pengantar tentang definisi firewall dan yang utama adalah kebijakan dan administrasi firewall untuk membantu mereka yang bertanggung jawab pada keamanan jaringan.

DAFTAR ISI

Halaman Judul	i
Abstrak	ii
Daftar Isi	iii
Daftar Gambar	v
Daftar Tabel	vi
1. Pendahuluan	1
1.1 Latar Belakang	1
1.2 Tujuan dan Ruang Lingkup Tulisan	1
1.3 Definisi Firewall	1
2. Kebijakan Keamanan Firewall	2
2.1 Kebijakan Firewall	2
2.2 Penerapan <i>Ruleset</i> Firewall	4
2.3 Pengujian Kebijakan Firewall	7
2.4 Pendekatan Penerapan Firewall	7
2.5 Perawatan dan Manajemen Firewall	8
2.6 Keamanan Secara Fisik Terhadap Lingkungan Firewall	9
2.7 Pemeriksaan Ulang (Review) Secara Berkala Terhadap Kebijakan Keamanan Informasi	9
2.8 Sebuah Contoh Topologi dan Seperangkat Aturan (Ruleset)	10
3. Administrasi Firewall	13
3.1 Akses ke Platform Firewall	13
3.2 User Account	14
3.3 Membangun Platform Sistem Operasi Firewall	14
3.4 Strategi Penanganan Kegagalan (Failover) Firewall	16
3.5 Fungsionalitas Pencatatan (Logging) Firewall	16
3.6 Gangguan Keamanan	17
3.7 Cadangan (Backup) Firewall	18
3.8 Integritas Sistem	19
4. Perbaikan/Pembaharuan Kebijakan Firewall	19
5. Contoh Kebijakan Secara Umum	19
5.1 Kebijakan Untuk Lingkungan Dengan Resiko Rendah	19
5.2 Kebijakan Untuk Lingkungan Dengan Resiko Sedang	21
5.3 Kebijakan Untuk Lingkungan Dengan Resiko Tinggi	21
6. Contoh Kebijakan Layanan Khusus	22
6.1 Manajer	23
6.2 Teknisi	23

7. Kesimpulan	25
Ucapan Terima Kasih	25
Daftar Pustaka	26

DAFTAR GAMBAR

Gambar 1.1 Contoh Sebuah Firewall	2
Gambar 2.1 Contoh Lingkungan Firewall (Firewall Environment)	11

DAFTAR TABEL

Tabel 2.1 Matriks <i>Ruleset</i> Trafik Aplikasi Firewall	3
Tabel 2.2 Contoh Ruleset Untuk Boundary Router	12
Tabel 6.1 Urusan Manajerial	23
Tabel 6.2 Kebijakan Layanan Khusus	23
Tabel 6.3 Ringkasan Kebijakan Keamanan	25

1. Pendahuluan

1.1 Latar Belakang

Internet merupakan sebuah jaringan komputer yang sangat terbuka di dunia, konsekuensi yang harus di tanggung adalah tidak ada jaminan keamanan bagi jaringan yang terhubung ke Internet. Artinya jika operator jaringan tidak hati-hati dalam mengatur sistemnya, maka kemungkinan besar jaringan yang terhubung ke Internet akan dengan mudah dimasuki orang yang tidak diundang dari luar. Ini merupakan tugas dari administrator jaringan yang bersangkutan, untuk menekan resiko tersebut seminimal mungkin. Pemilihan strategi dan kecakapan administrator jaringan ini, akan sangat menentukan apakah suatu jaringan mudah ditembus atau tidak.

Firewall merupakan garis pertahanan yang terdepan dari suatu organisasi, maka organisasi seharusnya menerapkan pertahanan ini dengan sungguh-sungguh untuk strategi keamanan departemennya, terkait dengan di lapisan-lapisan mana saja firewall dan sistem keamanan lainnya digunakan diseluruh jaringan. Firewall merupakan alat untuk mengimplementasikan kebijakan keamanan (security policy), sedangkan kebijakan keamanan, dibuat berdasarkan pertimbangan antara fasilitas yang disediakan dengan implikasi keamanannya. Semakin ketat kebijakan keamanan, semakin kompleks konfigurasi layanan (service) informasi atau semakin sedikit fasilitas yang tersedia di jaringan. Sebaliknya, dengan semakin banyak fasilitas yang tersedia atau sedemikian sederhananya konfigurasi yang diterapkan, maka semakin mudah orang-orang yang berniat jahat dari luar masuk kedalam sistem (akibat langsung dari lemahnya kebijakan keamanan).

1.2 Tujuan dan Ruang Lingkup Tulisan

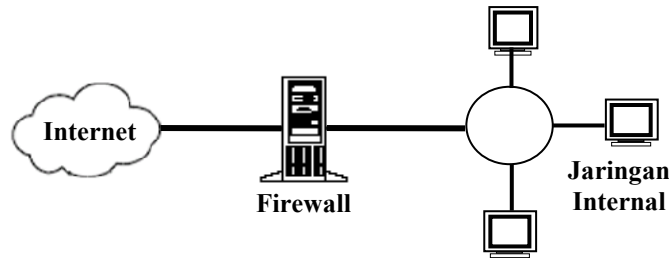
Tulisan ini mengandung informasi pengantar tentang firewall dan yang utama adalah kebijakan firewall untuk membantu mereka yang bertanggung jawab pada keamanan jaringan. Tulisan ini menunjukkan konsep-konsep yang berhubungan dengan kebijakan dan administrasi firewall. Tulisan ini tidak dimaksudkan untuk dijadikan suatu kerangka kerja yang wajib bagi firewall dan lingkungannya, tetapi tidak lebih untuk menyajikan pendekatan yang diusulkan kepada manajemen kebijakan keamanan firewall.

1.3 Definisi Firewall

Firewalls are designed to keep unwanted and unauthorized traffic from an unprotected network like the Internet out of a private network like your LAN or WAN, yet still allowing you and other users of your local network to access Internet services. (Marcus Goncalves, "Firewalls Complete")

A firewall is a network element that controls the traversal of packets across the boundaries of a secured network based on a specific security policy. A firewall security policy is a list of ordered rules that define the actions performed on network packets based on specific filtering conditions. (Ehab S. Al-Shaer and Hazem H. Hamed, "Modeling and Management of Firewall Policies")

Jadi dalam konteks keamanan jaringan, firewall didefinisikan sebagai suatu sistem yang dirancang untuk mencegah akses yang tidak diinginkan dari atau ke dalam suatu jaringan internal. Firewall bekerja dengan cara melacak dan mengendalikan jalannya data serta memutuskan aksi untuk melewatkan (pass), menjatuhkan (drop), menolak (reject), mengenkripsi atau melakukan pencatatan aktivitas (log) data. Firewall menjamin agar data sesuai dengan aturan (rule) yang terdapat didalam kebijakan keamanannya (security policy) yaitu seperangkat aturan yang telah didefinisikan di dalam keamanan jaringan internal. Firewall tidak dapat melindungi suatu jaringan dari aktivitas merusak yang dilakukan oleh para pemakai yang memiliki kewenangan.



Gambar 1.1 Contoh Sebuah Firewall

2. Kebijakan Keamanan Firewall

Menurut Ehab S. Al-Shaer and Hazem H. Hamed, kebijakan keamanan firewall adalah daftar aturan yang telah ditentukan untuk menetapkan tindakan yang harus dilakukan pada paket-paket jaringan berdasar pada kondisi-kondisi penyaringan khusus [5].

Kebijakan seharusnya menentukan segala sesuatu dari penggunaan yang dapat diterima untuk merespon skenario di mana suatu gangguan keamanan terjadi. Suatu kebijakan firewall berbeda dari kebijakan keamanan informasi, sejauh ini penggambaran sederhananya adalah bagaimana kebijakan keamanan informasi akan diterapkan oleh firewall dan dihubungkan dengan mekanisme keamanan.

Tanpa suatu kebijakan firewall, organisasi dan administrator seolah-olah terbang dalam kegelapan, sehingga firewall menjadi kompleks dan rumit untuk dikelola, dan gangguan keamanan dapat terjadi sehari-hari. Tanpa suatu kebijakan untuk memandu penerapan dan administrasi firewall, maka firewall itu sendiri dapat juga mendatangkan suatu masalah keamanan. Oleh karena itu, dirasa sangat penting untuk membuat kebijakan keamanan firewall sebelum memasang firewall pada sistem jaringan suatu organisasi.

Pada bagian ini akan diuraikan langkah-langkah untuk membuat suatu kebijakan keamanan firewall dan kemudian dilanjutkan dengan sebuah contoh. Ini berisi rekomendasi untuk pengujian dan pembaharuan (updating) kebijakan secara periodik.

2.1 Kebijakan Firewall

Suatu kebijakan firewall mendikte bagaimana firewall seharusnya menangani trafik aplikasi-aplikasi seperti web, email, atau telnet. Kebijakan itu seharusnya

menggambarkan bagaimana firewall dikelola dan diupdate. Sebelum suatu kebijakan firewall dapat dibuat, beberapa bentuk analisis resiko harus dilakukan pada aplikasi-aplikasi yang dibutuhkan dalam pencapaian misi organisasi. Hasil dari analisa ini meliputi sebuah daftar aplikasi-aplikasi dan bagaimana aplikasi-aplikasi tersebut akan diamankan. Proses untuk membuat daftar ini tidak dibahas secara terperinci disini, ini akan memerlukan pengetahuan tentang kerapuhan dari masing-masing aplikasi dan nilai keuntungan dari metoda-metoda yang digunakan untuk pengamanan aplikasi itu.

Analisis resiko menyangkut pengorganisasian infrastruktur teknologi informasi seharusnya dipertimbangkan berdasarkan pada evaluasi menyangkut unsur-unsur berikut: ancaman, kerapuhan, dan pembatasan jumlah pemakai (countermeasures) pada tempat tertentu untuk mengurangi kerapuhan dan dampak jika data penting dimanfaatkan bersama. Hasil akhirnya adalah untuk memahami dan mengevaluasi unsur-unsur ini sebelum penetapan suatu kebijakan firewall.

Hasil dari analisis resiko akan mendikte cara di mana sistem firewall menangani trafik aplikasi jaringan. Perincian dari aplikasi yang dapat melintasi suatu firewall dan dalam keadaan yang bagaimana aktivitas dapat berlangsung, seharusnya didokumentasikan dalam bentuk suatu matriks trafik aplikasi, seperti ditunjukkan pada Tabel 2.1.

Langkah-langkah yang ditempuh untuk membuat suatu kebijakan firewall adalah sebagai berikut:

- a. Identifikasi aplikasi jaringan yang diperlukan,
- b. Identifikasi kerapuhan yang berhubungan dengan aplikasi,
- c. Analisis nilai keuntungan dari metoda-metoda untuk pengamanan aplikasi,
- d. Pembuatan matriks trafik aplikasi yang menunjukkan metoda pengamanan, dan
- e. Pembuatan seperangkat aturan (ruleset) dasar firewall pada matriks trafik aplikasi.

**Tabel 2.1 Matriks *Ruleset* Trafik Aplikasi Firewall
(dari Wack John., Cutler Ken., and Pole Jamie.[1], hal 34)**

TCP/IP Application Service	Location	Internal Host Type	Internal Host Security Policy	Firewall Security Policy (Internal)	Firewall Security Policy (Eksternal)
Finger	Any	Unix	TCP Wrapper	Permit	Reject
Finger	Any	PC – TCP/IP	None	Permit	Permit
FTP	Any	Unix	No Anonymous; UserID/Password; Secure Shell (SSH)	Permit	Application Proxy With User Authentication
FTP	Any	PC – TCP/IP	Client Only; Anti Virus	Permit	Application Proxy With User Authentication

Tabel 2.1 Matriks *Ruleset* Trafik Aplikasi Firewall (lanjutan)
(dari Wack John., Cutler Ken., Pole Jamie.[1], hal 34)

TCP/IP Application Service	Location	Internal Host Type	Internal Host Security Policy	Firewall Security Policy (Internal)	Firewall Security Policy (Eksternal)
TFTP	Any	Unix Server with Diskless Clients Only	Secure Mode; Permit tftp to Limited Directories	Permit Only Local Domain; Reject Other	Reject
TFTP	Any	Unix; All Other	Disable	Reject	Reject
TFTP	Any	PC – TCP/IP	Disable	Reject	Reject
Telnet	Any	Unix	Secure Shell	Permit	Application Proxy With User Authentication
Telnet	Any	PC – TCP/IP	Client Only	Permit	Application Proxy With User Authentication
Telnet	Any	Router/ Firewall	2 Password Layer; Token Authentication	Token Authentication	Reject
NFS	Any	Unix	Limit Exports; Host/Groups (Granular Access)	Reject All, except by Written Authorization	Reject
NFS	Any	PC – TCP/IP	Client Only	Reject	Reject
NetBIOS over TCP/IP	Any	Windows NT/95/WFW	Limit Access to Shares	Permit Local Domain Only; Reject Others	Reject

2.2 Penerapan *Ruleset* Firewall

Kebanyakan platform-platform firewall menggunakan *ruleset* sebagai mekanisme mereka untuk menerapkan kontrol keamanan. Isi dari *ruleset* menentukan kemampuan yang nyata suatu firewall. Tergantung pada arsitektur platform firewall, *ruleset* firewall dapat berisi bermacam-macam informasi. Hampir semua *ruleset*, minimum akan berisi hal-hal berikut ini:

- a. Alamat sumber dari paket, yaitu alamat *layer* 3 dari sistem komputer atau perlengkapan paket jaringan berasal (suatu alamat IP seperti 192.168.1.1).
- b. Alamat tujuan dari paket, yaitu alamat *layer* 3 dari sistem komputer atau perlengkapan paket jaringan yang sedang dituju (misalnya 192.168.1.2).

- c. Jenis trafik, yaitu protokol jaringan khusus yang digunakan untuk komunikasi antara sistem atau perlengkapan sumber dan tujuan, seringkali berupa Ethernet pada *layer 2* dan IP pada *layer 3*.
- d. Mungkin beberapa karakteristik dari *layer 4* tentang komunikasi. Protokol seperti TCP, dan *port* sumber dan tujuan (seperti: TCP:80 untuk *port* tujuan *web server*, TCP:1320 untuk *port* sumber komputer pribadi yang mengakses server).
- e. Kadang-Kadang, menyinggung informasi tentang asal *interface* dari router dan *interface router* yang manakah dari paket yang dipersiapkan untuk penggunaan router dengan tiga atau lebih *interface* jaringan.
- f. Suatu tindakan, seperti menyangkal (*deny*) atau mengizinkan (*permit*) atau menjatuhkan paket dengan tidak memberikan suatu tanggapan kepada pengirim packet sebagai penolakan (*drop*).

Ruleset firewall dapat dibangun setelah melengkapi matrik trafik aplikasi. Tergantung pada firewall, ini mungkin dilaksanakan melalui suatu *interface web-style*; di dalam kasus *packet filter*, mungkin saja dilaksanakan dengan cara manual. *Ruleset* firewall seharusnya dibangun menjadi spesifik mungkin dengan memandang trafik jaringan yang mereka kontrol. *Ruleset* seharusnya dijaga agar sederhana mungkin, sehingga tidak secara disengaja memperlihatkan lubang keamanan di dalam firewall yang mungkin mengizinkan trafik yang tidak dikehendaki atau tidak diinginkan melewati firewall.

A firewall design policy is specific to the firewall. It defines the service-access policy implementation rules. You cannot design this policy without understanding the firewall capabilities and limitations, as well as the threats and vulnerabilities associated with TCP/IP. As mentioned earlier, firewalls usually do one of the following: - Permit any service unless it is expressly denied, - Deny any service unless it is expressly permitted. (Marcus Goncalves, "Firewalls Complete")

Dua pendekatan dalam perancangan firewall yang umum digunakan adalah sebagai berikut:

- segala sesuatu yang tidak secara eksplisit diizinkan berarti tidak diperbolehkan,
- segala sesuatu yang tidak secara eksplisit dilarang berarti diizinkan.

Kebijakan yang standar untuk firewall dalam penanganan trafik *inbound* seharusnya memblokir semua paket dan koneksi kecuali jika tipe trafik dan koneksi telah diizinkan secara khusus. Pendekatan ini lebih menjamin dibandingkan dengan pendekatan yang lain yang sering digunakan yaitu mengizinkan semua koneksi dan trafik secara *default* dan kemudian memblokir trafik dan koneksi yang khusus.

Ruleset firewall seharusnya selalu memblokir jenis-jenis trafik berikut:

- a. Trafik *inbound* dari sistem sumber tanpa diautentikasi (*non-authenticated*) dengan alamat tujuan dari sistem firewall itu sendiri. Paket jenis ini secara normal menggambarkan beberapa bentuk pemeriksaan atau serangan terhadap firewall. Satu pengecualian yang umum untuk aturan ini adalah jika firewall menerima kiriman email dari trafik *inbound* (SMTP pada port 25). Dalam kejadian ini,

- firewall harus mengizinkan koneksi inbound tersebut ke dirinya sendiri, tetapi hanya dibatasi pada port 25.
- b. Trafik inbound dengan suatu alamat sumber menunjukkan bahwa paket berasal dari jaringan di belakang firewall. Paket jenis ini kemungkinan besar menunjukkan beberapa bentuk usaha pemalsuan alamat sumber (source address spoofing atau IP spoofing).
 - c. Trafik inbound yang berisi trafik ICMP (Internet Control Message Protocol). Karena ICMP dapat digunakan untuk memetakan jaringan di belakang jenis firewall tertentu, ICMP seharusnya tidak dilewatkan dari Internet, atau dari jaringan eksternal manapun yang tidak dipercayai.
 - d. Trafik inbound atau outbound dari sebuah sistem yang menggunakan suatu alamat sumber yang tergolong dalam rentang alamat RFC 1918 yang disediakan untuk jaringan pribadi (private network).

Untuk tujuan referensi, RFC 1918 menyediakan rentang alamat jaringan pribadi berikut ini:

10.0.0.0 sampai 10.255.255.255 (Klas A atau “/8” dalam notasi CIDR)

172.16.0.0 sampai 172.31.255.255 (Klas B atau “/12” dalam notasi CIDR)

192.168.0.0 sampai 192.168.255.255 (Klas C atau “/16” dalam notasi CIDR)

Classless Inter-Domain Routing (CIDR) adalah sebuah pola pengalamatan IP yang menggantikan pola dasar pada klas A, B, dan C. Pengalamatan CIDR mengurangi ukuran dari tabel routing dan membuat pengalamatan IP lebih dapat digunakan (available) dalam organisasi. CIDR dibuat untuk membantu mengurangi masalah-masalah yang berhubungan dengan kehabisan alamat IP.

- Trafik inbound dengan alamat sumber ini secara umum menandai permulaan suatu serangan denial-of-service (DOS) menyertakan *TCP SYN flag*. Beberapa firewall memasukkan fungsi internal untuk melawan serangan ini, tetapi hanyalah jenis trafik jaringan tertentu yang seharusnya tetap diblokir dengan masukan dari ruleset.
- e. Trafik inbound dari sistem sumber tanpa diautentikasi yang mengandung trafik SNMP (Simple Network Management Protocol). Paket ini dapat merupakan indikator adanya penyusup yang sedang menyelidiki jaringan, tetapi ada beberapa pertimbangan sebuah organisasi mungkin menghendaki untuk mengizinkan trafik SNMP, dan ini seharusnya diblok jika intruder semakin banyak.
 - f. Trafik inbound yang berisi informasi *IP Source Routing*. *Source Routing* adalah suatu mekanisme yang mengizinkan sistem untuk menetapkan bagian rute trafik jaringan yang akan digunakan ketika perjalanan dari sistem sumber ke sistem tujuan. Dari sudut pandang keamanan, *source routing* mempunyai potensi mengizinkan penyerang untuk membuat suatu paket jaringan yang dapat menembus kontrol firewall. Di dalam jaringan modern, IP Source Routing jarang digunakan, dan aplikasi-aplikasi yang baik juga tidak umum menggunakannya di Internet.
 - g. Trafik jaringan inbound atau outbound berisi suatu alamat sumber atau tujuan dari 127.0.0.1 (localhost). Trafik seperti itu pada umumnya merupakan suatu bentuk serangan terhadap sistem firewall itu sendiri.

- h. Trafik jaringan inbound atau outbound berisi suatu alamat sumber atau tujuan 0.0.0.0. Beberapa sistem operasi menginterpretasikan alamat ini sebagai localhost yang lainnya atau sebagai alamat *broadcast*, dan paket ini dapat digunakan untuk tujuan menyerang.
- i. Trafik jaringan inbound atau outbound berisi alamat broadcast dengan satu arah (directed broadcast). *Directed broadcast* sering digunakan untuk memulai serangan perambatan *broadcast* seperti Smurf atau Distributed Denial Of Service (DDOS), yaitu serangan flooding untuk mendapatkan akses ke sistem yang digunakan untuk menyerang ke network lainnya. *Directed broadcast* mengizinkan satu sistem komputer untuk mengirim suatu pesan *broadcast* dengan suatu alamat sumber yang lain dari alamatnya atau dengan alamat sumber yang dipalsukan (spoofed). Sistem manapun yang merespon terhadap *directed broadcast*, kemudian akan mengirimkan tanggapannya kepada sistem yang dipalsukan alamatnya bukan kepada sumber pengirim pesan. Paket ini dapat digunakan untuk menciptakan serangan yang sangat besar pada trafik jaringan yang telah digunakan untuk melumpuhkan sebagian situs-situs di Internet.

2.3 Pengujian Kebijakan Firewall

Kebijakan diterapkan tiap hari tetapi kebijakan ini jarang ditinjau ulang dan diverifikasi. Untuk pendekatan semua organisasi seharusnya memeriksa dan memverifikasi firewall dan kebijakan keamanan sedikitnya triwulan sekali.

Dalam banyak kasus, kebijakan firewall dapat diverifikasi menggunakan salah satu dari dua metodologi. **Metodologi yang pertama**, dan betul-betul yang paling mudah, akan menghasilkan *hardcopies* dari konfigurasi firewall dan membandingkan *hardcopies* dengan konfigurasi yang diharapkan berdasarkan definisi kebijakan. Semua organisasi, minimum perlu menggunakan jenis ini untuk melakukan pemeriksaan ulang.

Metodologi yang kedua melibatkan pengujian konfigurasi yang nyata. Di dalam metodologi ini, organisasi menggunakan peralatan yang menilai konfigurasi suatu alat dengan percobaan untuk melaksanakan operasi yang seharusnya dilarang.

Jika penggunaan metodologi yang kedua jadi lebih kaku/tidak fleksibel, maka kedua metodologi tersebut seharusnya digunakan. Tujuannya adalah untuk meyakinkan bahwa firewall (seperti halnya peralatan lain yang terkait dengan keamanan) dikonfigurasi secara tepat sebagaimana seharusnya, berdasarkan atas kebijakan yang telah ditulis. Ini juga penting bahwa sistem firewall itu sendiri diuji menggunakan peralatan-peralatan penilaian keamanan (security assessment tools). Tool ini seharusnya digunakan untuk menguji sistem operasi yang mendasari firewall, seperti halnya perangkat lunak firewall dan implementasinya. Tool penilaian ini dapat diperoleh di domain publik atau komersil (atau kedua-duanya).

2.4 Pendekatan Penerapan Firewall

Ketika menerapkan firewall dan kebijakan firewall, organisasi harus memutuskan apakah menerapkan firewall sebagai suatu peralatan/hardware (appliance) atau menerapkan firewall di atas sistem operasi komersil (on top of a commercial

operating system). Jika keputusan ini sebagian besar ditentukan oleh kebutuhan organisasi, maka hal-hal berikut ini harus dipertimbangkan:

- a. Pada prinsipnya, firewall berbasis peralatan (appliance-based firewall) akan menjadi lebih menjamin dibandingkan yang diterapkan di atas sistem operasi komersil (on top of a commercial operating system). Firewall berbasis peralatan tidak mempunyai sifat kerapuhan (vulnerabilities) keamanan dihubungkan dengan dasar sistem operasinya. Firewall berbasis peralatan biasanya menggunakan teknologi ASIC (Application-Specific Integrated Circuit), dengan perangkat lunak firewall yang nyata dan kini sebagai dasar yang kokoh (firmware) teknologi ASICS. Firewall ini juga cenderung menjadi lebih cepat dari firewall yang diterapkan di atas sistem operasi komersil (on top of a commercial operating system).
- b. Keuntungan dalam menerapkan firewall di atas sistem operasi komersil (on top of a commercial operating system) adalah **skalabilitas**. Jika suatu lingkungan memerlukan performance untuk ditingkatkan, maka organisasi dapat membeli suatu sistem yang lebih besar dan di atasnya untuk menjalankan perangkat lunak firewall. Kebanyakan firewall berbasis peralatan tidak menawarkan fleksibilitas atau skalabilitas.
- c. Kerugian yang terbesar dalam menerapkan firewall di atas sistem operasi komersil (on top of a commercial operating system) adalah potensial mendatangkan sifat kerapuhan yang mungkin mengikis keamanan platform firewall itu sendiri. Dalam banyak keadaan firewall komersil dilanggar, dimana pelanggaran itu terjadi karena dimudahkan oleh sifat kerapuhan berdasarkan sistem operasinya. Banyak keahlian diperlukan dalam pengamanan berdasarkan sistem operasi dan pemeliharannya. Keputusan ini harus diambil berdasarkan pada biaya relatif, seperti halnya perkiraan kebutuhan di masa depan.

2.5 Perawatan dan Manajemen Firewall

Platform-platform firewall komersil menggunakan salah satu dari dua mekanisme konfigurasi dan pemeliharaan yang terus-menerus. Dua mekanisme konfigurasi firewall adalah sebagai berikut:

- a. Konfigurasi command-line interface (CLI), yang mana memungkinkan administrator untuk mengkonfigurasi firewall dengan mengetikkan perintah-perintah ke dalam command prompt. Teknik ini rentan kesalahan (error-prone) terkait dengan kesalahan pengetikan. Keuntungan yang utama dari bentuk command-line adalah bahwa keterampilan dan pengalaman administrator dapat mengkonfigurasi firewall dan bereaksi pada keadaan darurat akan lebih cepat dibandingkan dengan graphic interface.
- b. Konfigurasi firewall melalui Graphic User Interface (GUI). Graphic interface lebih sederhana dan memungkinkan administrator yang baru dapat mengkonfigurasi sistem lebih cepat dalam waktu yang tidak lama. Mekanisme ini yang paling umum digunakan, karena kemudahannya dimana dengan graphic interface proses terjadinya konfigurasi (configuration granularity) lebih interaktif. Pada banyak platform firewall modern, ada pilihan yang tersedia di dalam firewall yang tidak dapat dikonfigurasi menggunakan graphic interface. Dalam keadaan seperti ini, maka interface command-line harus digunakan. Untuk pilihan yang

lain, perhatian khusus harus diambil untuk memastikan bahwa semua trafik jaringan yang berhubungan dengan manajemen sistem firewall dijamin aman. Untuk interface berbasis web, keamanan ini akan mungkin diterapkan melalui enkripsi Secure Sockets Layer (SSL) dengan userID dan password. Untuk interface *non-web*, enkripsi pada layer transport pada umumnya diterapkan. Hal ini seharusnya diperhatikan pada kebijakan bahwa semua manajemen firewall berfungsi menjamin hubungan harus selalu menggunakan autentikasi dan enkripsi.

2.6 Keamanan Secara Fisik Terhadap Lingkungan Firewall

Keamanan secara fisik untuk lingkungan firewall kadang-kadang kurang mendapat perhatian. Jika firewall ditempatkan pada daerah yang tidak aman, maka firewall rentan untuk dirusak oleh para penyusup dan resiko yang lebih tinggi terjadi kerusakan secara tiba-tiba. Oleh karena itu, peralatan firewall seharusnya dijamin keamanannya dibalik pintu yang terkunci. Beberapa organisasi menempatkan lingkungan firewall mereka yang diamankan dengan fasilitas komputer, lengkap dengan penjagaan dan alarm keamanan secara fisik yang lain.

Faktor yang lain di dalam keamanan fisik adalah kualitas kelistrikan, koneksi jaringan, dan kontrol lingkungan. Fasilitas firewall seharusnya telah dibuatkan cadangan sumber daya (backup power supplies) dan terhadap kemungkinan koneksi yang berlebih-lebihan ke jaringan eksternal. Beberapa bentuk dari pengkondisian udara (air conditioning) dan penyaringan udara (air filtration) pada umumnya juga dibutuhkan. Pada akhirnya, fasilitas firewall seharusnya dilindungi secara layak dari bencana alam seperti api dan banjir. Sistem pemadam api adalah peralatan standar yang umum di dalam fasilitas komputisasi.

2.7 Pemeriksaan Ulang (Review) Secara Berkala Terhadap Kebijakan Keamanan Informasi

Seperti berhadapan dengan beberapa tipe kebijakan, kebijakan keamanan informasi harus periksa ulang secara berkala dalam rangka untuk memastikan ketelitian dan ketepatan waktu. Berdasarkan pengalaman bahwa kebijakan keamanan informasi itu seharusnya diperiksa dan diperbaharui sedikitnya dua kali setiap tahun. Pengalaman terbaik berikutnya menunjukkan bahwa beberapa kejadian dapat mencetuskan suatu pemeriksaan ulang kebijakan keamanan informasi. Pemicu ini mencakup kejadian seperti implementasi dari organisasi besar yang memperhitungkan perubahan lingkungan dan banyak kejadian yang berbahaya terhadap keamanan informasi utama.

Instalasi firewall seperti halnya sistem dan sumber daya lain harus diperiksa secara teratur dan periodik. Dalam beberapa kasus, pemeriksaan ulang secara berkala ini dapat diselenggarakan secara tertulis dengan susunan hardcopy pemeriksaan ulang yang disediakan oleh staff sistem administrasi. Di dalam kasus lain, pemeriksaan ulang secara berkala seharusnya mencakup hasil secara nyata penilaian pemeriksaan (audit) dan kerapuhan (vulnerability) dari backup infrastruktur komponen, sistem komputer, dan berbagai jenis sumber daya yang lain. Ini sama pentingnya bahwa organisasi-organisasi dengan koneksi Internet supaya menggunakan alat pemeriksa

tambahan untuk memastikan keseluruhan keamanan dari lingkungannya. Pemeriksaan atau penilaian tambahan ini secara khusus dikenal sebagai **analisis penetrasi**. Analisis penetrasi seharusnya dipakai sebagai tambahan dan bukan sebagai ganti suatu program pemeriksa konvensional.

Menurut Wack John, Cutler Ken. Dan Pole Jamie, analisis penetrasi ada dua macam yaitu analisis penetrasi *seeded* (penetration analysis seeded) dan analisis penetrasi *blind* (penetration analysis blind). Penggunaan analisis penetrasi *seeded* atau analisis penetrasi *blind* dalam pemeriksaan kebijakan keamanan tergantung pada keadaannya.

a. Analisis penetrasi *seeded*

Analisis penetrasi *seeded* adalah suatu analisa penetrasi di mana organisasi atau tim yang melaksanakan penilaian telah dilengkapi dengan perincian jaringan dan sistem informasi sebelum pelaksanaan penilaian. Oleh karena itu, penilaian jenis ini tidak memerlukan teknik penemuan terkini pada bagian kesatuan (entities) pelaksanaan penilaian. Penilaian jenis ini secara khusus diselenggarakan oleh entitas yang kurang ahli untuk melaksanakan penetrasi *blind*. Penetrasi *seeded* juga mungkin digunakan ketika suatu organisasi ingin membatasi lingkup dari suatu analisis ke lingkungan atau perangkat sistem yang ditentukan.

b. Analisis penetrasi *blind*

Analisis penetrasi *blind* adalah suatu penilaian di mana pertukaran informasi minimal terjadi sebelum permulaan penilaian. Oleh karena itu, tergantung pada organisasi atau tim yang melaksanakan penilaian untuk memperoleh semua informasi yang relevan untuk melaksanakan penilaian, dalam batas waktu penilaian. Penemuan awal dalam usaha membuat analisa penetrasi *blind* jauh lebih sulit dibanding analisis penetrasi *seeded*. Tetapi, hasil penetrasi *blind* jauh lebih realistis dan secara dramatis lebih menunjukkan tingkat resiko yang nyata dihubungkan dengan konektivitas global.

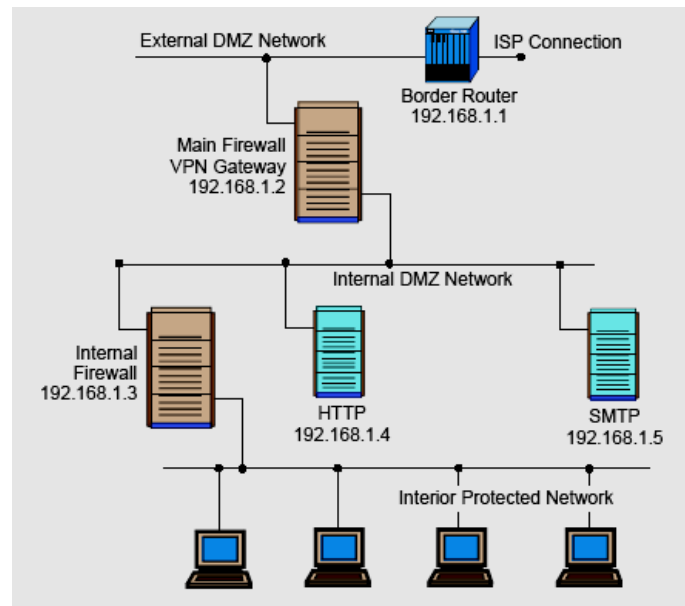
2.8 Sebuah Contoh Topologi dan Seperangkat Aturan (Ruleset)

Bagian ini memberikan suatu contoh topologi firewall dan dasar-dasar *ruleset* dengan syarat-syarat sebagai berikut:

- a. Semua trafik jaringan internal diizinkan mengakses keluar (outbound) ke semua lokasi melalui firewall dan boundary router,
- b. Inbound SMTP (email) diizinkan ke firewall utama (main firewall) di mana ini dilewatkan ke server proxy dan kemudian ke email klien internal,
- c. Outbound HTTP (web) trafik diizinkan ke firewall internal (internal firewall) di mana ini dilewatkan ke suatu server proxy HTTP, dan kemudian ke eksternal websites,
- d. *Inbound connections* dari sistem jarak jauh diizinkan ke port VPN firewall (*firewall's VPN port*) di mana ini dilewatkan ke sistem internal, dan
- e. Semua trafik inbound yang lain diblokir.

Pada kenyataannya daftar ini akan menjadi lebih panjang dan lebih khusus. Di dalam contoh ini, aplikasi proxy HTTP dapat menyembunyikan halaman web untuk pertimbangan performance dan dapat juga memfilter content aktif seperti Java, Javascript, atau ActiveX®, mengendalikan, dan mencatat koneksi outbound. Aplikasi

proxy SMTP akan menguji semua *email attachment* atau deretan baris berisi virus dan mengkarantina kode yang terkena infeksi virus jika diperlukan.



Gambar 2.1 Contoh Lingkungan Firewall (Firewall Environment)

Lingkungan firewall untuk jaringan ini ditunjukkan pada Gambar 2.1. Suatu jaringan *external De-Militarized Zone* (DMZ) akan dihubungkan ke Internet melalui layanan packet filter seperti boundary router. Firewall utama akan menggunakan port VPN untuk para pemakai jarak jauh (remote) dan para pemakai seperti ini akan memerlukan perangkat lunak VPN klien untuk terhubung ke firewall. Pertama, email inbound akan menghubungkan ke firewall utama, dan akan melewatinya menuju ke server aplikasi proxy yang lokasinya di DMZ internal. Trafik web *outbound* akan menghubungkan ke firewall internal, dan akan melewatinya ke lokasi proxy aplikasi HTTP pada DMZ internal.

Suatu ruleset untuk *boundary router* dapat dilihat pada Tabel 2.2 berikut ini. Ruleset ini berisi aturan bloking standard dan sangat disederhanakan, dimana untuk contoh secara nyata tentunya akan melibatkan persetujuan khusus dari vendor dan perincian lainnya.

Dari Tabel 2.2 dapat diartikan hal-hal sebagai berikut:

- **Aturan 1** mengizinkan pengembalian paket dari koneksi yang dibuat untuk mengembalikan ke sistem sumber (catatan bahwa jika boundary router adalah hybrid stateful firewall, aturan 1 tidak akan diperlukan).
- **Aturan 3** mengizinkan koneksi inbound untuk port VPN firewall utama.

- **Aturan 4 dan 5** menceritakan bahwa router melewati trafik SMTP dan HTTP ke firewall utama, kemudian akan mengirimkan trafik tersebut ke aplikasi proxy masing-masing.
- **Aturan 8** menolak semua koneksi inbound yang lainnya ke firewall utama (atau beberapa sistem lain yang mungkin berada pada *external DMZ*).

Tabel 2.2 Contoh Ruleset Untuk Boundary Router

	Alamat Sumber	Port Sumber	Alamat Tujuan	Port Tujuan	Aksi	Deskripsi
1	Sembarang	Sembarang	192.168.1.0	> 1023	Diizinkan	Aturan untuk mengizinkan kembali koneksi TCP ke internal subnet
2	192.168.1.1	Sembarang	Sembarang	Sembarang	Ditolak	Mencegah sistem firewall itu sendiri dari koneksi langsung ke mana saja
3	Sembarang	Sembarang	192.168.1.2	VPN	Diizinkan	Mengizinkan pemakai dari luar untuk terhubung ke server VPN
4	Sembarang	Sembarang	192.168.1.2	SMTP	Diizinkan	Mengizinkan pemakai dari luar untuk mengirim email ke proxy
5	Sembarang	Sembarang	192.168.1.2	HTTP	Diizinkan	Mengirim inbound HTTP ke proxy
6	Sembarang	Sembarang	192.168.1.1	Sembarang	Ditolak	Mencegah pemakai luar dari akses secara langsung ke sistem firewall
7	192.168.1.0	Sembarang	Sembarang	Sembarang	Diizinkan	Pemakai dari dalam dapat mengakses server eksternal
8	Sembarang	Sembarang	Sembarang	Sembarang	Ditolak	Mencakup semua aturan, segala sesuatu yang sebelumnya tidak diizinkan maka secara jelas ditolak

Firewall utama dan firewall internal akan menggunakan teknologi *stateful inspection* dan dapat juga mencakup kemampuan aplikasi proxy, walaupun ini tidaklah digunakan di dalam contoh ini. Firewall utama akan melaksanakan aksi-aksi berikut ini:

- Mengizinkan para pemakai eksternal untuk melakukan koneksi ke server VPN, di mana mereka akan dibuktikan keasliannya (be authenticated).
- Secara internal batas koneksi SMTP dan data ke server proxy, di mana data dapat difilter dan dikirimkan ke sistem tujuan.

- c. *Route* trafik HTTP outbound dari proxy HTTP dan *route* trafik SMTP outbound dari proxy SMTP.
- d. Kemudian menolak trafik outbound HTTP dan SMTP yang lain.
- e. Kemudian mengizinkan trafik outbound yang lain.

Firewall internal akan menerima trafik inbound hanya dari firewall utama dan aplikasi proxy. Selanjutnya, firewall internal akan menerima trafik SMTP dan HTTP hanya dari proxy saja, bukan firewall utama. Dan pada akhirnya, firewall internal akan mengizinkan semua koneksi outbound dari sistem internal.

Untuk membuat contoh ini supaya lebih dapat digunakan untuk lingkungan dengan keamanan lebih baik, beberapa materi dapat diubah, mencakup hal-hal sebagai berikut:

- a. Internal dan eksternal server DNS dapat ditambahkan untuk menyembunyikan sistem internal.
- b. Port Address Translation (PAT) dan Network Address Translation (NAT) dapat digunakan selanjutnya untuk menyembunyikan sistem-sistem internal.
- c. Trafik outbound dari sistem internal dapat difilter, termasuk trafik yang mungkin untuk site yang diragukan atau untuk layanan yang legalitasnya diragukan atau karena kebijakan manajemen.
- d. Multi firewall dapat digunakan untuk menyelamatkan kegagalan performance (unjuk kerja).

3. Administrasi Firewall

Firewall memiliki peran yang sangat penting pada keamanan jaringan, maka firewall harus dikelola dan dirawat dengan baik oleh seseorang. Kebijakan keamanan menentukan siapa yang bertanggung jawab untuk mengelola firewall.

Guttman Barbara and Bagwill Robert [4] mengemukakan bahwa dua administrator firewall (utama dan sekunder) akan ditunjuk oleh Pimpinan Petugas Keamanan Informasi (atau manajer) dan akan bertanggung jawab untuk memelihara firewall. pengurus Administrator yang utama akan membuat perubahan ke firewall dan administrator yang sekunder hanya akan melakukannya jika administrator utama berhalangan hadir, sehingga tidak secara bersama-sama atau berlawanan mengakses firewall. Masing-masing administrator firewall akan menyediakan nomor telepon rumah mereka, nomor pager, nomor telepon selular, nomor atau kode lainnya di mana mereka dapat dihubungi ketika diperlukan.

Dua orang berpengalaman biasanya direkomendasikan untuk mengadministrasi harian firewall. Cara ini diyakini mampu untuk menjalankan fungsi administratif firewall. Oleh karena itu, sangat diperlukan informasi tentang masing-masing administrator firewall dan dicatat sedemikian sehingga ia dapat dihubungi jika terjadi suatu masalah.

3.1 Akses ke Platform Firewall

Firewalls are the first line of defense visible to an attacker. By design, firewalls are generally difficult to attack directly, causing attackers to often target the administrative accounts on a firewall. The username/password of

administrative accounts must be strongly protected. (Guttman Barbara and Bagwill Robert, "Implementing Internet Firewall Security Policy")

Metoda yang paling umum untuk menerobos ke dalam firewall adalah untuk mengambil keuntungan dari sumber daya yang disediakan untuk manajemen firewall jarak jauh (remote). Kekhususan ini mencakup penggalian akses ke konsol sistem operasi atau akses antar muka (interface) manajemen grafis. Karena alasan ini, akses ke konsol sistem operasi dan beberapa interface manajemen grafis harus dikontrol secara hati-hati.

Metoda yang paling populer untuk pengendalian akses adalah melalui penggunaan enkripsi, autentikasi pemakai yang kuat (strong user authentication) dan pembatasan akses dengan alamat IP. Kebanyakan interface grafis untuk manajemen firewall menyertakan beberapa bentuk enkripsi internal, yang biasanya tidak dapat diamankan menggunakan enkripsi SSL. SSL pada umumnya dipilih untuk interface manajemen grafis yang mengandalkan pada HTTP untuk interface presentasi. Jika tidak ada enkripsi internal maupun SSL, maka terdapat solusi lain seperti Secure Shell (SSH) yang pada umumnya sesuai.

Autentikasi pemakai mempunyai beberapa pilihan: Pertama, kebanyakan interface manajemen firewall menyertakan beberapa format autentikasi internal. Dalam banyak kasus, melibatkan *userID* perorangan dan *password* yang harus diisi untuk memperoleh akses ke interface.

3.2 User Account

Firewall seharusnya tidak digunakan sebagai server umum. Account pemakai (user account) pada firewall seharusnya hanya administrator firewall itu dan backup administrator. Sebagai tambahan, hanya administrator ini perlu mempunyai hak istimewa (privilege) untuk melakukan pembaharuan sistem atau perangkat lunak sistem lainnya.

Hanya administrator firewall dan backup administrator akan diberi user account pada organisasi firewall. Beberapa modifikasi perangkat lunak sistem firewall harus dilakukan oleh administrator firewall atau backup administrator dan memerlukan persetujuan Manajer Layanan Jaringan.

3.3 Membangun Platform Sistem Operasi Firewall

Faktor pokok yang lain didalam kesuksesan manajemen lingkungan firewall adalah konsistensi platform. Platform firewall seharusnya diterapkan pada sistem yang berisi sistem operasi yang dibangun dan dijadikan handal sebagai aplikasi-aplikasi keamanan, seperti *bastion host*. Firewall seharusnya tidak pernah ditempatkan pada sistem yang dibangun dengan semua kemungkinan pilihan instalasi.

Membangun sistem operasi firewall seharusnya berdasarkan pada feature minimal. Semua feature sistem operasi yang tidak dibutuhkan seharusnya dihilangkan sebelum firewall diterapkan, terutama compiler. Semua sistem operasi tambahan seharusnya diterapkan sebelum beberapa instalasi komponen firewall.

Membangun sistem operasi seharusnya tidak mempercayakan sepenuhnya pada modifikasi yang dibuat oleh proses instalasi firewall. Program instalasi firewall mengandalkan pada pendekatan kesamaan umum yang paling dasar dimana paket atau modul software yang tidak ada hubungannya boleh tidak dihilangkan atau tidak dimatikan (disable) selama proses instalasi.

Pembekuan prosedur digunakan selama proses instalasi seharusnya disesuaikan secara khusus dengan sistem operasi yang dibekukan. Beberapa hal yang perlu diperhatikan adalah sebagai berikut:

- a. Protokol jaringan manapun yang tidak digunakan seharusnya dihilangkan dari sistem operasi firewall yang dibangun. Protokol jaringan yang tidak digunakan berpotensi digunakan untuk melewati (bypass) atau merusak lingkungan firewall. Pada akhirnya, dengan mematikan (disable) protokol yang tidak digunakan, maka dipastikan bahwa serangan pada firewall yang memanfaatkan teknik enkapsulasi protokol tidak akan efektif.
- b. Service atau aplikasi jaringan manapun yang tidak digunakan seharusnya dihilangkan atau dimatikan. Aplikasi yang tidak digunakan sering dimanfaatkan untuk menyerang firewall sebab banyak administrator yang lalai menerapkan pembatasan standar akses kontrol firewall. Sebagai tambahan, service jaringan dan aplikasi yang tidak digunakan kemungkinan besar berjalan menggunakan konfigurasi standar yang pada umumnya sangat sedikit mengamankan dibanding konfigurasi aplikasi atau service produk yang siap pakai.
- c. Account sistem atau pemakai manapun yang tidak digunakan seharusnya dibuang atau dimatikan. Pada kenyataannya adalah adanya kekhususan sistem operasi, karena semua sistem operasi berbeda-beda syarat-syarat account yang ditampilkan dengan standar seperti halnya bagaimana account dapat dihilangkan atau dimatikan.
- d. Penerapan semua tambahan sistem operasi yang relevan adalah juga penting. Karena tambahan dan perbaikan secara normal dikeluarkan untuk hal yang berhubungan dengan keamanan alamat, maka tambahan dan perbaikan ini seharusnya diintegrasikan ke dalam proses pembangunan firewall. Tambahan seharusnya selalu diuji pada sistem non-production sebelumnya untuk dipublikasikan ke beberapa sistem produksi. Pengujian pra-publikasi seharusnya meliputi beberapa hal khusus, sebagai berikut:
 - Suatu perubahan menyangkut sistem waktu (menit demi menit dan jam demi jam).
 - Suatu perubahan menyangkut sistem tanggal (kedua-duanya alami, dan manual).
 - Penambahan dan penghapusan dari sistem sesuai pemakai dan kelompok.
 - Startup dan shutdown sistem operasi.
 - Startup dan shutdown perangkat lunak firewall itu sendiri.
 - Sistem backups, jika sesuai.
- e. Interface jaringan fisik yang tidak digunakan seharusnya dimatikan atau dihilangkan dari server.

3.4 Strategi Penanganan Kegagalan (Failover) Firewall

Ada banyak pilihan untuk menyediakan layanan redundansi dan penanganan kegagalan (failover) untuk lingkungan firewall. Pilihan ini mencakup dimanapun penggunaan switch jaringan yang didesain khusus untuk “mekanisme denyut jantung (heartbeat)” yang biasanya digunakan untuk menilai dan mengkoordinir ketersediaan dari firewall utama sehingga backup dapat mengambil alih jika terjadi kegagalan. Switch jaringan yang menyediakan kemampuan *load balancing* dan *failover* menjadi yang paling baru dan terdepan dalam menyediakan solusi secara langsung.

Di dalam konfigurasi failover, switch menangkap respon-respon yang dihasilkan oleh firewall dan menggeser semua trafik ke firewall backup seandainya ada suatu kegagalan pada *production firewall*. Keuntungan utama jenis solusi ini adalah bahwa switch menyamakan kedua firewall dengan alamat MAC yang sama (Media Access Control OSI Lapisan 2).

Solusi yang berbasis *heartbeat* secara khusus melibatkan suatu back-end atau interface jaringan biasanya memberitahu sistem backup jika terjadi kegagalan sistem utama. Sistem ini dibuat dengan teknologi yang dapat diandalkan untuk menangani failover. Kelemahan utama pada pendekatan ini adalah bahwa ditentukannya bagian yang melewati *production firewall* hampir selalu hilang di dalam transisi dari *production firewall* ke firewall backup. Keputusan untuk menerapkan metoda failover biasanya tergantung pada biayanya, dimana solusi jaringan yang berbasis switch failover biasanya lebih mahal dibanding sistem berbasis heartbeat.

3.5 Fungsionalitas Pencatatan (Logging) Firewall

Kebanyakan firewalls menyediakan cakupan luas tentang kemampuan untuk pencatatan trafic dan kejadian-kejadian pada jaringan. Beberapa kejadian yang relevan dengan keamanan yang harus direkam pada firewall adalah: perangkat keras dan kesalahan media disk, aktivitas login/logout, waktu koneksi, penggunaan hak istimewa administrator sistem, trafik email inbound dan outbound, usaha menghubungi jaringan TCP, tipe trafik proxy inbound dan outbound.

Menurut Wack John., Cutler Ken., Pole Jamie [1] Hampir semua firewall sistem menyediakan fungsi pengurutan logging. Keluaran logging dari firewall proxy application gateway cenderung untuk menjadi jauh lebih sempurna dibanding keluaran serupa dari firewall dengan teknologi packet filter atau stateful inspection packet filter. Ini disebabkan oleh firewall proxy application gateway memperhatikan porsi yang jauh lebih besar dari OSI model.

Secara umum dapat diterima untuk kemampuan logging pada aplikasi syslog UNIX. Syslog UNIX menyediakan logging terpusat, seperti halnya berbagai pilihan untuk menguji dan menguraikan catatan-catatan (logs). Program logging ini atau daemon tersedia untuk hampir semua sistem operasi utama, termasuk Windows® NT, Windows® 2000 dan XP, dan semua UNIX dan jenis-jenis Linux. Sekali satu set logs firewall telah diberikan kepada server logging terpusat, beberapa paket software

mampu untuk menguji logs itu. Lingkungan logging berbasis syslog dapat juga menyediakan masukan ke pendeteksian penyusupan dan paket analisa forensic. Firewall yang tidak mendukung interface syslog apapun, harus menggunakan kemampuan logging internal yang dimiliki. Tergantung pada platform firewall, ada banyak tool pendukung untuk perbaikan dan penguraian logging.

3.6 Gangguan Keamanan

Tidak ada jawaban sederhana bagi pertanyaan: Apakah gangguan keamanan itu? Menurut Wack John., Cutler Ken., Pole Jamie [1], gangguan keamanan adalah kejadian apapun di mana akses individu tidak syah atau usaha untuk mengakses sistem komputer atau sumber daya yang mana mereka tidak mempunyai hak.

Kekejaman dari gangguan dapat bervariasi dan ini tergantung kepada para organisasi atau individu untuk menentukan secara pasti definisi dari gangguan keamanan. Berdasarkan tingkat kekejaman maka gangguan keamanan diklasifikasikan menjadi tiga, yaitu:

- a. Pada tingkat kekejaman rendah, gangguan keamanan kecil dapat terdiri dari pemeriksaan jaringan atau sistem yang bertujuan untuk memetakan jaringan organisasi. Jika orang yang tidak syah melaksanakan pemeriksaan ini, maka dapat dikatakan gangguan keamanan telah berlangsung. Dalam kaitan dengan kegiatan pemeriksaan sistem ini, kebanyakan organisasi tidak menetapkan bahwa kegiatan pemeriksaan ini sebagai gangguan keamanan.
- b. Pada tingkat kekejaman menengah, gangguan keamanan dapat dalam bentuk usaha aktif untuk memperoleh akses tidak syah ke suatu sistem komputer.
- c. Pada tingkat kekejaman tinggi, yaitu jika usaha mereka sukses maka akan diperoleh akses tidak syah ke suatu sistem atau sumber daya. Kejadian ini mempunyai potensi untuk menyela penggunaan sumber daya yang ada dan bahkan digunakan dengan sepenuhnya. Ketika dikenali identitas mereka, maka beberapa organisasi akan berusaha untuk menuntut pelaku kejahatan. Dalam semua kasus, gangguan seharusnya dicatat dan dilaporkan. Misalnya ke suatu badan yang berwenang untuk menangani kejahatan komputer seperti Federal Computer Incident Response Center (FedCIRC) dengan alamat situsnya <http://www.fedcirc.gov>.

Dalam penanganan gangguan keamanan, firewall mempunyai peranan penting untuk membuat laporan dan pencatatan. Menurut Guttman Barbara and Bagwill Robert [4], pelaporan gangguan keamanan adalah proses di mana keganjilan tertentu dilaporkan atau dicatat pada firewall. Suatu kebijakan diperlukan untuk menentukan seperti apa macam laporan untuk dicatat dan apa yang akan dilakukan dengan laporan yang yang dihasilkan. Kebijakan berikut adalah sesuai untuk semua lingkungan resiko:

- Firewall akan dikonfigurasi untuk mencatat semua laporan berbasis harian, mingguan, dan bulanan, sehingga aktivitas jaringan dapat dianalisis ketika diperlukan.
- Catatan firewall harus diuji berbasis mingguan untuk menentukan jika serangan telah dideteksi.

- Administrator firewall akan diberitahu pada setiap waktu tentang segala tanda bahaya (alarm) keamanan melalui email, pager, atau alat-alat lain, sehingga administrator dapat dengan segera merespon alarm tersebut.
- Firewall akan menolak segala macam *tool* pemeriksaan (probing) atau pengamatan (scanning) yang diarahkan ke firewall, sehingga informasi yang sedang dilindungi tidaklah keluar oleh firewall. Di dalam kasus yang serupa, firewall akan memblokir semua tipe perangkat lunak yang dikenal untuk merepresentasikan ancaman keamanan jaringan (seperti Aktif X dan Java) untuk lebih baik memperketat keamanan jaringan.

Pada intinya, definisi dari gangguan keamanan akan ditentukan oleh kebijakan keamanan suatu organisasi itu sendiri. Selama terjadi gangguan keamanan, administrator mempunyai beberapa tanggung jawab. Idealnya, perbaikan akses ke sistem dapat berlangsung tanpa berdampak pada hilangnya bukti forensik yang diperlukan untuk menuntut orang yang dituduh sebagai pelaku. Secara umum, tanggung jawab administrator akan didikte oleh beberapa entitas manajemen. Tanggung jawab ini seharusnya diuraikan terlebih dahulu sebelum sistem dibangun.

Firewall dapat menyediakan pandangan penting dalam konteks gangguan keamanan atau kejadian yang berhubungan (*event correlation*) dengan keamanan. Konsep *event correlation* melibatkan fakta bahwa firewall berada dalam posisi yang khusus pada hampir semua serangan yang berbasis jaringan dimana akses harus melewati firewall dalam rangka memasuki suatu jaringan. Ini menempatkan firewall di dalam posisi yang khusus dari kelemahan yang dimilikinya atas aktivitas tidak syah. Karena alasan ini, semua firewall dan sistem logging lainnya, seperti sistem deteksi penyusupan (IDS), seharusnya memiliki sinkronisasi waktu. Mekanisme yang paling umum untuk sinkronisasi waktu adalah protokol waktu jaringan atau Network Time Protocol (NTP). Ketika semua sistem yang mempunyai kelemahan telah disinkronkan waktunya, sehingga memungkinkan sistem untuk merekonstruksi tahap-tahap suatu gangguan keamanan.

3.7 Cadangan (Backup) Firewall

Melakukan dan memelihara backup adalah kunci utama bagi kebijakan administrasi firewall manapun. Semua firewall seharusnya diutamakan supaya tiada hari tanpa backup. Semua firewall seharusnya dibackup dengan segera sebelum diluncurkan. Sebagai prinsip umum, semua backup firewall seharusnya backup secara penuh. Untuk mendukung perbaikan (*recover*) setelah kegagalan atau bencana alam, suatu firewall seperti jaringan host lainnya sudahkah mempunyai beberapa kebijakan yang didefinisikan sistem backup. File-file data seperti file konfigurasi sistem perlu mempunyai beberapa backup yang direncanakan dalam kasus kegagalan firewall.

Menurut Barbara and Bagwill Robert, firewall (perangkat lunak sistem, konfigurasi data, file database, dan lain lain) harus di-backup harian, mingguan, dan bulanan sehingga dalam kasus kegagalan sistem, file data dan konfigurasi dapat direcover. File backup harus disimpan dengan aman pada suatu media dengan atribut *read-only* sehingga data dalam media penyimpanan tidak dapat ditulis ulang dengan sembarangan dan untuk mengamankan sehingga media hanya dapat diakses oleh orang yang sesuai.

Alternatif backup lainnya adalah dengan mempunyai firewall lain yang dikonfigurasi sebagai firewall yang siap dipasang dan dijaga dengan baik sehingga jika ada yang kegagalan pada firewall utama, maka firewall backup ini akan dengan mudah dipasang dan menggunakan sebagai firewall ketika firewall utama sedang diperbaiki. Sedikitnya satu firewall akan dikonfigurasi dan dipesan (tidak digunakan) sehingga dalam kasus kegagalan firewall, firewall backup ini dapat diswitch untuk melindungi jaringan.

3.8 Integritas Sistem

Untuk mencegah modifikasi oleh orang yang tidak berhak terhadap konfigurasi firewall, beberapa bentuk jaminan integritas proses harus digunakan. Secara khusus, pemeriksaan jumlah (checksums), pemeriksaan pemborosan siklus (cyclic redundancy check), atau kriptografi *hash* (cryptographic hashes) dibuat dari gambar pada saat dijalankan dan disimpan pada media yang dilindungi. Pada saat konfigurasi firewall telah dimodifikasi oleh orang yang diberi hak (pada umumnya administrator firewall) diperlukan bahwa integritas sistem database online diperbaharui dan disimpan ke dalam sistem file jaringan atau media yang dapat dipindahkan. Jika pemeriksaan integritas sistem menunjukkan bahwa file konfigurasi firewall telah dimodifikasi, akan diketahui bahwa sistem telah disepakati bersama.

Database integritas sistem firewall akan diperbaharui setiap kali konfigurasi firewall dimodifikasi. Integritas sistem file harus disimpan pada media read-only atau media penyimpan off-line. Integritas sistem akan diperiksa secara teratur pada firewall sesuai perintah administrator untuk menghasilkan suatu daftar dari semua file yang mungkin telah dimodifikasi, digantikan, atau dihapus.

4. Perbaikan/Pembaharuan Kebijakan Firewall

Dengan memberikan pengenalan yang cepat tentang teknologi baru, dan kecenderungan organisasi untuk secara terus menerus memperkenalkan layanan baru, kebijakan keamanan firewall seharusnya ditinjau ulang secara teratur. Misalnya terjadi kebutuhan perubahan jaringan, maka perlu perbaikan atau pembaharuan kebijakan keamanan.

5. Contoh Kebijakan Secara Umum

Pernyataan kebijakan berikut hanya merupakan contoh. Ini bukan kebijakan firewall yang lengkap, dan bahkan jika perlu sebaiknya jangan dipergunakan di lingkungan organisasi Anda. Pernyataan dikelompokkan ke dalam pemakaian lingkungan resiko rendah, menengah, dan tinggi. Di dalam masing-masing kategori, mereka dibagi menjadi pernyataan-pernyataan dengan sasaran para pemakai, manager, dan teknisi. Secara umum, semua organisasi akan menggunakan paling tidak kebijakan dengan resiko rendah. Contoh kebijakan untuk lingkungan dengan resiko rendah, sedang, dan tinggi adalah sebagai berikut:

5.1 Kebijakan Untuk Lingkungan Dengan Resiko Rendah

a. User/pemakai

- Semua pemakai yang memerlukan akses ke layanan Internet harus dilakukan dengan menggunakan perangkat lunak yang disetujui organisasi dan gateway Internet.

- Firewall telah ditempatkan di antara jaringan pribadi dan Internet untuk melindungi sistem. Para karyawan harus tidak menghindari firewall dengan menggunakan modem atau perangkat lunak penembus jaringan untuk melakukan koneksi ke Internet.
- Beberapa protokol telah diblokir atau dialihkan trafiknya. Jika pemakai mempunyai bisnis yang membutuhkan protokol khusus, maka pemakai harus menghubungi manajer dan petugas keamanan Internet.

b. Manajer

- Suatu firewall akan ditempatkan antara jaringan organisasi dan Internet untuk mencegah pengaksesan jaringan organisasi ke jaringan yang tidak dipercayai atau tidak dikenal. Firewall akan dipilih dan dipelihara oleh Manajer Layanan Jaringan (Network Service Manager).
- Semua bentuk lain akses Internet (seperti: melalui dial-out modem) dari situs-situs yang dihubungkan ke Wide Area Network (WAN) organisasi adalah dilarang.
- Semua pemakai yang memerlukan akses ke layanan Internet harus melakukannya dengan menggunakan perangkat lunak yang disetujui organisasi dan gateway Internet.

c. Teknisi

- Semua firewall seharusnya gagal jika dikonfigurasi untuk menolak semua layanan, dan memerlukan administrator firewall untuk mengaktifkan (re-enable) layanan-layanan setelah kegagalan tersebut.
- *Routing* ke sumber akan dimatikan (disable) pada semua firewall dan *external router*.
- Firewall seharusnya tidak menerima trafik pada interface eksternal yang nampak seperti berasal dari alamat jaringan internal.
- Firewall sebaiknya mengadakan pemeriksaan catatan (log) secara terperinci dari semua bagian sehingga log dapat ditinjau untuk melihat keganjilan-keganjilan (anomalies).
- Mengamankan media yang akan digunakan untuk menyimpan laporan log (seperti akses ke media ini dibatasi hanya untuk orang yang berhak).
- Firewall akan diuji secara off-line dan konfigurasi yang sesuai akan dibuktikan.
- Firewall akan dikonfigurasi untuk menerapkan ketransparanan untuk semua layanan outbound. Kecuali jika yang disetujui oleh Manajer Layanan Jaringan, semua layanan inbound akan ditangkap dan diproses oleh firewall.
- Sesuai dokumentasi Firewall akan dipelihara pada media penyimpanan off-line secara terus menerus. Demikian, informasi akan masuk tetapi tidak dibatasi untuk diagram jaringan, tetapi termasuk semua alamat IP alat jaringan, alamat IP dari host yang terkait dengan Internet Service Provider (seperti server eksternal baru, router, server DNS, dan lain-lain) dan semua parameter konfigurasi lainnya seperti aturan *packet filter*, dan lain-lain. Demikian dokumentasi akan diupdate setiap konfigurasi firewall diubah.

5.2 Kebijakan Untuk Lingkungan Dengan Resiko Sedang

a. User/pemakai

Ketika pemakai sedang off-site, maka pemakai hanya boleh mengakses sistem internal dengan penggunaan yang diizinkan oleh organisasi dengan satu kali password dan tanda perangkat keras (hardware) untuk membuktikan keaslian pemakai kepada firewall. Alat-alat yang lain dalam mengakses sistem internal dilarang.

b. Manajer

- Autentikasi yang kuat dengan satu kali password dan tanda hardware digunakan atas persetujuan organisasi untuk semua akses jarak jauh ke sistem internal melalui firewall.
- Kebijakan keamanan jaringan akan ditinjau secara teratur (minimum setiap tiga bulan) oleh administrator firewall atau berdasarkan informasi penting lainnya dari manajer keamanan. Misalnya kebutuhan untuk koneksi dan layanan jaringan telah diubah, maka kebijakan keamanan akan diperbaharui dan disesuaikan. Jika perubahan telah dilakukan, maka administrator firewall harus memastikan bahwa perubahan itu telah diterapkan dan kebijakan keamanan telah dimodifikasi.
- Perincian organisasi internal jaringan yang terdaftar seharusnya tidak kelihatan dari luar firewall.

c. Teknisi

- Firewall akan dikonfigurasi untuk menolak semua layanan yang jelas-jelas tidak diizinkan dan nantinya secara teratur diperiksa dan dimonitor untuk mendeteksi penyusupan atau penyalahgunaan.
- Firewall akan memberitahu administrator sistem pada waktu yang mendekati real-time tentang segala hal yang mungkin memerlukan perhatian segera, seperti usaha menerobos ke dalam jaringan, ruang disk yang tersedia sedikit, atau pesan-pesan lainnya yang terkait sehingga suatu tindakan dengan segera dapat diambil.
- Perangkat lunak firewall akan berjalan pada komputer yang ditentukan dan semua perangkat lunak yang tidak berhubungan dengan firewall, seperti compiler, editor, perangkat lunak komunikasi, dll., akan dihapus atau dimatikan (disable).

5.3 Kebijakan Untuk Lingkungan Dengan Resiko Tinggi

a. User/pemakai

- Semua penggunaan Internet untuk kepentingan selain bisnis (non-business) dari sistem organisasi dilarang. Semua akses ke layanan Internet dicatat. Karyawan yang melanggar kebijakan ini akan dikenai tindakan disipliner.
- Browser pemakai telah diatur dengan daftar situs terlarang. Usaha apapun untuk mengakses situs itu akan dilaporkan kepada manajer pemakai.

b. Manajer

Semua penggunaan Internet untuk kepentingan selain bisnis (non-business) dari sistem organisasi dilarang. Semua akses ke layanan Internet dicatat. Karyawan yang melanggar kebijakan ini akan dikenai tindakan disipliner.

c. Teknisi

Semua akses ke layanan Internet dicatat. Laporan ringkasan dan perkecualian (exception) akan disiapkan untuk manajer jaringan dan keamanan.

6. Contoh Kebijakan Layanan Khusus

Menghubungkan ke Internet membuat suatu cakupan yang luas untuk menyediakan layanan bagi para pemakai internal dan eksternal. Dipengaruhi oleh kebutuhan-kebutuhan bisnis atau misi organisasi, maka kebijakan harus tertulis dengan jelas untuk menyatakan apakah layanan diizinkan atau ditolak bagi kedua sisi jaringan yaitu jaringan internal dan eksternal.

Ada suatu cakupan luas dari layanan Internet yang tersedia, seperti FTP, telnet, HTTP, dan lain lain. Berkeley Software Distribution (BSD) UNIX “r” perintah-perintah seperti rsh, rlogin, rcp, dll., adalah yang dirancang untuk mengizinkan para pemakai sistem UNIX mengeksekusi perintah-perintah pada sistem jarak jauh. Kebanyakan penerapan ini tidak mendukung autentikasi atau enkripsi, sehingga sangat berbahaya jika menggunakan pada Internet.

- Post Office Protocol (POP) adalah suatu client-server protokol untuk mengambil surat elektronik dari suatu server. POP adalah suatu layanan berbasis TCP yang mendukung penggunaan password yang tidak dapat dipakai kembali (*nonreusable password*) untuk autentikasi, yang dikenal sebagai APOP. POP tidak mendukung enkripsi pada saat pengambilan email sehingga rapuh terhadap penyadapan.
- Network News Transfer Protocol (NNTP) digunakan untuk mendukung *Usenet newsgroups*. NNTP adalah suatu layanan yang berbasis TCP yang menerapkan protokol penyimpanan (store) dan meneruskan (forward). NNTP server seharusnya tidak dijalankan pada firewall, tetapi standar layanan proxy tersedia untuk melewati NNTP.
- finger dan whois adalah fungsi yang serupa. finger digunakan untuk mengambil informasi tentang sistem diantara pemakai. finger sering memberikan lebih banyak informasi dibandingkan dengan kebutuhan. Kebanyakan organisasi seharusnya mematikan (disable) atau membatasi fungsi finger pada firewall. whois di sistem unix (linux) berfungsi untuk mencari informasi tentang sebuah domain. Whois seharusnya juga dimatikan atau dibatasi pada firewall.
- Protokol pencetakan jarak jauh (remote) UNIX lp dan lpr mengizinkan *remote host* untuk melakukan pencetakan menggunakan pencetak yang ada pada host lain. lpr adalah suatu protokol penyimpan dan penerus, sedangkan lp menggunakan fungsi rsh untuk menyediakan kemampuan mencetak jarak jauh. Secara umum, lp dan lpr seharusnya dimatikan (disable) pada firewall kecuali jika vendor yang mensuplai proxy menyediakan fasilitas ini.
- Network File System (NFS) mengizinkan disk drive dapat diakses oleh para pemakai dan sistem antar jaringan. NFS menggunakan bentuk autentikasi yang lemah dan tidak dipertimbangkan masalah keamanan untuk menggunakannya ke jaringan lain yang tidak dipercayai. NFS seharusnya tidak diizinkan melewati firewall. *Real Audio* menyediakan pengiriman audio digital pada jaringan TCP/IP. Untuk mengambil keuntungan kemampuan multimedia dari world wide web (www), sejumlah layanan baru telah dikembangkan. Yang mana layanan internet

untuk mengizinkan atau menolak harus dipengaruhi oleh kebutuhan dari organisasi. Contoh kebijakan keamanan untuk sebagian dari layanan Internet yang mungkin dibutuhkan oleh organisasi khusus diilustrasikan pada **Tabel 6.1**.

6.1 Manajer

Berikut ini adalah sebuah tabel urusan level manajerial.

Tabel 6.1 Urusan Manajerial

TUJUAN	PROTOKOL	APAKAH	MENGAPA
Email		User mempunyai alamat email eksternal tunggal	Tidak dapat membuka info bisnis
	SMTP	Server tunggal atau kelompok server menyediakan layanan email untuk organisasi	<ul style="list-style-type: none"> • Email terpusat akan lebih mudah dipelihara • Server SMTP sulit untuk diatur keamanannya
	POP3	Pemakai POP harus menggunakan identifikasi autentikasi	Mencegah sniffing password
	IMAP	Grup didorong untuk beralih ke IMAP	Dukungan lebih baik untuk travel, enkripsi
USENET news	NTTP	Diblokir pada firewall	Tidak ada bisnis yang membutuhkan
www	HTTP	Diarahkan ke www.my.org	<ul style="list-style-type: none"> • www dipusatkan lebih mudah untuk dipelihara • Server www sulit untuk diatur keamanannya
*	Yang lainnya	Di route (routed)	

6.2 Teknisi

Tabel 6.2 Kebijakan Layanan Khusus

LAYANAN	KEBIJAKAN				Contoh Kebijakan
	Dari Dalam ke Luar		Dari Luar ke Dalam		
	Status	Auth	Status	Auth	
FTP	y	n	y	y	Akses FTP akan diizinkan dari jaringan internal ke eksternal. Autentikasi yang kuat akan dibutuhkan untuk akses FTP dari dari luar ke dalam.
telnet	y	n	y	y	Akses telnet akan diizinkan dari jaringan dalam ke luar. Untuk telnet dari jaringan luar ke dalam, autentikasi akan dibutuhkan.

Tabel 6.2 Kebijakan Layanan Khusus (Lanjutan)

LAYANAN	KEBIJAKAN				Contoh Kebijakan
	Dari Dalam ke Luar		Dari Luar ke Dalam		
	Status	Auth	Status	Auth	
rlogin	y	n	y	y	rlogin untuk pengorganisasian hosts dari jaringan eksternal membutuhkan izin tertulis dari manajer layanan jaringan dan menggunakan autentikasi kuat.
HTTP	y	n	n	n	Semua server www dimaksudkan untuk akses user eksternal dari host di luar organisasi firewall. Tidak ada akses HTTP ke arah dalam yang diizinkan melalui organisasi firewall.
SSL	y	n	y	y	Sesi SSL menggunakan sertifikat client side diperlukan ketika sesi SSL dilewat-kan melalui organisasi firewall.
POP3	n	n	y	n	Organisasi server POP adalah untuk host di dalam organisasi firewall. Firewall akan melewatkan hanya trafik POP ke server POP.
NNTP	y	n	n	n	Tidak ada akses eksternal yang diizinkan ke server NNTP.
Real Audio	n	n	n	n	Tidak ada kebutuhan bisnis secara langsung untuk mendukung streaming sesi audio melalui organisasi firewall. Beberapa unit bisnis memerlukan dukungan, seharusnya menghubungi manajer layanan jaringan.
lp	y	n	n	n	Layanan lp ke jaringan internal dimatikan pada organisasi firewall.
finger	y	n	n	n	Layanan finger ke jaringan internal dimatikan pada organisasi firewall.
gopher	y	n	n	n	Layanan gopher ke jaringan internal dimatikan pada organisasi firewall.
whois	y	n	n	n	Layanan whois ke jaringan internal dimatikan pada organisasi firewall.
SQL	y	n	n	n	Hubungan dari host-host eksternal ke database internal harus disetujui oleh manajer layanan jaringan dan digunakan persetujuan layanan proxy SQL (SQL proxy service).
rsh	y	n	n	n	Layanan rsh ke jaringan internal dimatikan pada organisasi firewall.
Yang lain-nya seperti: NFS	n	n	n	n	Akses ke layanan lainnya yang tidak disebutkan di atas akan ditolak dalam kedua arah.

Keterangan Tabel 6.2:

- Status (y/n) = apakah para pemakai dapat menggunakan layanan
- Auth (y/n) = apakah sembarang bentuk dari autentikasi (kuat atau yang lainnya) dilakukan sebelum layanan dapat digunakan.

Suatu organisasi mungkin ingin mendukung beberapa layanan tanpa menggunakan autentikasi yang kuat. Sebagai contoh, suatu server FTP tanpa nama mungkin digunakan untuk mengizinkan semua pemakai eksternal untuk download informasi secara bebas. Dalam hal ini, beberapa layanan seharusnya hostnya diluar firewall atau pada layanan jaringan yang tidak dihubungkan ke jaringan organisasi yang berisi data penting. Tabel berikut merupakan ringkasan suatu metoda untuk menggambarkan beberapa kebijakan untuk layanan seperti FTP.

Tabel 6.3 Ringkasan Kebijakan Keamanan

Kebijakan	Layanan FTP Dengan Nama	Layanan FTP Tanpa Nama
Menempatkan mesin server diluar firewall	N	Y
Menempatkan mesin server pada layanan firewall	N	Y
Menempatkan mesin server pada jaringan yang diproteksi	Y	N
Menempatkan mesin server pada firewall itu sendiri	N	N
Server akan diakses oleh setiap orang pada Internet	N	Y

7. Kesimpulan

Kebijakan keamanan merupakan langkah kritis pertama dalam rangka mengamankan jaringan organisasi. Kebijakan keamanan merupakan suatu dokumen tertulis sehingga seharusnya mudah untuk dibaca. Dokumen ini menyatakan sumber daya mana saja yang harus diamankan serta dalam kondisi yang bagaimana agar akses dapat diizinkan atau ditolak.

Dalam pembuatan kebijakan keamanan supaya hasilnya baik diperlukan manajemen kebijakan keamanan firewall yang terdiri dari analisis resiko dan langkah-langkah dalam pembuatan kebijakan keamanan firewall. Hasil dari analisa ini meliputi sebuah daftar aplikasi-aplikasi dan bagaimana aplikasi-aplikasi tersebut akan diamankan.

Firewall merupakan alat bantu teknis yang digunakan untuk menerapkan kebijakan keamanan. Dengan suatu kebijakan yang didefinisikan dengan jelas, maka organisasi akan mampu mengetahui dengan tepat siapa yang akan menjaga perangkat firewall serta perubahan seperti apa saja yang diperkenankan. Aturan-aturan yang secara acak ditambahkan dan diganti tanpa melalui suatu perencanaan yang matang, hasilnya dapat berupa konfigurasi perangkat yang kurang efektif.

Ucapan Terima Kasih

Saya sangat berterima kasih kepada Ir. Budi Rahardjo, MSc., PhD. selaku dosen mata kuliah Keamanan Sistem Lanjut (EC 7010) yang telah membimbing dan memberikan saran-saran dalam menyelesaikan tugas akhir ini. Ucapan terima kasih juga Saya sampaikan kepada teman-teman yang telah *sharing* pengetahuan tentang kebijakan keamanan pada firewall, sehingga membantu Saya dalam proses penyelesaian tugas akhir ini.

DAFTAR PUSTAKA

- [1] Wack John., Cutler Ken., Pole Jamie., *Guidelines on Firewalls and Firewall Policy*, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology: Gaithersburg, 2002.
- [2] Wisnu Baroto, *Memahami Dasar-Dasar Firewall*, PT Elexmedia Komputindo, Jakarta: 2003.
- [3] Goncalves, Marcus., *Firewalls Complete*, The Mc Graw-Hill Companies Inc., New York: 1998.
- [4] Guttman Barbara, and Bagwill Robert, *Implementing Internet Firewall Security Policy*, National Institute of Standards and Technology, Gaithersburg: 1998.
- [5] Ehab S. Al-Shaer and Hazem H. Hamed, *Modeling and Management of Firewall Policies*, DePaul University: 2004 <http://comsoc.org-livepubs-etn-private-2004-apr-hamed.html>